

An OID-Based Identifier Framework Supporting the Interoperability of Heterogeneous Identifiers

Euihyun Jung*, Younghwan Choi**, Jun Seob Lee**, Hyoungh Jun Kim**

*Dept. of Computer Science, Anyang University, San 102-3, Buleun-myeon, Ganghwa-gun, Inchon, Korea

**ETRI, 218 Gajeong-ro, Yuseong-gu, Daejeon, 305-700, Korea

jung@anyang.ac.kr, yhc@etri.re.kr, juns@etri.re.kr, khj@etri.re.kr

Abstract— The Interoperability of heterogeneous identifiers is rising as a main prerequisite to realize the Internet of Thing (IoT) vision. However, it seems to be a very difficult issue due to the heterogeneity of things in the IoT such as hardware capability, interworking protocol, address schemes, and etc. In the research, the Virtual Identifier Layer (VIL) is proposed to overcome the heterogeneity and to provide the unified identification service. The VIL is a virtual identifier framework constructed over the existing identifier infrastructures using the concept of meta-resolution and metadata repository. It can provide an interoperable resolution between things belonging to heterogeneous identifier infrastructure while letting the existing identifier infrastructures to keep their own territories.

Keywords— OID, IoT, Identification Infrastructure, metadata

I. INTRODUCTION

Since Kevin Ashton's presentation [1], many researchers have been forecasting the IoT would be a core infrastructure to provide the future IT services enabling the smart society [2-4]. The IoT is defined as a pervasive network infrastructure consisting of various "things" such as RFID embedded objects, sensors, actuators, or mobile phones. In the IoT environment, these things interact with each other and work together to provide smart IT services transparently to users. In order to realize the IoT vision, the IoT needs a close cooperation of various physical and virtual things in spite of the heterogeneity of hardware capability, interworking protocol, communication interface and address scheme of these things. However, the research of the IoT is still in the beginning phase, so there exists no agreed and common solution to overcome these issues yet [3][4].

Although there are a lot of issues in the IoT research, the unified identification of things on the heterogeneous environment is the foremost issue for things to interact with each other. In order to resolve the issue of the IoT identification, several identifier infrastructures have been studying by several research groups such as IPSO Alliance [5] and Auto-ID Labs [6]. The IPSO Alliance is a primary

advocate for IP networked devices for the IoT. The Auto-ID Labs insist that the networked RFID would be a main identifier infrastructure for the IoT. Their proposed identifier infrastructures have their own pros and cons, but they are all common not to answer the interoperability of other identifiers. Since the IoT would be comprised of various resources and technologies, it cannot avoid involving in the different kinds of identifiers simultaneously to provide the smart IT services promised by the IoT. However, interworking heterogeneous identifiers are very difficult to achieve due to the difference in a hardware capability, a network routing, operation modes, and etc. It is more complicating for USNs because USNs do not have the globally accepted standards and they are naturally application and hardware dependent networks [7][8].

In order to resolve this issue, we suggested a new identifier framework to mediate between heterogeneous identifiers and to serve a unified identification while maintaining the territory of the each identifier. The suggested framework adopts the Object Identifier (OID) [9] to tag an individual identifier and to lead a resolution-initiating thing to its own resolution service by using the concept of meta-resolution. It also suggests the concept of metadata repository to make things access and to communicate with peers with heterogeneous identifiers.

The remainder of this paper is organized as follows: The existing identifier infrastructures for IoT are reviewed and design issues are discussed in Section II. In Section III, the structure of the proposed framework is stated. This follows Section IV which discusses several application scenarios of the proposed framework. Finally, Section V gives the conclusion.

II. EXISTING IDENTIFIERS AND DESIGN ISSUES

A. Status of Competing Identifiers for The IoT

There are several organizations that announced an identification infrastructure for the IoT. All of them insisted their frameworks are superior to others'. The pros and cons of each identification infrastructure are as below.

1) **IPSO Alliance:** The IPSO alliance is an organization to promote the use of IP for smart objects. It advocates IP is the open, flexible, light-weight, versatile, ubiquitous, scalable and manageable identifier standard for smart objects [5]. However, many researchers, especially USN researchers, are suspicious that IP is too heavy for tiny embedded devices and cost too much in ad-hoc wireless environment [7].

2) **Auto-ID Labs:** With the EPCglobal, The Auto-ID Labs [6] have been conducting research in the field of the networked RFID and the architecture of the IoT. RFID is still considered as the prominent technology to realize the IoT vision because of its technology maturity and the strong support from the business community [10]. However, some researchers claim the IoT vision goes beyond the current RFID technology [11].

3) **OID:** The Object Identifier (OID) is used to uniquely name an object and it is standardized by the ITU-T and the ISO/IEC [9]. Since an individual OID consists of a node in a hierarchically-assigned namespace and successive numbers of the nodes, any identifier authority can freely create new nodes under the registration authority's top node. Interestingly, the OID is not competing identifier against the existing identifiers though it can be used to identify things uniquely. Instead, the OID focuses on identifying a type of an identifier and on delegating an actual resolution to a proper identifier infrastructure. This delegation policy has the OID to be neutral and it has the existing identifier infrastructures to gather under the umbrella of the OID. Although the OID itself is not considered as a global and unique identifier for the IoT, it could be a meta-identifier to locate the proper identification service.

B. Design Issues

In order to make an interoperable identifier framework for heterogeneous identifiers of the IoT, there are several design issues which must be addressed.

1) **Keep One's Own Territory:** Currently, there is no widely accepted ID/address scheme for the IoT. To make matters worse, several identifier schemes compete against each other and try to bring others to their knees. They have no plan to interoperate with each other for the IoT. Therefore, an interoperable identifier framework must invent a way for existing players not only to cooperate with each other, but also to keep their territories.

2) **Interaction of Heterogeneous Things:** There are many heterogeneous things in the IoT environment such as sensors of USN, mobile phones, RFID-tag embedded objects, and etc. They are different in the address scheme, an interworking protocol, and an operation mode. Most RFID tags operate in the passive mode, but some RFID tags operate in the active mode. The difference of the operation mode greatly affects the structure and protocol of a communication session between things. The problem is more serious in considering USNs. USNs do not have the unified address scheme yet. Some USNs use IP, but others adopt the proprietary address or even

non-physical address such as the attribute of a specific area. It seems nearly impossible for these heterogeneous things to cooperate with each other.

3) **Support Both Communication and Identification:** The purpose of conventional identifier infrastructures is classified into either the identification or the creating session. IP presents the packet routing information, that is, it is mainly used to make a session although IP research groups suggested the ID/locator separation [12]. In comparison, RFID or barcode just identifies an object itself and the identifier should be resolved to gain meaning. However, an interoperable identifier framework should support both identification and creating session.

III. STRUCTURE OF THE PROPOSED FRAMEWORK

In order to resolve the design issues, we suggest the concept of meta-resolution and metadata repository. Meta-resolution means the resolution for resolution servers. In the concept, all things query the target ID to a meta-resolution server instead of directly querying to the resolution server of peer things. With this mechanism, each identifier framework can not only keep its own territory, but also be the part of the interoperable identifier framework.

A metadata repository suggested in the research is a new kind of resolution server to provide resolution-initiating things with plentiful metadata for session and identification information of the peer. Since the given metadata has a form of XML, the information can contain any information such as a device profile, an operation mode, an address type, and etc. of peers.

A. Virtual Identifier Layer

We proposed a Virtual Identifier Layer (VIL) constructed over heterogeneous identifier infrastructures to support meta-resolution and metadata repository. Now, USNs, IP network, RFID and barcode are the target identifiers to be part of the VIL. In order to join the VIL, each identifier infrastructure should prepare a metadata repository to provide metadata answers for requests of things. Conceptually, a thing sends a query containing an OID of a target thing's identifier to a meta-resolution server on the VIL, and the meta-resolution server would return the URL of the metadata repository which provides the metadata of the target thing. Since the VIL can give metadata corresponding to each identifier, a thing can easily make a session or refer the peer thing belonging to other identifier infrastructures only with the peer thing's identifier and its OID. Figure 1 shows a conceptual structure of the VIL.

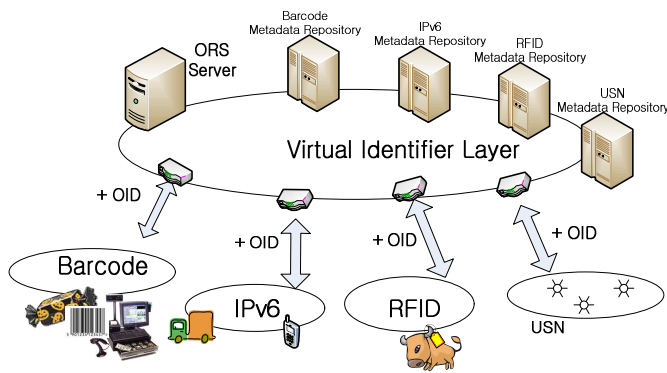


Figure 1. Conceptual structure of the VIL

B. Meta-Resolution with OID

In order to realize the meta-resolution service, the OID and the OID Resolution Server (ORS) are adopted in the research. On the VIL, an OID as a prefix must be attached to each identifier to distinguish the type of identifiers. Therefore, each identifier is represented as the form of “OID + local identifier” on the VIL. For a resolution, all resolution requests must be route to the ORS before the resolution requests are handled by corresponding resolution servers. The ORS performs a meta-resolution which locates the target metadata repository with the OID of the request. From the result of this meta-resolution, things can get the URL of the target metadata repository. This process is already suggested in the ORS resolution process [10]. After things get the URL of the metadata repository of the requested ID, they request the repository to give the peer thing’s metadata which contains the session and profile information. The process of the meta-resolution is shown in Figure 2.

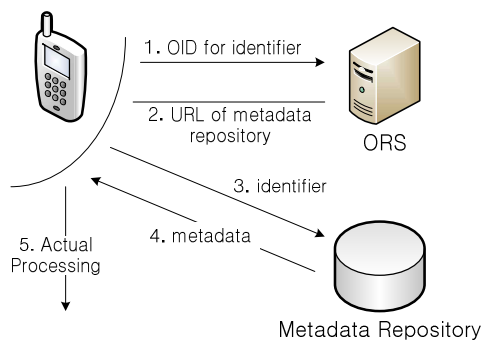


Figure 2. Process of meta-resolution with ORS

C. Metadata Schema

The metadata returned from a metadata repository has essential information for things belonging to heterogeneous identifier infrastructures to interoperate with each other. The metadata could contain any information so far as the data format is defined in advance between applications and metadata repositories. The proposed framework does not limit the format and contents of the metadata, and it leaves the format up to the individual identifier authority. In this stage, we decided that a session and a profile are mandatory fields in the metadata. These fields would be used to make a session to

or consult information of a thing which the identifier refers. The XML schema is shown in Figure 3. The information fields can be easily extended and can contain any information because the format and contents of the metadata are in the hands of each identifier authority.

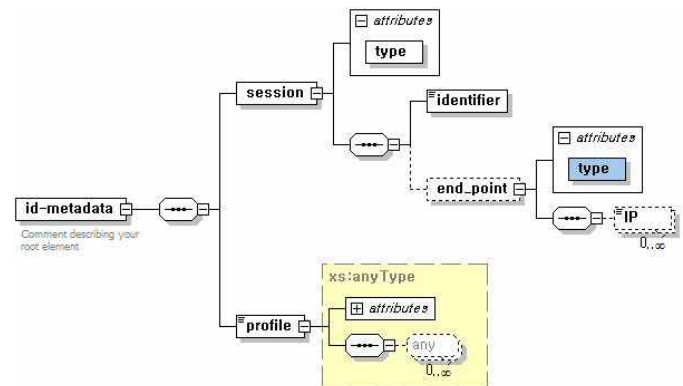


Figure 3. An XML shema for metadata stored in a metadata repository

IV. APPLICATION SCENARIOS

The proposed framework could be operated with any identifier infrastructures from the passive barcode to the attribute-based USN. To show the usefulness and detail operation, we present three application scenarios in which different identifiers of things are smoothly resolved and things work together with each other.

A. Barcode Reader App. of Smartphone

In this scenario, a user scans a printed ISBN barcode of a book with his/her Smartphone’s barcode reader app. Then, the app queries the ORS on the VIL with the OID number of ISBN barcode service such as “1.2.3.3”. The ORS returns the URL of the ISBN barcode metadata repository by referring “1.2.3.3”. After getting the URL, the ISBN barcode app queries the ISBN number to the metadata repository, which returns the metadata containing a profile of the target book. As shown in Figure 4, since the “type” attribute of the <session> tag is “identification”, there is no session end point in the <session> tag. Instead, the metadata contains enough information describing the book in the <profile> tag and this information can be shown in the user’s Smartphone. A noteworthy phenomenon is that Smartphone is not a part of the identifier infrastructure of the ISBN barcode, but this app can use the information of the ISBN barcode easily.

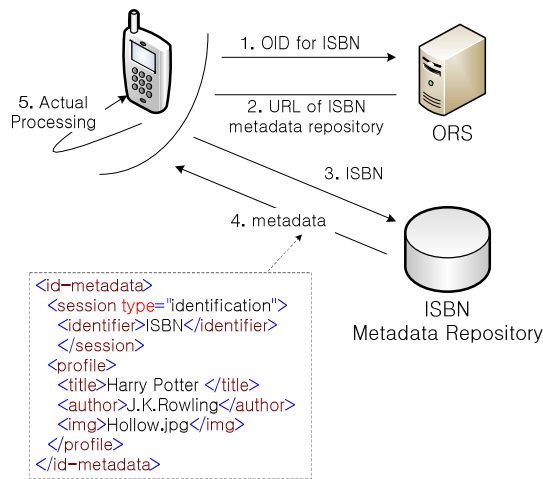


Figure 4. Resolution process and returned metadata describing book

B. Attribute-Based USN Access

Let us assume a scenario in which a user takes a walk in a forest, he/she just wants to know the humidity of the forest where an USN is deployed. The USN assumes to use ZigBee address and to communicate outside through a gateway with attribute ID such as humidity. He/she starts the USN access App given at the entrance of the forest to query the humidity. The app queries the VIL with an OID number indicating the USN. After the ORS returns the URL of the USN metadata repository, the app queries an attribute ID, "humidity:GeoPt", to the USN metadata repository. The repository would return the metadata containing the <end-point> tag to be used to make a session. By using the information, the app would send the attribute ID to a gateway and then the gateway would return the data related to the attribute ID. Using the process shown in Figure 5, the app can get the humidity of the forest with even non-physical ID.

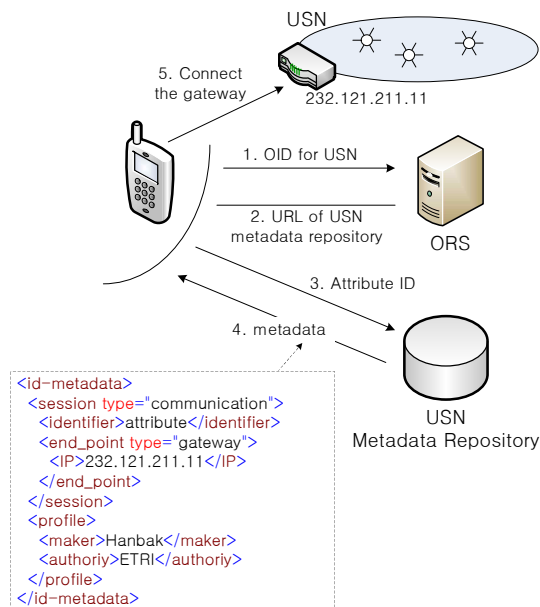


Figure 5. The process of getting the humidity of the forest

C. Another Case of USN Access

In this scenario, we assumed that sensors of a target USN have IP address and some sensors equip a hygrometer function. Since sensors can make a direct session with outer things, the corresponding metadata repository might return different metadata comparing to the previous case.

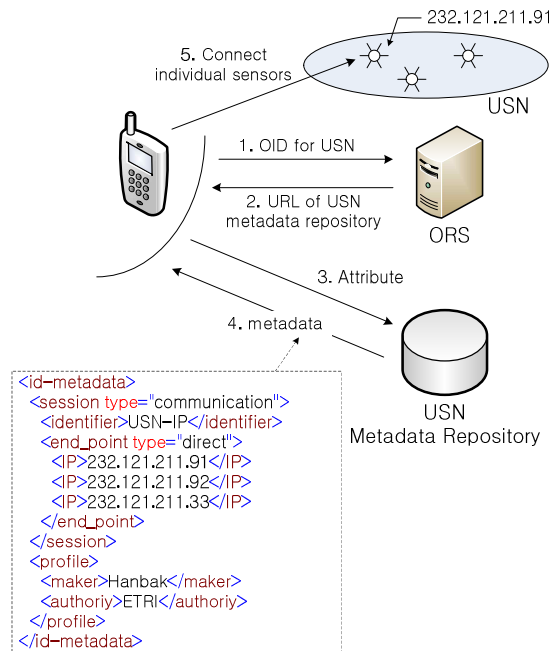


Figure 6. The process of getting humidity when sensors of USN have IP

As shown in Figure 6, using IP addresses in the returned metadata, the Smartphone App directly queries the target sensors for humidity of the forest.

D. Discussion

The application scenarios show the pros and cons of the proposed framework. The main advantage of the framework is that it enables the things to transparently interact with each other although they belong to the different identifier infrastructures. With only peer's ID, even non-physical ID, things can get the identification and communication information by using the meta-resolution and metadata.

On the contrary to this, the proposed framework has also a weakness. In the experiments, apps must understand the contents of the metadata to interact with the target peer thing. That means a resolution-initiating application has to understand the format and contents of the resolved metadata. This results that the applications using the framework may be proprietary without the proper semantic negotiation. However, if the standardized semantic ontology describing identifiers is prepared, developers can easily make applications which cross over several identifier infrastructures.

V. CONCLUSION

In order to realize the IoT vision, the interoperability of heterogeneous identifiers is a main prerequisite. However, the existing identifier infrastructures do not make any effort for

the compatibility and integration with each other. In addition to this, the differences in the hardware compatibility, the operation mode, and the address scheme make the situation more complex.

We proposed an OID-based identifier framework to support the interoperability of the heterogeneous identifiers. The proposed framework suggests the concepts of meta-resolution and metadata repository. By adopting these two concepts, it enables things with heterogeneous identifier to cooperate with each other. From the several application scenarios, the proposed framework shows its usefulness to fulfil the design issues of the interoperable identification of the IoT. The result means that the identification, especially the interoperable identification, could be a base and core technology to achieve the IoT vision. Although the proposed framework reveals a problem of the semantic understanding of metadata, the problem could be resolved with the Semantic Web technology. Our further study would focus on the structure of metadata repository that provides things with machine understandable metadata.

ACKNOWLEDGMENT

This research was supported by the ICT Standardization program of MKE (The Ministry of Knowledge Economy).

REFERENCES

- [1] G. Santucci, "From Internet of Data to Internet of Things," *International Conference on Future Trends of the Internet*, 2009.
- [2] T. R. Regina, T. Tome, and C. E. Rothenberg, "Scenario of Evolution for a Future Internet Architecture," pp.57-77, *New Network Architectures*, Springer-Verlag, 2010.
- [3] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49-69, 2011.
- [4] L. Atzori, A. Iera, and G. Morabito, "Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, Oct. 2010.
- [5] (2011) The IPSO Alliance website. [Online]. Available: <http://www.ipso-alliance.org/>
- [6] (2011) The Auto-ID Lab website. [Online]. Available: <http://www.autoidlabs.org/>
- [7] C. Chong, S. P. Kumar, and B. A. Hamilton, "Sensor Networks: Evolution, Opportunities, and Challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247-1256, Aug. 2003.
- [8] I. F. Akyildiz and M. C. Vuran, *Wireless Sensor Networks*, Wiley, 2010.
- [9] O. Dubuisson, "Introduction to Object Identifiers (OID) and Registration Authorities," France Telecom Orange, [Online]. Available: [http://www.oid-info.com/doc/introduction to object identifiers \(OIDs\).pdf](http://www.oid-info.com/doc/introduction%20to%20object%20identifiers%20(OIDs).pdf)
- [10] E. Ngai, K. Moon, F. Riggins and C. Yi, "RFID research: An academic literature review (1995-2005) and future research directions," *International Journal of Production Economics*, vol. 112 pp. 510-520, 2008.
- [11] A. Dunkels and J. Vasseur, "IP for Smart Objects," White Paper #1, IPSO Alliance Website. [Online]. Available: <http://www.ipso-alliance.org/white-papers>, Jul. 2010.
- [12] V. P. Kafle, H. Otsuki, and M. Inoue, "An ID/Locator Split Architecture of Future Internet," *Innovations for Digital Inclusions*, pp. 1-8, Aug. 2009