An ID/Locator Separation-Based Mobility Management Architecture for WSNs

Jinho Kim, *Member, IEEE*, Jun Lee, Hyoeng Kyu Kang, Dae Sun Lim, Choong Seon Hong, *Senior Member, IEEE*, and Sungwon Lee, *Member, IEEE*

Abstract—In this paper, we focus on a scheme that supports mobility for groups of sensor networks. Mobility in wireless sensor networks (WSNs) is one of the most important WSN technologies for applications such as healthcare, vehicular communication systems, intelligent transport systems, and logistics applications. This paper proposes a new mobility management architecture for WSNs that is based on the ID/LOC separation concept for ID-based communications with location-based routing. The proposed architecture supports energy-efficient lightweight mobility control for a large number of WSNs by distributed management manner. Furthermore, the discover-before-forward concept is proposed for route optimization. Performance results show that the proposed ID/LOC separation-based mobility architecture for supporting 6LoWPAN is more efficient and lighter than the existing HIP scheme in terms of energy consumption, total signaling cost and packet delivery cost ratio.

Index Terms—ID/Locator separation, 6LoWPAN, sensor network mobility

1 Introduction

In the nearest future, there will be much more wireless sensor devices than mobile phones. Various ubiquitous services will be enabled when wireless sensor devices are connected to the Internet. The term wireless sensor network (WSN) has become popular in the industry referring to the aspects of remote monitoring and control of devices over the Internet.

Of particular interest is IPv6 over Low Power Wireless Personal Area Network (6LoWPAN) [1], [2], which allows simple wireless connectivity with limited power and low-cost communication and is the key technology for WSNs.

6LoWPAN adopts the IPv6 stack for seamless connectivity between IEEE 802.15.4 [3] based networks and IPv6-based infrastructure, enabling wireless sensor devices to ensure that sensor data can be accessed anytime and anywhere. The 6LoWPAN protocol could be suitable for smaller devices with low energy consumption. Additionally, it enhances the scalability and mobility of WSNs.

In this paper, we focus on a scheme that supports mobility for groups of sensor networks. There are many possible mobility applications in 6LoWPAN sensor networks. Mobility in 6LoWPAN is utilized in realizing applications where sensor nodes transmit the sensed data to a monitoring server. The requirement for mobility and 6LoWPAN can be seen in usage scenarios for healthcare, vehicular communication systems, intelligent transport systems, and logistics applications. 6LoWPAN sensor networks are especially envisioned to be used in healthcare systems [4]. In these cases, patients have sensor nodes on their body for sensing some of their important health parameters like pulse rate, temperature, etc. These sensor nodes can sense the data and transmit it to a monitoring facility, even when a patient is moving. 6LoWPAN-based sensor networks have been considered as the most suitable technology for supporting mobility in sensor networks due to their low power and low data rate characteristics.

In order to provide mobility for sensor devices or sensor networks, an efficient IP mobility management protocol is needed to maintain connectivity of the sensor devices while they are on the move.

However, there is a problem concerning the use of IP addresses in the current Internet architecture, namely, IP addresses acting both as host identifiers (IDs) and locators (LOCs). In other words, an IP address is used on the network layer as a LOC for topological locations or routing packets. Furthermore, the IP address is also being used on the transport and application layer as an ID for names of host interfaces or for the identification of communication sessions.

The current Internet architecture requires that IP addresses remain unchanged during a session. This means that a changing IP address indicates a changing endpoint ID, and the communication session is terminated. Combining the roles of host ID and LOC in a single IP

- *J. H. Kim is with the Department of Computer Engineering, Kyung Hee University, Yongin 446-701, Korea, and also with the Advanced Institute of Technology, KT Corporation, Korea. E-mail: jinhowin@gmail.com.*
- *J. Lee, H. K. Kang, C. S. Hong, and S. Lee are with the Department of Computer Engineering, Kyung Hee University, Yongin 446-701, Korea. E-mail: {khunet, mirinae85}@gmail.com; {cshong, drsungwon}@khu.ac.kr.*
- *D. S. Kim is with the Department of Computer Engineering, Kyung Hee University, Yongin 446-701, Korea, and also with the IP Network Division at KDDI R&D Laboratories Inc., Fujimino, Japan. E-mail: dskim@khu.ac.kr.*

Manuscript received 18 Oct. 2011; revised 4 Aug. 2013; accepted 10 Oct. 2013. Date of publication 3 Nov. 2013; date of current version 26 Aug. 2014. For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier 10.1109/TMC.2013.142

1536-1233 © 2013 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

address is unsuitable for future mobile environments since mobility needs to changing the IP address.

Many solutions have been proposed for supporting mobility based on the current Internet architecture, such as Mobile IPv4 (MIPv4) [5], Mobile IPv6 (MIPv6) [6], and Proxy Mobile IPv6 (PMIPv6) [7]. However, such available incremental patches in the form of patch-on increase the complexity and reduce the network performance.

To overcome problems associated with the dual use of IP addresses, the ID and LOC roles should be split into IDs used by applications from LOCs used by routing. However, the existing ID/LOC separation architectures still have some limitations.

In the existing ID/LOC separation architectures, the end-host ID is used for mapping with a LOC so that ID/LOC mapping systems need to manage the entire end-host ID for tracking their location. This causes the ID/LOC mapping table entries to increase in size so that the existing architectures are not suitable to support a large number of sensor devices.

In order to support ID/LOC split over WSN as efficiently as possible, we consider a distributed mobility management as one of the main design goals. In the proposed architecture, all IDs of the user-owned sensor devices are managed by each user device while localized mapping systems in the network only manage the prefix as the part of the user device ID. The prefix is used as the key for mapping with a LOC. Since a user mobile network, including the user's device and sensor devices, has the same globally unique prefix, the mapping systems only need to manage one mapping entry about the prefix for the user's device as well as a number of user-owned sensor devices, but not every end-host IDs.

This paper proposes a new ID/LOC separation-based lightweight mobility management architecture for 6LoWPAN that supports mobility for groups of sensor networks. We explain how the proposed architecture supports ID-based communication with location-based routing and energy-efficient 6LoWPAN mobility in the distributed management manner.

Our paper is organized as follows: In Section 2, we briefly introduce related work on conventional IP mobility management based on the current Internet architecture and ID/LOC separation architecture, including problem statements. In Section 3, we describe our proposed ID/LOC separation-based architecture for supporting 6LoWPAN. Section 4 presents performance evaluations and analysis. In Section 5, acronyms newly defined in this paper are summarized. Section 6 concludes our work.

2 Related Work

In this section, we introduce related works regarding IP mobility management protocols in 6LoWPAN and ID/LOC separation architectures.

2.1 IP Mobility Management Protocols

Efficient IP mobility management protocols, which are based on the current Internet, are needed in order to maintain connectivity during movement of sensor devices or groups of sensor networks movement. Such protocols can be classified as host-based mobility or network-based mobility protocols. In the case of the host-based mobility approach, such as MIPv6, when a sensor device moves to another PAN, an exchange of signaling messages with its home agent (HA) is required in order to maintain the session. The host-based mobility approach is unsuitable for energy-constrained sensor devices because all of the sensor devices should have a mobility protocol stack.

On the other hand, in case of the network-based mobility approach, such as Network Mobility (NEMO) [8] and PMIPv6, it is possible to support mobility for the sensor devices without any additional mobility functions. If the network-based mobility is applied in 6LoWPAN, the sensor device does not require any mobility-related signaling. A mobile router or a special mobility agent in the network is responsible for detecting the movements of the sensor device, exchanging mobility-related signaling messages and managing mobility on behalf of the sensor device.

There are some proposals for IP-based mobility management in 6LoWPAN which follow the network-based mobility approach. In our previous works [9] and [10], we have presented network-based mobility management schemes in 6LoWPAN that are applied to NEMO and PMIPv6, respectively.

We have proposed 6LoWPAN with the NEMO protocol [9] that includes a new header compression scheme for mobility headers in 6LoWPAN and a lightweight NEMO protocol to minimize the signaling overhead using the compressed mobility header.

Furthermore, we have proposed 6LoWPAN with the PMIPv6 protocol [10] that includes the movement notification of the sensor device to support its mobility based on PMIPv6 as well as detecting PAN attachment in a multi-hop-based 6LoWPAN environment.

The authors of [11] had presented intra-PAN mobility support schemes for the 6LoWPAN, which are network-based mobility for sensor devices in which the mobility of the sensor devices is handled by the network-side.

However, the approach of IP mobility management makes it difficult to design an efficient solution for 6LoWPAN mobility because the dual use of IP addresses as both IDs and LOCs is not suitable for mobile environments. Furthermore, IP mobility management protocol based on 6LoWPAN must be implemented as a patch on a conventional mobile network. This causes increased complexity and reduced the network performance.

2.2 ID/LOC Separation Architectures

Basically, for a moving sensor device, the location cannot be fixed, and changing the locations without changing the IDs is required. This is because changing the LOC means changing the ID and breaking the pending sessions in the current Internet architecture. The best solution is to split the LOC and ID roles to avoid communication disruption.

The ID/LOC separation concept has been discussed in the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Study Group 13 [12], and the Internet Engineering Task Force (IETF) Working Groups (WGs) to fundamentally change the current Internet architecture. ITU-T Study Group 13

has been discussing the general requirements for ID/LOC separation in the Next-Generation Network (NGN). In the IETF WGs, several proposals have been made to address the problem of ID/LOC separation, such as Site Multi-homing by IPv6 Intermediation (SHIM6), Locator/Identifier Separation Protocol (LISP) and Host Identify Protocol (HIP).

The SHIM6 WG has developed the SHIM6 protocol [13] with a layer 3 shim approach and protocol for providing LOC agility according to the transport protocols so that multi-homing can be provided for IPv6 with failover and load-sharing properties. However, the SHIM6 protocol focuses on multi-homing and traffic engineering in IPv6.

The LISP WG has proposed the LISP protocol [14] that supports the separation of the IPv4 and IPv6 address spaces following a network-based map-and-encapsulate scheme. The LISP defines end-point identifiers (EIDs) in order to identify routing locators (RLOCs) and end-hosts. The EID is non-globally routable address, and the RLOC is attached to routers with globally routable address by consulting a mapping system, which maps EID prefixes onto site router's RLOCs. However, the LISP protocol still has a limitation because it does not consider sensor devices or group mobility. In other words, the LISP is not applicable for 6LoWPAN mobility where many small sensor devices support only lightweight communications.

The HIP WG has developed the HIP protocol [15], [16] that is a host-based ID/LOC split protocols for secure mobility and multi-homing. However, the HIP protocol needs to reduce the heavyweight cryptographic cost for supporting low power sensor devices.

The authors of [17] present a HIP-based network mobility protocol (HIP-NEMO). This scheme was mainly designed to optimize packet routes as well as to reduce mobility-related signaling and header overhead that does not require the mobile network devices to be involved in mobility management. However, security functions of the HIP-NEMO protocol are still computationally heavy for resource-limited devices.

The HIP Diet Exchange (HIP DEX) protocol [18] is a lightweight version of the HIP protocol that is designed for sensor devices with fewer cryptographic primitives. However, the HIP DEX cannot support the major features of 6LoWPAN (e.g., header compression, mesh routing and fragmentation of the 6LoWPAN packet on the IEEE 802.15.4). In addition, every end-device has to support the HIP DEX protocol functions for end-to-end communications since the HIP DEX is based on a full host-based ID/LOC split approach.

Meanwhile, in order to improve reachability and operation when HIP nodes are mobile, the HIP rendezvous server (RVS) [19] is introduced. The RVS stores the HIP-IP mappings for mobile what are registered to it. However, the RVS should maintain all mapping information about HIP-IP bindings, even though the HIP nodes are small sensor devices. That is, the RVS is not distributed; it is not suitable for 6LoWPAN environments that include a number of small sensor devices.

The Routing Architecture for the Next Generation Internet (RANGI) [20] is a new ID/LOC split-based routing and addressing architecture to address the issues with the current Internet (e.g., mobility, multi-homing, traffic engineering, etc). However, RANGI does not support optimized packet delivery paths. Additionally, RANGI causes a high degree of packet delivery cost since IP-in-IP tunneled packets are used in access networks, and this can make it difficult to fit the 6LoWPAN that has limited packet sizes.

3 Proposed Architecture

In this section, we present the proposed mobility management architecture for WSNs that is based on the ID/LOC separation concept. This section includes an overview of the proposed network architecture, secure device bootstrapping, location discovery, packet routing, and mobility scenarios.

The following are the major features of the proposed ID/LOC separation-based mobility management architecture for WSNs.

- *Distributed Mobility Management*: efficient network mobility support for a large number of WSNs in a distributed manner. For more details on distributed mobility management feature, refer to Section 3.1.
- *Secure Device Bootstrapping Support*: providing authentication between devices/routers. For more details on secure device bootstrapping support feature, refer to Section 3.2.
- *Route Optimization*: location discovery based on 'discover-before-forward' principle. For more details on route optimization feature, refer to Section 3.3.
- *Packet Delivery based on ID/LOC Separation*: locator-based global routing, access ID-based local access routing, and ID-based end-to-end communication. For more details on packet delivery based on ID/LOC separation feature, refer to Section 3.4.
- *Various Mobility Scenarios Support*: intra-domain mobility within home network domain, inter-domain mobility between home and visiting network domains, and intra-domain mobility within visiting network domain. For more details on various mobility scenarios support feature, refer to Section 3.5.

3.1 Overview of Proposed Network Architecture

Fig. 1 illustrates the proposed architecture. The architecture is composed of a signaling control network, an IPv6-based transit network, an access network, and a user mobile network.

Major components involved in the proposed ID/LOC separation-based mobility management architecture for WSNs are:

- *Primary Mobile Device (PMD)*: A device capable of changing its point of attachment to the Internet, moving from one link to another link with network mobility functionality. A PMD acts as a mobile gateway between the user mobile network including sensor devices and the rest of the access network.
- *6LoWPAN device (6LD)*: A sensor device that belongs to the user mobile network is attached to an ingress interface of the PMD.

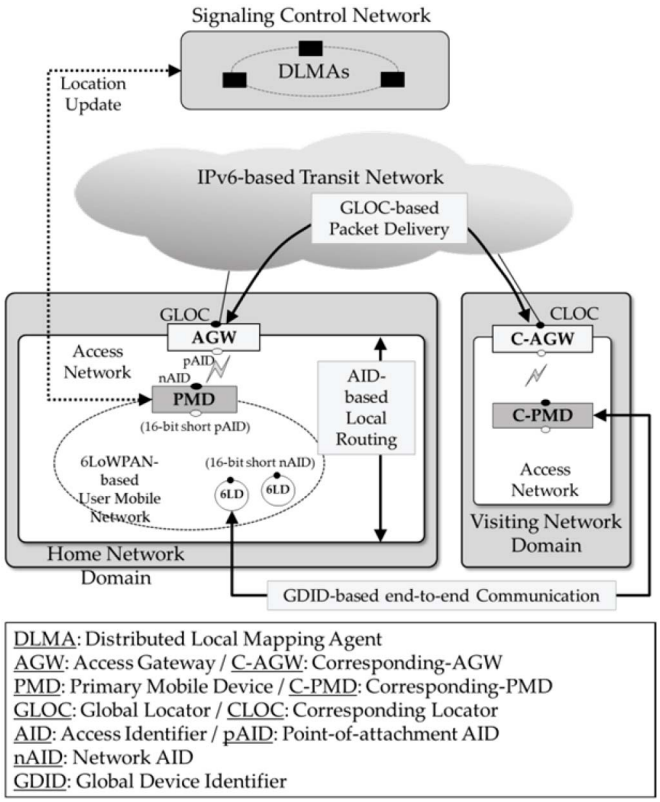

Fig. 1. Overview of the proposed network architecture and components.

- *Access Gateway (AGW)*: An access router, which acts as a global locator that is used to represent the location of the PMD for providing Internet access. An AGW performs inter-networking between the local access network and the external network with location update for the PMDs, corresponding device discovery and route setup functionalities.
- *Distributed Local Mapping Agent (DLMA)*: A mapping system, which maps between ID and LOC of the PMD. A DLMA performs ID/LOC resolution service and location binding update according to the PMD's mobility.

3.1.1 User Mobile Network

We assume that users have a PMD for accessing the Internet (e.g., smartphone, tablet PC, etc.). A user's mobile router supports NEMO functionality for moving as a user mobile network unit. We consider that a user mobile network is based on 6LoWPAN communications and includes 6LoWPAN devices (6LDs). The 6LDs located within the user mobile network are attached to an ingress interface of the PMD. The 6LDs can be classified into two device types: private-type communication devices and public-type communication devices. The private-type communication device is a device owned by the user (e.g., a medical sensing device or home networking device) that is relevant to sensitive personal information. Only the permitted nodes can thus access the private-type communication device. On the other hand, the public-type communication device can be accessed by any other node.

As the user mobile network is based on 6LoWPAN, there is high probability of packet loss in the user mobile network. In order to minimize packet transmission failures, we assume that the PMD is able to recognize whether the status of the 6LD is active or inactive. Also, the PMD manages a list of all 6LDs' sleep interval information. Upon receipt of the packet from the external network, the PMD first checks the status of the 6LD. If the status of the 6LD is active, the PMD can immediately forward the packet to the 6LD. On the other hand, if the status of the 6LD is inactive, the PMD should wait for a specified time until the 6LD wakes up.

3.1.1.1 Global Unique Device Identifier and User Prefix Identifier

All PMDs and 6LDs have a 128-bit global unique device identifier (GDID), which is used for end-to-end communication. Similarly, this GDID is used for the identifier that is defined in the existing architectures such as EID of LISP [14], Host Identity Tag (HIT) of HIP [15], and ID of Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation (HIMALIS) [21], [22], etc.

The proposed GDID consists of two parts. The leftmost 64-bit part indicates the user prefix identifier (UPID) of the user mobile network, which includes the domain identifier (32-bit) and user identifier (32-bit) information. The domain and user identifier portions can be used to identify the home domain of the registering user and a particular user that belongs to the home domain, respectively. The remaining 64-bit part indicates the user device identifier of the user mobile network including the 6LDs as well as the PMD.

In the existing proposed schemes based on host-centric ID/LOC separation architecture, the end-host ID is used for mapping with a LOC so that ID/LOC mapping systems need to manage the entire end-host ID for tracking their location. This causes the ID/LOC mapping table entries to increase in size so that the existing architectures are not suitable to support WSN devices.

On the other hand, the proposed architecture based on ID/LOC separation considers that a user can have a large number of WSN devices. In the proposed architecture, the prefix, namely UPID, is used as the key for mapping with a LOC. A PMD and 6LDs that are owned by a user have the same globally unique 64-bit UPID. The mapping systems only need to manage one mapping entry about a UPID for the PMD as well as a number of 6LDs, not every end-host ID that is defined as GDID in the proposed architecture. The user-owned 6LDs are managed by each of the user PMD in a distributed manner.

3.1.1.2 Access Identifier

An access identifier (AID) is used to identify a network interface for data packet delivery within the local access network. In order to forward a data packet in the access network, the link-layer address can be used as the AID according to the radio access technologies that are currently being used, for example, IEEE 802.11-based MAC address, IEEE 802.15.4-based 16-bit short address, or cellular network-based tunnel endpoint ID.

We define two types of AIDs: point of attachment AID (pAID) and network AID (nAID). The pAID is used to

represent an ingress interface of the AGW that the PMD is attached to. The nAID is used to represent an egress interface of the PMD. The PMD dynamically changes its point of attachment to the AGW, namely pAID, while maintaining ongoing sessions via the nAID that supports WiFi or cellular data connections. In the case of the user mobile network, the PMD acts as a mobile gateway for the 6LDs so that an ingress interface of the PMD is a pAID for the 6LDs. In the proposed architecture, since the user mobile network assumes IEEE 802.15.4-based 6LoWPAN, the ingress interface of the PMD and the wireless interface of the 6LDs are used as 16-bit pAID and 16-bit nAID, respectively.

In addition, multiple nAID can be assigned to each of wireless interfaces if the PMD supports multiple radio access technologies (e.g., WiFi and cellular wireless interfaces) for accessing the Internet.

3.1.2 Access Gateway

The access gateway (AGW) is an access router providing Internet access to the PMDs and is used for internetworking between the local access network and the external network. An egress interface of the AGW acts as a global locator (GLOC) that is used to represent the location of the PMD.

The AGW performs a variety of functionalities such as location update on behalf of the PMDs, corresponding device location discovery, and route setup with corresponding-AGW (C-AGW) for GLOC-based packet routing over the IPv6-based transit network. These functionalities are invisible processes to the PMDs and 6LDs for the protection of user location privacy.

In order to perform these functionalities, the AGW maintains routing cache entries, including downlink-routing and uplink-routing caches, as well as dynamic mapping information, including UPID-to-nAID and UPID-to-GLOC mapping tables.

The downlink-routing cache is managed by an egress interface of the AGW for forwarding inbound traffic from the external network toward the local access network. On the contrary, the uplink-routing cache is managed by an ingress interface for forwarding outbound traffic from the local access network toward the external network or local traffic from the local access network toward within the same local access network.

The UPID-to-nAID mapping table is used for looking up mapping information between the UPID of the 6LD in the user mobile network and nAID of the PMD. The downlink-routing cache and uplink-routing cache refer to this UPID-to-nAID mapping table for forwarding inbound traffic and local traffic, respectively. By referring to the UPID-to-nAID mapping table, data packets transferred toward the 6LD can be delivered to the PMD to which the 6LD belongs.

The UPID-to-GLOC mapping table is used when the AGW needs to forward outbound traffic from the local access network toward the external network. The uplink-routing cache refers to the UPID-to-GLOC mapping table for looking up mapping information between the UPID of the corresponding device in the external network and its LOC, which is an egress interface IPv6 address of the C-AGW. By referring to this UPID-to-GLOC mapping table, the outbound data packets can be routed over the IPv6-based transit network to the C-AGW, which acts as the GLOC for the corresponding device.

3.1.3 Distributed Local Mapping Agent

The signaling control network is based on the logical overlay network architecture that supports distributed mapping systems, namely, the DLMA. Each local network domain includes the DLMA that manages UPID-to-GLOC mapping information. The UPID-to-GLOC mapping table entries are used to determine which PMD of the user (i.e., PMD's GDID) belongs to a particular GLOC (i.e., IPv6 address on the egress interface of the AGW).

The DLMA has two major functionalities including UPID-to-GLOC resolution service and location binding update.

The UPID-to-GLOC resolution service is performed by exchanging location discovery request/response messages between the DLMA and AGW. When the DLMA receives the location discovery request message from the AGW, it replies the current location of the PMD with the GLOC information.

The location binding update process depends on PMD's mobility scenarios. In case of intra-domain mobility, the PMD changes the GLOC, moving between AGWs, in the same network domain that is managed by a home-DLMA (H-DLMA). In this case, the location binding update is performed by exchanging location update/ack message between the AGW and H-DLMA. The AGW, which is located in the same network domain, can send the location update message on behalf of the PMD directly to the H-DLMA.

On the other hand, in case of inter-domain mobility, when the PMD moves to a visiting network domain that is managed by a visiting-DLMA (V-DLMA), the location binding update is performed between the H-DLMA and V-DLMA. When the H-DLMA receives the location update for the PMD from the V-DLMA, it updates the UPID-to-GLOC mapping information in the mapping table entry.

3.2 Secure Device Bootstrapping

In order to perform device bootstrapping that consists of device ID generation, PMD discovery with ID registration, the neighbor discovery (ND) optimization for 6LoWPAN [23] can be used. Since the optimized ND protocols are not secure, a lightweight secure neighbor discovery for low-power and lossy networks (LSEND for LLN) [24] is proposed as a lightweight version of the SEND [25] protocol. LSEND extends the optimized ND for 6LoWPAN with a cryptographically generated address (CGA) [26].

We use the CGA for user device IDs in order to provide authentication between the PMD and the 6LDs. By using CGA, the verifier can authenticate the message from the corresponding sender, only if the source address and the public key are known. This method requires no public key infrastructure so that it is suitable for low power sensor devices. As introduced in [24], we use elliptic curve

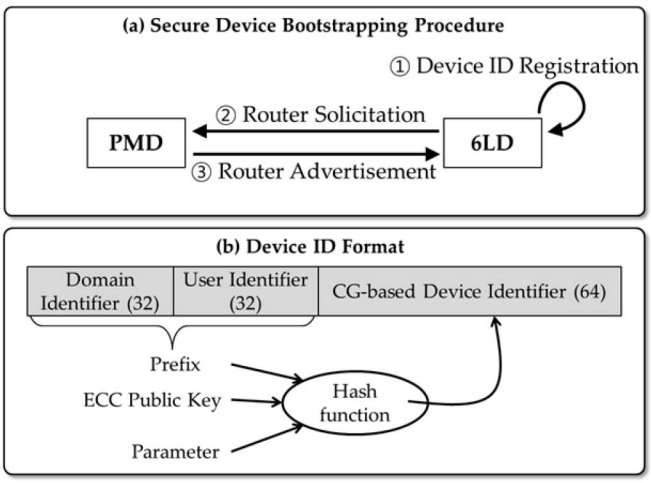

Fig. 2. (a) Secure device bootstrapping procedure. (b) Device ID format.

cryptography (ECC) [27] for CGA generation and elliptic curve digital signature algorithm (ECDSA) [28] for calculating signature. This is known to be lightweight which is different from an RSA signature that is used in the SEND protocol.

ECC can use shorter keys for security levels where RSA would need much longer keys. In recent years, ECC has attracted much attention as a security solution for wireless networks due to a very small key size and low computational overhead. For example, 160-bit ECC key and a 1024-bit RSA key offer a similar level of security. Therefore, using ECC and ECDSA, we can minimize public key, signature sizes and signature calculation cost.

The 6LD first performs the link-layer security process to acquire a key and secure access at the link-layer in 6LoWPAN. It is assumed that IEEE 802.15.9 key management protocol over 802.15.4 can be applied for link-layer security.

Fig. 2(a) illustrates the sequence of the device bootstrapping procedure. The detailed operations are described as follows.

3.2.1 CG-Based Device ID Generation

As described in Section 3.1.2, a format of GDID consists of two portions that include UPID (domain ID and user ID) as a 64-bit prefix of the user mobile network and device ID as a 64-bit local unique identifier of 6LDs within 6LoWPAN.

For beginning bootstrapping of a device in the user mobile network, a 6LD performs cryptographically generated (CG)-based device ID generation as Step (1). The CG-based device ID is generated by computing a cryptographic one-way hash function from the UPID (prefix), ECC public key and additional parameter, as shown in Fig. 2(b). The CG-based device ID has a security parameter that determines its strength against brute-force attacks. This security parameter is a three-bit unsigned integer and it is encoded in the three leftmost bits (i.e., bits 0-2) of the interface identifier. This additional parameter is included to enhance privacy, recover from collision of ID generation and to protect from attacks.

3.2.2 Secure PMD Discovery with Device ID Registration

The 6LD then attempts to perform the initial PMD discovery procedure with a PMD, which acts as a mobile default gateway for the 6LDs.

In order to perform securing mobile router discovery, router solicitation (RS) and router advertisement (RA) messages are exchanged between the PMD and the 6LDs, as shown in Fig. 2(a). The source and destination addresses of the RS and RA are based on CGAs, and these messages are included in the ECC public key and digital signature. The public key and CG-based device ID can be verified by recomputing the hash function and comparing the result with the device ID. In order to authenticate the message, the message is signed with the private key so that the receiver can authenticate the message with the device ID and public key.

The secure PMD discovery is performed by sending a unicast RS message to the PMD as Step (2). The source address of the RS is set to 64-bit CG-based 6LD ID that is generated in Step (1). The destination address of the RS is set to the link-layer address of the PMD, which is obtained through the link-layer security operation. The RS contains CGA parameters option, including UPID of the 6LD, ECC public key of the 6LD, and an additional parameter, as well as a digital signature option computed by using ECDSA.

Upon the receipt of the RS message from the 6LD, the PMD verifies the source address of the RS using the CGA parameters information in the option. The PMD then performs a cryptographical check of the signature that is included in the digital signature option. After successfully verifying the source address of the RS, the PMD assigns a 16-bit short nAID address for the 6LD.

The PMD then performs the device ID registration by creating a device list table entry and mapping between the registered CG-based 6LD ID and the assigned 16-bit short nAID address. Furthermore, the PMD stores the public key of the 6LD in the device list table entry.

In the proposed architecture, as described in this subsection, secure communications are basically supported for secure authentication of the default gateway by using a CG-based device ID with ECC public key and digital signature.

The PMD replies a unicast RA message to the 6LD as Step (3). The source address of the RA is set to the 64-bit CG-based pAID of the PMD. The destination address of the RA is set to the verified 64-bit CG-based 6LD ID. The RA contains CGA parameters, including UPID of the PMD, ECC public key of the PMD and additional parameters, as well as a digital signature option computed by using ECDSA, the same as the RS options. In addition, the RA contains 16-bit address options, including an assigned 16-bit short AID for 6LD (i.e., 16-bit short nAID) as well as a PMD's 16-bit short AID (i.e., 16-bit short pAID).

If the 6LD receives the RA message from the PMD, it verifies the source address of the RA using the CGA parameters as described in Step (2). The 6LD also checks the digital signature. If all checks succeed then the secure PMD discovery with CG-based device ID registration procedure is successfully completed.

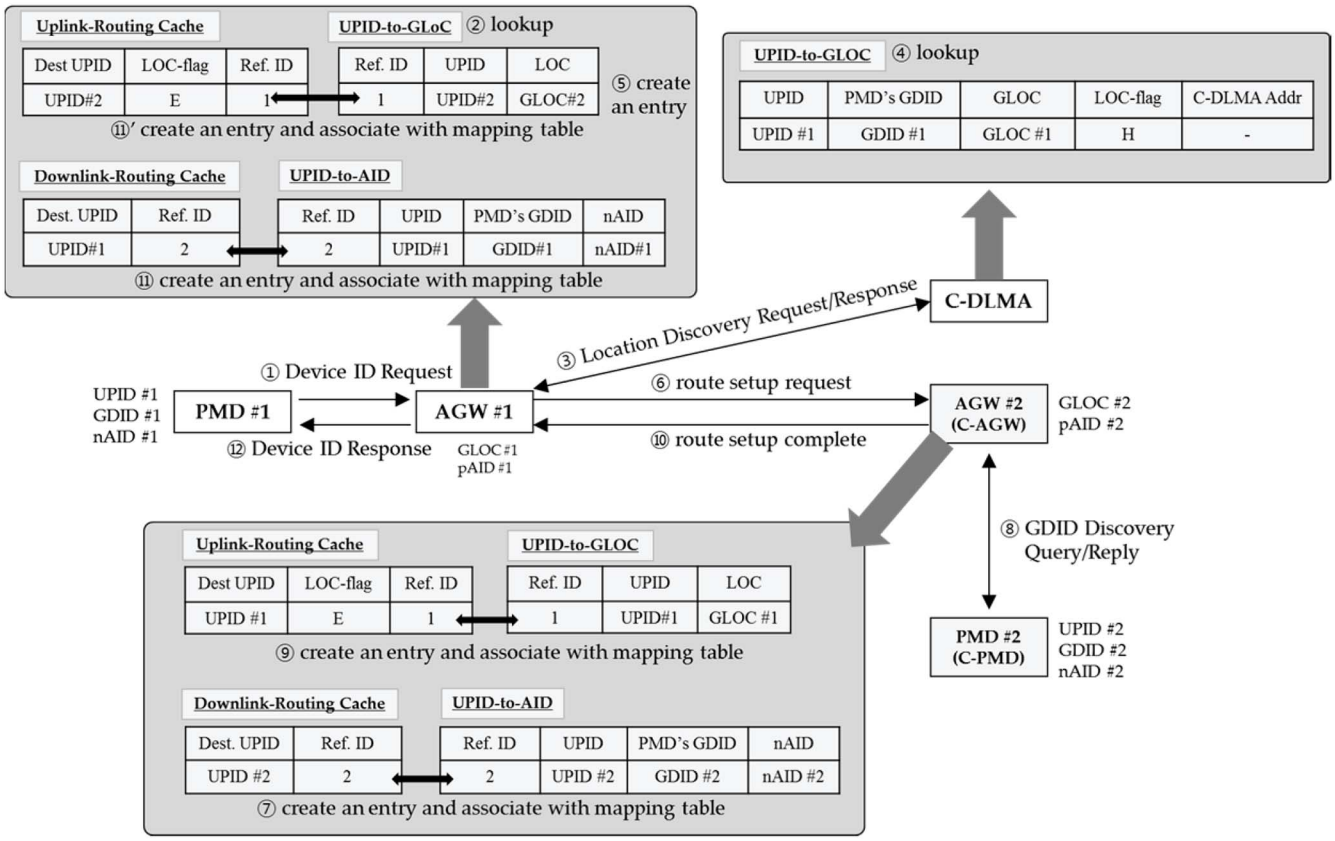

Fig. 3. The sequence of the location discovery procedure.

3.3 Location Discovery

Fig. 3 illustrates the sequence of the location discovery procedure. The detailed operations are described as follows.

We basically assume that the proposed new network entities such as the AGW and the DLMA are completely safe, reliable, and secure. Since both the AGW and DLMA are located in the network infrastructure with strong trustworthiness, no one can access the GLOC and routing table information.

If a user wants to communicate with a particular device (e.g., a corresponding-6LD (C-6LD)) that is owned by the corresponding-PMD (C-PMD), it sends a device ID discovery request message, including the UPID of the corresponding user mobile network and the device name, to the AGW in order to obtain a GDID of the C-6LD (Step 1). The AGW checks the UPID-to-GLOC mapping table whether the requested UPID exists (Step 2). If there is no mapping entry between the UPID and GLOC, the location discovery service is performed by exchanging the location discovery request/response messages between the AGW and corresponding-DLMA (C-DLMA), which acts as the H-DLMA for the C-PMD (Step 3). The C-DLMA looks up the UPID-to-GLOC mapping table by using the requested UPID, and it replies the GLOC information of the C-PMD which is the output of the mapping lookup (Step 4).

Upon the receipt of the location discovery response message from the C-DLMA, the AGW creates an entry for UPID-to-GLOC mapping information (Step 5). The AGW then sends a route setup request message, including the UPID and device name, to the GLOC of the C-PMD in order to configure downlink/uplink-routing caches for enabling GLOC-based global routing as well as AID-based local access routing (Step 6).

When the C-AGW receives the route setup request message from the AGW, it creates the downlink-routing cache entry on the egress interface for forwarding inbound traffic towards the requested UPID. The created new cache entry is associated with UPID-to-nAID mapping table entry by using the reference ID field that is correctly mapped between the requested UPID and nAID of the C-PMD to which the C-6LD belongs (Step 7).

The C-AGW then sends a GDID discovery query, including the device name of the C-6LD, to the C-PMD in order to request the GDID of the C-6LD (Step 8). If the C-AGW receives a GDID discovery reply message with the GDID from the C-PMD, it creates the uplink-routing cache entry on the ingress interface. Also, the UPID-to-GLOC mapping table entry is created for forwarding outbound traffic toward the sender UPID. Since the UPID of the sender is located in the external network, the LOC-flag of the uplink-routing cache entry is set to 'E' which means an external network. This entry is associated with the UPID-to-GLOC mapping table entry by using the reference ID. On the other hand, if the sender is located in the same local network, the LOC-flag of the uplink-routing cache entry is set to 'L'. And, this entry is associated with the UPID-to-AID mapping table entry (Step 9).

After completing the route setup for the C-AGW side, the C-AGW replies a route setup complete message to the AGW including the GDID of the 6LD (Step 10). The

AGW creates the downlink-routing and uplink-routing cache entries that are associated with the UPID-to-AID and the UPID-to-GLOC mapping table entries, respectively, in the same manner as the C-AGW (Step 11 and 11').

When the route setup process is successfully completed between the AGW and C-AGW, the AGW replies a device ID discovery response message, including the corresponding GDID of the C-6LD. It is then ready to communicate between the PMD and C-6LD (Step 12).

In short, the proposed architecture is based on 'discover-before-forward' manner so that the data packets can be delivered with an optimal routing path over the IPv6-based transit network.

3.4 Packet Routing

In the proposed architecture, the network layer of the devices (every PMD and 6LD) is separated into identifying and routing layers. The GDID is used for end-to-end communications between devices in the upper-layer protocols above the routing layer (e.g., application, transport, and identify). The routing layer uses the AID, which is only available within the local access networks, for forwarding between the PMD and the AGW (or the 6LD and the PMD).

If the PMD sends or receives data packets through a cellular radio access network interface, a radio bearer ID is used for the AID. On the other hand, the PMD uses a WiFi interface to send or receives data packets; an IEEE 802.11-based MAC address can be used for the AID. In case of the 6LD, an IEEE 802.15.4-based 16-bit short address is used for the AID in the 6LoWPAN. In some cases such as multiple overlay network or wireless mesh network, IPv6 or IPv4 addresses may be used for the AID.

Fig. 4 illustrates an example of the packet routing on how to deliver data packets between devices.

3.4.1 Outbound Traffic

If the PMD sends the data packets to the C-6LD after successfully completing the location discovery procedure, the PMD's GDID and C-6LD's GDID of the data packet are used as the source GDID and destination GDID, respectively. The PMD then encapsulates the packet in a frame for AID-based routing in the local access network. The AID header carries a nAID of the PMD and a pAID of the AGW as the source and destination AID addresses, respectively.

When the AGW receives the data packet from an ingress interface, it decapsulates the packet and removes the AID header from the packet. The AGW then first checks the UPID of the destination GDID in the UPID-to-nAID mapping table in order to determine whether the packet needs to be routed within the local access network (i.e., local traffic). If there is no destination UPID in the mapping table, the packet is regarded as outbound traffic so that the AGW checks the uplink-routing cache with the UPID-to-GLOC mapping table for looking up mapping information between the destination UPID and its GLOC.

If the AGW obtains the destination UPID's GLOC that is an IPv6 address of the C-AGW, it encapsulates the packet with the IPv6 header for GLOC-based packet delivery over the IPv6-based transit network. The source and destination

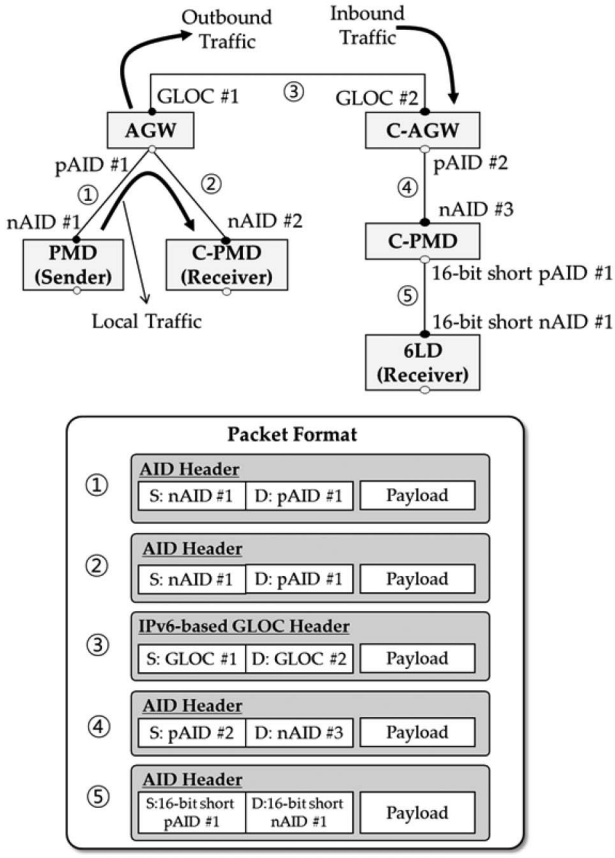

Fig. 4. Example of the packet routing and packet addressing format.

GLOC addresses are egress interface IPv6 addresses of the AGW and C-AGW, respectively.

3.4.2 Inbound Traffic

When the C-AGW receives the data packet from the egress interface, it decapsulates the packet and removes the IPv6-based GLOC header which is an outer header of the tunneled packet. The C-AGW then checks the UPID of the destination GDID in the downlink-routing cache. If it is discovered in the cache entry, the destination UPID is referred to the UPID-to-nAID mapping table entry for looking up mapping information between the UPID and its nAID address.

If the C-AGW obtains the destination UPID's nAID address that is an egress interface address of the C-PMD, it encapsulates the packet in a frame for AID-based routing in the local access network. The AID header carries the pAID of the C-AGW and the nAID of the PMD as the source and destination AID addresses, respectively.

Upon the receipt of the data packet from the egress interface, the C-PMD decapsulates the packet and removes the AID header. The C-PMD then checks the destination GDID. The C-PMD checks the device list table, which maps between the 64-bit device ID of the 6LD and its 16-bit short nAID address. The 64-bit device ID of the C-6LD can be derived from the rightmost 64-bit portion of the destination GDID in the received packet. The 16-bit short nAID address is set to the destination AID in the 6LoWPAN-based user mobile network. The source 16-bit short pAID

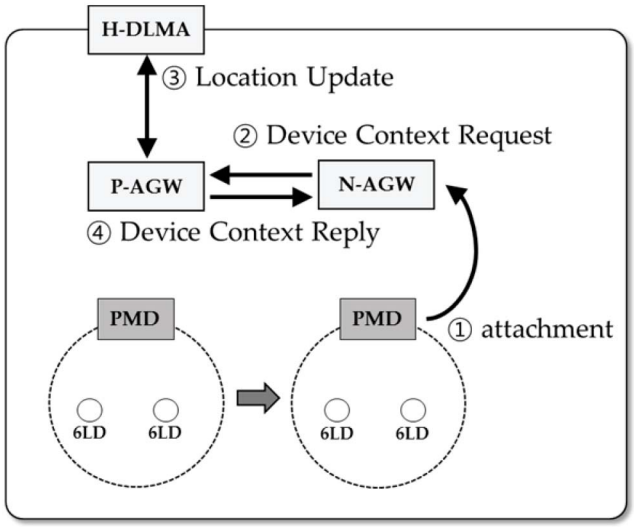

Fig. 5. The sequence of the intra-home-domain mobility procedure.

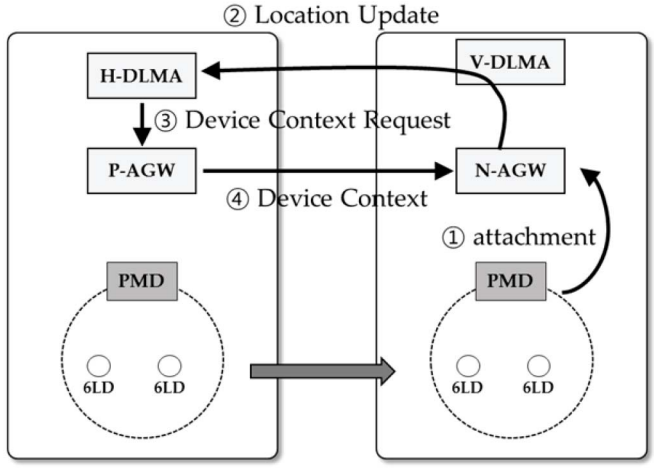

Fig. 6. The sequence of the inter-domain mobility procedure.

is set to the ingress interface of the PMD. Therefore, the C-6LD can receive the packet with the compressed header from the sender device by performing the 16-bit short AID-based routing in the 6LoWPAN-based user mobile network.

Meanwhile, the source 16-bit short pAID address in the 6LoWPAN-based user mobile network is set to the temporary 16-bit short AID address assigned by the PMD, not the ingress interface of the PMD, unlike the AGW.

3.5 Mobility Scenarios

3.5.1 Intra-Home-Domain Mobility

Fig. 5 illustrates the sequence of the intra-home-domain mobility procedure of the user mobile network when the PMD changes the GLOC for movement between AGWs within the home network domain, which is managed by an H-DLMA. The detailed operations are described as follows.

(Step 1) If the user mobile network moves from a previous-AGW (P-AGW) to a new-AGW (N-AGW) within the home network domain, the PMD sends an attachment trigger message to the N-AGW that includes the UPID of the user mobile network and P-AGW address information.

Upon receiving the attachment trigger, the N-AGW first checks the domain identifier information that is included in the UPID. If the domain identifier indicates the current home network domain, the movement of the user mobile network can determine the intra-home-domain mobility.

(Step 2) If the N-AGW is aware of the intra-home-domain mobility, it sends a device context request message to the P-AGW in order to perform the location update process with the H-DLMA, as well as to receive from the P-AGW about all the necessary PMD-related routing information for communications with corresponding devices such as routing caches and mapping entries.

(Step 3) Before transferring the PMD-related routing information to the N-AGW, the P-AGW performs the location update process by exchanging the location update request/response messages with the H-DLMA. Upon receiving the location update request message from the P-AGW, the H-DLMA updates the new GLOC information in the UPID-to-GLOC mapping table entry.

(Step 4) If the P-AGW receives the location update response message from the H-DLMA after successfully updating the location of the PMD, it transfers the PMD-related routing information, which is stored in the uplink/downlink-routing caches as well as UPID-to-nAID and UPID-to-GLOC mapping table entries, by sending a device context reply message to the N-AGW. The N-AGW creates the routing caches and mapping table entries for the PMD as the final step of the intra-home-mobility procedure.

3.5.2 Inter-Domain Mobility

Fig. 6 illustrates the sequence of the inter-domain mobility procedure of user mobile network when the PMD first visits to a non-home network domain, which is managed by a V-DLMA. The detailed operations are described as follows.

(Step 1) Sending an attachment trigger message to an N-AGW in the visiting network domain for the initial attachment procedure is the same as the intra-home-domain mobility scenario that is described in the previous subsection.

If the domain identifier is different from the current network domain after checking the domain identifier in the UPID, the N-AGW can recognize that the user mobile network is visiting the non-home network domain.

In addition, the N-AGW checks the P-AGW address whether the P-AGW is located in the same network domain, or not. If the P-AGW is located in different network domains, the movement of the user mobile network can determine the inter-domain mobility.

(Step 2) If the N-AGW is aware of the inter-domain mobility, the sequence of mobility procedure is changed, compared to the inter-home-domain mobility. In case of the inter-domain mobility scenario, the N-AGW sends a location update request message to the V-DLMA. This location update request message is relayed to the H-DLMA. Upon receipt of the location update request message from the V-DLMA, the H-DLMA updates the new GLOC information and LOC-flag in the UPID-to-GLOC mapping table entry.

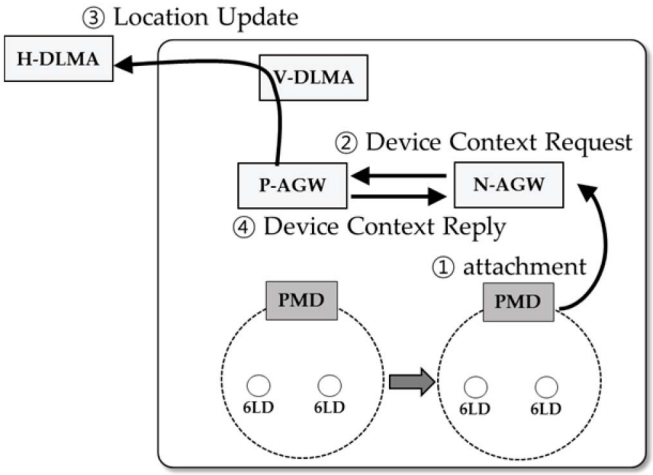

Fig. 7. The sequence of the intra-visiting domain mobility procedure.

(Step 3) The H-DLMA sends a device context request message to the P-AGW in order to transfer the PMD-related routing information, which is stored in the uplink/downlink-routing caches and UPID-to-nAID/UPID-to-GLOC mapping table entries. At the same time, the H-DLMA also sends a location update response message to the N-AGW via the V-DLMA.

(Step 4) If the P-AGW receives the device context request message from the H-DLMA, it transfers the PMD-related routing information to the N-AGW. The N-AGW then creates the routing caches and mapping table entries for the PMD as the final step of inter-domain mobility procedure.

3.5.3 *Intra-Visiting-Domain Mobility*

Fig. 7 illustrates the sequence of the intra-visiting-domain mobility procedure of user mobile network when the PMD changes the GLOC by a movement between AGWs within the visiting network domain, which is managed by the V-DLMA. The detailed operations are described as follows.

(Step 1) Sending an attachment trigger message to an N-AGW in the visiting network domain is the same as the intra-home-domain mobility scenario.

The N-AGW also first checks the domain identifier information. If the N-AGW recognizes that the user mobile network is visiting the non-home network domain, it then checks the P-AGW address as described in Step 1 of the inter-domain mobility. If the P-AGW is located in the same network domain, the movement of the user mobile network can determine the intra-visiting domain mobility.

(Step 2) If the N-AGW is aware of the intra-visiting-domain mobility, it sends a device context request message to the P-AGW in the same manner as Step 2 of the intra-home-domain mobility.

(Step 3) The P-AGW sends a location update request message to the H-DLMA via the V-DLMA in the same manner as Step 3 of the intra-home-domain mobility. Upon receipt of the location update request message from the V-DLMA, the H-DLMA updates the new GLOC information in the UPID-to-GLOC mapping table entry.

(Step 4) If the P-AGW receives the location update response message from the H-DLMA via the V-DLMA after successfully completing the location of the PMD, it transfers the PMD-related routing information in the same manner as Step 4 of the intra-home-domain mobility.

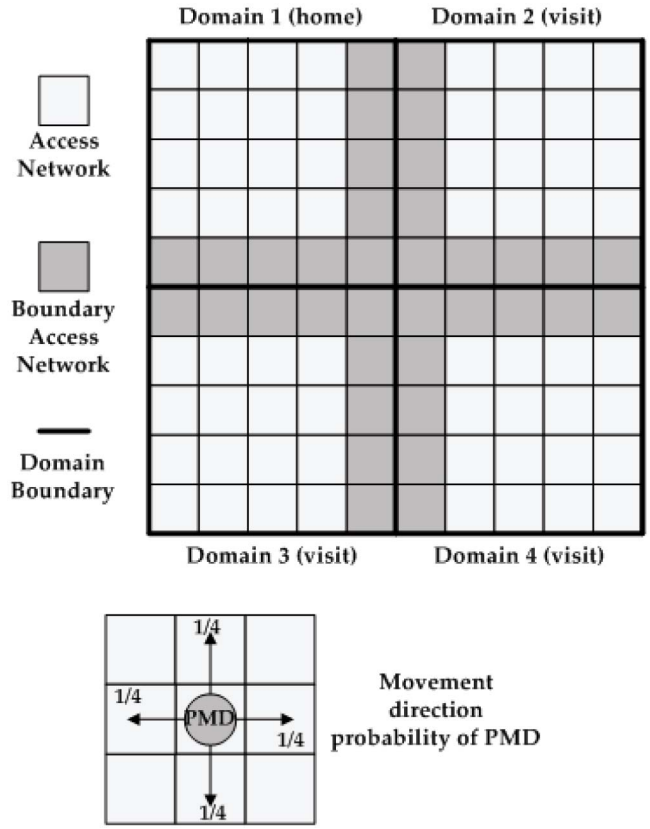

Fig. 8. Network topology and mobility model.

4 Performance Evaluation

In this section, we compare the proposed architecture with extended HIP, enabling both HIP DEX and HIP RVS, in terms of the average energy consumption of sensor devices, total signaling cost and packet delivery cost ratio.

4.1 Network Topology and Mobility Model

In order to evaluate performance, we use a modified two-dimensional random walk mobility model with absorbing states, which is modeled by our previous work [10]. In this model, the PMD with user mobile network moves with a particular speed and in a particular direction for a given interval. The modified two-dimensional random walk mobility model is designed for movement between dynamic location areas, and is suitable for user movements where the location update procedure can be classified according to different mobility scenarios (e.g., intra-domain and inter-domain mobility).

Fig. 8 shows a network topology for simulation using the two-dimensional random walk mobility model. The network topology has four different domains. Each domain is composed of 25-square access networks (i.e., 25 AGWs are deployed in a domain), including a DLMA and five PMDs with three 6LDs. In this network, every access network has four neighbors, and a PMD with user mobile network can only move to one of the four neighboring access networks with the same probability of *1/4* in each direction.

Parameters for Channel Control Module	
Carrier frequency	2.4GHz
Channel model	IEEE802.15.4 CSMA/CA
Transmitter power	1 mW
Carrier sense sensitivity	-85 dBm
Bit-rate	250 kbps
Channel Number	11

Parameters for Energy Module	
Battery capacity	3000 mAh
Battery TX	17.4 mA
Battery RECV	23 mA
Current draw (idle)	21 uA
Current draw (sleep)	1 uA
Update interval	1s

Parameters for MAC Module	
Synchronization mode	Beacon-enabled
Topology	Cluster

Parameters for the Mobility Module	
Mobility type	Modified two-dimensional random walk mobility model
Mobility speed	1m/s ~15m/s

Fig. 9. Parameter values for simulation.

If the user mobile network moves within home-domain, intra-domain mobility procedure can be performed as defined in Section 3.5.1. In case of movement into the boundary square in the visiting-domain, inter-domain mobility procedure can be performed as defined in Section 3.5.2. When the user mobile network moves within the visiting-domain (i.e., the outside of the home-domain), intra-visiting-domain mobility can be performed as defined in Section 3.5.3.

Using this network and mobility model, we perform a number of simulation experiments in order to evaluate the performance of the average energy consumption of sensor devices, total signaling cost and packet delivery cost ratio. We have implemented the proposed ID/LOC separation-based lightweight mobility architecture based on the modified two-dimensional random walk mobility model with the 3-layer square access networks using the Objective Modular Network Testbed in C++ (OMNeT++) [29]. The user mobile network can move with different movement speeds over the entire domain area based on the mobility model. We simulate 10 times for each step, and every simulation time runs 60 seconds. We find an average value in each simulation step. Fig. 9 shows the parameters used in the simulation and their values.

The components of the proposed architecture include the following: PMD with mobile router functions, 6LD with IEEE 802.15.4-based 6LoWPAN protocol stack, DLMA with UPID-to-GLOC mapping table, and the AGW with uplink/downlink-routing caches and UPID-to-GLOC/UPID-to-AID mapping tables. In addition, the main functionalities of the proposed architecture are implemented: secure device bootstrapping, location discovery, packet routing, and intra/inter domain mobility.

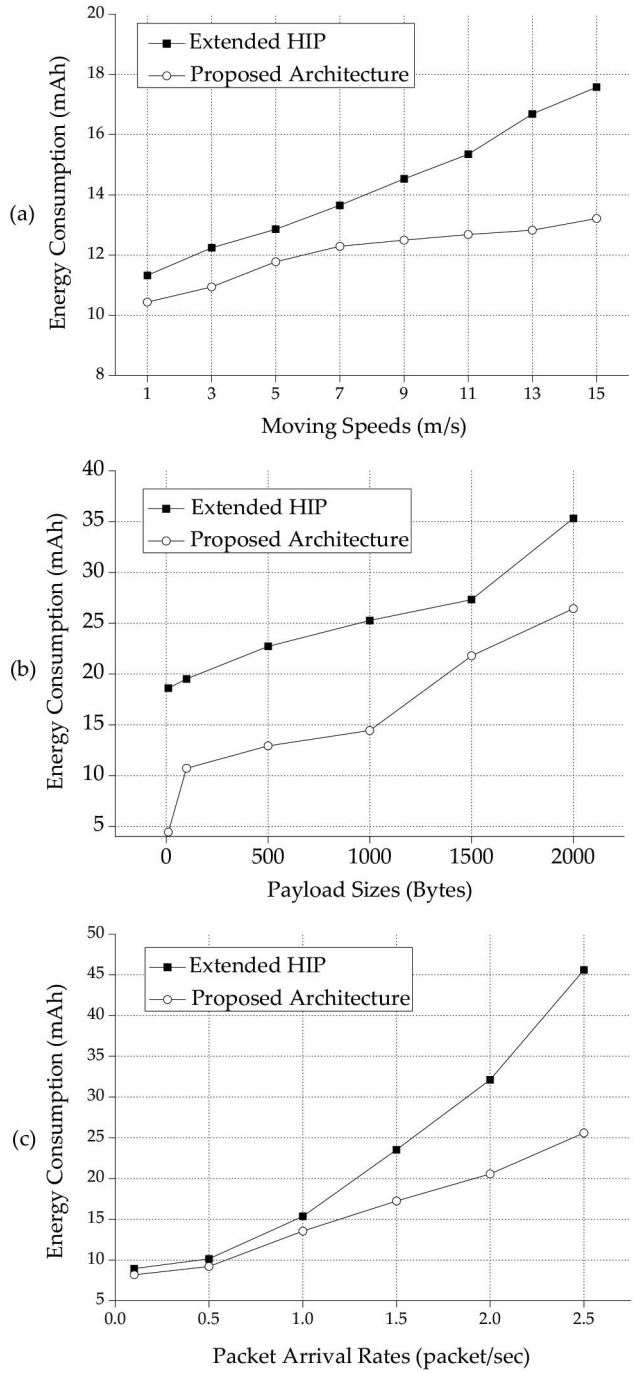

Fig. 10. The average energy consumption of the 6LDs.

4.2 Simulation Results

4.2.1 Energy Consumption

We perform a variety of experiments to evaluate the average energy consumption of all 6LDs in the simulation network topology (i.e., there are 60 6LDs in total) with the modified two-dimensional random walk mobility model. The PMD with 6LDs is able to move in all access networks, which are in charge of the AGWs, following the modified two-dimensional random walk mobility model.

We assume that the maximum battery capacity of all 6LDs is 3000 mAh. In addition, the power consumption is 17.4 mA, while transmitting at 0 dBm and 23 mA in the receiving mode. If the RF transceiver is in idle mode and the voltage regulator is on, the current draw of the 6LD is 21 uA. When the RF transceiver is in sleep mode and the voltage regulator is off, the current draw is 1 uA.

The first experiment on the average energy consumption measures the differences in the PMDs moving speed. The PMDs moves to all access networks at different speeds according to the mobility model. Fig. 10(a) shows the results of the average energy consumption of the 6LDs at different speeds. In the case of extended HIP, energy consumption rapidly increases at faster speeds, while the proposed architecture consumes less energy, even though the moving speed is increased.

This is because all nodes of extended HIP perform the location update to the RVS for updating HIP-IP information whenever they move on the access network. On the other hand, in the proposed architecture, the user-owned 6LDs are managed by each of the user PMDs in the distributed management manner. Since the 6LDs does not require any mobility-related signaling message, the energy consumption can be reduced.

The second experiment on the average energy consumption measures increasing payload size for each transmission packet from the 6LD using the mobility model. In this experiment, the 6LD transmits the UDP packets with payload sizes of 10 bytes to 2000 bytes. Fig. 10(b) shows the results of the 6LD energy consumption for different data packet payload sizes. Extended HIP architecture consumes more energy than the proposed architecture with larger payload sizes.

This is because extended HIP architecture does not support the header compression and fragmentation schemes within 6LoWPAN. Every end-device should support the HIP DEX protocol functions for end-to-end communications since extended HIP is based on a full host-based ID/LOC split approach. On the other hand, the proposed architecture fully supports 6LoWPAN features including header compression, mesh routing and fragmentation so that packet size can be reduced and the total energy consumption can be minimized.

The maximum transmission unit (MTU) size for 6LoWPAN is 1280 octets. However, the full IPv6 packet does not fit in an IEEE 802.15.4 frame due to the maximum IEEE 802.15.4 physical frame size of 127 octets. The total header size of the UDP packet is 74 octets, including the IEEE 802.15.4 PHY/MAC frame size of 25 octets, mesh header size of 17 octets, IPv6 header size of 24 octets, and UDP header size of 8 octets. Therefore, only 53 octets are left for the UDP payload.

Furthermore, fragmentation and reassembly of the 6LoWPAN packet occurs by the 6LD and the PMD after the payload size reaches 100 bytes since the UDP packet exceeds the maximum packet size of 127 octets. This is why energy consumption rapidly increases for the 6LD when the payload size is increased from 10 bytes to 100 bytes, as shown in Fig. 10(b).

The third experiment on the average energy consumption involves increasing the packet arrival rates from the corresponding node according to a Poisson distribution using the mobility model. The 6LD receives the data packet as the packet arrival rates increase from 0.1 to 2.5. Fig. 10(c) shows the results of the 6LDs' energy consumption at different packet arrival rates. Extended HIP rapidly increases the 6LDs' energy requirements when the packet arrival rate increases, while the proposed architecture consumes less energy, even though the packet arrival rate increases.

From the energy consumption results in this subsection, we conclude that the proposed architecture conserves more energy than does extended HIP architecture.

4.2.2 Signaling Cost and Packet Delivery Cost Ratio

This subsection evaluates the performance of the proposed architecture and extended HIP based on the cost functions, including moving speeds, payload sizes, and packet arrival rates. The cost ratio indicates how much the total signaling cost and packet delivery cost of the proposed architecture can be saved, as compared to extended HIP. It is defined as the ratio of the cost of proposed architecture divided by the cost of extended HIP. A ratio lower than 100% indicates the cost of the proposed architecture is less than extended HIP.

Fig. 11(a) shows the total signaling cost and packet delivery cost ratio of the proposed architecture compared to those of extended HIP as the moving speed is changed.

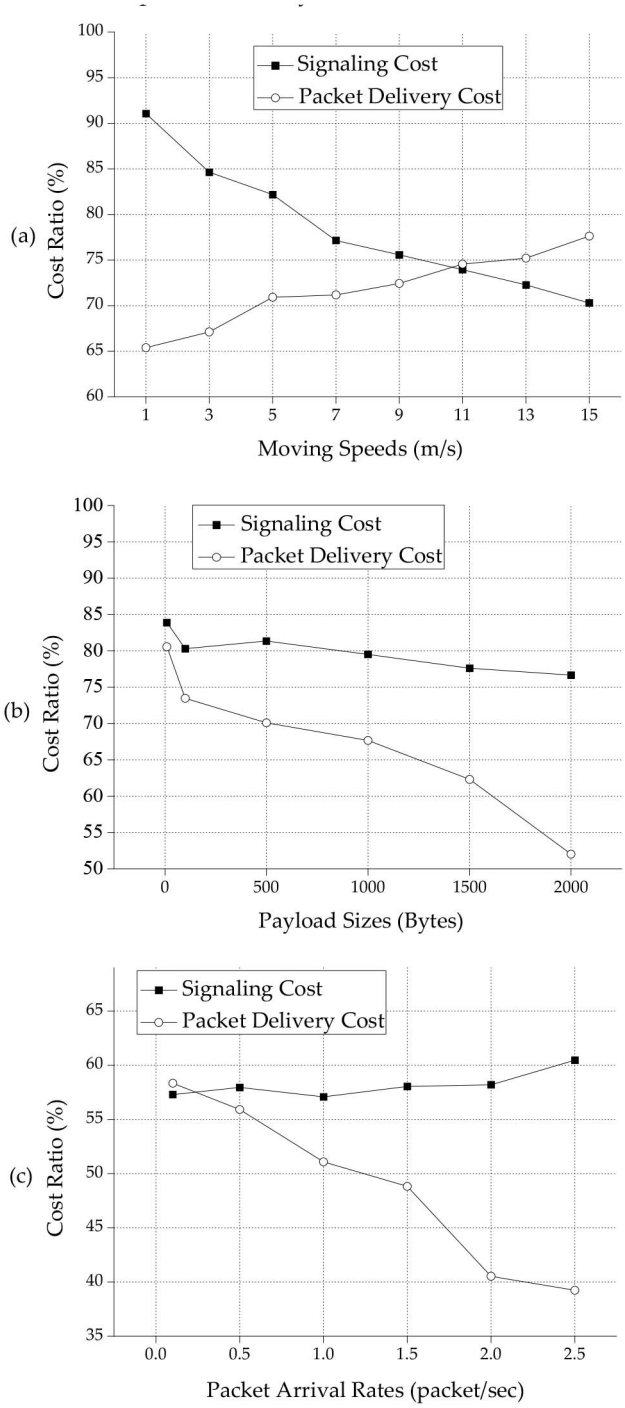

Fig. 11. (a) The total signaling cost ratio and packet delivery cost ratio at different moving speeds, (b) the different in packet sizes, and (c) the different packet arrival rates.

TABLE 1
Summarized Table of Entity-Related Acronyms

Group	Acronyms	Full Name
Mapping Agent	DLMA	Distributed Local Mapping Agent
	H-DLMA	Home-DLMA
	V-DLMA	Visiting-DLMA
	C-DLMA	Corresponding-DLMA
Device	PMD	Primary Mobile Device
	C-PMD	Corresponding-PMD
	6LD	6LoWPAN Device
	C-6LD	Corresponding-6LD
Gateway	AGW	Access Gateway
	C-AGW	Corresponding-AGW
	P-AGW	Previous-AGW
	N-AGW	New-AGW

TABLE 2
Summarized Table of Address-Related Acronyms

Group	Acronyms	Full Name
Identifier (ID)	GDID	Global Unique Device Identifier
	UPID	User Prefix Identifier
	AID	Access Identifier
	pAID	Point of Attachment AID
	nAID	Network AID
Locator (LOC)	GLOC	Global Locator
	CLOC	Corresponding Locator

According to the moving speed of the PMD, the proposed architecture can save 23%-35% of the packet delivery cost and 9%-30% of the total signaling cost, respectively, compared to extended HIP. This is due to the fact that the proposed architecture does not require mobility-related messages within the access network area regardless of where the PMD is located. On the other hand, extended HIP requires mobility-related messages when the PMDs move to home-domain or visiting-domains.

Fig. 11(b) shows the total signaling cost and packet delivery cost ratio of the proposed architecture compared to that of extended HIP as the payload size of the data packet is changed. According to the payload size, the proposed architecture can save 20%-48% of the packet delivery cost and 17-24% of the total signaling cost, respectively, compared to extended HIP.

This is because the signaling messages are not affected by the payload size of the data packet. The packet delivery cost of the proposed architecture is reduced in comparison with those of extended HIP as the payload size is increased due to the routing problem of extended HIP. Extended HIP needs more processing to handle the packet transmission and reception if the payload size is larger. Furthermore, the proposed architecture provides route optimization between the 6LD and its CN regardless of the location of the 6LD.

Fig. 11(c) shows the total signaling cost and packet delivery cost ratio of the proposed architecture to extended HIP as the packet arrival rates is changed. The proposed architecture requires only 57%-61% of the total signaling cost of extended HIP. Similarly with payload size, the total signaling cost is largely unchanged regardless of the packet arrival rates. The packet delivery cost of the proposed architecture is also reduced in comparison with extended HIP as the packet arrival rate is higher. Due to the routing problem as described above, if the packet arrival rate is higher, extended HIP needs more processing in order to handle the packet transmission and reception.

From the cost ratio results, we can verify that the proposed ID/LOC separation-based mobility architecture for supporting 6LoWPAN mobility is more efficient and lighter than extended HIP in terms of the total signaling cost and the packet delivery cost.

5 Acronyms

We summarize acronyms that are newly defined by the proposed architecture. Table 1 shows the entity-related acronyms, and Table 2 shows the address-related acronyms, respectively.

6 Conclusion

In this paper, we propose a new ID/LOC separation-based lightweight mobility management architecture for 6LoWPAN that supports groups of mobile sensor networks. The focus of the proposed architecture is to design a general purpose mechanism that can be used by a wide range of applications.

We believe that this scheme provides comprehensive application-adaptation for mobility in 6LoWPAN. The proposed new ID/LOC separation architecture for 6LoWPAN mobility supports energy-efficient lightweight mobility control, ID-based communications with location-based routing, packet route optimization and separation of mobility control from data transport. Furthermore, the proposed architecture utilizes network-based mobility that supports minimal signaling messages.

Performance results show that the proposed ID/LOC separation-based mobility architecture for supporting 6LoWPAN is more efficient and lighter than the existing HIP architecture in terms of the average energy consumption of sensor devices, total signaling cost and packet delivery cost ratio.

Acknowledgment

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2010-0020728) and by the Ministry of Science, ICT & Future Planning (MSIP), Korea, under the Information Technology Research Center (ITRC) support program supervised by the National IT Industry Promotion Agency (NIPA) (NIPA-2013-(H0301-13-2001). Dr. C. S. Hong is the corresponding author.

References

[1] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals," IETF RFC 4919, Aug. 2007.

[2] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15.4 networks," IETF RFC 4944, Sep. 2007.
[3] *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs),* IEEE Standard 802.15.4-2006, Sep. 2006.
[4] K.-C. Chen, "Machine-to-machine communications for healthcare," *J. Comput. Sci. Eng.*, vol. 6, no. 2, pp. 119–126, Jun. 2012.
[5] C. Perkins, P. Roberts, and B. Patil, "IP mobility support for IPv4," IETF RFC 3344, Aug. 2002.
[6] D. Johnson, C. Perkins, and J. Arkko, "Mobility support in IPv6," IETF RFC 3775, Jun. 2004.
[7] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy mobile IPv6," IETF RFC 5213, Aug. 2008.
[8] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network Mobility (NEMO) basic support protocol," IETF RFC 3963, Jan. 2005.
[9] J. H. Kim, C. S. Hong, and T. Shon, "Lightweight NEMO protocol to support 6LoWPAN," *ETRI J.*, vol. 30, no. 5, pp. 685–695, Oct. 2008.
[10] J. H. Kim, R. Haw, E. J. Cho, C. S. Hong, and S. Lee, "A 6LoWPAN sensor node mobility scheme based on proxy mobile IPv6," *IEEE Trans. Mobile Comput.*, vol. 11, no. 12, pp. 2060–2072, Dec. 2012.
[11] G. Bag, M. T. Raza, K.-H. Kim, and S.-W. Yoo, "LoWMob: Intra-PAN mobility support schemes for 6LoWPAN," *Sensors*, vol. 9, no. 7, pp. 5844–5877, Jul. 2009.
[12] ITU-T SG13. *Future Networks Including Cloud Computing, Mobile and Next-Generation Networks* [Online]. Available: http://itu.int/ITU-T/go/sg13
[13] E. Nordmark and M. Bagnulo, "Shim6: Level 3 multihoming shim protocol for IPv6," IETF RFC 5533, Jun. 2009.
[14] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "The locator/ID separation protocol (LISP)," IETF RFC 6830, Jan. 2013.
[15] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host identity protocol," IETF RFC 5201, Apr. 2008.
[16] P. Nikander, A. Gurtov, and T. Henderson, "Host Identity Protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks," *IEEE Commun. Surv. Tuts.*, vol. 12, no. 2, pp. 186–204, Apr. 2010.
[17] S. Novaczki, L. Bokor, G. Jeney, and S. Imre, "Design and evaluation of a novel HIP-based network mobility protocol," *J. Netw.*, vol. 3, no. 1, pp. 10–24, Jan. 2008.
[18] R. Moskowitz, "HIP Diet EXchange (DEX)," IETF draft-moskowitz-hip-rg-dex-06, May 2012.
[19] J. Laganier and L. Eggert, "Host identity protocol (HIP) rendezvous extension," IETF RFC 5204, Apr. 2008.
[20] X. Xu, "Routing architecture for the next generation internet (RANGI)," IETF draft-xu-rangi-04, Aug. 2010.
[21] V. P. Kafle and M. Inoue, "Mobility management in HIMALIS architecture," in *Proc. IEEE CCNC*, Jan. 2010.
[22] V. P. Kafle, H. Otsuki, and M. Inoue, "An ID/locator split architecture for future networks," *IEEE Commun. Mag.*, vol. 48, no. 2, pp. 138–144, Feb. 2010.
[23] Z. Shelby, S. Chakrabarti, E. Nordmark, and C. Bormann, "Neighbor discovery optimization for IPv6 over low-power wireless personal area networks (6LoWPANs)," IETF RFC 6775, Nov. 2012.
[24] B. Sarikaya, F. Xia, and G. Zaverucha, "Lightweight secure neighbor discovery for lowpower and lossy networks," IETF draft-sarikaya-6lowpan-cgand-03, Apr. 2012.
[25] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "Secure neighbor discovery (SEND)," IETF RFC 3971, Mar. 2005.
[26] T. Aura, "Cryptographically generated addresses (CGA)," IETF RFC 3972, Mar. 2005.
[27] "Standards for Efficient Cryptography Group. SEC 1: Elliptic Curve Cryptography Version 2.0," May 2009.
[28] "American National Standards Institute (ANSI), ANS X9.62-2005: The Elliptic Curve Digital Signature Algorithm (ECDSA)," Nov. 2005.
[29] *Objective Modular Network Testbed in C++ (OMNeT++)* [Online]. Available: http://www.omnetpp.org

Jinho Kim received his M.S. and Ph.D. degrees from the Department of Computer Engineering at Kyung Hee University, Korea, in 2007 and 2010, respectively. Since November 2012, he is a manager of the Advanced Institute of Technology at KT Corp., Korea. He was a senior research engineer of Research Laboratories at NTT DOCOMO, INC., Japan from 2010 to 2012. He is a member of the IEEE, KIISE, KICS, and KIPS. His research interests include traffic offloading, mobility management, future Internet, advanced wireless network protocols, and wireless sensor networks.

Jun Lee received his B.S. and M.S. degrees from the Department of Computer Engineering at Kyung Hee University, Korea, in 2010 and 2012, respectively. His research interests include advanced wireless network protocols, mobility management, and Ad hoc Network.

Hyoeng Kyu Kang received his B.S. and M.S. degrees from the Department of Computer Engineering at Kyung Hee University, Korea, in 2010 and 2012, respectively. His research interests include congestion control, and network management in multipath communication.

Dae Sun Lim received his M.S. and Ph.D. degrees from the Department of Computer Engineering at Kyung Hee University, Korea, in 2004 and 2009, respectively. Since September 2009, he is an associate research engineer of IP Network Division at KDDI R&D Laboratories Inc. He is a member of ITU-T Study Group 13, KIISE, KICS, and KIPS. His research interests include future networks, network virtualization, cloud network, and mobility management.

Choong Seon Hong received his B.S. and M.S. degrees in electronic engineering from Kyung Hee University, Seoul, Korea, in 1983, 1985, respectively. In 1988 he joined KT, where he worked on Broadband Networks as a member of the technical staff. From September 1993, he joined Keio University, Japan. He received the Ph.D. degree at Keio University in March 1997. He had worked for the Telecommunications Network Lab., KT as a senior member of technical staff and as a director of the networking research team until August 1999. Since September 1999, he has worked as a professor of the department of computer engineering, Kyung Hee University. He has served as a General Chair, TPC Chair/Member, or an Organizing Committee Member for International conferences such as NOMS, IM, APNOMS, E2EMON, CCNC, ADSN, ICPP, DIM, WISA, BcN, TINA, SAINT, and ICOIN. Also, he is now an associate editor of the *IEEE Transactions on Network and Service Management, International Journal of Network Management, Journal of Communications and Networks, and an associate technical editor of IEEE Communications Magazine*. And he is a senior member of the IEEE, and a member of ACM, IEICE, IPSJ, KIISE, KICS, KIPS and OSIA. His research interests include Future Internet, Ad hoc Networks, Network Management, and Network Security.

Sungwon Lee received the Ph.D. degree from Kyung Hee University, Korea. Since March 2008, he is a professor of the Department of Computer Engineering at Kyung Hee University, Korea. He was a senior engineer of Telecommunications and Networks Division at Samsung Electronics Inc. from 1999 to 2008. He is a editor of the *Journal of Korean Institute of Information Scientists and Engineers: Computing Practices and Letters*. His research interests include mobile broadband networks and communication protocols. He is a member of the IEEE, KIISE, KICS, and KIPS.

▷ **For more information on this or any other computing topic, please visit our Digital Library at** www.computer.org/publications/dlib.