Dual Addressing Scheme in IPv6 over IEEE 802.15.4 Wireless Sensor Networks

Sooyoung Yang, Sungjin Park, Eun Ju Lee, Jae Hong Ryu, Bong-Soo Kim, and Hyung Seok Kim

This paper proposes a dual addressing scheme (DAS) for IPv6 over IEEE 802.15.4 wireless sensor networks (WSN). DAS combines a global unicast address to cope with association link changes and node mobility, and it links local addresses to lighten the overhead of the system to save energy and resources. This paper describes DAS address formats, address autoconfiguration, and address translation tables in the gateway. A detailed description of DAS is provided through examples. Simulations are performed to demonstrate the performance improvements of the DAS compared with the IPv6-based WSN, which uses the conventional single address.

Keywords: IPv6, IEEE 802.15.4, wireless sensor network, dual addressing, gateway.

Manuscript received Jan. 31, 2008; revised Aug. 19, 2008; accepted Aug. 22, 2008.

This work was supported by the IT R&D program of MIC/IITA, Rep. of Korea [2005-S-038, Development of UHF RF-ID and Ubiquitous Networking Technology] and in part by the Korea Research Foundation Grant funded by the Korean Government (MOEHRD, Basic Research Promotion Fund) (KRF-2007-331-D00388).

Sooyoung Yang (phone: +82 2 448 8908, email: sooyoung80@gmail.com), Sungjin Park (email: parksj@sju.ac.kr), and Hyung Seok Kim (phone: +82 2 3408 3696, email: prof.hskim@gmail.com) are with the Department of Information and Communication Engineering, Sejong University, Seoul, Rep. of Korea.

Eun Ju Lee (email: leeej@etri.re.kr), Jae Hong Ryu (email: jhryu@etri.re.kr), and Bong-Soo Kim (email: bskim@etri.re.kr) are with IT Convergence Technology Research Laboratory, ETRI, Daejeon, Rep. of Korea.

I. Introduction

The wireless sensor network (WSN), which is a spatially distributed monitoring network consisting of wireless devices using sensors, is expected to result in ubiquitous computing. Rapid advances in wireless networks, embedded systems, and sensor technologies have introduced various WSN-related industries that are becoming more important in every day life. In order for WSN to become more practically utilized, however, various useful services have to become available, and improvements must be made in terms of network management and resource restriction.

There have been recent attempts to integrate Internet services with the WSN through studies concerning the integration of the IEEE 802.15.4 protocol [1] and the Internet protocol (IP). Furthermore, if we use IPv6 in place of the IPv4 network, whose IP address capacity has already been saturated, IPv6 addresses can be automatically assigned to numerous sensor nodes, thereby facilitating node management. A sensor node that acts as an individual server needs to be directly accessed using a global unicast IPv6 address with IP-based management protocols.

IP-based protocols such as TCP/IP usually require heavy resources to be allocated to a sensor node. There have been studies conducted to resolve the problems that occur when operating IP-based stacks in sensor nodes with limited system resources [2]-[4], and the 6LoWPAN working group (WG) has worked on IPv6 over IEEE 802.15.4 [5]. The technical standard proposed by the WG regarding 6LoWPAN involves placing an adaptation layer between the MAC and network layers to handle interoperation between these layers and to reduce resources.

There have been studies similar to the 6LoWPAN study that

cover hybrid ad hoc networks, which are integrations of ad hoc networks and IP networks. Research on hybrid ad hoc networks has focused on selecting the best path towards the gateway for wireless connection to the Internet [6]-[8], energy-saving self-configuration [9], [10], as well as mobility and duplicated address detection [11]. Research on reducing power consumption [10], [12] categorizes network construction into nodes with and without energy restriction. The characteristics of these networks are different from those of typical WSNs, in which all sensor nodes except gateways are energy-restricted. Although [11] deals with mobility, it does not cover power considerations.

In 6LowPAN, the stateless address autoconfiguration scheme uses either an interface identifier generated from IEEE 802.15.4's 16-bit short address or the IEEE extended unique identifier address (EUI-64). Its adaptation layer writes a mesh subheader which includes a short address or EUI-64 for MAC routing. Short addressing distinguishes nodes within the WPAN. It is used by most IEEE 802.15.4 systems due to its small overhead. EUI-64 provides an addressing scheme unique to each sensor node. Although the short-address-based IPv6 address incurs little overhead, it is not globally unique to a sensor node. The short-address-based IPv6 address may be duplicated and may change due to a link change of node or intra/inter-network mobility. In other words, individual sensor nodes may not be distinguished or accessed in a lossy mobile WSN. EUI-64-based IPv6 addressing maintains unique sensor node addresses during link changes and mobility; however, it makes the overhead larger than that of the short address. Furthermore, EUI-64-based address generation does not provide hierarchical addressing for applications in hierarchical tree routing (TR) that can be executed with low power and low memory consumption.

For the reliable and stable operation of an IPv6 enabled WSN, each sensor node must have a global unicast address, which is maintained during link changes or inter/intra-WPAN mobility, and also must reduce headers to save the limited resources of the WSN. To satisfy these requirements, this paper proposes the dual addressing scheme (DAS) for the IPv6-enabled WSN. DAS combines and incorporates advantages from the two previously mentioned addressing schemes. DAS provides sensor nodes with global unicast addresses and allows communication with a smaller overhead.

This paper is organized as follows. Section II describes the DAC in detail. It suggests an IPv6 address format for WSN, address autoconfiguration, and gateway for DAS. In section III, a method to route packets using DAS is suggested, with several examples. In relation to the simulation described in section IV, the expected benefits of applying DAS in WSN are presented from the perspective of energy saving. Finally, section VI concludes this paper.

II. Dual Addressing Scheme

1. Dual IPv6 Addressing

To generate IPv6 addresses that are globally unique but have low overhead for intra-subnetwork communication, DAS uses both link local addresses created from the 16-bit short address and global unicast addresses from EUI-64. Combining both the addressing schemes, the overhead can be reduced in the sensor network, intra/inter-subnetwork mobility can be supported in the WSN, and each sensor node can be accessed and managed.

As shown in Fig. 1(a), a link local address is produced using an interface identifier created from the 16-bit short address of IEEE 802.15.4 and a prefix FE80::0 allocated in the high 10 bits. In hierarchical address allocation, when a sensor moves to associate with another parent, it changes the short address to another one, and the link local address can also be modified. In random address allocation, because the short address is not globally unique, there is a possibility of duplicate addresses occurring. The global unicast address shown in Fig. 1(b) is generated by a stateless IPv6 autoconfiguration by combining the global prefix and the EUI-64 based interface identifier. Basically, the EUI-64, which is defined by IEEE, can be either assigned to a network adapter or derived from IEEE 802 addresses, this method is well explained in [13]. Constructed with the 16-bit short-address-based interface identifier, the link local address can be compressed in the header in the WSN, and the global unicast address provides direct access to each node.

WSN connected to the Internet must have a gateway, and

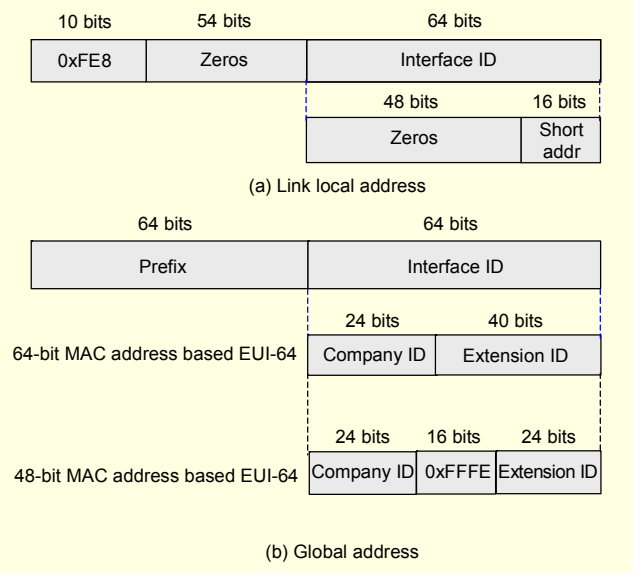


Fig. 1. Dual IPv6 addressing.

Table 1. Example of a translation table in the gateway.

16-bit short address	64-bit EUI address
0	0211:22FF:FE44:5566
1	0211:22FF:FE44:5567
2	0211:22FF:FE44:6667
3	0222:22FF:FE44:6667
4	0211:33FF:FE44:6667
5	0211:33FF:FE55:6667

considering the topology and the information contained, it is desirable that a wireless personal area network (WPAN) coordinator should act as the gateway of an IEEE 802.15.4 network. Since a gateway is generally linked to the Internet via a wired connection, it is assumed that a gateway has a power supply and, therefore, infinite energy, unlike wireless sensor nodes. Furthermore, we can assume that the gateway is a system with unlimited resources in terms of memory and computing power when compared to sensor nodes. Accordingly, DAS transfers the functions of sensor nodes to the gateway as a means of saving the sensor nodes' limited resources and focuses on using the resources of the gateway.

In DAS, a gateway must use its abundant resources to store the global unicast address, link local address of all the nodes in the subnetwork, and maintain a translation table for matching the addresses. Since the global unicast address and link local address are created with an EUI-64-based interface identifier and a 16-bit short-address-based interface identifier, respectively, the translation table must store each pair of short addresses and EUI-64 as shown in Table 1.

When the number of nodes in the subnetwork increases, there can be a time delay in searching a gateway's table. As assumed earlier, a gateway can have infinite resources. If more performance is necessary, installing additional gateways and coordinated storage/search using multiple gateways can minimize the performance decrease due to time delay. By allocating DAS functions to the gateways, sensor nodes can be relieved of power and capacity burdens.

Before illustrating an example of address conversion with reference to the translation table, we first demonstrate the packet format used in WSN with DAS, and the compressed IP header in relation to packet flow. The maximum packet size provided by the IEEE 802.15.4 standard is 127 bytes, and the payload size depends on packet headers. In IPv6-enabled WSN, since IPv6 addresses occupy a large part of the packet size, IPv6 addressing schemes and address-compressing methods have a significant impact on determining payload size. Before explaining DAS in detail, we therefore need to examine these issues.

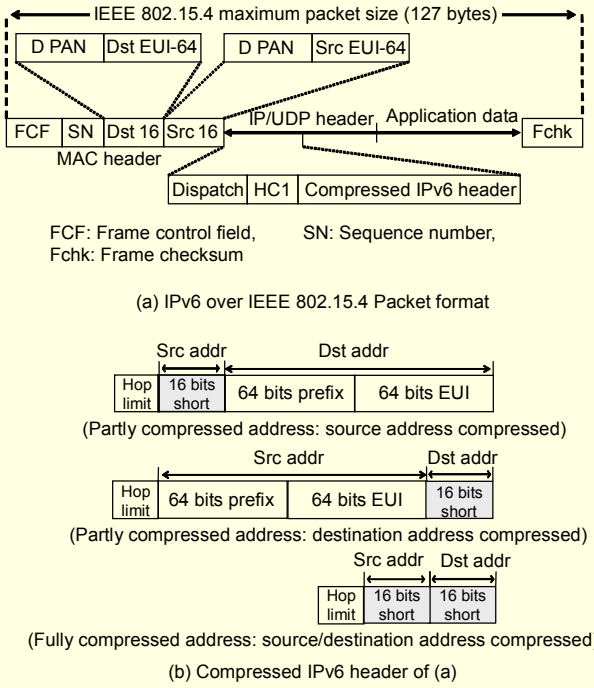


Fig. 2. IEEE 802.15.4 packet with DAS.

Figure 2(a) displays the whole format of the IEEE 802.15.4 packet with DAS. Basically, it is based on IPv6 over the IEEE 802.15.4 packet format introduced in [5]. It begins with the IEEE 802.15.4 MAC header of 25 bytes described in [1]. Dispatch and HC1 just follow in order. Dispatch is one byte long and indicates the IPv6 header's compression and type. HC1 is also one byte long and contains compression information for each field in the IPv6 header. Here, the distinction from other protocols like 6LowPAN and DAS is that it supports L3 routing; therefore, it does not require any additional headers to support L2 routing. Accordingly, without forcing any additional overhead, the IPv6 header follows the MAC header.

The fields of the IPv6 header, except for hop limit, can be compressed in various ways. Among the fields of the IPv6 header, we focus on the source and destination address fields, which occupy most of the space in the IPv6 header. DAS has three types of compression for source/destination address fields. Figure 2(b) shows each type of IPv6 header format. The top two headers shown in Fig. 2(b) represent a partly compressed IPv6 header in which the source or destination addresses are compressed. They are used in communication between the sensor nodes and the gateway and are also used in communication between two sensor nodes in the same subnet of a mobile and lossy WSN, where most links are intermittently connected, thus causing frequent topology changes. The last example in Fig. 2(b) represents a fully compressed IPv6 header in which both addresses are

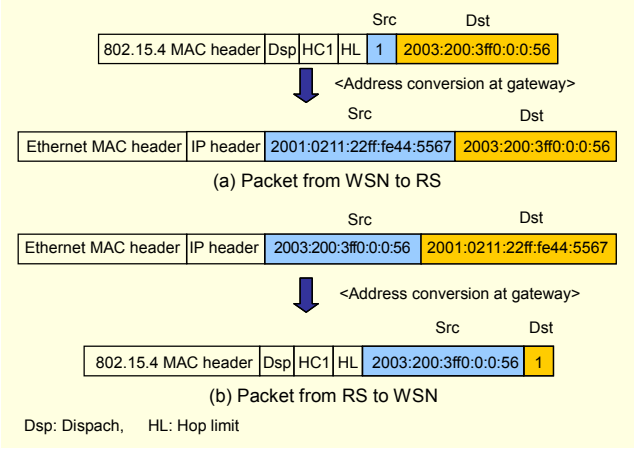


Fig. 3. Address conversion according to the translation table.

compressed. It can be used in communications between two sensor nodes which belong to the same subnet of a static and stable WSN. The IPv6 header format's usage is described in section 3 through a set of examples.

Figure 3 shows address conversion in IPv6 header fields, according to the translation table, when a packet moves through a gateway in a session between a sensor node and a station on the Internet. Let us assume that a 16-bit short address in a sensor node is 1, and its link local address is FE8::1.

Let us also assume that a sensor node with the global unicast IPv6 address 2001::0211:22FF:FE44:5567 is sending a sensor data packet to a remote station (RS) with IPv6 address 2003::200:3FF0:0::56. The packet created by the sensor node has a MAC header and codes (dispatch and HC1) for compressing the IPv6 header, followed by a compressed IPv6 header. Since it is an outgoing packet, it has a global unicast address in the destination address field and the short address 1 as the compressed format in the source field. The IPv6 packet is then transferred to a gateway, which decompresses the packet and appends a full IPv6 header after the Ethernet MAC header. Here, the source address of the IPv6 header references the translation table shown in Table 1, converts the compressed 1 to the global unicast address 2001::0211:22FF:FE44:5567, and fills the source address field. When a packet enters the WSN from the Internet, it is processed in the reverse order of the above process. The gateway removes the Ethernet header, and the global unicast address in the destination field is converted into a link local IPv6 address, which is compressed and entered into the destination field in the form of a short address.

2. Dual IPv6 Address Autoconfiguration

First, the general IPv6 stateless autoconfiguration is conducted in the following order. When a new node comes into

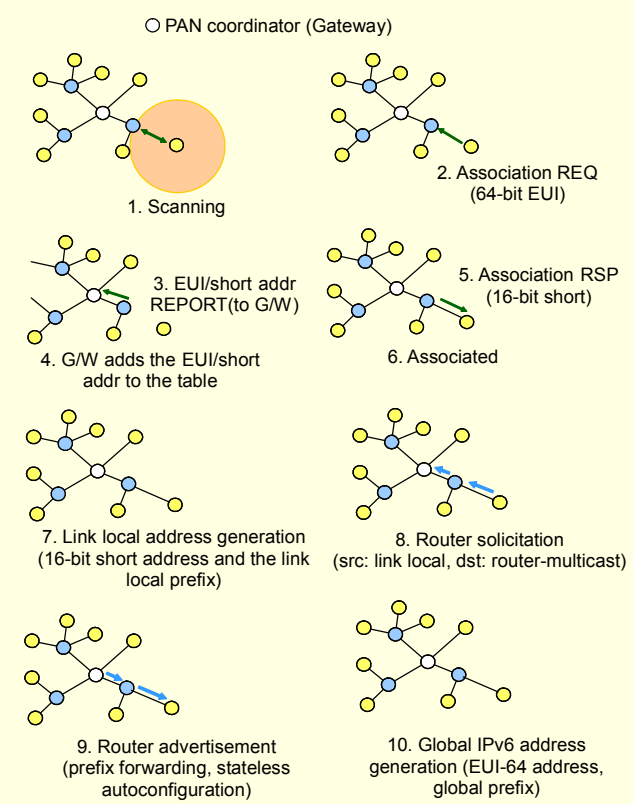


Fig. 4. Dual IPv6 address autoconfiguration.

a network, it first creates a link local address by combining the interface identifier and known link local prefix. It then performs duplicated address detection (DAD), which detects a duplicated address that is already used in the network. To ensure that the address is unique to the network, the new node performs this procedure using a neighbor solicitation (NS) message and neighbor advertisement (NA) message. It first sends the NS message to its neighbor nodes belonging to the same network and then waits for an NA message indicating that the address is duplicated in the network. If no NA message is received, the node assumes that the address is unique, and assigns it an interface. On the other hand, however, if an NA message is received, the new node cannot use that address. In this case, it obtains a link local address from manual configuration or the DHCP server. After creating a link local address, the new node sends a router solicitation message to the network, using the link local address, in order to obtain network information. However, this is not the only way to get the network information. Since the router advertisement (RA) message is sent periodically to all the nodes by multicast, the new node may wait for the RA message until it is received. After receiving the RA message, the new node obtains the global IPv6 prefix from the prefix information options contained in the RA message. Finally, it creates a global

address by combining the interface identifier and the global IPv6 prefix [14].

As shown in Fig 4, DAS is carried out based on the conventional IPv6 address autoconfiguration scheme with the objectives of reducing power consumption for WSN and creating IPv6 addresses with two MAC addresses. When a new node enters a WSN, a sensor node locates an adjacent neighbor (parent) by scanning. An association message that includes its EUI-64 is sent to the parent node for association. The parent node then reports the new node's 16-bit short address and EUI-64 address to the gateway, which adds the pair to the translation table.

The parent node adds the node's 16-bit short address into an association RSP message for transmission, and the node generates a link local address based on the short address. Once the link local address is generated, the node indicates its link local address as the origin address in the router solicitation message and sends it to the gateway using the router multicast address to generate a global address. When a router advertisement message is received as a response, a global unicast address is created using the global prefix contained in the message as well as the node's EUI-64. The sensor node now possesses two IPv6 addresses created with two different MAC addresses: a link local address and a global unicast address. When a node fails DAD, the gateway plays the role of a DHCPv6 server, utilizing the list of addresses in the translation table.

3. DAS for Mobile and Lossy WSN

DAS provides a global unicast address for a sensor node, thereby creating a seamless connection between the sensor node and other sensor nodes or stations on the Internet, despite link losses caused by unattended wireless sensor nodes or address changes due to physical mobility. This section uses examples to explain the DAS mechanism in more detail.

In Fig. 5, link loss between node 1 and node 6 occurs. Because node 6 associates with node 2 due to the link loss, a problem is created in that node 6 changes to the new short address provided by node 2. Using DAS, node 6 goes through the autoconfiguration process explained in section II.2. Its EUI-64 and a new short address, 11, are sent to a gateway while it associates with node 2. By searching the translation table, the gateway acknowledges that EUI-64 of node 6 is already registered with the translation table and updates its new link local address. Accordingly, even if node 6 loses its link during communication with other nodes, the gateway, as a central controller, can quickly react to prevent connection loss and minimize transmission packet loss. The sensor node can also be continuously accessed from outside with an identical

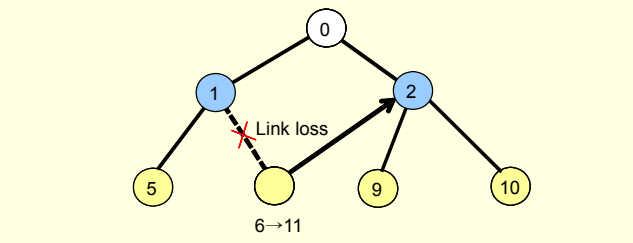


Fig. 5. Example of link loss in WSN.

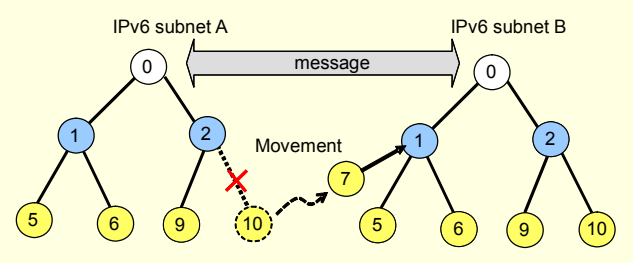


Fig. 6. Example of node movement to another subnet.

global unique address.

Figure 6 shows an example of node movement to another subnet. Node 10 of subnet A moves to subnet B and becomes child 7 of node 1. When node 10 moves to subnet B, it connects to node 1 and receives the new 16-bit short address 7 in subnet B. The new information is sent to subnet B's node 0 (gateway), whose table is updated. Node 7 sends the previous gateway address to subnet B's gateway, and the gateway of subnet B transmits a message containing node 7's EUI-64 address to subnet A's gateway to request information about node 7 via the Internet connection. When node 2 in subnet A detects the secession of node 10, its status is delivered to subnet A's node 0. Subnet A's gateway requests an update from the transmitting node so that the packet coming to the previous node 10 is sent to subnet B's gateway to maintain communication even during sensor node movements between subnets. In this handover procedure, a node needs only less than tens of milliseconds for the association procedure by 16-bit short address. Since DAS provides a global unicast address, it can apply the mobile IPv6 handover procedure. According to RFC 3775 document [15], it takes a couple of seconds or less for the network layer handover. Assuming that the gateways use Fast Ethernet for a wired connection, the overall time to transmit the data for node 10 (subnet A) to node 7 (subnet B) may take a couple of seconds or less.

III. Routing Using DAS

Since DAS is based on dual addressing, it enables routing in the network (L3) layer rather than using a separate mesh subheader between the MAC and IP headers. Therefore, it can

avoid redundant address information, which can be beneficial in the low-capacity IEEE 802.15.4 frame.

In addition to tree routing, DAS can be applied with table-driven routing (TDR) including the ad hoc on-demand distance vector (AODV) routing protocol. If link local/global IPv6 addresses are generated with DAS, and the MAC address translation table is maintained, address compression can save energy even if internal routing is performed with TDR. Although TDR is expected to incur the large overhead required to search for a path to a gateway when the links are lossy and nodes move frequently, it has the advantage of achieving a minimum distance path between two random nodes in a wireless network. For examples of routing with DAS, only the application of DAS to tree routing will be explained in this work.

1. Between Sensor Nodes in the Same Subnetwork

If DAS is used in a WSN, the sensor node can have both link local addresses, which can be compressed and used internally, and a global unicast address, which provides global accessibility. Since link local addresses can be used for the source and destination addresses for internal node communication, energy consumption can be reduced within the network. According to the ZigBee 2006 specification [16], addresses are hierarchically allocated to child nodes, starting from zero at the WPAN coordinator. A hierarchical routing scheme is used for nodes that are not mobile.

Since the link local address of each node does not change in an ideal WSN with static nodes and stable links, the IP header of a data packet can express its destination and source addresses using link local addresses during routing. As shown in Fig. 7, the data packet can be delivered with a simple approach using the link local IPv6 address of each node in an IPv6 enabled WSN.

Figure 8 illustrates a packet delivery from node 10 to node 5 in a mobile and lossy network. The originator node 10 inserts the global unicast address of the destination node 5 into the packet's IP destination address. The data packet is transmitted to a gateway, which references the address translation table updated with the latest data and converts the global unicast address of the final destination in the header to a link local address so that it can be delivered to the final destination with little overhead. Thus, the packet can be consistently delivered to a single address even if the destination node associates with a different node due to mobility or link loss.

2. Between the Internet and WSN

Figure 9 illustrates the route and destination/source address field of the headers when a sensor node sends a data packet to a RS in an external network (the Internet). In a WSN connected to the Internet, because the RS in the Internet monitors sensor nodes or controls actuator nodes over the Internet, most of the traffic in the network passes through gateways. Initially, node 10 saves the energy required for intra-subnet routing by using its link local IPv6 address as the source address for transmission to a gateway. Upon receiving a packet, the gateway references the address translation table to convert node 10's link local address written in the source field of the IP header into a global unicast address and sends it to the RS to establish an end-to-end link between the RS and node 10 using global unicast addresses.

Figure 10 illustrates a case in which dedicated RSs that have

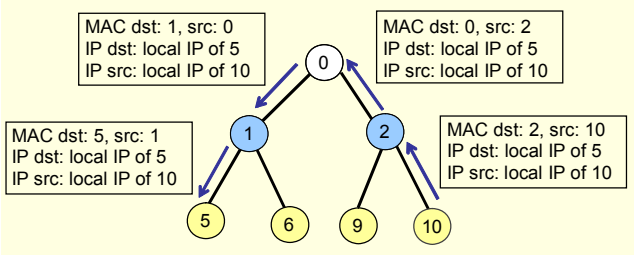


Fig. 7. Example of static and stable network.

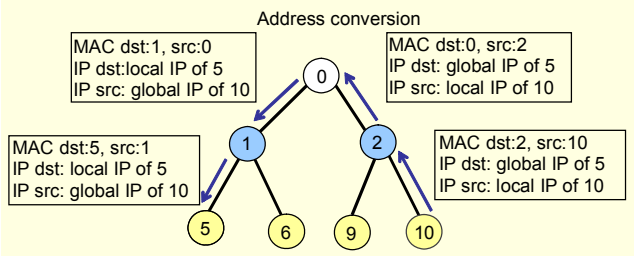


Fig. 8. Mobile and lossy wireless sensor network.

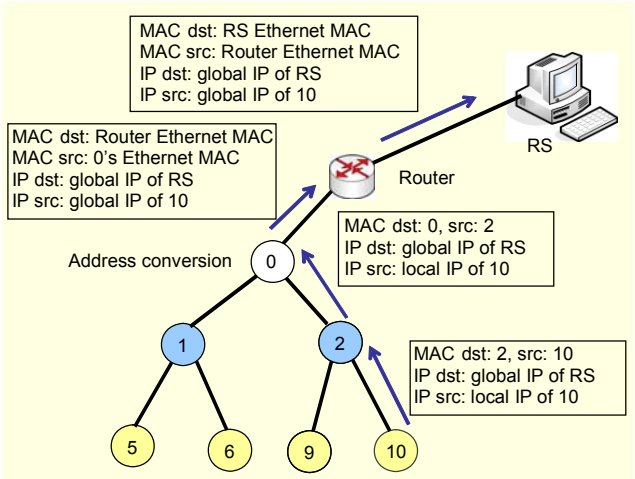
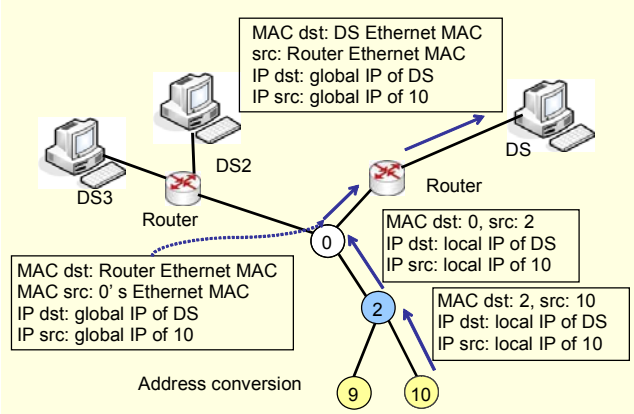


Fig. 9. Packet transmission to an external station.



<MAC translation table for DS>

16-bit short address	Prefix	EUI-64
65535 (DS)	2000:0:0:1	0414:21FF:FE44:3276
65534 (DS2)	2000:0:0:2	0213:21FF:FE44:2336
65533 (DS3)	2000:0:0:2	0114:21FF:FE44:1373

Fig. 10. Packet transmission to dedicated remote stations.

privileged access to the WSN have been assigned in advance. In general, a sensor network implemented by a service provider has a dedicated station for monitoring and controlling the network. The RSs collect and store the sensor node data. If an RS transmits queries to the sensor nodes' global unicast IPv6 addresses, or if sensor nodes send measures to an RS's global unicast IPv6 address, the overhead becomes large and efficiency is severely compromised. To solve this problem, unused 16-bit short addresses in a subnetwork can be registered as the RSs' virtual short addresses, and each node and gateway is notified of this. By matching a reserved address to an RS's global unicast IPv6 address in the gateway translation table, the 128-bit global unicast IPv6 address overhead can be reduced to 16 bits. Accordingly, inefficient data transmission due to frequent exchange of queries and sensor measures between sensor nodes and dedicated RSs can be eliminated. We call this dedicated RS a *dedicated station* (DS), and when applying DAS to the communication between sensor node and the DS, we call it DAS-DS instead of DAS.

IV. Simulation

The critical advantage of DAS is that it reduces the communication overhead of the system while guaranteeing global uniqueness. Accordingly, under the condition that individual sensor nodes are supposed to be accessed through the Internet, DAS is superior to other schemes. This section aims to show the performance improvement over other schemes by using DAS under this condition. In this section, 6LoWPAN as a related scheme is referred to as a single addressing scheme (SAS), which uses either a link local address or a global address with a mesh subheader. However, SAS cannot satisfy both communication overhead reduction and global accessibility at the same time. To satisfy global accessibility, it has to follow the general IPv6 stateless address autoconfiguration described at the beginning of section II.2 and use a mesh header. To demonstrate the expected benefits of DAS, we base the performance comparison on the simulation in terms of energy saving. We simulate DAS, DAS-DS, and SAS as the hierarchical tree routing protocol for communication between the sensor node and RSs (or dedicated stations).

We also demonstrate by simulation how energy is saved when DAS is applied to other conventional routing protocols. For this purpose, we used the QualNet 4.0 simulation tool. The parameter settings required for the simulation are listed in Table 3. To facilitate the experiment and prevent fragmentation, the packet size, including the payload, does not exceed 127 bytes, which is the maximum packet size of the IEEE 802.15.4 PHY layer. Accordingly, if an IEEE 802.15.4 MAC header of 25 bytes, an IPv6 header of 40 bytes, and a UDP of 8 bytes are included, the payload size is confined to 54 bytes. Moreover, if a TCP of 20 bytes is used instead of UDP, the payload size is further reduced to 42 bytes.

In this simulation, compression is achieved using "dispatch" and HC1 for the IPv6 header and the UDP header as described in section 2. Therefore, the payload takes up 59 bytes of the IEEE 802.15.4 packet used in the simulation. In this section, for brevity, we use the terms packet instead of IEEE 802.15.4 packet. As explained in section III, DAS uses the link local address for the source and destination addresses, instead of the global unicast address. Accordingly, the header overhead can be reduced by 14 or 28 bytes. Table 2 lists the parameter settings used for the simulation.

Figure 11 shows a captured picture of a WSN with an RS used by the simulation tool. Sensor nodes are randomly distributed over 500 meters from one hop to four hops in the simulation window. The PAN coordinator is designated as the

Table 2. Parameter settings used for the simulation.

Parameters	Values
MAC/PHY	IEEE 802.15.4
IP version	IP version 6
Transport protocol	UDP
Antenna model	Omnidirectional
Antenna tx power	-5.0 dBm
Energy model	MICAz energy model

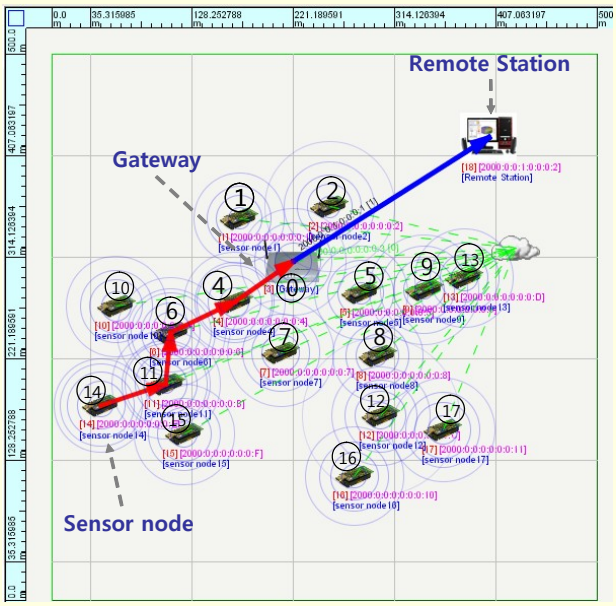


Fig. 11. Simulation window of DAS in IPv6-enabled WSN.

Table 3. Simulation scenario parameters.

Parameters	Values
Source node (node ID)	14, 15, 16, 17
Destination node (node ID)	18
Simulation start time (min)	1
Simulation end time (min)	540 (135 for each connection)
Application data type	CBR
Payload size (byte)	2 to 58
Maximum packet size (byte)	127
Packets to send (unit)	135
Packet interval (min)	1

gateway, and the Ethernet-based wired interface provides a link to the RS. All the simulations run for 540 minutes.

As shown in Table 3, when the simulation starts, node 14 begins to send a packet every minute to deliver a total of 135 packets for 135 minutes, and in the same manner, nodes 15, 16, and 17 send packets in order. In order to measure DAS's power consumption during repeated communication between a sensor node and an RS on the Internet, an experiment is conducted based on the scenario shown in Table 3. Two schemes, DAS and DAS-DS, are compared with SAS. The DAS-DS scheme, which is shown in Fig. 10, uses short addresses to represent dedicated stations. The RS in the simulation scenario is either a dedicated RS in DAS-DS or a typical RS in DAS.

The energy consumption for transmission of each node is shown in Fig. 12 for the scenario of Table 3 using DAS, DAS-DS, and SAS. The payload size is set to 18 bytes to sufficiently accommodate sensor measurement values. For DAS, DAS-DS, and SAS, packets are transmitted through the gateway. Nodes 4, 5, 6, 8, 11, and 12 which are located between the source node and the gateway, forward multiple packets with different sources, resulting in more energy consumption. Since DAS and DAS-DS deliver packets with smaller headers than those of SAS, they yield energy savings in ranges from 14% to 15% and from 28% to 30%, respectively, varying with each node.

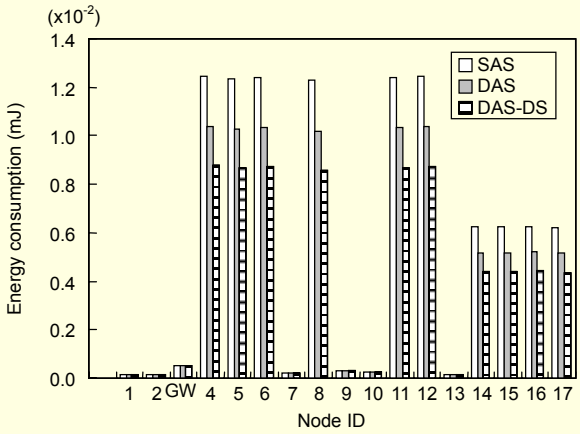


Fig. 12. Energy consumption for transmission (per node).

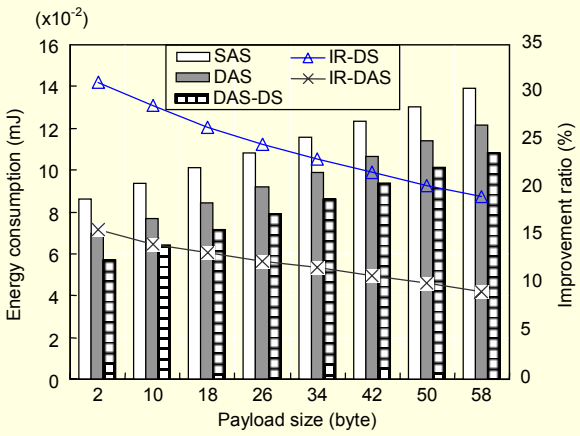


Fig. 13. Impact of different payload sizes on energy consumption.

The total energy consumption results are shown in Fig. 13. To see the impact of different payload sizes on energy consumption, we increase the payload size from 2 bytes to 58 bytes in 8 byte increments. The *x* axis of the figure represents the payload size, the *y* axis on the left is the total energy consumption for transmission, and the *y* axis on the right is the improvement ratio (IR), which indicates the performance improvement of DAS and DAS-DS compared to SAS for each scenario. The IR is displayed as IR-DAS and IR-DS for the DAS and DAS-DS schemes. As the payload size increases, smaller portions are taken up by the compressed address

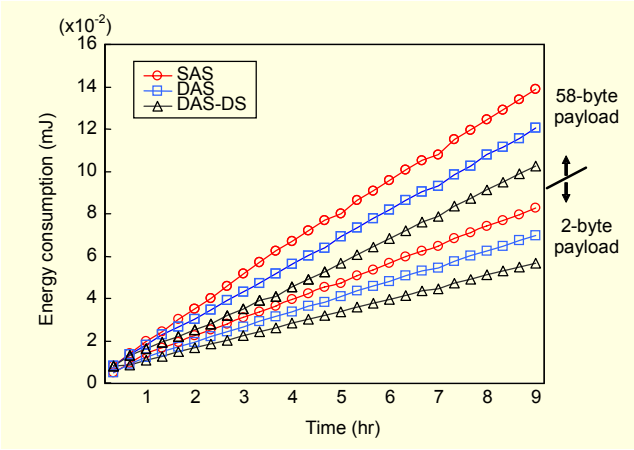


Fig. 14. Cumulative energy consumption (for various addressing schemes with two payload sizes: 2 bytes and 58 bytes).

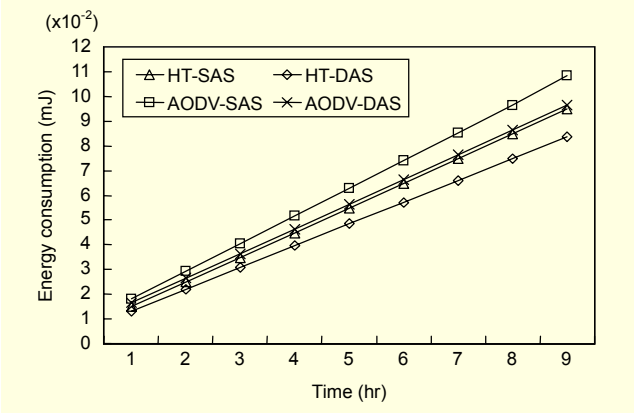


Fig. 15. Cumulative energy consumption for SAS and DAS with HT routing and AODV routing.

overhead in the DAS and DAS-DS headers, thereby decreasing IR-DAS and IR-DS, as shown in Fig. 13. Therefore, DAS is more effective when a small payload is used. Since the size of the sensor measurement values sent from a WSN to the Internet is less than a few bytes, DAS is expected to achieve outstanding performance in WSNs.

Figure 14 shows the accumulated energy consumption as the time increases with DAS, DAS-DS, and SAS, respectively.

The figure also shows the performance difference between payload sizes of 2 bytes and 58 bytes. The upper and lower pairs in the graph indicate payload sizes of 2 bytes and 58 bytes, respectively. This experiment shows how much energy is saved by DAS as time passes. As this simulation is based on the scenario shown in Table 3, a total of 540 transmissions occur during the simulation time, each line indicates increasing energy consumption in proportion to increasing time. The gap between two adjacent lines represents the difference in accumulated energy consumption. As shown in Fig. 14, it is clear that the gaps increase as time passes, and DAS and DAS-DS save more energy than SAS. Comparing DAS-DS with SAS, since it is possible for DAS-DS to use a 16-bit short address for both source address and destination address, DAS-DS offers more energy savings than DAS as compared to SAS.

We have shown that DAS has a positive effect on energy savings when it is used with the HT routing protocol. This experiment was performed to determine how DAS affects network performance when it is applied to other conventional routing protocols. For comparison, we use the AODV routing protocol. Assuming that most routing protocols used in wireless networks are divided into two types, one based on the TDR protocol and the other based on tree routing. Since AODV is a representative TDR protocol, we can prove that other TDRs and tree-based routing protocols take advantage of DAS from an energy and memory savings point of view.

Figure 15 shows this performance improvement when DAS is applied to HT and AODV, respectively. We set the payload size to 34 bytes and the total simulation time is 9 hours. In this graph, two pairs of lines are displayed. The upper one represents AODV with SAS and AODV with DAS; the lower one represents HT with SAS and HT of DAS. It is clear that when DAS as opposed to SAS is applied to AODV, the accumulated energy consumption decreases approximately 13%, as in the case of HT. The reason for this is that although DAS's hierarchical address concept is useless in AODV routing, the opportunity to use less memory is supported; thus, DAS helps to reduce energy consumption as compared to SAS.

V. Conclusion

This paper proposed a DAS, which provides a sensor node with both a global unicast IPv6 address and a link local IPv6 address based on the IEEE 802.15.4 MAC addresses and allows the gateway to convert these addresses. DAS offers seamless communication by maintaining the existing global address, even during link changes or inter/intra-WPAN mobility. It also conserves the limited resources of WSNs in intra-network communication by reducing the address size and overhead. This paper explained how dual IPv6 addresses are generated when a sensor node is introduced to a WSN and showed that DAS can be deployed in various circumstances, including inter/intra-network communications and mobile/lossy WSNs. Simulation results indicated that DAS saves energy consumption for transmission by up to 31% when sensor nodes communicate with a node on the Internet network, as compared to the single addressing scheme. We also demonstrated that DAS is applicable with various routing protocols. This study provides a guideline for future research activities that aim to integrate WSN and IP for low-capacity, low-power WSN, and to cope with lossy links and node mobility.

References

[1] IEEE TG 15.4b, *Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), IEEE Standard for Information Technology*, 2006.

[2] K. Mayer and W. Fritsche, "IP-Enabled Wireless Sensor Networks and Their Integration into the Internet," *ACM Int'l Conf. Proceeding Series, Proc. First Int'l Conf. Integrated Internet ad hoc and Sensor Networks*, vol. 138, May 2006.

[3] N. Kushalnagar and G. Montenegro, *6LoWPAN: Overview, Assumptions, Problem Statement, and Goals*, IETF draft, 2006.

[4] H. Huo at al., "MSRLab6: An IP6 Wireless Sensor Networks Testbed," *Proc. 8th Int'l Conf. Signal Processing*, ICSP 2006, vol. 4, 2006.

[5] G. Montenegro et al., *RFC 4944 - Transmission of IPv6 Packets over IEEE 802.15.4 Networks*, IETF, Sept. 2007.

[6] C. Jelger and T. Noel, "Proactive Address Autoconfiguration in IPv6 Hybrid Ad Hoc Networks," *IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, SECON 2005, Sept. 2005, pp. 107-117.

[7] R. Baumann et al., "Routing Packets into Wireless Mesh Networks," *Wireless and Mobile Computing, Networking and Communications, Third IEEE Int'l Conf. WiMOB*, Oct. 2007, pp. 38-46.

[8] M. Michalak and T. Braun, "Common Gateway Architecture for Mobile Ad Hoc Network," *Second Annual Conf. Wireless On-Demand Network System and Services*, 2005, pp. 70-75.

[9] R. Teng et al., "Network-Layer and MAC-Layer Address Autoconfiguration in Self-Organized Sensor Networks," *6th Int'l Conf. ITS Telecommunications Proceedings*, June 2006, pp. 1005-1010.

[10] H.J. Lee et al., "Interworking of Self-Organizing Hierarchical Ad Hoc Networks and the Internet," *ICCS*, May 2006, pp. 930-937.

[11] H.M. Ammari, "A Survey of Current Architectures for Connecting Wireless Mobile Ad Hoc Networks to the Internet," *Int'l J. Communication Systems*, vol. 20, no. 8, Aug. 2007, pp. 943-968.

[12] L. Wang and S.S. Kulkarni, "Sacrificing a Little Coverage Can Substantially Increase Network Lifetime," *Sensor and Ad Hoc Communications and Networks*, Sept. 2006, pp. 326-335.

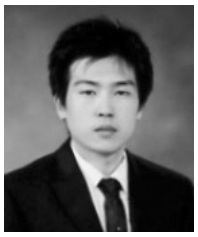
[13] R. Hinden and S. Deering, *RFC 2373: IP Version 6 Addressing Architecture*, IETF, July 1998.

[14] Zhong Fan, "IPv6 Stateless Address Autoconfiguration in Ad Hoc Networks," *PWC*, Sept. 2003, pp. 665-678.

[15] D. Johnson, C. Perkins, and J. Arkko, *RFC 3775 - Mobility Support in IPv6*, IETF, June. 2004.

[16] ZigBee Alliance, ZigBee Specification Document 053474r13, Dec, 2006.

Sooyoung Yang received the BS degree in information and communication engineering from Sejong University, Republic of Korea, in 2007. He is currently a master student with the Department of Infomation and Communication Engineering of Sejong University. His current research interests include MAC and radio resource management in wireless environments.



Sungjin Park received the BS degree in computer engineering from Sejong University, Republic of Korea, in 2007. He is currently a master student with the Department of Infomation and Communication Engineering of Sejong University. His current research interests include embedded network systems.

Eun Ju Lee received the BS and MS degrees in computer engineering from Chungnam National University, Korea, in 1992 and 1994, respectively. Since 1992, she has been with ETRI, Daejeon, Korea. She is currently a senior member of engineering staff. Her current research interests include ubiquitous sensor networks, wireless communication, and WSN applications.

Jae Hong Ryu received the BS degree in electronic engineering from Pusan National University, Busan, Korea, in 1991, and the MS degree in electronic engineering from Chungbuk National University, Korea, in 2005. Since 1991, he has been with LGIC and ETRI Korea. He is currently the senior member of engineering staff. His current research interests include embedded software, ubiquitous sensor networks, and telematics.

Bong-Soo Kim received the BS and MS degrees in electronic engineering from Hongik University, Korea, in 1982 and 1984, respectively. Since 1984, he has been with ETRI, Daejon, Korea. He is currently a principal member of engineering staff. His current research interests include embedded software, ubiquitous sensor networks, and telematics.

Hyung Seok Kim received the BS degree in electrical engineering from Seoul National University, Korea, in 1996, and the MS and PhD degrees in electrical engineering and computer engineering from Seoul National University, in 1998 and 2004, respectively. In 2003 and 2004, he held visiting researcher positions in University of Virginia. From 2004 to 2006, he worked for the Telecommunication R&D Center of Samsung Electronics. He is currently a faculty member with the Department of Information and Communication Engineering of Sejong University. His current research interests include ubiquitous sensor networks, mobile WiMAX, and embedded systems.