# IDNet: Beyond All-IP Network

Heeyoung Jung, Wan-Seon Lim, Jungha Hong, Cinyoung Hur, Joo-Chul Lee, Taewan You, Jeesook Eun, Byeongok Kwak, Jeonghwan Kim, Hae Sook Jeon, Tae Hwan Kim, and Woojik Chun

**Recently, new network systems have begun to emerge (for instance, 5G, IoT, and ICN) that require capabilities beyond that provided by existing IP networking. To fulfill the requirements, some new networking technologies are being proposed. The promising approach of the new networking technology is to try to overcome the architectural limitations of IP networking by adopting an identifier (ID)-based networking concept in which communication objects are identified independently from a specific location and mechanism. However, we note that existing ID-based networking proposals only partially meet the requirements of emerging and future networks. This paper proposes a new ID-based networking architecture and mechanisms, named IDNet, to meet all of the requirements of emerging and future networks. IDNet is designed with four major functional blocks — routing, forwarding, mapping system, and application interface. For the proof of concept, we develop numeric models for IDNet and implement a prototype of IDNet.**

**Keywords: All-IP network, identifier, ID-based networking, IDNet, recursive inter-domain routing, reactive ID forwarding, ID/LOC mapping system, ID based API.**

Manuscript received Feb. 26, 2015; revised July 27, 2015; accepted Sept. 9, 2015.

Heeyoung Jung (corresponding author, hyjung@etri.re.kr), Wan-Seon Lim (wslim@etri.re.kr), Jungha Hong (jhong@etri.re.kr), Cinyoung Hur (cyhur@etri.re.kr), Joo-Chul Lee (rune@etri.re.kr), Taewan You (twyou@etri.re.kr), Jeesook Eun (jseun@etri.re.kr), Byeongok Kwak (kwakbok@etri.re.kr), Jeonghwan Kim (ditto@etri.re.kr), Hae Sook Jeon (hsjeon88@etri.re.kr), and Tae Hwan Kim (thkimetri@etri.re.kr) are with the Communications & Internet Research Laboratory, ETRI, Daejeon, Rep. of Korea.

Woojik Chun (woojikchun@gmail.com) is with the Department of Information & Communications Engineering, Hankuk University of Foreign Studies, Yongin, Rep. of Korea.

## I. Introduction

With the huge rise in popularity of Internet services, IP networking is becoming the base technology for most kinds of fixed, mobile networks. The networks based on IP networking are usually known as "All-IP networks" and provide an effective solution for network providers in terms of capital expenditures and operating expenses.

However, recently, new network systems have begun to emerge that require capabilities beyond that provided by existing IP networking. For instance, the 5G system envisions large traffic volume for mobile data, a greater number of connected devices, lower latency, and longer battery life for low-power devices [1]. Existing IP networking has difficulty in satisfying these visions, especially in terms of scalability, traffic distribution, and the support of constraint environments. In a similar sense, the Internet of Things (IoT) is another big challenge for IP networking because of its limited capability to support essential IoT requirements, such as scalability, resource constraints, different traffic characteristics, handling mobility, and so on [2]. In addition, it is argued that IP networking cannot efficiently support data or information-centric networking, which is a crucial requirement in the popular information-based applications of today, because of its location-centric feature [3].

Due to the limited capability of IP networking, new networking technologies have been proposed in evolutionary and revolutionary manner. We note that the promising approach is to try to overcome the architectural limitations of IP networking, which originate from the fact that an IP address is tightly coupled with a specific location and forwarding mechanism, by adopting an identifier (ID)-based networking concept. In ID-based networking, an ID uniquely identifies communication objects irrespective of specific locations and mechanisms.

As evolutional approaches, many kinds of ID/locator (ID/LOC) split proposals pursue the separation of an ID from location information to solve problems of location-based routing and forwarding in IP networking. However typical ID/LOC split proposals, such as Locator/ID Separation Protocol (LISP), Host Identity Protocol (HIP), and Identifier/Locator Network Protocol (ILNP), still have a high dependency on existing IP networking; thus, they inherit some limitations [4]–[6]. In these proposals, some existing mechanisms (such as IP address–based identification, location based routing/forwarding mechanisms, and BSD socket API) are still used. Furthermore, we note that they focus on specific problems such as BGP scalability and security rather than provide a holistic solution.

Recently, there have been more revolutionary proposals for ID-based networking — Mobile Oriented Future Internet (MOFI), Named Data Networking (NDN), Network of Information (NetInf), expressive Internet Architecture (XIA), and MobilityFirst (MF) being some typical examples [7]–[11]. These proposals not only adopt the ID-based networking concept but also introduce new architectures and mechanisms to support emerging networking environments. However, they still have some critical open issues, such as support for various kinds of communication objects, scalable routing/forwarding, support for constrained environments, practical deployment, and so on. Based on an analysis of existing ID-based networking proposals, we conclude that there is no such proposal that can yet adequately meet all of the needs of the newly emerging networks. Section II will discuss the limitations of the evolutionary and revolutionary approaches in detail.

In this paper, we propose a new ID-based networking architecture and mechanisms, named IDNet, to meet the requirements for emerging and future networks. IDNet is aiming to resolve most of today's critical issues to realize ID-based networking, such as ID-based identification, scalable routing/forwarding, and efficient support of dynamic network environments. IDNet is functionally composed of four major blocks — routing, forwarding, mapping system, and application interface. We also evaluate the scalability of IDNet with numerical models and develop a prototype of IDNet on Linux and Android platforms.

This paper is organized as follows. Section II describes related work. Section III introduces the overall architecture and procedures of IDNet. Section IV shows our numerical analysis and implementation results. Finally, Section V briefly summarizes the main features of IDNet and concludes this paper.

## II. Related Work

ID/LOC split protocols are mainly proposed to overcome routing scalability, multi-homing, and mobility problems by introducing host IDs into the current Internet. LISP, ILNP, and HIP are typical examples of ID/LOC split protocols. LISP [4] separates an End host ID (EID) from Routing Locators (RLOC) to mainly address board gateway protocol (BGP) routing scalability. In LISP, both EID and RLOC have identical formats to a current IPv4 or IPv6 address, which are allocated to a network interface rather than a host. The major benefit of LISP is to reduce growth of BGP routing table size without disruption of current Internet architecture. On the other hand, ILNP [5] creates an EID by splitting IP addresses into two distinct namespaces. In the case of ILNPv6, the first 64 bits are used as a locator and the last 64 bits are used as an ID. From the perspective of practical deployment, ILNP is considered the most applicable ID/LOC split protocol. However, in both protocols, ID assignment to network-interface and IP address–based networking mechanisms remains unchanged from conventional IP networking; so, they have to inherit some limitations of IP networking.

Unlike LISP and ILNP, HIP [6] introduces a new namespace for a host to decouple the role of endpoint ID from IP address while the IP address is still used as a locator. The Host ID (HI) is a public cryptographic key and is used to easily implement an IP security protocol for security enhancement. HIP acts as a limited form of trust mechanism between two end hosts, enhanced mobility, and multi-homing. However, HIP, as with LISP, still uses an IP networking mechanism for the communication between two hosts.

MOFI, NDN, NetInf, XIA, and MF are typical revolutionary proposals. MOFI [7] is targeting a new networking technology optimized for a mobile oriented environment. MOFI introduces a new namespace for the host ID and provides two-tier ID/LOC, intra- and inter-mapping systems, and adopts a query-first-packet delivery mechanism. MOFI provides an optimized solution for a mobile-host-dominant environment; however, it considers only hosts as communication objects and does not provide ID-based routing/forwarding mechanism.

NDN [8] replaces a network service model from delivering data to a given destination address with the aim of fetching data identified by a given name. In NDN, hierarchical names are used as IDs to identify various types of data. Also, NDN reduces network traffic and latency with an in-network caching mechanism in which intermediate NDN routers maintain copies of original data. However, NDN primarily focuses only on specific communication objects (data); thus, there are some critical issues, such as scalable name-based routing, that have yet to be realized.

NetInf [9] also uses the data name as the ID and proposes a hybrid name/address-based routing and name resolution scheme for Information Centric Networking (ICN). NetInf


ETRI Journal, Volume 37, Number 5, October 2015
http://dx.doi.org/10.4218/etrij.15.2415.0045

forwards a Name Data Object request and transfers the corresponding objects by using name-based routing and forwarding or with the assistance of name resolution services. The hybrid routing approach also provides efficient mobility and multi-homing support. However, the realization of a scalable mapping system and name-based routing are still open issues.

XIA [10] supports IDs for multiple communication objects with abstraction principals. XIA defines four basic XIA Identifier (XID) types — Host XIDs, Service XIDs (SIDs), Content XIDs, and Network XIDs — and these four XIDs are formed in self-certifying IDs to achieve intrinsic security properties. XIA also supports technology evolvability with a fallback mechanism using directed acyclic graphs (DAGs). However, the representation of various communication types should be included into DAGs in advance and provision of additional information to declare service types in a scalable manner are still open issues.

MF [11] proposes a globally unique ID (GUID) for various types of communication objects and dynamic network address (NA) to improve mobility and trustworthiness. MF considers two different forwarding ways in which routers directly use NA as fast path and resolve GUID again as slow path. MF, as with NetInf, is required to verify scalable resolution systems, such as Name Certification Service and Global Name Resolution Service, to support a large quantity of content or devices.

## III. IDNet

### 1. Design Principles

Based on the observations on the requirements for new networking technology and the limitations of existing solutions, we have identified the following design principles for a new ID-based networking architecture.

#### *A. Location and Mechanism–Independent ID*

If an ID contains certain information regarding a location or packet forwarding, then it is likely to cause an inefficient delivery path in a dynamic network environment (for instance, mobility) or act as a barrier against the future evolution of the network. Therefore, ID-based networking should use an ID in such a way so that it is independent of a location and an underlying mechanism. In addition, a fixed size ID is preferred for fast exact-matching (EM) forwarding in intermediate nodes. Note that an ID can also be a non-aggregatable flat ID so as to provide a secure function; for instance, a hash of a public key.

#### *B. Gateway (GW)-Based Internetworking*

Considering emerging heterogeneous or constrained networking environments (for instance, 5G and IoT), ID-based networking should adopt GW-based internetworking rather than existing end host–based networking, which requires high capability of the end host. GW-based internetworking allows a minimum implementation in constrained communication objects, by placing most network functions on GW, and allows each domain to use its own networking technologies for optimized intranetworking.

#### *C. Dynamic and Scalable Routing Protocol*

It has been noted that many kinds of newly emerging networks are designed for supporting mobile or wireless environments having a dynamic network topology. Also, a destination object can reside at multiple locations due to the existence of copies. Accordingly, a routing protocol for ID-based networking should support the aforementioned dynamics in an efficient manner. In addition, considering the huge number of communication objects, such as in the IoT, services, and contents, the routing protocol should provide scalability too. Note that scalability is also closely coupled with network dynamics, as can be seen in the BGP routing table size explosion problem.

#### *D. Scalable and Fast ID-Based Forwarding Mechanism*

Not only a huge number of hosts but also various kinds of communication objects, such as contents and services, should be considered in ID-based networking. In such a case, if IDs are non-aggregatable, then the size of the forwarding table for IDs will be of crucial concern. To overcome this problem, a scalable ID-based forwarding mechanism should be provided. In addition, to support futuristic services requiring low latency, the processing delay for packet forwarding should be minimized as much as possible. In this context, EM using a fixed-size flat ID is preferred to longest prefix matching (LPM) of existing IP networking.

#### *E. Scalable Mapping System Supporting Locality*

From the point of view of scalability, a Lookup by ID (LBI) mechanism is generally preferred to that of a Route by ID (RBI). In the case of an LBI, a mapping system for mapping IDs to locators is an essential element. To support a tremendous number of non-aggregatable IDs, the mapping system should be scalable. In addition, it should provide locality to make the location keeping the mapping information manageable, from an administrative perspective. Quick responses to location queries are another essential requirement for real-time services.

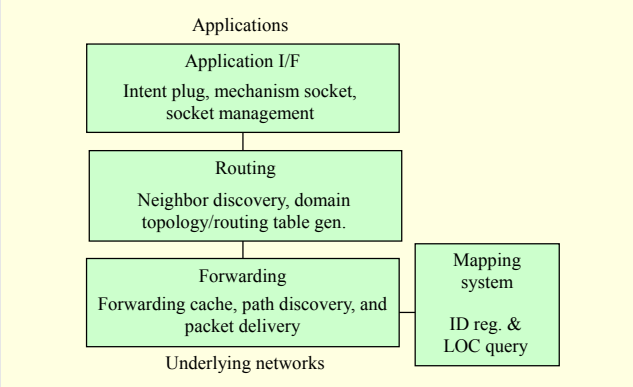



Fig. 1. Four major blocks of IDNet.

### *F. Application Interface with Separation of Intent from Location and Mechanism*

The separation of intent (for instance, data, user, or service) of a communication initiator from a specific location and an underlying delivery mechanism is a common requirement for ID-based networking. Therefore, an application interface for ID-based networking should separate any intent from a predefined location and mechanism to deliver the intent.

## 2. Overall Architecture

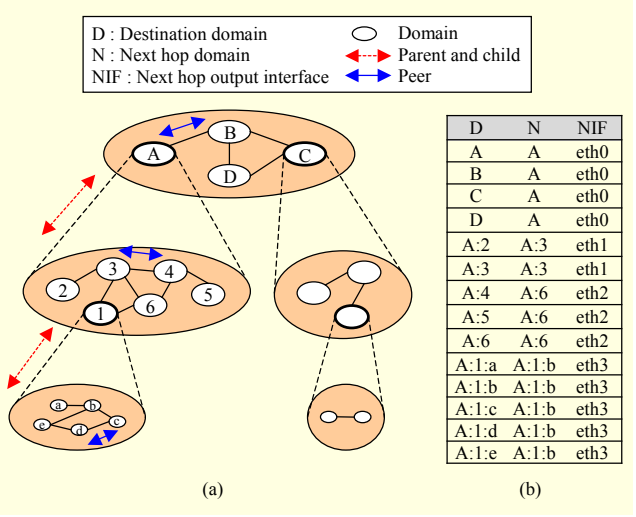
In IDNet, we assume a fixed-size flat ID, which uniquely identifies a communication object without the need for additional information regarding location and underlying mechanisms. An ID can be allocated to any type of object, such as a host, a user, a content, a service, and can be a self-certifying form for trustworthy communication, if required. A hash of a public key could be a typical example of a self-certifying ID.

The four major functional blocks of IDNet are illustrated in Fig. 1. Note that packet delivery within a domain is accomplished with an underlying networking technology and applications use new ID-based application interfaces.

### *A. Recursive Inter-domain Routing*

For scalable inter-domain routing, IDNet proposes recursive hierarchical domain structures, as shown in Fig. 2(a). The domains may be aggregated into a larger domain by federating domains with either parent-child or peer-to-peer relations.

Based on the structure, we propose a recursive inter-domain routing (RDR) protocol for IDNet. The proposed protocol is based on the link-state protocol and adopts a link state advertisement (LSA) filtering mechanism to reduce routing table size. In particular, each IDGW, which is an entry or exit point of a domain, broadcasts link states of equal or higher-tier domain only by sending LSAs. With the information gathered from the LSAs, each IDGW builds a global topology DB and




| D | N | NIF |
|---|---|---|
| A | A | eth0 |
| B | A | eth0 |
| C | A | eth0 |
| D | A | eth0 |
| A:2 | A:3 | eth1 |
| A:3 | A:3 | eth1 |
| A:4 | A:6 | eth2 |
| A:5 | A:6 | eth2 |
| A:6 | A:6 | eth2 |
| A:1:a | A:1:b | eth3 |
| A:1:b | A:1:b | eth3 |
| A:1:c | A:1:b | eth3 |
| A:1:d | A:1:b | eth3 |
| A:1:e | A:1:b | eth3 |

Fig. 2. RDR: (a) example topology and (b) corresponding routing table.

generates a routing table. Figure 2(b) shows a routing table of IDGW at domain "A:1" in Fig. 2(a). Since the change in a specific domain affects only peer and lower domains, RDR can rapidly respond to a change of network topology and efficiently address network dynamics.

### *B. Reactive ID Forwarding*

In IDNet, a forwarding path between communication objects is set up in a reactive manner and unused entries are removed on a timeout basis for scalability. With this reactive path setup, the size of a forwarding table can be reduced by a reasonable level.

When an IDGW receives the first packet from the sending of an object and has no forwarding entry in the forwarding table for a destination ID, it obtains a locator of the destination ID in the form of concatenated domain IDs (for example, "A:1:c" in Fig. 2(a)) from an ID/LOC mapping system (ILMS). Then, it performs a path-setup procedure based on the locator and finds the next hop according to its routing table. After the path setup, two objects can communicate with each other. Note that packet forwarding after a path setup can be processed quickly by an EM using fixed-size flat-IDs.

### *C. ID/LOC mapping system (ILMS)*

Since IDNet adopts an LBI approach, it essentially needs a system to provide a mapping between IDs and LOCs. We design an ILMS that stores and maintains the binding between ID and locator to provide a hint for the reactive path setup.

As Fig. 3 shows, an ILMS is constructed hierarchically as a network of mapping servers (MSs) including peering relationships, where several distinct trees are fully peered on


ETRI Journal, Volume 37, Number 5, October 2015
http://dx.doi.org/10.4218/etrij.15.2415.0045

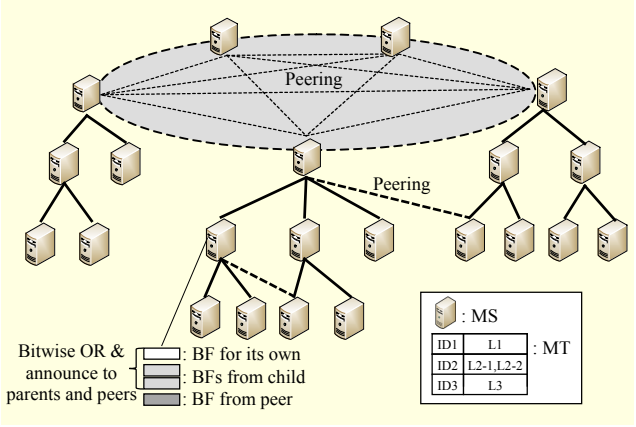



Fig. 3. ILMS structure.

the top. A bloom filter (BF) is an aggregated form of flat-IDs. Each MS consists of a mapping table (MT) and BFs for itself, from children, and from peers. Each MS announces the union of all the BFs from children and the BF for itself through a bitwise 'OR' operation to parents and peers. Flat-IDs can be registered anywhere according to a user's request, and a BF update then transcends to the top of trees. A map-request message is forwarded toward the MS where the binding is actually stored by the BF test, and the map-reply message then takes the reverse path.

To address the scalability on the ever-increasing number of IDs, flat-IDs are distributed and aggregated through the hierarchical structuring of a BF. Locality can be also easily supported since there is no constraint on registering flat-IDs in an ILMS.

### *D. ID-Based API*

To achieve the decoupling of an ID from a specific location and networking mechanism, IDNet requires new ID-based APIs. Figure 4 shows the components of an API and the actions among them.

The iPlug takes charge of application-specific capabilities and has customizable functions, such as a new naming scheme and flow control. The dSocket acts as the cut-off point of separation and contains the responsibilities of a network, such as addressing, mobility, and multi-homing. The dSocket Manager dynamically matches iPlug and dSocket by plugging in and out.

In contrast with Internet BSD socket API that uses an IP address and port pairs, the ID-based API here allows applications to use both a source ID and a destination ID to identify communication entities. An application can also be dynamically bound to a specific communication environment by plugging its iPlug into a dSocket. Since applications can select, move between different communication environments, or join multiple environments simultaneously, an ID-based API

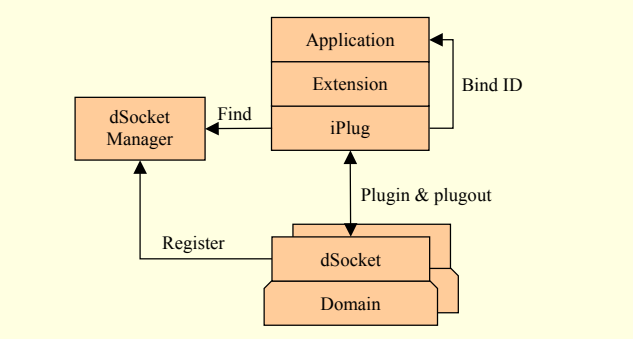



Fig. 4. ID-based networking API components.

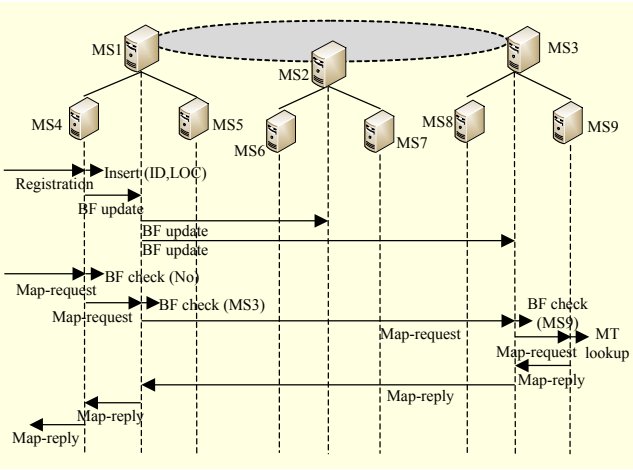



Fig. 5. Procedures of ID registration and locator query/reply.

can efficiently support mobility, multi-homing, N-screen, evolvability, and so on in an efficient manner.

## 3. Procedures

Communication between two objects basically consists of ID registration, locator query/reply to/from ILMS, and packet delivery. Detailed procedures are given in the following subsections.

### *A. ID Registration and Locator Query/Reply*

Figure 5 shows an example of procedures of ID registration and locator query, where three trees having nine MSs are fully peered on the top. When MS4 receives a registration message for an ID, it inserts the ID and locator into its MT and updates its own BF. Then, it sends a "BF update" message to its parents (MS1), and then MS1 updates BFs for its peers (MS2 and MS3). In the example shown in Fig. 5, we assume that MS4 receives a "Map-request" message for the ID registered in MS9. MS4 first searches its own BF, but it returns a negative answer. In the next step, a "Map-request" message is forwarded to its parents (MS1) and MS1 forwards it to MS3

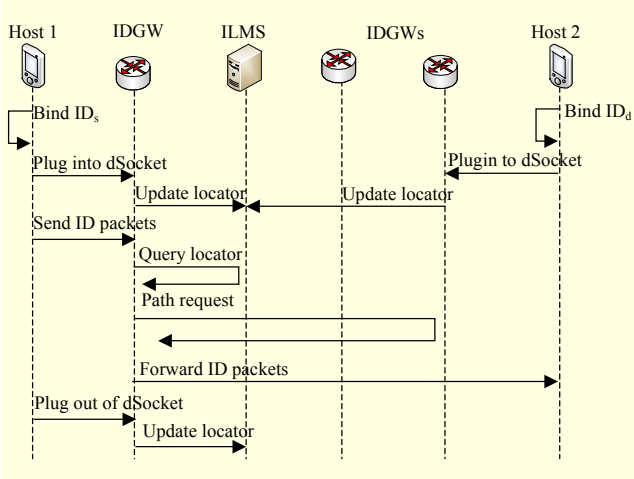



Fig. 6. Procedures of ID packet delivery.

through its BF search. Then, the "Map-request" message is forwarded from MS3 to MS9. MS9 looks up its MT and finds out the requested mapping information. Now, MS9 sends a "Map-reply" message on the locator of the ID to MS3. Finally, the "Map-request" message is forwarded to the *map requester* going through MS1 and MS4.

### *B. Packet Delivery*

Figure 6 depicts an example of packet delivery between two hosts. If an application begins communication, then it should first bind its ID to an iPlug. After binding to the iPlug, the application becomes an entity of IDNet, called ID entity, and it can communicate with other ID entities by sending ID packets through the iPlug. The ID entity plugs into a dSocket to use the IDNet. The dSocket may be in a local host, which supports the IDGW functionalities or one of the IDGWs of the current domain. When the ID entity plugs into the dSocket, the owner of the dSocket becomes a default IDGW of the ID entity. The default IDGW updates the ID entity's current locator to ILMS. Then, ID packets sent from the ID entity are forwarded to the default IDGW via the dSocket.

If the default IDGW has an entry for the destination ID in its forwarding cache, then the packet can be forwarded to a next-hop IDGW immediately. Otherwise, it performs the path setup procedure as follows. The IDGW queries a current locator for the destination ID from ILMS. After obtaining the locator, the IDGW sends a "Path request" message to the next IDGW based on the routing table information, which is generated via an RDR protocol. This message propagation repeats until the "Path request" message reaches a final IDGW, which is the default IDGW of the destination ID or an IDGW that has an existing forwarding cache entry for the destination ID. After the path setup procedure ends successfully, ID packets are forwarded according to the forwarding cache information. The ID entity can plug out of dSocket after finishing communication or to move to a different domain. If a locator of the destination ID changes during communication, then the path setup procedure is triggered by the previous default IDGW of the destination ID. The location-change scenarios will be described in detail in Section IV-2.

## IV. Numerical Analysis and Implementation

A proof of concept of IDNet is accomplished in two ways — numerical analysis and the development of a prototype. The former is mainly to verify the scalability of the proposed routing protocol (RDR) and ILMS, and the latter is to prove superiority of IDNet in dynamic network environments.

### 1. Numerical Analysis

To verify the scalability issues of RDR and ILMS, we have developed numerical models for each.

#### *A. RDR*

For analysis of RDR, we made the following assumptions:

- With the exception of leaf domains, each domain has an equal number of child domains (or as equal as possible).
- There is only one IDGW per domain.
- The location shape of the peer domains in the same parent domain is of a grid type.
- The total number of domains in the whole network is $n$.
- The lowest tier number is denoted by $t$, where the tier number of the top-level domain is 1.

We first derive equations for the topology graph size, which is the most intuitive metric for the routing scalability. Let $d$ be the average number of child domains. We then have

$$n \approx d + d^2 + \ldots + d^t = \frac{d(d^t - 1)}{d - 1}. \quad (1)$$

If we fix the value of $t$, then we can obtain the value of $d$ from (1). When a gateway belongs to tier $x$ ($1 \le x \le t$), the size of its topology graph is about $x \times d$ owing to the LSA filtering rule in RDR. Therefore, we can obtain the average topology graph size by

$$\frac{d \times d + d^2 \times 2d + \cdots + d^t \times t \times d}{n}. \quad (2)$$

Figure 7 shows the topology graph size obtained from (2) with varying $t$. Note that when $t = 1$, RDR works as a legacy link-state routing protocol with no hierarchy. When $t = 1$, because every IDGW has a complete topology graph, the topology graph size is $n$. As we can see in the figure, the topology graph size is dramatically reduced with an increase in

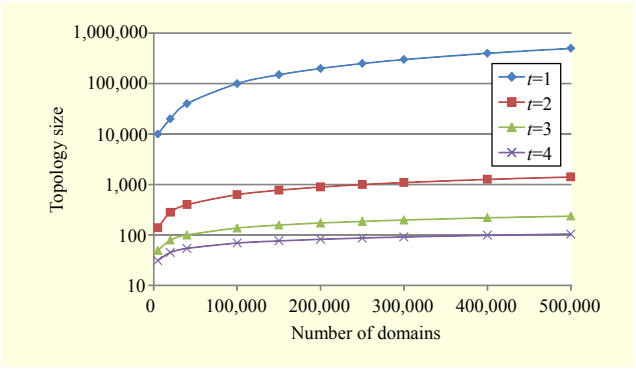



Fig. 7. Average topology graph size of RDR with varying $t$.

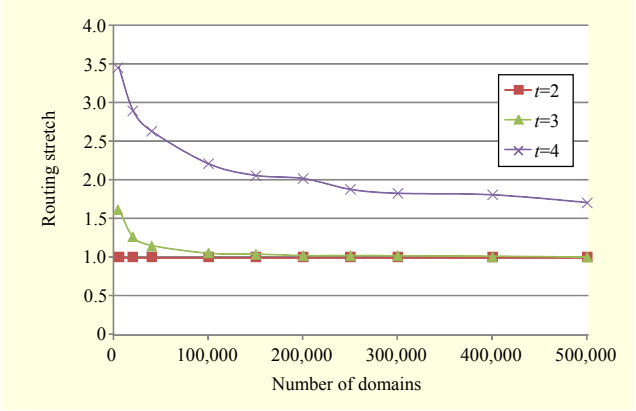



Fig. 8. Routing stretch of RDR with varying $t$.

the value of $t$ ($y$-axis in the logarithmic scale). If we set $t = 4$, then we can keep the topology graph size under 100 until $n$ is $4 \times 10^5$, which is much larger than the total number (66,249) of autonomous system numbers (ASNs) on the Internet today.

The main disadvantage of RDR over a legacy link-state routing is the route optimality. Since gateways in RDR maintain an abstracted topology graph, they cannot always find the optimal end-to-end routes. To test the route optimality, we measure the routing stretch of RDR, which is defined by the ratio between the length of the selected route in RDR and the length of the optimal route. Here, we only consider routes between two leaf domains.

Let $l_k$ denote the average number of hops among peer routers, where $k$ peer domains belong to the same parent domain. The probability of two leaf domains having a different top level domain is $(d-1)/d$. In this case, the route length is

$$(t-1)(l_d+1)+l_d+(t-1)(1+l_d). \tag{3}$$

Otherwise, the probability of the two leaf domains having the same domains from the top tier to tier $x$ ($1 \le x < t-1$) is $1/d^x \times (d-1)/d$, and the route length in this case is

$$(t-1-x)(l_d+1)+l_d+(t-1-x)(1+l_d). \tag{4}$$

Finally, the probability of the two leaf domains having the same domains from the top tier to tier $t-1$ is $1/d^{t-1}$. In this case, the route length is $l_d$ because they are peer domains of each other. Therefore, the average route length is

$$\sum_{x=0}^{t-2}\frac{d-1}{d^{x+1}}\times\left(2(t-1-x)(l_d+1)+l_d\right)+\frac{l_d}{d^{t-1}}. \tag{5}$$

Based on (5), we calculated the routing stretch of RDR. As shown in Fig. 8, the routing stretch is highly affected by the value of $t$. With RDR, the network administrator can opportunistically adjust the value of $t$ by considering the total number of domains and the administrator's preference. For example, if routers have significant computing power and a low end-to-end delay is required, then $t$ should be set to a small value. Otherwise, $t$ can be set to a large value for reducing the overhead.

### B. ILMS

In ILMS, it is important to minimize the number of queries to MSs, since a large number of queries will be translated to the additional burden of MSs, which eventually leads to performance degradation and inefficiency. Thus, we build an analytical model to calculate the average number of MS accesses per a locator query.

We assume that ILMS is constructed by a perfect $d$-ary tree, which means that all leaves of the ILMS structure are at the same depth, and every parent MS has exactly $d$ child MSs. We omit the peering relationship in the analytical model to make it simpler, which yields an upper bound in terms of the number of MS accesses per a locator query. We also assume that all IDs are uniformly registered in all leaf MSs and every BF has a uniform false-positive probability. Although this assumption may be unrealistic, our analysis can be viewed as the upper bound if a false-positive probability on the top of the hierarchy is used. Alternatively, an average value of the false-positive probabilities in the ILMS structure can be used. Let $d$ represent the degree of an MS, $h$ the height of an ILMS tree, and $p$ the false-positive probability of a BF. Then, the average number of MS accesses per a locator query, $f(h, d)$, can be found in the following recursion formula, in terms of $h$:

$$f(h,d)=\begin{cases}1 & h=0,\\ \frac{1}{d}f(h-1,d) & \\ +\frac{d-1}{d}\left[2h+1+\sum_{i=1}^{3}g_i(h,d)\right] & h\ge 1,\end{cases} \tag{6}$$

where $1/d$ is the probability that the look-up process succeeds

Table 1. Average number of MS accesses/LOC query with $N = 10^9$, $p = 0.001$.

| $h$ | $d$ | $f(h, d)$ |
|---|---|---|
| 2 | 31,622 | 1099.72 |
| 3 | 999 | 15.967 |
| 4 | 117 | 10.3903 |
| 5 | 62 | 11.5407 |
| 6 | 31 | 13.2688 |

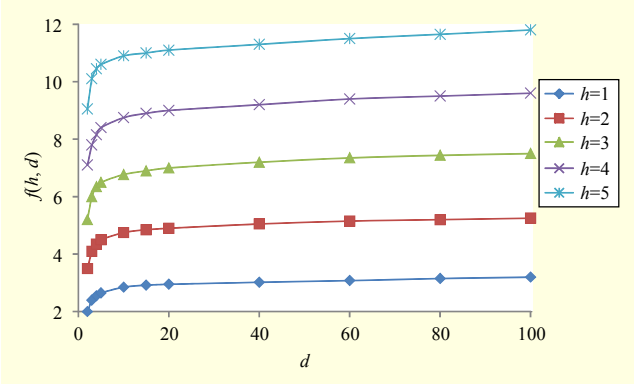



Fig. 9. Average number of MS accesses per locator query with $p = 0.001$.

within a subtree that includes the very first accessed MS by the locator query, and $g_i(h, d)$ represents the following false-positive error cases:

- $g_1(h, d)$: the subtree including the very first accessed MS
- $g_2(h, d)$: the subtree passed the BF test from root
- $g_3(h, d)$: the $(d-2)$ subtrees by false-positive error from root

The variable $g_i(h, d)$ can be obtained as follows:

$$g_1(h,d) = g_2(h,d) = \sum_{m=0}^{h-2}\sum_{n=0}^{m}(dp)^n\, p(d-1), \tag{7}$$

$$g_3(h,d) = (d-2)\sum_{n=0}^{h-1}(dp)^n\, p. \tag{8}$$

To minimize the average number of MS accesses per a locator query, we fix the total number of MSs in an ILMS to be $N$ and have observed that there exits an optimal pair, $h$ and $d$. Table 1 shows that $h = 4$ and $d = 117$ provides the optimal value of the average number of MS accesses per a locator query, $f(h, d)$, as 10.3903, when $N = 10^9$ and $p = 0.001$ are assumed. This result shows that ILMS performs better than a DHT-based approach, which is the most popular for distributing IDs, since a DHT-based approach can guarantee that a message can be forwarded in $O(\log N)$ hops, on average, resulting in a complexity of 29.8974 by $\log_2 N$. Table 1 also shows that the average number of MS accesses per a locator query significantly drops as $h$ increases, and then it increases gradually and converges.

Figure 9 shows $f(h, d)$, for different $h$ and $d$ values where $p = 0.001$ is used. As can be seen, the average number of MS accesses per a locator query increases according to a logarithmic scale, which is a similar result with the DHT-based system.

## 2. Implementation

We have implemented a prototype of IDNet to verify its feasibility and performance on real systems. The prototype includes all of IDNet components (routing/forwarding, mapping system, and APIs) and test applications. Our implementation is based on the Click modular router [12], and it provides C/C++ style APIs for supporting IDNet application programming. The prototype source code will be available on the IDNet homepage [13] soon.

Figure 10 shows the main modules of an IDGW. When an ID packet is delivered to an IDGW from its local domain or other IDGW, it is passed to the "Forwarding" module. The "Forwarding" module has an "FW cache," which is maintained in a reactive manner. If there is no entry in the "FW cache" for a destination ID, then the "Locator fetching" and "Path discovery" procedures are performed to register a new entry in the "FW cache." The "Routing" module has a "Routing table," which is updated by the "Neighbor discovery" and "Domain LSA flooding" procedures. The "Routing table" is accessed by the "Forwarding" module during the "Path discovery" procedure. The API module provides dSocket and

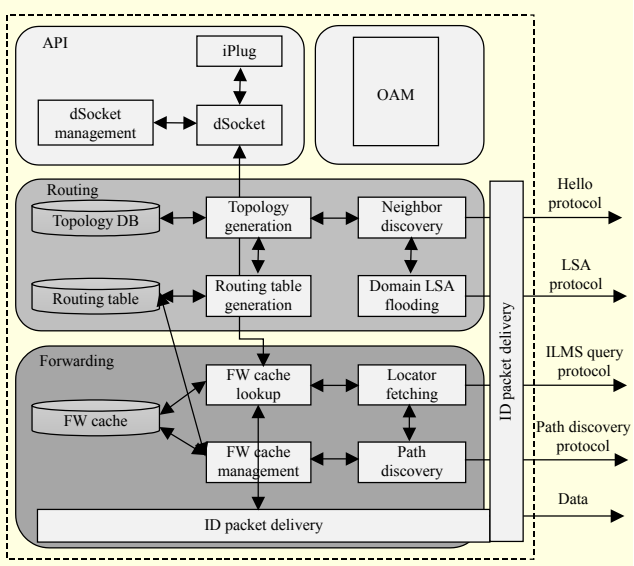



Fig. 10. Main modules of IDGW.


ETRI Journal, Volume 37, Number 5, October 2015
http://dx.doi.org/10.4218/etrij.15.2415.0045


(a) (b)

Fig. 11. Photos of testbed: (a) gateway and ILMS and (b) Android application.

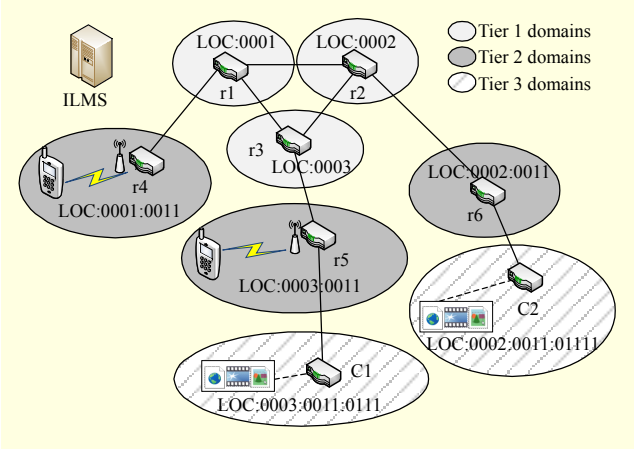



Fig. 12. Network topology of testbed.

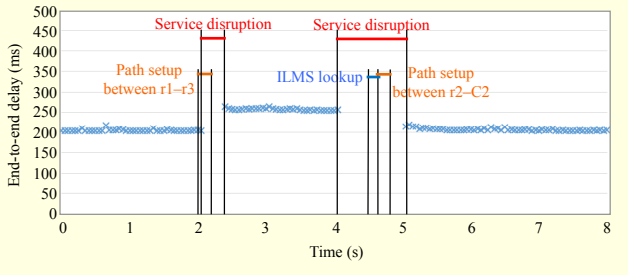



Fig. 13. End-to-end delay and timing diagram of link failure scenario.

iPlug for applications.

In the prototype, we assume that there is a single MS in ILMS. The MS has a simplified forwarding module since it does not need to forward ID packets sent by other entities. The ID/LOC mapping module has the ID/LOC DB, which stores mapping information between IDs and locators.

We installed our prototype on a Linux platform, as shown in Fig. 11(a). We also implemented a multimedia streaming client and server that exploits our ID-based API. The streaming client and server are implemented on an Android platform and a Linux platform, respectively. We assign a unique ID to each music content, video content, and image file on the server. In addition, the client application and server application also have their own unique ID. Figure 11(b) shows a GUI of the client. When a user requests a multimedia content, it is delivered to the client from the closest server in the network.

Figure 12 shows a topology configuration. There are six IDGWs (r1–r6), two contents server (C1 and C2), and one MS. The IDGWs and contents servers are connected through Ethernet. To emulate a link delay typical of large-scale networks, we add an additional link delay of 50 ms to each link. The Android client is connected to r4 or r5 via Wi-Fi connection. The MS is connected to each IDGW via Ethernet switch; however, in the figure, connections between the MS and other IDGWs is not shown. Based on the topology, we test the performance of IDNet in three scenarios to verify the basic operations in dynamic network environments.

The first scenario is client mobility. In this scenario, the client moves from domain r4 to domain r5 while receiving a video stream from server C1. When the client stays in r4, the locator "00001111:11111111" is registered in the MS for the client application. After moving to r5, the gateway of r5 sends a location update message to the MS to update the locator of the client application to "00003333:11111111," the locator of r5. The locator change does not affect the client application with the help of the separate ID/LOC mechanism of IDNet.

The second scenario is server relocation. In this scenario, the client stays in r4, and it first receives a video stream from server C1. Then, we terminate the server application on C1. When the r5 gateway detects the termination of the server application, it requests the MS to delete its locator for the server application ID. After that, the packets from the client are automatically forwarded to a new server, C2.

In the last scenario, we test how to recover link failure events in IDNet. First, the client stays in r4, and it first receives a video stream from server C1, as in the other scenarios. Then, we terminate the link between gateway r1 and gateway r3. In this case, the gateways find another path that goes through gateway r2. After that, we terminate the link between gateway r2 and gateway r3. Since there is no path to server C1, gateway r2 finds a new server, C2, with the help of the MS. When gateway r2 obtains the locator of C2, the path between r2 and C2 is set up, and then communication is resumed.

Figure 13 shows the end-to-end delay and timing diagram of the third scenario. In the case of the first link failure event (link between r1 and r3), the service disruption time is about 300 ms.

Table 2. Forwarding paths between client and server.

| Event | Forwarding path |
|---|---|
| Original path | C1-r5-r3-r1-r4 |
| Client mobility | C1-r5 |
| Server relocation | C2-r6-r2-r1-r4 |
| Link failure #1 | C1-r5-r3-r2-r1-r4 |
| Link failure #2 | C2-r6-r2-r1-r4 |

Since there is no query to the MS, the new path through r2 is set up quickly. In the case of the second link failure event (link between r2 and r3), the service disruption time is relatively long compared to the former case, since the query to the MS results in an additional delay (as shown in the figure). However, due to the buffering mechanism of the video streaming application, video can be played smoothly.

Table 2 summarizes the forwarding path between the client and server for each scenario. As we can see from these results, IDNet can efficiently support not only the client mobility scenario but also other useful scenarios such as finding out alternative destinations in server relocation and link failure conditions. In any scenario, the communication between end applications is not disrupted if there is an available path between them. This ID/LOC split makes applications simple and improves network utilization.

In particular, from the point of view of mobility support, it is worth noting that IDNet does not have the same disadvantages of other future Internet architectures. MOFI does not consider various types of communication objects, such as contents, so it cannot support a server relocation scenario or link failure scenario. MF has a similar mobility support procedure with IDNet. However, IDNet has an advantage over MF using DHT in terms of session-setup delay and handover delay with the help of an efficient ILMS. In the case of NDN, when a content source moves from one network to another, it needs to announce the reachability of the content through the routing protocol, and this may lead to a routing update message and further propagating in the global routing tables. In XIA, XID has to include location information for delivering packets to a mobile host, so an ID and locator are not completely separated as in IDNet.

## V. Conclusion

Recently emerging and envisioned networks require capabilities beyond those provided by All-IP networks, and ID-based networking is recognized as a promising solution to meet such requirements. We noted that various kinds of ID-based networking technologies have been proposed, but they have their own limitations. This paper proposed a new ID-based networking architecture with mechanisms, named IDNet, to satisfy the requirements.

With numerical analysis, IDNet shows that it can solve the scalability issue in ID-based networking, which is still a big challenge among other ID-based networking proposals. Also, through an implementation, IDNet shows that it can efficiently support dynamic network environments, such as host mobility and finding alternative destinations in server relocation and link failure situations. Note that the latter could be an essential function for traffic distribution, as we can see in ICN. In addition, from an architectural perspective, IDNet has an advantage in providing low latency services due to its fast EM forwarding mechanism compared to the existing LPM. Regarding IoT, since a GW, as opposed to constrained devices, can handle most of the functions required for networking, IDNet could be a good solution.

As the next step, we're elaborating on a couple of usage cases of IDNet. 5G core networks and the IoT are the appropriate candidates of the use cases. We also recognize that ID-based networking can be a prospective solution for trustworthy networking by adopting the concepts of self-certifying IDs and trusted domains. Therefore, it is also a future research topic of IDNet.

## References


[1] A. Osseiran et al., "Scenarios for 5G Mobile and Wireless Communications: The Vision of the METIS Project," *IEEE Commun. Mag.*, vol. 52, no. 5, May 2014, pp. 26–35.

[2] IRTF ICNRG draft draft-zhang-iot-icn-architecture-01, *ICN based Archit. for IoT*, IRTF, June 2014.

[3] V. Jacobson et al., "Networking Named Content," *Int. Conf. Emerging Netw. Experiments Technol.*, Rome, Italy, 2009, pp. 1–12.

[4] IETF RFC 6830, *The Locator/ID Separation Protocol (LISP)*, IETF, Jan. 2013.

[5] IETF RFC 6740, *Identifier-Locator Network Protocol (ILNP) Architectural Description*, IETF, Nov. 2012.

[6] IETF RFC 5201, *Host Identity Protocol*, IETF, Apr. 2008.

[7] J.-I. Kim, H. Jung, and S.-J. Koh, "Mobile Oriented Future Internet (MOFI): Architectural Design and Implementations," *ETRI. J.*, vol. 35, no. 4, Aug. 2013, pp. 666–676.

[8] L. Zhang et al., "Named Data Networking," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, July 2014, pp. 66–73.

[9] C. Dannewitz et al., "Network of Information (NetInf) - An Information-Centric Networking Architecture," *J. Comput. Commun.*, vol. 36, no. 7, Apr. 2013, pp. 721–735.

[10] D. Naylor et al., "XIA: Architecting a More Trustworthy and

Evolvable Internet," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 3, July 2014, pp. 50–57.
[11] D. Raychaudhuri, K. Nagaraja, and A. Venkataramani, "MobilityFirst: A Robust and Trustworthy Mobility-Centric Architecture for the Future Internet," *ACM SIGMOBILE Mobile Comput. Commun. Rev.*, vol. 16, no. 3, July 2012, pp. 2–13.
[12] Click Modular Routers. Accessed Feb. 3, 2014. http://www.read.cs.ucla.edu/click/
[13] IDNet homepage. Accessed Feb. 3, 2014. http://www.idnet.re.kr

**Heeyoung Jung** joined ETRI in 1991 and is currently a principal research member. He received his PhD degree in information and communications engineering from Chungnam National University, Daejeon, Rep. of Korea, in 2004. His major research interests include the Internet/Future Internet and mobile network technologies, and he has been closely related to standardization activities in ITU-T, IETF/IRTF, and so on. His current research topic is next-generation networking technology based on identifiers.

**Wan-Seon Lim** works as a senior researcher at ETRI. He received his BS, MS, and PhD degrees in computer science and engineering at Pohang University of Science and Technology, Rep. of Korea, in 2004, 2006, and 2010, respectively. He was a research fellow with the Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, USA. His research interests include Future Internet, wireless LAN MAC protocols, ad-hoc networks, and video streaming over wireless networks.

**Jungha Hong** received her BS and MS degrees in mathematics from Korea University, Seoul, Rep. of Korea, in 1999 and 2001, respectively. After receiving her MS and PhD degrees in computer science from the University of Missouri, Kansas City, USA, in 2006 and 2010, respectively, she joined ETRI in 2010 and is currently a senior research member. Her current research interests include ID/LOC separation schemes in Future Internet and the analysis of computer networks.

**Cinyoung Hur** works an engineer at ETRI. She received her BS and MS degrees in computer science from Sookmyung Women's University, Seoul, Rep. of Korea, in 2007 and 2009, respectively. Her major research interest is networking support and management in distributed systems. She is currently involved in networking APIs based on identifiers.

**Joo-Chul Lee** is a member of the ID-Based Communication Research Team at ETRI. He was responsible for the development of an IPv4/IPv6 translation toolbox named "6TALK" between 2001 and 2003. The 6TALK box supports NAT-PT, DSTM, and several basic tunneling mechanisms. His major contribution to the 6TALK box is the NAT-PT translation module. In 2004, he developed the DHCPv6 client module supporting prefix delegation. Between 2005 and 2007, he worked on a standard for NGN in ITU-T, joined an automotive project, and developed a configuration tool & platform for the AUTOSAR standard from 2008 to 2012. Now, he has been developing an ID-based network platform based on Click-router.

**Taewan You** joined ETRI in 2011 after finishing his PhD degree in computer engineering at Seoul National University, Rep. of Korea. Currently, he is a senior research member. He received his MS degree in computer science and engineering from SNU in 2004. His major research interests include Future Internet, IPv6, mobility, and multi-homing technologies. His work is also closely related to standardization activities in IETF as well as ITU-T. He has published five ITU-T recommendations as an editor and has participated in EU-FP7 SMARTFIRE.

**Jeesook Eun** joined ETRI in 2000 after receiving her MS degree in computer engineering from Chonbuk National University, Chunju, Rep. of Korea. Currently, she is a senior research member. She has worked on many projects, including the Ethernet-PON system, RFID-middleware system, and Vehicle-Infotainment system, where she was responsible for the development of software components. Her current research interest is trustworthy communication in next-generation networking technology based on identifiers.

**Byeongok Kwak** received his MS degree in computer science from Chungbuk National University, Cheongju, Rep. of Korea, in 1996. Since 2000, he has been with ETRI as a principal researcher. His major research interests include the Internet/Future Internet and cloud computing technologies. His current research topic is next-generation networking technology based on identifiers.

**Jeonghwan Kim** joined ETRI in 1999 after receiving his MS degree in electronic engineering from Kyungpook National University, Daegu, Rep. of Korea. Currently, he is a principal research member. His major research interests include the Internet/Future Internet, service oriented architecture, and semantic technologies. His current research topics are API provisioning and testbed virtualization of identifier-based networking technology.

**Hae Sook Jeon** joined ETRI in 2000. She received her BS, MS, and PhD degrees in computer engineering from Chungnam National University, Daejeon, Rep. of Korea, in 1992, 1995, and 2015, respectively. She is currently a senior member of the engineering staff at ETRI. Her major research interests include the Internet/Future Internet and machine learning.

**Tae Hwan Kim** received his BS and MS degrees in computer engineering from Korea Aerospace University, Seoul, Rep. of Korea, in 2008 and 2010, respectively. He had been working with the Future Internet Research Team, National Institute for Mathematical Sciences, Daejeon, Rep. of Korea, until 2013 and joined the ID-based Networking Research Lab at ETRI in 2014. His research interests include future Internet and network and information security — particularly DDoS and botnet defense.

**Woojik Chun** has been an invited researcher at Hankuk University of Foreign Studies, Yongin, Rep. of Korea, since 2012. From 2009 to 2012, he worked as a researcher at ETRI. He founded a venture company, Raonet Systems, Inc., Bundang, Rep. of Korea, in 2000 and served as the CEO until 2009. From 1992 to 2001, he worked as a professor of computer engineering at Chungnam National University, Daejeon, Rep. of Korea. He received his BS and MS degrees in computer engineering from Seoul National University, Rep. of Korea, in 1982 and 1984, respectively. He received his PhD degree in information and computer sciences from the University of Delaware, Newark, USA, in 1992. His major research interests include the Internet/Future Internet and protocol engineering. His current research topic is identifier-based communication networking.