Hindawi
Journal of Sensors
Volume 2018, Article ID 3176967, 9 pages
https://doi.org/10.1155/2018/3176967

Research Article

Efficient Heterogeneous Network-Routing Method Based on Dynamic Control Middleware for Cyber-Physical System

Hyungsoo Lee, Jaehwan Lee, Sanghyuck Nam, and Sangoh Park

School of Computer Science and Engineering, Chung-Ang University, Seoul 06974, Republic of Korea

Correspondence should be addressed to Sangoh Park; sopark@cau.ac.kr

Received 22 February 2018; Accepted 23 April 2018; Published 20 May 2018

Academic Editor: Ka L. Man

A cyber-physical system depends on stable control and interaction between the many systems and devices connected to the network. Dynamic control middleware, which considers the characteristics of a cyber-physical system, supports the dynamic search and control of devices existing on the global network using Internet protocol version 6 (IPv6). However, systems and devices may connect to a network using a variety of heterogeneous protocols, not just IPv6. To solve the problem of heterogeneous protocols, this paper proposes a routing technique which enables network devices to communicate using different protocols. The proposed network-routing module can register devices with various protocols and improve the stability of the efficient heterogeneous network.

1. Introduction

Cyber-physical systems (CPS) [1–7] consider the physical characteristics of the embedded system. A CPS depends on stable control and interaction between the many systems and devices connected to the network. Thus, CPS enables the convergence of the varied components of information technology (IT) that are crucial to every industry, including energy, transportation, health care, and defense. Therefore, a CPS can facilitate the construction of a network that can contain a large area. Unlike existing middleware [8–10], dynamic control middleware (DCM) [4] efficiently constructs a large-scale network using an Internet protocol version 6- (IPv6-) based two-layer architecture that supports dynamic search and control of networked devices. However, real-world systems and devices connect to the network using numerous heterogeneous protocols rather than a single protocol. For example, the myriad of small devices employed in health care use a variety of protocols. However, existing DCM does not support these varied heterogeneous protocols. Therefore, to connect devices that use heterogeneous protocols, middleware must provide a routing method that enables various protocols to communicate with each other. Furthermore, health care devices are frequently connected and disconnected from the network owing to frequent movements. This paper suggests providing a dynamic reconfiguration method to stabilize the network by addressing the errors caused by frequent and unanticipated device connections and disconnections. In this paper, we propose extended middleware that can register heterogeneous devices as components of DCM using a variety of protocols such as IPv6, Bluetooth, and ZigBee. To improve the stability of the efficient heterogeneous network, this paper also suggests a mechanism to dynamically reconfigure the network even if the controller responsible for the intermediate node in the routing path is unexpectedly removed from the network due to unanticipated errors.

This paper is organized as follows. In the next section, we discuss related research. The Materials and Methods is comprised of three subsections: Subsection 3.1 introduces an extended DCM system with a novel network-routing module that supports various heterogeneous network protocols. Subsection 3.2 of Materials and Methods explains how to construct the routing table when inserting or deleting nodes. Subsection 3.3 introduces a testbed that creates a hybrid network environment which combines several heterogeneous

protocols. Here, we demonstrate that a message can be normally delivered. Section 4 presents conclusions and future research topics.

2. Related Work

Dynamic control middleware (DCM) efficiently controls connected devices throughout the IPv6-based global network, across all temporal and physical conditions. To search efficiently, DCM has a two-layer logical architecture consisting of a lower layer and an upper layer. The lower layer consists of control devices (CDs) connected to each local network, and the upper layer consists of control device managers (CDMs) that manage information from lower-layer devices. The upper layer can reduce the number of messages by only sending messages to devices belonging to the same IPv6 multicast group. In addition, because DCM has a two-layer architecture, and not a centralized server structure, devices can discover, search, and control other devices through multicasting, regardless of their global network location. However, DCM supports only IPv6 and in real-world applications, networked systems and devices often use different heterogeneous protocols.

Object-based middleware for smart home network (OSHNet) [11] supports interoperability regardless of device protocols using a device-routing table (DRT). However, although the DRT can deliver messages to other smart devices in the home, it cannot control external devices on the global network.

3. Materials and Methods

3.1. Extended DCM. Figure 1 diagrams the architecture of the proposed extended DCM (EDCM). The EDCM added a network-routing module so that CDs that do not support IPv6 can control each other with other devices. The network-routing module determines the path of the message and selects the appropriate network protocol for each transmission. The EDCM proposed in this paper can support various network protocols including IPv4, Bluetooth, ZigBee, and IPv6. In this subsection, we examine the four components that comprise the network-routing module.

3.1.1. Routing Mapper. The routing mapper identifies the destination of the message delivered from the upper layer of the EDCM. After referring to the routing table, the routing mapper maps the route to the message destination and adds it to the head of the message.

Table 1 shows an example of a routing table. The "Source" is the starting node. The "Destination" is the destination node. The "Interface" is the network protocol used to transmit messages between the two nodes. The "Source address" is the address of the starting node, and the "Destination address" is that of the destination node.

Box 1 shows an example of the content added by the routing mapper to the message head. Line 01 is the number of remaining routes to the destination node. Line 02 and Line 03 indicate the starting and destination nodes, while Line 04 through Line 24 store the mapping information in the routing table. Each time a message passes through an intermediate node, the number of routes in Line 01 is decremented by one, and one instance of routing table tag data is removed from the set represented between Line 04 and Line 24.

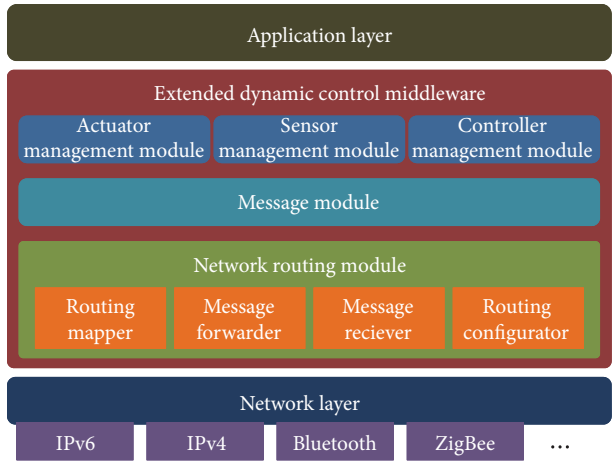

Figure 1: Extended DCM architecture.

Figure 2 shows a flowchart of the routing mapper. The routing mapper receives the message (MSG) from the upper layer. If the command of the MSG is "CDM Search Request," the routing mapper generates a "CDM Route Search Request" (CSRQ) message to obtain the route from the other CD to the CDM. Then, the message is forwarded to the message forwarder. At this time, the RouteCfg of the CSRQ message is changed to "true" to send the message to the routing configurator when the message arrives at another CD. The CD that sent the CSRQ message checks if there is routing information in the routing table to communicate with the CDM. If the required routing information is in the table, then the MSG is forwarded using the message forwarder.

3.1.2. Message Forwarder. Figure 3 shows a flowchart of the message forwarder. The message forwarder receives the MSG from the routing mapper or message receiver. The message forwarder extracts the NextRoute from the MSG and delivers the MSG based on the extracted information. At this time, the network protocol to be used is determined according to the information of the NextRoute.

If the message transmission fails, a new routing path is established using the CSRQ message to reconfigure the path currently connecting the CDMs. The message forwarder then retransmits the MSG using the modified routing information.

3.1.3. Message Receiver. Figure 4 shows a flowchart of the message receiver. The message receiver receives the MSG through various communication protocols such as IPv6, Bluetooth, or ZigBee. If MSG.Route is nonzero, the MSG is passed to the next path through the message forwarder. If MSG.Route is zero, the message receiver checks whether MSG.RouteCfg is "True" or "False." If "True," the MSG is a message related to the routing configuration and is forwarded to the routing configurator. If "false," the MSG is a generic message and is forwarded to the upper layer.

Table 1: Example of routing table.

Source	Destination	Interface	Source address	Destination address
CDM	CD-1	IPv6	2001:1F00:388::2	2001:1F00:388::3
CD-1	CD-2	Bluetooth	01:23:45:67:89:AB	01:23:45:67:89:AC
CD-2	CD-3	ZigBee	1001	1002

```
01: <Route>3</Route>
02: <Src>CDM</Src>
03: <Dest>CD-3</Dest>
04: <Routing_Table>
05:       <Src>CDM</Src>
06:       <Dest>CD-1</Dest>
07:       <Interface>IPv6<Interface>
08:             <Src_Address>2001:1F00:388::2</Src_Address>
09:             <Dest_Address>2001:1F00:388::3</Src_Address>
10: </Routing_Table>
11: <Routing_Table>
          <!– CD-1 to CD-2 –>
17: </Routing_Table>
18: <Routing_Table>
          <!– CD-2 to CD-3 –>
24: </Routing_Table>
          <!– End of Routing Table Part –>
```

Box 1: Routing table part in extended dynamic control middleware (ECDM).

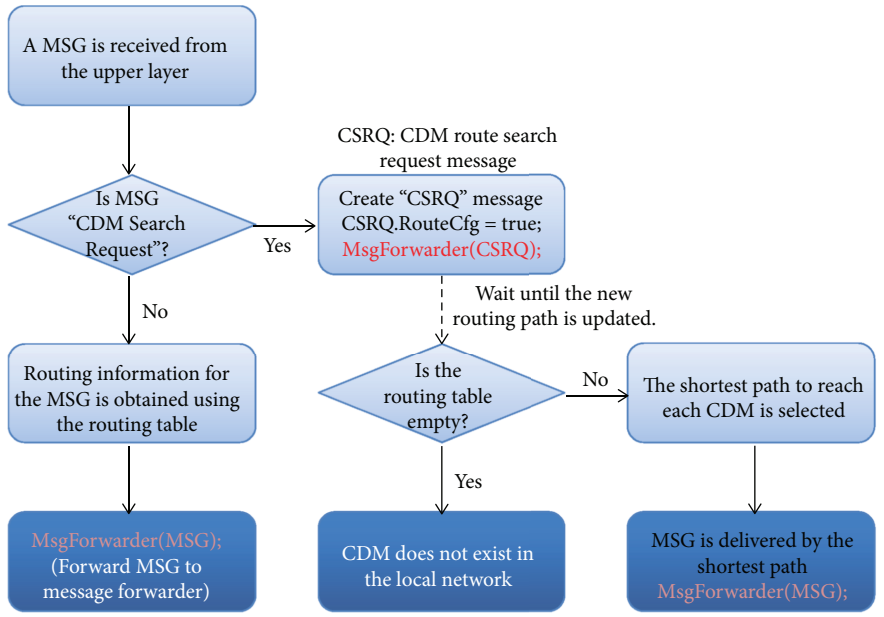

Figure 2: Flowchart of the routing mapper.

3.1.4. Routing Configurator. Figure 5 shows the flowchart of the routing configurator. The routing configurator that receives the MSG from the message receiver determines whether MSG is a CSRQ message. In the case of a CSRQ message, a "CDM Route Search Response" (CSRP) message is created. The CSRP message includes route information from the current controller to the CDM. In the case of a CSRP message, the routing configurator checks whether there is an existing CDM route. If no route exists, the route obtained from the CSRP message is stored in the routing table. If the routing table has an existing route, the length of the route obtained from the CSRP message is compared with that of the existing route. The shorter of the two compared routes is then stored or retained in the routing table.

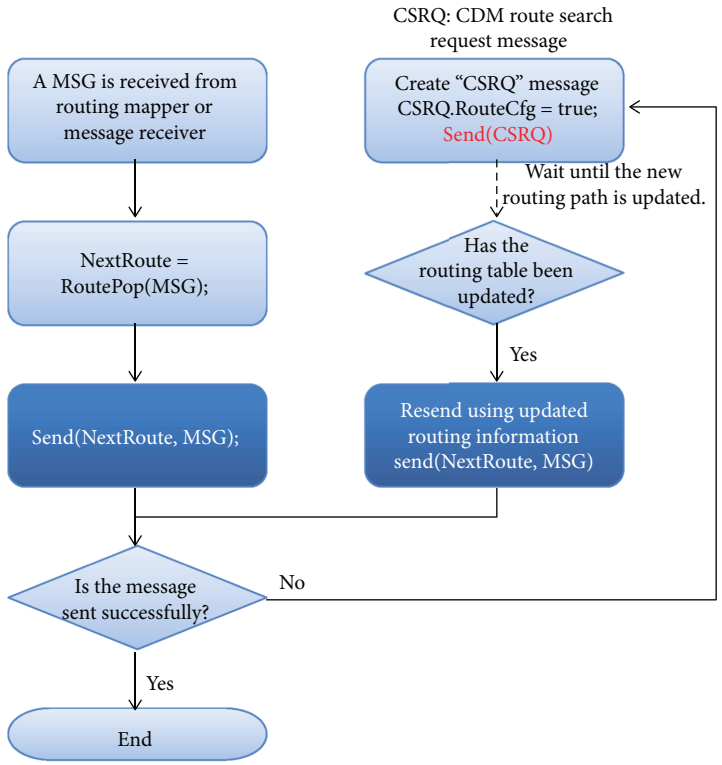

Figure 3: Flowchart of the message forwarder.

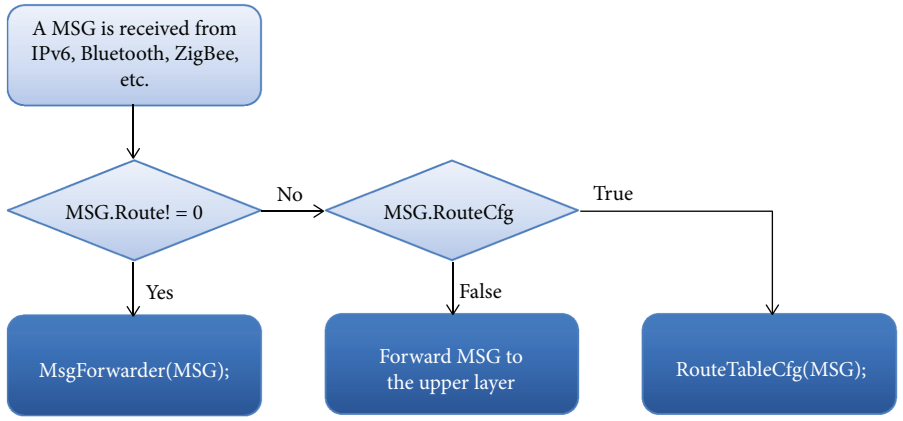

Figure 4: Flowchart of the message receiver.

3.2. Routing Table Configuration Policy. When a new CD is connected to a local network in the DCM, all CDs and CDMs use the same network protocol, IPv6, so the new CD sends a direct message to the CDM to register as a lower node of the CDM. However, although the DCM may support heterogeneous networks, the CDM may not support the specific network protocols used by the new CD.

Figure 6 shows an example of a CDM configuration in an EDCM regional network. Figure 6 assumes that CD-1 and CD-2, and CD-2 and CD-3, share physical proximity close enough to allow wireless transmission. The configuration also assumes that the CDM supports only IPv6, while CD-1 supports IPv6 and Bluetooth, CD-2 supports Bluetooth and ZigBee, and CD-3 only supports ZigBee. In this scenario, because CD-2 and CD-3 do not support IPv6, they cannot directly exchange messages with the CDM. Thus, CD-2 and CD-3 can only send and receive messages to and from the CDM by routing through one or more other CDs that directly or indirectly connect to the CDM. As shown Figure 6, CD-2 can indirectly connect to the CDM by using Bluetooth to connect to CD-1, which has a direct IPv6 connection to the CDM. Extending the concept of indirect connection, CD-3 can be indirectly connected to the CDM by connecting to CD-2 using ZigBee and then following the previously described connections from CD-2 to CD-1 to the CDM.

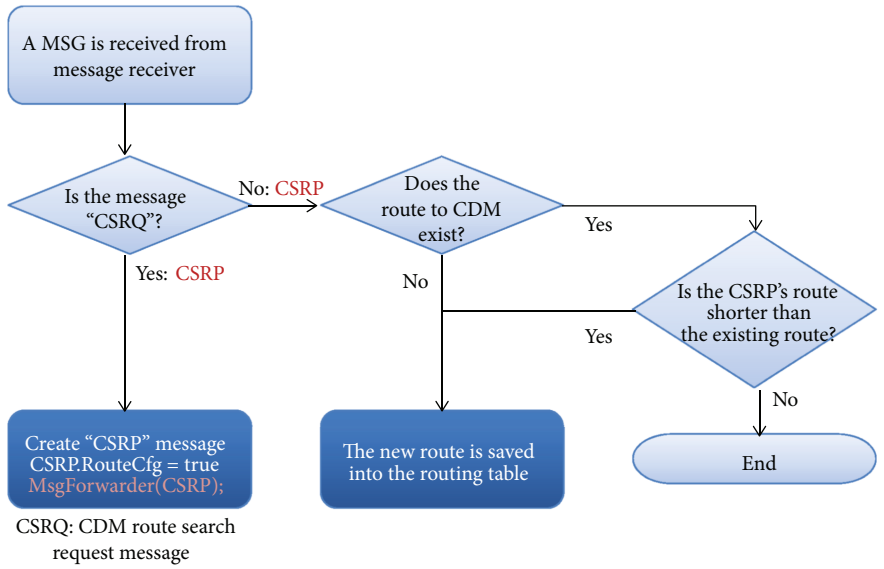

Figure 5: Flowchart of the routing configurator.

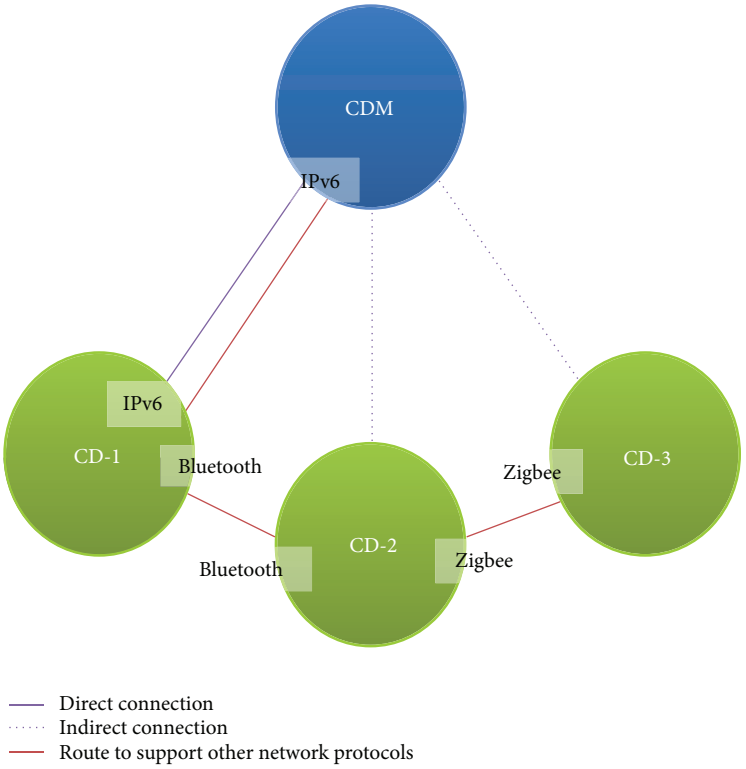

Figure 6: CDM configuration in ECDM local network.

Table 2: CD-1 routing table.

Source	Destination	Interface	Source address	Destination address
CDM	CD_1	IPv6	2001:1F00:388::2	2001:1F00:388::3

Tables 2–4 are the routing tables held by each CD. This routing table enables direct and indirect message transmission between CDM and CD.

The following subsections describe the network topology reconfiguration technique applied to solve the problems that occur when a new CD is connected and other connected CDs

Table 3: CD-2 routing table.

Source	Destination	Interface	Source address	Destination address
CDM	CD-1	IPv6	2001:1F00:388::2	2001:1F00:388::3
CD-1	CD-2	Bluetooth	01:23:45:67:89:AB	01:23:45:67:89:AC

Table 4: CD-3 routing table.

Source	Destination	Interface	Source address	Destination address
CDM	CD-1	IPv6	2001:1F00:388::2	2001:1F00:388::3
CD-1	CD-2	Bluetooth	01:23:45:67:89:AB	01:23:45:67:89:AC
CD-2	CD-3	ZigBee	1001	1002

Figure 7: New controller device connection in heterogeneous networks. (a) A new CD, CD-4, is connected to the EDCM. (b) CD-1 responds to CD-3. (c) A routing path is completed between CD-4 and the CDM.

Table 5: CD-4 routing table.

Source	Destination	Interface	Source address	Destination address
CDM	CD-1	IPv6	2001:1F00:388::2	2001:1F00:388::3
CD-1	CD-4	Bluetooth	01:23:45:67:89:AB	01:23:45:67:89:AD

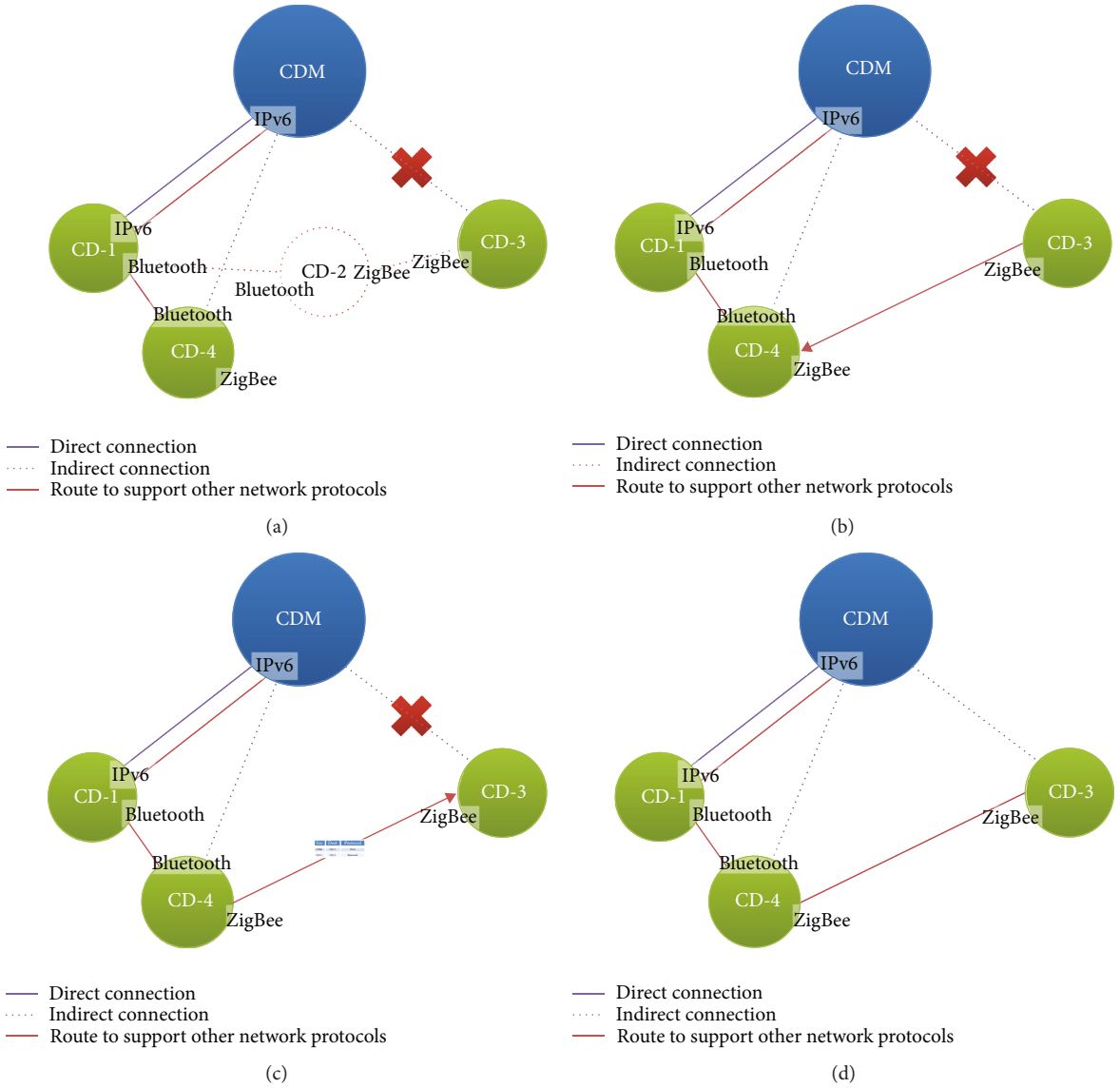

Figure 8: Dynamic reconfiguration in heterogeneous networks. (a) Intermediate node CD-2 is disconnected. (b) CD-3 searches for a new connection using broadcasting. (c) CD-4 transmits its routing table to CD-3. (d) CD-3 establishes a new routing path through CD-4.

are abnormally terminated. The proposed network topology reconfiguration technique is based on the CDM configuration shown in Figure 6.

3.2.1. New Controller Connection. Figure 7(a) depicts a new CD, CD-4, connecting to the EDCM local network. Since CD-4 does not support IPv6, CD-4 registers with the CDM by transmitting its information to the network indirectly through the other connected CDs using Bluetooth and ZigBee connections.

Figure 7(b) shows the responses of the other CDs to CD-4. After receiving the connection message of CD-4, CD-1, CD-2, and CD-3 all transmit their routing table information to CD-4. CD-4 receives the routing table information previously detailed in Tables 2–4 from all three CDs. If a message is sent over the routing path of CD-1, it reaches the CDM in two hops. However, if a message is transmitted through the routing paths through CD-2 or CD-3, two to four hops may be required. Therefore, CD-4 selects the shortest route, consisting of the fewest hops, and the routing table shown

Table 6: New routing table of CD-3.

Source	Destination	Interface	Source address	Destination address
CDM	CD-1	IPv6	2001:1F00:388::2	2001:1F00:388::3
CD-1	CD-4	Bluetooth	01:23:45:67:89:AB	01:23:45:67:89:AD
CD-4	CD-3	ZigBee	1003	1002

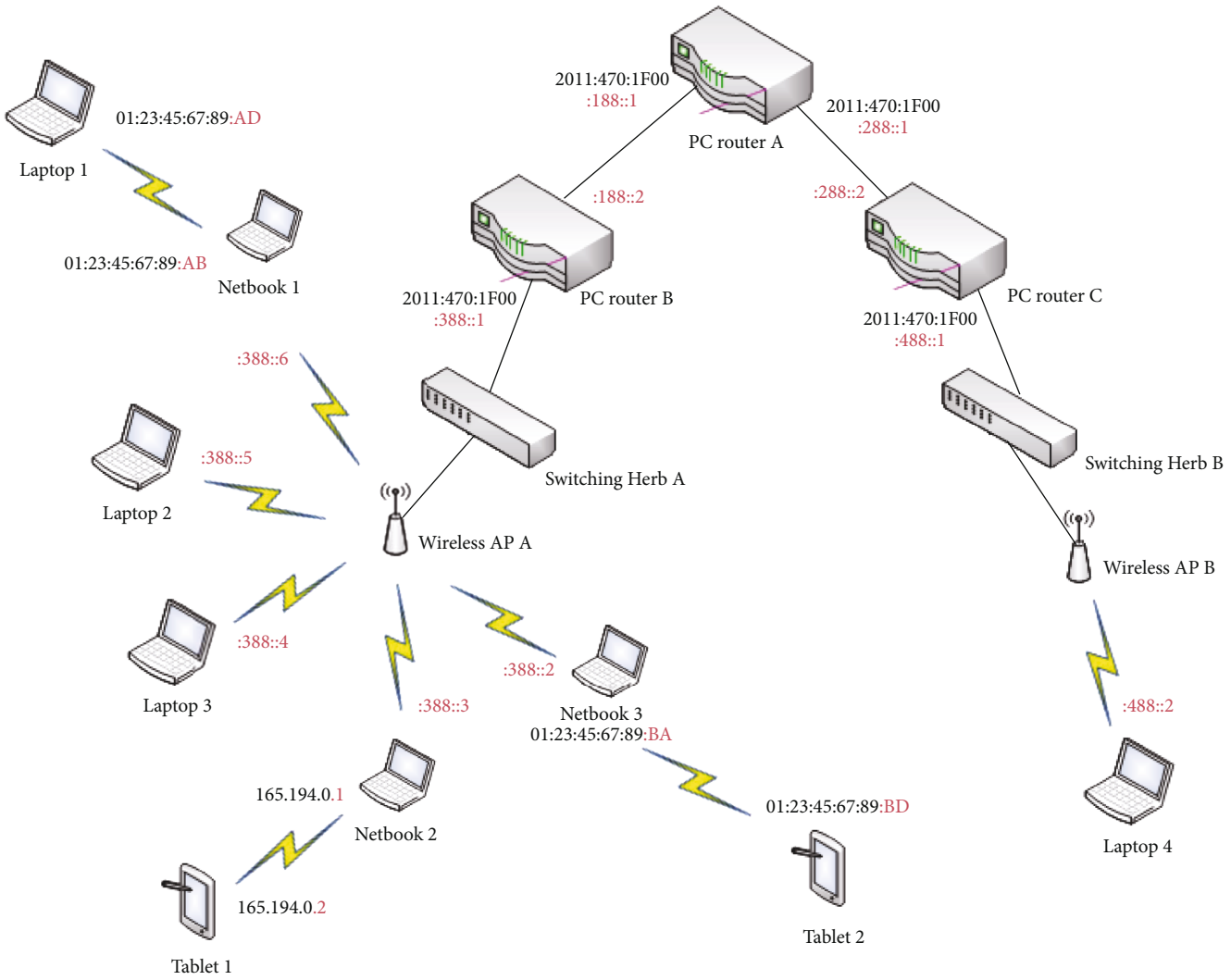

Figure 9: Testbed heterogeneous network-routing model.

in Table 5 is created for CD-4. Figure 7(c) shows that the routing path between CD-4 and the CDM is complete. This allows the CD-4 to communicate indirectly with the CDM via CD-1.

3.2.2. Dynamic Reconfiguration. Figure 8(a) shows that if an intermediate node is released, any CDs indirectly connected to the CDM through that node cannot communicate with the CDM. Therefore, the middleware must be able to dynamically reconfigure the network topology. Figure 8(b) shows that CD-3, which has an error in one of its intermediate nodes, searches for neighboring CDs by broadcasting, and requests the routing table of CD-4. Figure 8(c) depicts CD-4 transmitting its routing table to CD-3. Figure 8(d) displays the new, completed path established by CD-3. In Figure 8, CD-3 appears to only receive CD-4's routing table, but it actually receives the routing table from each CD that received its broadcast search message. CD-3 selects the routing table of CD-4 because it provides the shortest routing path to connect with the CDM. A new routing table for CD-3 is generated as shown in Table 6.

3.3. Performance Evaluation. To test the EDCM proposed in this paper, we constructed the testbed environment illustrated in Figure 9. To represent the global network, two regional networks were constructed using three PC routers

with XORP [12] router software installed. We used four laptops, three netbooks, and two tablets as EDCM CDs.

This test bed assumes that Laptop 1 uses Bluetooth, Laptops 2, 3, and 4 use IPv6, Netbooks 1 and 3 use IPv6 and Bluetooth, Netbook 2 uses IPv6 and IPv4, Tablet 1 uses IPv4, and Tablet 2 uses Bluetooth. We confirmed that control messages are normally transmitted from Laptop 1 and Tablets 1 and 2, which are not IPv6-enabled devices, to Laptop 4, which belongs to a different local area network. Our experiment confirmed that when Netbook 1 or Netbook 3 was disconnected, the routing tables on Laptop 1 and Tablet 2, respectively, were reconfigured. This test demonstrates the stability of the proposed efficient heterogeneous network-routing scheme based on the dynamic control middleware.

4. Conclusions

Many industries rely on the ability to connect numerous devices to heterogeneous networks to deliver fundamental services, as observed in health care. However, DCM, a middleware for existing cyber-physical systems, only supports IPv6. Therefore, the many devices that do not use IPv6 cannot connect to a DCM-based CSP. In this paper, a network-routing module is designed to support CDM connections through IPv6 and other various network protocols such as IPv4, Bluetooth, and ZigBee. Through the proposed network-routing module, devices with heterogeneous protocols can be registered as components of an EDCM. Furthermore, if an intermediate node in a routing path is removed from the EDCM network, the network recovers dynamically.

Regarding future work, an EDCM network is constructed on a large scale, so it is necessary to study techniques for efficient traffic distribution. Also, authentication techniques to enable only authorized users to control the EDCM controller must be explored. Finally, we also plan to develop an encryption technique suitable for low-performance embedded devices.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean Government (Ministry of Science and ICT) (No. 2017R1C1B5075856).

References

[1] E. A. Lee, "Cyber physical systems: design challenges," Tech. Rep. UCB/EECS-2008-8, University of California, Berkeley, CA, USA, 2008.

[2] E. A. Lee, "Cyber-physical systems—are computing foundations adequate?," in *Position Paper for NSF Workshop On Cyber-Physical Systems: Research Motivation, Techniques and Roadmap*, pp. 1–9, Austin, TX, USA, October 2006.

[3] E. A. Lee, "Computing foundations and practice for cyber-physical systems: a preliminary report," Tech. Rep. UCB/EECS-2007-72, University of California, Berkeley, CA, USA, 2007.

[4] S. O. Park, T. H. Do, Y. S. Jeong, and S. J. Kim, "A dynamic control middleware for cyber physical systems on an IPv6-based global network," *International Journal of Communication Systems*, vol. 26, no. 6, pp. 690–704, 2013.

[5] S. W. Ahn, C. Yoo, S. H. Lee, H. S. Lee, and S. J. Kim, "Implementing virtual platform for global-scale cyber physical system networks," *International Journal of Communication Systems*, vol. 28, no. 13, pp. 1899–1920, 2015.

[6] T. Yang, Z. Huang, H. Pen, and Y. Zhang, "Optimal planning of communication system of CPS for distribution network," *Journal of Sensors*, vol. 2017, Article ID 9303989, 10 pages, 2017.

[7] N. Jabeur, N. Sahli, and S. Zeadally, "Enabling cyber physical systems with wireless sensor networking technologies, multiagent system paradigm, and natural ecosystems," *Journal of Sensors*, vol. 2015, Article ID 908315, 15 pages, 2015.

[8] M. C. Kim and S. J. Kim, "A scenario-based user-oriented integrated architecture for supporting interoperability among heterogeneous home network middlewares," in *Computational Science and Its Applications—ICCSA 2006. ICCSA 2006. Lecture Notes in Computer Science, vol 3983*, M. L. Gavrilova, O. Gervasi, V. Kumar, C. J. Kenneth, T. D. Taniar, A. Laganà, Y. Mun, and H. Choo, Eds., pp. 669–678, Springer, Berlin, Heidelberg, 2006.

[9] Y. W. Kim, H. S. Jang, J. H. Choi, C. H. Song, and Y. I. Eom, "Design of a multi-middleware bridge for supporting interoperability in home network environments," in *2008 International Conference on Advanced Language Processing and Web Information Technology*, pp. 477–482, Dalian Liaoning, China, July 2008.

[10] K.-D. Moon, Y.-H. Lee, C.-E. Lee, and Y.-S. Son, "Design of a universal middleware bridge for device interoperability in heterogeneous home network middleware," *IEEE Transactions on Consumer Electronics*, vol. 51, no. 1, pp. 314–318, 2005.

[11] S. O. Park, J. S. Kim, and S. J. Kim, "An object-based middleware supporting efficient interoperability on a smart home network," *Multimedia Tools and Applications*, vol. 63, no. 1, pp. 227–246, 2013.

[12] XORP, "XORP user manual version 1.6," http://www.xorp.org/.