

Internetworking Between ZigBee/802.15.4 and IPv6/802.3 Network

Reen-Cheng Wang

Department of Computer Science
and Information Engineering,
National Dong Hwa University
1, Sec. 2, Da Hsueh Rd., Shoufeng,
Hualien, 97401, Taiwan, R.O.C.
+886-3-8632741

rcwang@mail.ndhu.edu.tw

Ruay-Shiung Chang

Department of Computer Science
and Information Engineering,
National Dong Hwa University
1, Sec. 2, Da Hsueh Rd., Shoufeng,
Hualien, 97401, Taiwan, R.O.C.
+886-3-8632031

rschang@mail.ndhu.edu.tw

Han-Chieh Chao

Department of Electronic
Engineering,
National Ilan University
1, Sec. 1, Shen-Lung Rd.,
I-Lan, 260, Taiwan, R.O.C.
+886-3-9357400#251

hcc@niu.edu.tw

ABSTRACT

With the rising demand of home automation and sensor networks, the IEEE 802.15.4 specification outlines a new class of physical and MAC layer protocols targeted at low power devices, personal area networks, and sensor nodes. Based on IEEE 802.15.4, many upper layer protocols are proposed. The ZigBee is the most popular one. However, the ZigBee itself is not compatible with the IP-based network. It is a great challenge to integrate these two kinds of networks together. In this paper, we proposed an internetworking mechanism to overcome this problem. The architecture forms an overlay network on both ZigBee and IPv6 networks and helps the packets to transmit crossover the regions. The design is dedicated to the IPv6 only because many features of IPv6 are used inside the framework.

Categories and Subject Descriptors

C.2.1 [Computer-Communication Networks]: Network Architecture and Design – *Network communications, Wireless communication.*

General Terms

Design.

Keywords

IEEE 802.15.4, IEEE802.3, Interworking, IPv6, ZigBee.

1. INTRODUCTION

With the rising demand for pervasive computing and ubiquitous network access, wireless local area networks (WLANs) become very popular in the past few years. To convey information over relatively short distances, several wireless technologies and wireless personal area networks (WPANs) are proposed and being

extensively discussed. Unlike WLANs, connections effected via WPANs involve little or no infrastructure. This feature allows small, power-efficient, and inexpensive solutions to be implemented for a wide range of devices. IEEE approved the standard for the low-rate WPAN (LR-WPAN) as 802.15.4 [1] in 2003.

Especially designed for low data rate wireless connectivity devices with limited battery consumption, 802.15.4 defines the physical layer (PHY) and medium access control (MAC) sublayer specifications typically operating in the radius of 10m and more. The maximum raw data rate is 250 kb/s to satisfy a set of simple needs such as consumer electronics, home automation, industrial controls, and sensor applications. The specification is focused on low complexity, low cost, low power consumption, and low data rate wireless connectivity among inexpensive devices.

For the same LR-WPAN purpose and based on 802.15.4, the most popular upper layer protocol, ZigBee [2], was developed by the ZigBee Alliance in 2004. The ZigBee protocol standard contains the specifications of the network layer (NWK) and application layer (APL). Inside the APL, functions are defined separately as the application support sub-layer (APS), the ZigBee device objects (ZDO), the ZigBee device profile (ZDP), the application framework (AF), and ZigBee security services. The comparisons of ISO OSI, TCP/IP, and ZigBee/802.15.4 are shown in Figure 1.

Since the TCP/IP has become the dominant protocol in the Internet due to its widespread use and reliability, and also the 802.3 Ethernet is a de facto networking standard, the demand for

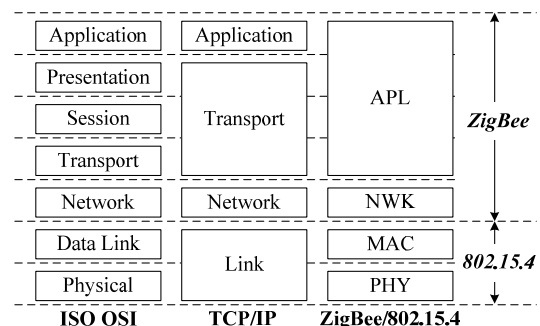


Figure 1. Protocol Stacks Mapping

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

IPv6 '07, August 31, 2007, Kyoto, Japan.

Copyright 2007 ACM 978-1-59593-790-2/07/0008...\$5.00.

internetworking between ZigBee/802.15.4 and TCP/IP/802.3 is inevitable. However, the design of ZigBee/802.15.4 is incompatible with the TCP/IP network. In this paper, we propose an internetworking architecture to overcome this problem. The design is dedicated to IPv6 only because many features of IPv6 are used inside the framework.

The rest of this paper is organized as follows. Section 2 presents an overview of other approaches and their problems. Section 3 outlines some design criteria and our solutions. Section 4 explains our mechanism with examples. And finally, the paper is concluded in Section 5.

2. RELATED WORKS

In this section, we review some related technologies first. Because of the many problems occurred in IPv4, such as the IP address shortage, all the solutions for integrating LR-WPAN and IP are focused on IPv6 only. They include IPv6 over ZigBee, IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [3], IP-Net [4], and a translation solution [5]. The comparisons of the first three protocols are shown in Figure 2. Because 802.15.4 and 802.3 are different at physical layer, it is undoubtedly that there should have an interconnect node, which acts as a gateway between two networks. A simple network diagram is presented in Figure 3 for the following discussions.

2.1 IPv6 over ZigBee

The straight forward method to make IPv6 work over ZigBee is to put the IPv6 stack on the top of ZigBee NWK layer. All the ZigBee nodes are assigned with an IPv6 address. At Gateway B, if a packet is received from the 802.3 network, it will be encapsulated into ZigBee NWK and forwarded to the 802.15.4 network. On the other hand, when a packet is transmitted from Node C to Host A, Gateway B will decapsulate the packet and use the IPv6 payload inside to continue the transmission. Because the data communication in ZigBee/802.15.4 is asynchronous message-passing, only UDP can be used with IPv6 in this scenario.

The key issue of IPv6 over ZigBee is the packet size problem. According to the 802.15.4 specification, the maximum PHY service data unit is 127 bytes. In a data frame, after reducing the 23 bytes MAC header, 2 bytes frame check sequence (FCS), and 8 bytes NWK header, there are only 94 bytes left for the IPv6 packet. If the security mechanism (such as AES-CCM-128) is enabled, only 81 bytes will be left. This is quite tight for an IPv6 packet, which has 40 bytes basic header and even more extension headers. Also, the ZigBee/802.15.4 does not support packet fragmentation. It can not handle the 1280 bytes minimum transfer unit required by IPv6.

ZigBee APL	ZigBee APL	Application Transport	ZigBee APL	Proprietary Applications
ZigBee NWK	IPv6/UDP ZigBee NWK	IPv6 Adaptation	ZigBee NWK	IPv6
802.15.4 MAC	802.15.4 MAC	802.15.4 MAC	802.15.4 MAC	
802.15.4 PHY	802.15.4 PHY	802.15.4 PHY	802.15.4 PHY	
ZigBee	IPv6 over ZigBee	6LoWPAN	IP-Net	

Figure 2. Protocol Stacks of Different Approaches

2.2 6LoWPAN

6LoWPAN is a working group in the IETF. It focuses on defining the transmission of IPv6 Packets over IEEE 802.15.4 networks. As shown in Figure 2, it creates an adaptation layer above the 802.15.4 MAC to support the IPv6 data packet. The adaptation layer is used to handle the packet fragmentation so that an IPv6 packet can be separated into many 802.15.4 frames for transmitting.

The working group lists lots of problems in current development in [6]. Besides, it throws the ZigBee stack away. Without ZigBee NWK, all the routing structures, address assignment, and data forwarding must be redesigned. This poses a great challenge for future realization.

2.3 IP-Net

IP-Net is designed by the Helicomm Inc. and used in their product, IP-Link, which is developed with the Silicon Laboratories Inc. As presented in Figure 2, it is a dual stack approach. Both the 6LoWPAN design and ZigBee stack are working on the same 802.15.4 MAC.

Although it endows a node with both IPv6 and ZigBee functions, only one of them can be used at the same time. Thus, it is not an internetworking solution. Also, it has all the problems that 6LoWPAN has.

2.4 A Translation Solution

The only internetworking mechanism we can find today is in [5]. It is a NAT-PT [7] like solution. Take Figure 3 for example. When the network initiates, Host C must register its IPv6 address (IP_C) to pre-assigned Gateway B (IPv6 address: IP_B ; ZigBee address: Z_B). B will help C to get its ZigBee address (Z_C). Node A must register its ZigBee address (Z_A) to B, too. If A wants to communicate with C, it sends out the packet to Z_C . B will translate the packet into IPv6 format with "Destination IP address = IP_C " and "Source IP address = IP_B ". In the reverse path, for communicating from C to A, A will send the packet to IP_B with a data payload which contains "Destination ZigBee address = Z_C " and "Source ZigBee address = Z_A ". After B receives the packet, it decapsulates the packet, looks for the payload, and translates it to 802.15.4 format.

The framework works. But users must pre-configure their hosts with fixed gateway address. The NAT-PT like design also breaks

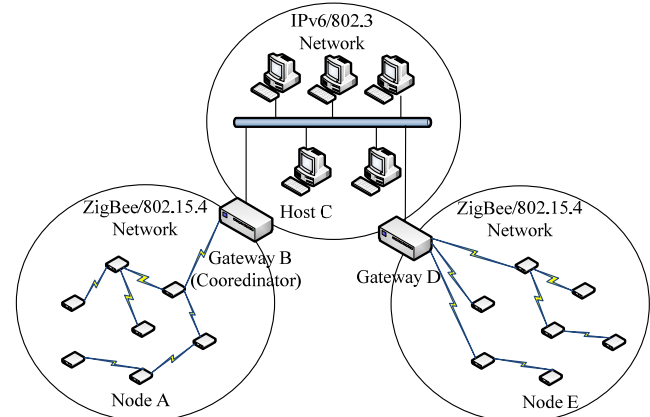


Figure 3. Network Diagram

many end-to-end features such as information security. Service discovery, one of the most important functions in ZigBee network, is unsolved. Also, the mechanism can not perform cross regions transmission, such as the communication between A and E.

Because all the mechanisms above are not proper to integrate ZigBee/802.15.4 and IPv6/802.3 networks together, we design a novel overlay mechanism for the internetworking.

3. THE OVERLAY INTERNETWORKING DESIGN

In this section, we will state the design criteria and our solutions for each criterion.

Design Criteria:

- C.1. Each ZigBee node should be assigned with a global unicast IPv6 address.
- C.2. Each IPv6 host which may communicate with ZigBee node should obtain a ZigBee address.
- C.3. Service discovery should be propagated to different network domain.
- C.4. Broadcast data in ZigBee network should be transferred to proper IPv6 hosts.
- C.5. Data packet transformations in the gateways should be as simple as possible and should not break the end-to-end model above the transport layer.

To satisfy the above criteria, we integrate many techniques to form an overlay network. The details are discussed in the following.

3.1 IPv6 Prefix Delegation [8][9]

To keep the end-to-end communication model between hosts and nodes, we would like to assign each ZigBee node with an IPv6 address. Although the gateway at the edge is a more powerful ZigBee device with Ethernet interface, it is still hard to guarantee that the gateway can perform all the functions of a classical IPv6 router, running the RIPng or OSPFv3. Thus, we make the gateway support the IPv6 prefix delegation function and act as a requesting router. With the delegated prefix, every ZigBee device can have its own IPv6 address. It is obvious that ZigBee nodes can not perform IPv6 Stateless Autoconfiguration, and also the nodes may not have enough memory to keep its IPv6 address. The address assignment is done in a simple mapping method shown in Figure 4. This mapping mechanism is very useful when a packet is transferred from an IPv6 host to a ZigBee node. The gateway can easily remove the prefix part of the destination address and get the destination ZigBee address. It is not necessary to parse the payload to get the information about the real destination. The IPv6 address does not really exist on the ZigBee nodes. It is only

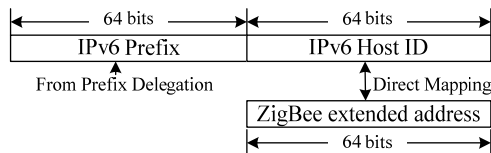


Figure 4. IPv6 Address Assignment to ZigBee nodes

a pseudo address at the gateway. Thus, the gateway can ignore the processes such as sending out a Prefix Advertisement to the 802.15.4 side after prefix delegation received. Also, the ZigBee extended addresses are globally unique so that we can guarantee the mapping addresses will not conflict with each other even without IPv6 duplicate address detection (DAD) process. This will solve criteria C.1 and part of C.5.

3.2 UPnP [10]

UPnP is used to solve both criteria C.2 and C.3.

3.2.1 UPnP with C.2

When an IPv6 host wants to join a ZigBee network, it must find a ZigBee coordinator to obtain its ZigBee address. The PAN ID is the keyword of the type of device in UPnP SSDP (Simple Service Discovery Protocol) discovery. When a gateway receives the SSDP discovery, it will transform the packet to ZigBee Service Discovery format and pass it to the 802.15.4 network. The transformation will keep the record in a table for a period so that the response ZigBee address assignment packet can reply to the proper IPv6 host.

3.2.2 UPnP with C.3

UPnP is also used in the two way service discoveries when an IPv6 host or a ZigBee node wants to find some services in another network. In this case, the service discovery functions which are defined in ZDO will be transformed to the XML format at the gateway for the SSDP discovery and vice versa.

With UPnP, the network will be more flexible. We do not have to manage a lot of pre-assigned parameters such as gateway address at the beginning.

3.3 IPv6 Multicast

Because ZigBee is an ad-hoc wireless network, it has to support the broadcast function for many purposes. For example, the beacon frame is this kind of packet without specific destination. This raises a problem while IPv6/802.3 hosts join in the ZigBee network. If we transform all the broadcast messages in the ZigBee network and the all node multicast messages in IPv6 network to each other, the huge amount of IPv6 all node multicast message will crash the low data rate ZigBee network. Thus, we set up an IPv6 multicast group for each PAN ID. The gateway which is at

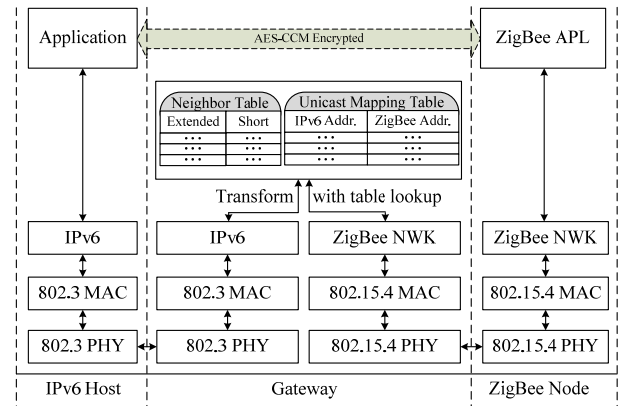


Figure 5. IPv6 Address Assignment to ZigBee nodes

the same network of the coordinator (such as the Gateway B) will act as the rendezvous point of the multicast group. This can satisfy criterion C.4.

3.4 Extended IP Switching [11]

Now all the nodes in the ZigBee network have their ZigBee and IPv6 unicast address, all the gateways has their ZigBee, IPv6 unicast, and IPv6 multicast address, and all the hosts in the IPv6 network have their ZigBee, IPv6 unicast, and IPv6 multicast address. The ZigBee network and IPv6 network are overlaid together. The last thing we want to do is to accelerate the transforming speed for data packet and also keep the end-to-end security.

Unlike the [5], we use an IP-switching like mechanism to accomplish our purpose. All the data packet transformations are done below the network and the NWK layer, with simple header replacement just as IP Switching does. Without digging information from APL payload, the replacement will work with a simple table lookup. Because the entire NWK payload can keep untouched, we can enable the AES-CCM at APL layer to safeguard our data security. This fulfills criterion C.5.

4. EXAMPLES OF TRANSMISSION FLOWS

The protocol stack of our mechanism is presented in Figure 5. Use the network diagram in Figure 3 as an example. Three kinds of flows are discussed in this section to explain more details about our mechanism.

4.1 From ZigBee/802.15.4 to IPv6/802.3

Figure 6 shows the process of Node A (ZigBee/ 802.15.4) communicating with Host C (IPv6/802.3) through Gateway B.

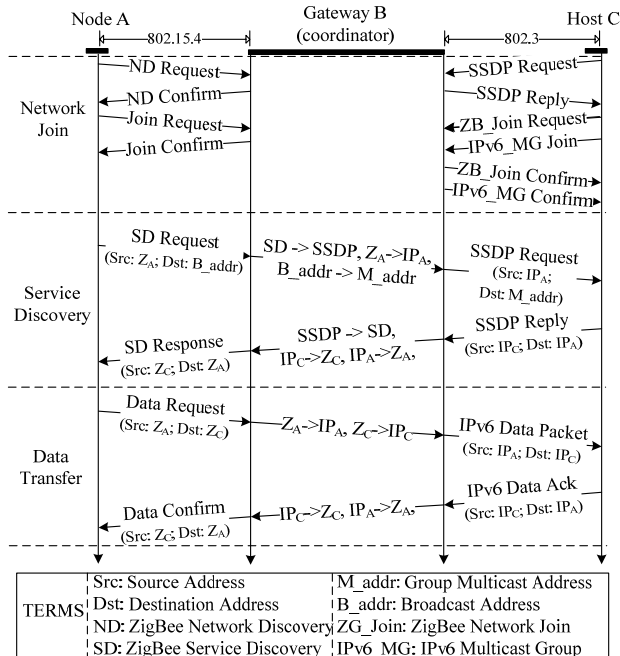


Figure 6. From ZigBee/802.15.4 to IPv6/802.3

Network Join is the necessary initiation step to form a ZigBee network. Because B is set up to be the coordinator, all nodes have to send their Join Request to B. From the viewpoint of A, B is at the same ZigBee network as A. Thus, the join process follows the ZigBee standard. The extended ZigBee address of A is fixed on the chip as the MAC address of an Ethernet network interface card. The network discovery (ND) Request/Confirm process is used to scan the wireless communication channel. And Join Request/Reply helps A to get its short ZigBee Address. Both extended and short ZigBee address of A are defined as Z_A because ZigBee can use any of them. At the same time, B will build up a pseudo IPv6 address IP_A (IPv6 Prefix from prefix delegation + Extended ZigBee Address of A) in its Unicast Mapping Table for A.

Besides, from the viewpoint of C, it has its own IP_C without any information about the coordinator at the beginning. The UPnP SSDP Request can help C to lookup the coordinator B in the IPv6 network. Because C is in a wire network, the ND Request/Confirm process can be ignored. C is a host (not a gateway) so that the Join Request will indicate it as "End node" type. This is used for the CSKips algorithm to calculate the ZigBee short address for C. The Join Reply will assign a short ZigBee address Z_C to C and record the mapping $IP_C \rightarrow Z_C$ in the unicast mapping table in B. At the same time, IPv6 Multicast Group Join/Confirm will assign an IPv6 Group Multicast Address to C for the ZigBee broadcast message purpose.

The transmission process starts from ZigBee service discovery. A would like to access a service which C has, but A does not know it. A performs a standard broadcast ZigBee service discovery to all nodes. When B receives the packet, it transforms the SD request to SSDP Request message by mapping the source address to IP_A and destination address to IP_A Group Multicast Address. C will receive this multicast packet. C knows it can provide the service that A wants, so it replies to IP_A with a confirmation. B will transform this SSDP reply to SD response format by mapping all the IPv6 address in network layer header to ZigBee address in the NWK header.

When the peering is set up, the data transmission is quite simple. A sends out a packet to Z_C directly. B will transform the packet to IP_C with simple header replacement. The acknowledge (Ack) message from C will reply to IP_A , which is also simply transformed by B to A. The only thing should be mentioned here is that the IPv6 Data Ack is not the TCP acknowledgment packet. Because ZigBee network is connectionless and transmits via message passing, the IPv6 Data Ack must be handled by the application layer so that the TCP timeout and the retransmission problems will not occur.

4.2 From IPv6/802.3 to ZigBee/802.15.4

Figure 7 shows the reverse path communication which is initiated by Host C (IPv6/802.3) through the Gateway B to the Node A (ZigBee/802.15.4).

The network join process is the same so that we will not explain it again. The same as previous scenario, C has no idea that A owns the matched service in the beginning. The service discovery is started from C sending out an SSDP request message. When the Gateway B gets the request packet, it then transforms the packet to broadcast ZigBee Service Discovery format with the source

address mapped to Z_C . A will get the SD request, finds out that it has the service, and replies with an SD response. When the response packet reaches B, it then transforms it to a unicast SSDP reply format, with the address mapping $Z_C \rightarrow IP_C$ and $Z_A \rightarrow IP_A$. After C receives the SSDP reply, the peering connection is established.

Now, A can start to transfer messages to C. The data packet is a standard IPv6 packet, with the payload containing ZigBee APL data type which is used to communicate with ZDO or ZDP. This is implemented in the application layer in hosts. The benefit of the payload following the ZigBee specification is to keep the security and limit the packet length so that it will not be too large while in transformation. The gap between ZigBee APL data size (94 bytes) and IPv6 MTU in 802.3 (1280 bytes) is filled with zero so that the gateway can transform the payload with just simply discard the filler bits. B will replace the IPv6 Header with ZigBee NWK header and forward the packet. After A gets the data, a Data Confirm will be sent back to Z_C . B will replace the ZigBee NWK Header with IPv6 header. All the necessary information can be found in its unicast mapping table. Finally A gets the confirmation and the transition then finishes.

4.3 Cross Regions Example

The last flow we would like to show is a cross regions communication. The data goes from a ZigBee/802.15.4 network, through an IPv6/802.3 network, and reaches a node in another ZigBee/802.15.4 network. An example is shown in Figure 8 when Node A communicates with the Node E through Gateway B and Gateway D.

The network begins with network join. A joins the ZigBee network using the standard procedure. D is a gateway which is also a ZigBee node and has to join the network. From the viewpoint of the coordinator B, D is from an 802.3 network. So the join process is the same as an IPv6 host does, such as the

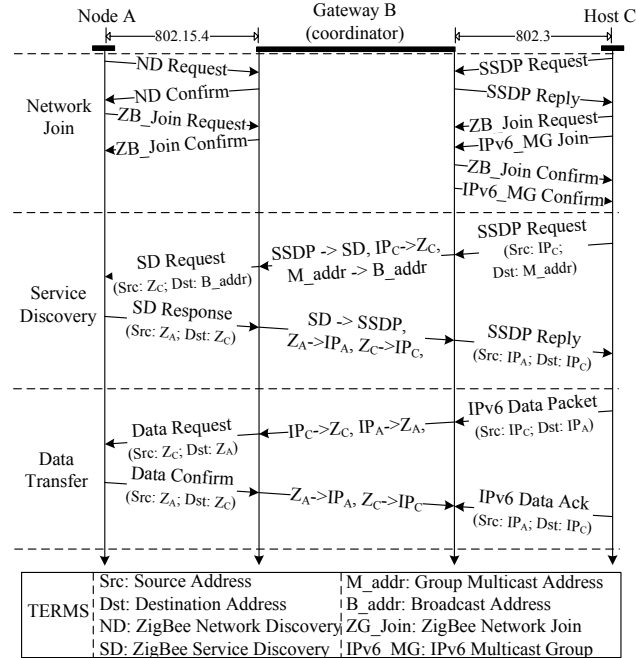


Figure 7. From IPv6/802.3 to ZigBee/802.15.4

Host C's process in Section 4.1. The difference is that D is a gateway, which must indicate itself as "Router node" type in the Join Request. This makes some differences in ZigBee address assignment based on the CSkip algorithm. Also, it has to synchronize with the coordinator gateway periodically to get the updated unicast mapping table. The joining of E is a little different. E sends out an ND Request, which D will handle and response the ND Confirm. After that, E sends out its Join Request. Because D already knows where the coordinator is, D will replace the NWK header with IPv6 header and forward the packet to B. B will treat E as an IPv6 host and assign a ZigBee short address to E in the Join Confirm. Because D has already joined the IPv6 multicast group, it is not necessary to do again while E joins the network.

The service discovery processes are not much different. A sends out a broadcast SD Request. B transforms it to the SSDP Request with multicast. And D transforms the packet again to the broadcast SD Request. After E matches the service, it sends back an SD Response. D transforms it to the SSDP Response with destination address IP_A . B transforms it to the SD Response with destination address Z_A . A gets the packet at the end and establishes the peering.

The data communication now can start. A sends out the data request to Z_E directly. B replaces the NWK and forwards to IP_E . D replaces IPv6 header to NWK header with destination to Z_E . Then E will receive the data. The Data Confirm is sent to Z_A , which converts to IP_A at D and back to Z_A at B.

All the above examples show our mechanism is working in ZigBee/802.15.4 to IPv6/802.3, IPv6/802.3 to ZigBee/802.15.4, and cross regions scenarios.

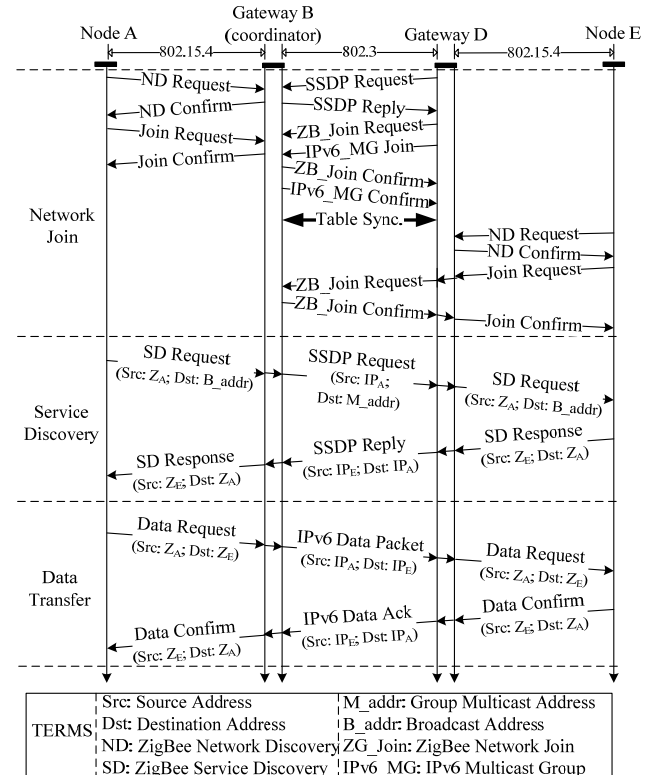


Figure 8. Cross regions

5. CONCLUSIONS

In this paper, we present a novel gateway design which can overlay the ZigBee/802.15.4 and the IPv6/802.3 networks together and internetworking among them. It can easily be extended to all kind of IPv6 networks such as IPv6/802.11, IPv6/UMTS, etc. Unlike the IPv6/802.15.4 which is discussed by IETF 6LoWPAN working group or the ZigBee bridge mode which is drafted by ZigBee Alliance to connect two ZigBee networks together, our mechanism is operative not only between ZigBee/802.15.4 and IPv6/802.3 but also multiple ZigBee/802.15.4 networks connected by IPv6/802.3 networks.

In our design, each ZigBee devices is assigned with a Global Unicast IPv6 address so that every IPv6 node can communicate with it directly. On the other hand, each IPv6 node who wants to communicate with the ZigBee devices is also assigned with a ZigBee short address. The IPv6 Multicast Group is also established in all correlated IPv6 nodes for relaying broadcast messages from ZigBee network.

From the viewpoint of a ZigBee node, every IPv6 host is like another ZigBee node because it has a ZigBee address for communication. Besides, from the viewpoint of an IPv6 host, every ZigBee nodes is like another IPv6 host because it has an IPv6 address. The gateways will handle all the transformation. All the other ZigBee nodes and IPv6 hosts can keep unchanged. The design is quite useful for connecting the two kinds of networks.

The mechanism works on Layer 3 and below so that it can keep the APL layer security if needed. However, a known problem is the "address in address" issue. Future ZigBee profiles may contain address information inside the APL layer. This is like the application layer gateway (ALG) problem in the IPv4/IPv6 NAT-PT design. It is a future work.

6. ACKNOWLEDGEMENT

The research is supported by Taiwan NICI IPv6 Steering Committee.

7. REFERENCES

- [1] *Standard 802.15.4-2003, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)*. IEEE, May 2003.
- [2] *ZigBee Specification Version 1.0*. ZigBee Alliance, December 2004.
- [3] Montenegro, G., Kushalnagar, N., Hui, J., and Culler, D. *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*. IETF Internet Draft draft-ietf-6lowpan-format-13 (work in progress), April 2007.
- [4] Karayannis, G. *IPv6 over IEEE 802.15.4*, IETF 61st meeting presentation, November 2004.
- [5] Sakane, S., Ishii, Y., Toba, K., Kamada, K., and Okabe, N. A translation method between 802.15.4 nodes and IPv6 nodes. In *Proceeding of the International Symposium on Applications and the Internet Workshops 2006 (SAINT 2006)* (Phoenix, Arizona, USA, January 23-27, 2006), 34-37.
- [6] Kushalnagar, N., Montenegro, G., and Schumacher, C. *6LoWPAN: Overview, Assumptions, Problem Statement and Goals*. IETF Internet Draft draft-ietf-6lowpan-problem-08 (work in progress), February 2007.
- [7] Tsirtsis, G., and Srisuresh, P. *Network Address Translation - Protocol Translation (NAT-PT)*. IETF RFC 2766, February 2000.
- [8] Troan, O., and Droms, R. *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*. IETF RFC 3633, December 2003.
- [9] Miyakawa, S. and Droms, R. *Requirements for IPv6 Prefix Delegation*. IETF RFC 3769, June 2004.
- [10] *UPnP Device Architecture*. UPnP Forum, June 2000.
- [11] Newman, P., Lyon, T., and Minshall, G. Flow Labelled IP: A Connectionless Approach to ATM, In *Proceeding of IEEE Infocom 1996*, (San Francisco, CA, USA, March 24-28, 1996), 3, 1251-1260.