International Journal of Smart Home
Vol. 9, No. 11, (2015), pp. 111-122
http://dx.doi.org/10.14257/ijsh.2015.9.11.13

Novel Gateways and Sensor Nodes Applying an Object Identifier to Monitor Gas Facilities

Hojoong Kim, Hyunjune Shin and Junho Shin

Korea Electronics Technology Institute
{khj123abc, hyunjune.shin, jhshin}@keti.re.kr

Abstract

With the technological development of the Internet of Things (IoT), a wide variety of IoT-based monitoring systems have been developed in various domains. An IoT-based monitoring system provides an administrator with efficient management and information collection. Due to such advantages, the demand for monitoring systems in the gas industry domain has dramatically increased. In this paper, we propose two kinds of novel gateways and sensor nodes that apply an object identifier (OID) to monitor gas facilities. The proposed gateways and sensor nodes collect gas and environment data with various sensors and communicate with a monitoring server. If an exceptional event happens at the inspection site where our devices are installed, sensor nodes can take action by issuing control commands from the monitoring server. Moreover, we have also designed an OID that provides resources and devices in a gas monitoring system with a unique identification. By applying an OID to each message for transmission among sensor nodes, gateways, and monitoring servers, gas facilities and related devices can be accurately and safely managed. To evaluate the proposed devices, we properly installed our gateways and sensor nodes near operating gas facilities and verified their operation.

***Keywords**: gas monitoring system, gateway, sensor node, OID, IoT*

1. Introduction

Recently, Internet of Things (IoT) technology has been paid considerable attention, with an advanced communication technology[1]. Specifically, as various industries are rapidly converged with communication technology, the number of demands on information management systems with IoT technology continuously increases.

Owing to such reasons, a substantial number of IoT-based devices, applications, and systems have been recently developed in various domains. For example, in the transportation and logistics domain, advanced cars, trucks, buses, and bicycles are equipped with various sensors, GPS, and tags, providing positional information, real-time transportation status, and product information. Using these devices, logistics managers can monitor and track the location and status of their products. A real-time management system in the retail industry can provide customers and shop managers with more accurate and detailed information about products in stores[2]. Moreover, some information for vehicles, such as moving and still images, can be processed and sent to a cloud server to quickly support adapted services and to reduce the cost and time for the development of the related system [3]. In the healthcare domain, IoT technology also helps improve automatic data collection and the diagnosis and monitoring of patients. Most resources and entities, such as patients, hospitals, medicines, and medical devices, can be monitored and managed thoroughly. Digitalized data can be stored for a long time and be easily classified according to its usage. Remote patient-monitoring services using a heterogeneous wireless access network can be especially useful for eHealth service providers so they can offer flexible and cost-effective monitoring services to remote or mobile patients [4]. Similar to these examples, as IoT-based systems in many domains can effectively and quickly

ISSN: 1975-4094 IJSH

provide useful information that existing systems are unable to handle[5-7], the demand for IoT-based systems has dramatically and continuously increased.

However, in the gas industry domain, regardless of such an advanced technology and the great demand for IoT-based systems, the research and development of an IoT-based monitoring system for the gas industry have progressed only slightly. For example, only small efforts have been made to install a closed-circuit television (CCTV) and to check gas leaks by using analog-based measuring systems near gas facilities without the benefit of IoT technology. Otherwise, it is necessary that the gas management system be remotely controlled anywhere and anytime and be safely managed because trivial faults in gas facilities can threaten human life and cause considerable financial damage.

Moreover, due to the increase in the use of integrated systems applying this advanced communication technology, it is inadequate to maintain the identification systems that were used in the past for monitoring gas facilities. The reason is that an IoT-based monitoring system for gas facilities consists of a large number of sensor nodes and gateways, which are connected in heterogeneous networks. Thus, it is inevitable to integrate the global identification systems for monitoring gas facilities.

In our earlier paper[8], we designed and implemented gateways and sensor nodes for monitoring gas facilities. In this paper, we propose two kinds of gateways and sensor nodes that apply an object identifier (OID) to monitor gas facilities by extending the previous work. The gateways and sensor nodes are utilized for collecting gas and environment data and transmitting it to a monitoring server. Then, the transmitted data is processed and analyzed by the monitoring server. If an emergency situation such as a gas leak happens at the gas facilities site where gateways and sensor nodes are installed, our proposed devices can take action to block it off by issuing control commands from the monitoring server. Additionally, we have designed an OID system that can provide a gas monitoring system with a unique identification for its resources and devices. By utilizing an OID in the messages for data transmission, specific information or the devices in a gas monitoring system can be accurately and efficiently managed.

The rest of this paper is organized as follows. Section 2 discusses a review of gateways and sensor nodes for IoT-based monitoring systems and an OID for the identification system. Section 3 presents the architecture of an IoT-based monitoring system for gas facilities. Section 4 explains the proposed gateways and sensor nodes that apply an OID to monitor gas facilities. Finally, Section 5 draws conclusions.

2. Related Work

The related work can be categorized into two groups: research on gateways and sensor nodes for IoT-based monitoring systems and research on an OID for the identification system.

2.1. Gateways and Sensor Nodes for IoT-based Monitoring Systems

There have been many efforts in designing and implementing gateways and sensor nodes for IoT-based monitoring systems in various domains.

The works in [9] present the design and implementation of a remote monitoring and controlling system, using ZigBee for a home network. Their Zigbee devices and a home gateway are connected to a web server and web services, and a smartphone is used for the client system to monitor and control the home. In [10], methods and devices for the remote control of legacy home appliances with a ZigBee-based home network are proposed.

Some works have been done to make their gateways support smarter and more complex functions. The works presented in [11] propose gateways based on Zigbee and general packet radio service (GPRS) protocols, which enable data forwarding, protocol transformation, and wireless sensor network (WSN) management and control. In [12], they present the design of a middleware for a smart gateway with some levels of intelligence by executing an application code. The middleware for the gateway also provides protocol conversion, request caching, and intelligent caching with sensor discovery.

Regarding the works in [13], the gateway provides the network convergence with multiple interfaces—RS232, Bluetooth, and onboard LCD, according to different application scenarios—for users to gain access to the home network.

Despite such works in recent years, there are still limited improvements in smart gateways specializing in a monitoring system for gas facilities. Most of the proposed gateways and sensor nodes are general-purpose devices that have not attained full optimization in their applied domains. The identification system is also limited in its resources and devices. Although some works utilize their own identification system, it is insufficient to be deployed and extended as a global identification system that can cover all the resources and devices in an IoT-based monitoring system for gas facilities.

2.2. OID as an Identification System

An OID is defined by ITU-T X.680 & ISO/IEC 8824-1[14] as “A globally unique value associated with an object to unambiguously identify it.”. An OID is an identification mechanism for identifying tangible or intangible objects as a global standard. An OID applies to various domains, such as Internet network management, radio-frequency identification (RFID), security, and healthcare.

The system follows a hierarchical structure based on the OID tree. The most significant node refers to management organization, with three types of values—{0}, {1}, and {2}—where {0} indicates ITU-T, {1} indicates ISO, and {2} indicates ISO/ITU-T. Each node has its own child nodes, and each layer is called an arc. An OID is created with consecutive values from the top to the bottom nodes.

An OID repository[15] provides registered OIDs and their information through a web service. About 100,000 OIDs are registered there for various usages, and it is easy to search subtrees in detail. Registering a new OID requires permission from the standard group.

An OID is widely utilized as an identification system in various domains. For example, since a lot of facilities and systems have been connected to an integrated network with the recent development of communications technology, new systems cause the demand for proper Internet network management. Specifically, the simple network management protocol (SNMP) provides worldwide identification for network management in communication systems. The SNMP defines a managed object (MO) to identify tangible objects, such as switches, servers, and control devices, as well as intangible objects, such as functions and services, and an OID is assigned to each MO. In the security domain, OIDs are used for standards in the digital signature and cryptography technology, providing the security service

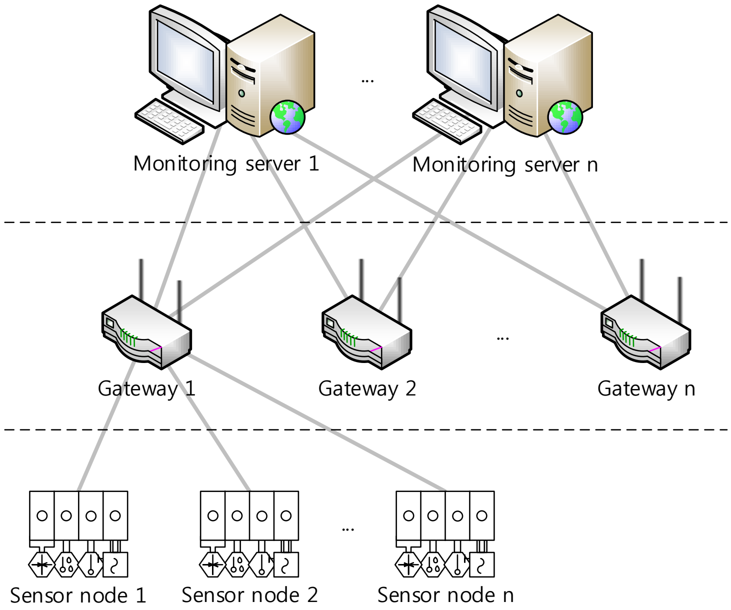


Figure 1. Architecture of an IoT-based Monitoring System for Gas Facilities

with safety and reliability. Therefore, banks and electronic documents take advantage of OIDs for identifying each policy or algorithm. The RFID domain uses an OID to offer a unique code identification. According to the ISO/IEC 18000-6 standard, types of non-electronic product code (EPC) codes are identified by OIDs. An OID in RFID ensures service interoperability with the uniqueness of RFID. In the healthcare domain, as remote medical diagnoses and digitalized medical records have been gradually developed, OIDs are applied to these techniques for efficient management. For instance, Health Level Seven International (HL7)[16] provides a comprehensive framework and related standards for the exchange, integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery, and evaluation of health services. Particularly, HL7 advises that each OID be assigned to a newly developed product for a unique identification system.

3. Architecture of an IoT-based Monitoring System for Gas Facilities

An IoT-based monitoring system for gas facilities consists of gateways, sensor nodes, and monitoring servers. One monitoring server is interconnected with several gateways, and one gateway is interconnected with a lots of sensor nodes in the network. Figure 1 demonstrates the architecture of an IoT-based monitoring system for gas facilities.

The characteristics and functions of main components in the IoT-based monitoring system for gas facilities are as follows:

3.1. Gateway

A gateway allows sensor nodes to send their collected data to monitoring servers. It consolidates the data from each of the separate sensor nodes that is physically connected with sensors and transmits data to monitoring servers with the function of protocol conversion. In addition, it forwards control commands from the monitoring server to specific sensor nodes.

3.2. Sensor Node

A sensor node is a component that collects sensor data and communicates with a gateway. It is directly connected with several individual environmental sensors that provide information on the risk factors related to the gas facilities and surrounding environment. If it receives control commands from a monitoring server through a gateway, it performs the control functions, such as blocking off a gas leak.

3.3. Monitoring Server

A monitoring server stores the sensing data from sensor nodes through gateways and the status and configuration logs of gateways and sensor nodes in its database. It then implements data processing for analysis, management of devices, and control of risk factors. If an exceptional event happens at the inspection site or management errors in the gateways or sensor nodes occur, the monitoring server identifies the problem and takes action by sending control commands to related devices.

4. Proposed Gateways and Sensor Nodes Applying an OID to Monitor Gas Facilities

Our work can be categorized into three groups: an OID for monitoring gas facilities, gateways and sensor nodes, and data transmission.

4.1. OID for Monitoring Gas Facilities

An OID for monitoring gas facilities has been designed with consideration for the characteristics of related devices and the functions of a system. It comprises six kinds of main fields, including the country, registered corporation, project, participating corporation, device, and serial, with one extension field, which is the extension device. Table 1 partially demonstrates the proposed OID for monitoring gas facilities.

4.1.1. Country

This field is used by the ISO for an allocated country. The ISO designates the country code in the subfield of iso(1)-member-body(2). This field’s fixed value is 1.2.410(kr) in our proposed OID, which refers to the Republic of Korea.

4.1.2. Registered Corporation

This field is used for the name of a corporation that requests an OID registration with the ISO. This field’s fixed value is keti(2000060) in our proposed OID, which signifies the Korea Electronics Technology Institute.

4.1.3. Project

This field is used for the project name. This field’s fixed value is lpg(1) in our proposed OID, which indicates the monitoring systems for gas facilities.

4.1.4. Related Corporation

Table 1. OID for Monitoring Gas Facilities

OID								Description	Detail
1.2.410								Kr	Republic of Korea
1.2.410	2000060							Keti	Korea Electronics Technology Institute
1.2.410	2000060	1						Lpg	Monitoring systems for gas facilities
1.2.410	2000060	1	1					Keti	Korea Electronics Technology Institute
1.2.410	2000060	1	1	1				Gateway	Gateway
1.2.410	2000060	1	1	1	101			serial-101	Serial number 101
Skip									
1.2.410	2000060	1	1	2				Sensornode	Sensor node
1.2.410	2000060	1	1	2	1001			serial-1001	Serial number 1001
Skip									
1.2.410	2000060	1	1	2	1001	1		Sensor	Sensor
1.2.410	2000060	1	1	2	1001	1	1	gas-sensor	Gas sensor
1.2.410	2000060	1	1	2	1001	1	2	temperature-sensor	Temperature sensor
Skip									
1.2.410	2000060	1	1	2	1001	2		gas-isolation-valve	Gas isolation valve
Skip									
1.2.410	2000060	1	2					Yagins	Yaginstek
1.2.410	2000060	1	2	1				Server	Monitoring server
1.2.410	2000060	1	2	1	101			serial-101	Serial number 101
Skip									
1.2.410	2000060	1	2	1	110			serial-110	Serial number 110

This field is used for the name of a corporation joining the project. This field consists of two values, keti(1) and yagins(2), which refer to the Korea Electronics Technology Institute and Yaginstek, respectively.

4.1.5. Device

This field is used for a device name made by the relevant corporation. The value of this field varies, depending on the related corporation field. If the value of the related corporation field is keti(1), the device field comprises two values, gateway(1) and sensornode(2). If the value of the related corporation field is yagins(2), the value of the device field is only server(1).

4.1.6. Serial

This field is used for the serial number of a device. The value of this field varies, depending on the device field. If the value of the device field is gateway(1), the value of the serial field ranges from 101 to 999. If the value of the device field is sensornode(2), the value of the serial field ranges from 1001 to 9999. If the value of the device field is server(3), the value of the serial field ranges from 101 to 110.

4.1.7. Extension Device

This field is used for an additional device for the sensor node only. If the value of the device field is sensornode(2), the extension device field follows the serial field. The extension device field comprises two values, sensor(1) and gas-isolation-valve(2).

4.1.8. Sensor

This field is used for various sensors connected with sensor nodes. The values of the sensor field consist of gas-sensor(1), temperature-sensor(2), pressure-sensor(3), corrosion-sensor(4), vibration-sensor(5), weight-sensor(6), windvelocity-sensor(7), and humidity-sensor(8).

4.2. Gateways and Sensor Nodes

4.2.1. A-type Gateways and Sensor Nodes

The A-type gateway comprises a programmable board and various modules via communication interfaces. The board contains a 720-MHz ARM Cortex-A8 processor, SDRAM 256MB, and NAND Flash 256 MB. Embedded Linux is installed as an operating system. Additional SD memory in the board is utilized for logging an exceptional event and transmitted data and for updating the system. Power is provided by converting AC 220 V to DC 5 V as the input voltage. If an unexpected problem in the wired power supply occurs, an internal subsidiary battery module provides input voltage. The gateway performs communication functions with the sensor nodes by Bluetooth 4.0 (Bluetooth low energy [BLE]) [17], so it can be simultaneously connected with several sensor nodes. Additionally, it interacts with monitoring servers over TCP and HTTP via a 3G/LTE modem or internal Ethernet. Table 2(a) demonstrates the main specifications of the A-type gateway and Figure 2(a) demonstrates the A-type gateway.

The A-type sensor node comprises a small board that contains a low-power-based ARM Cortex-M3 processor and many sensor modules, including those for gas detection, temperature, pressure, corrosion, vibration, weight, wind velocity and humidity. As noted above, a sensor node interacts with the gateway by Bluetooth 4.0 (BLE). It uses converted DC 5 V as input voltage from AC 220 V and also contains an internal subsidiary battery module for an exceptional situation. Table 2(b) demonstrates the main specifications of the A-type sensor node and Figure 2(b) demonstrates the A-type sensor node.

4.2.2. B-type Gateways and Sensor Nodes

The B-type gateway is made of a Raspberry Pi 2 Model B[18]. The Raspberry Pi 2 Model B is a suitable board as a gateway in a limited environment because it contains a 900-MHz quad-core ARM Cortex-A7 processor and SDRAM 1 GB; it demonstrates a high performance for data processing and communications despite being tiny. It runs embedded Linux as an operating system and receives and transmits data with sensor nodes like the A-type gateway. The communication function between the gateway and sensor node is reliably carried out over TCP via the Ethernet. Therefore, the gateway has the advantage of being able to interconnect with many more sensor nodes compared to Bluetooth 4.0 (BLE) in the A-type gateway. It also interacts with monitoring servers over TCP and HTTP via the Ethernet. Table 3(a) demonstrates the main specifications of the B-type gateway and Figure 3(a) demonstrates the B-type gateway.

The B-type sensor node is made of Arduino UNO[19] with additional shields. The Arduino UNO is a microcontroller board that is based on an open-source platform. It contains a low-power AVR 8-bit microcontroller and provides high compatibility that allows a range of sensors to be easily connected. It collects data from a gas detection sensor, a temperature sensor, a pressure sensor, a vibration sensor, and a humidity sensor, and performs communication functions via Wi-Fi. Figure 3(b) demonstrates the B-type sensor node and Table 3(b) demonstrates the main specifications of the B-type sensor node.

Table 2. Main Specifications of the A-type: (a) Gateway (b) Sensor Node

Item	Detail
CPU	720MHz ARM Cortex-A8 (Low-power)
OS	Embedded Linux
Memory	256MB SDRAM, 256MB NAND Flash
Communication	3G/LTE
	Bluetooth 4.0 (BLE)
Power Supply	220ACV/60Hz to 5DCV/2A Adapter
	Subsidiary Battery

(a)

Item	Detail
MCU	ARM Cortex-M3 (Low-power)
Communication	Bluetooth 4.0 (BLE)
Sensors	Gas Sensor
	Temperature Sensor
	Pressure Sensor
	Corrosion Sensor
	Vibration Sensor
	Weight Sensor
	Wind Velocity
	Humidity Sensor
Power Supply	220ACV/60Hz to 5DCV/2A Adapter
	Subsidiary Battery

(b)

Table 3. Main Specifications of the B-type: (a) Gateway (b) Sensor Node

Item	Detail
CPU	900MHz ARM Quad-core Cortex-A7
OS	Embedded Linux
Memory	1GB SDRAM
Communication	Wi-Fi
	Bluetooth 4.0 (BLE)
Power Supply	5DCV/600mA

(a)

Item	Detail
MCU	AVR 8-bit MCU
Communication	Wi-Fi
	Bluetooth 4.0 (BLE)
Sensors	Gas Sensor
	Temperature Sensor
	Pressure Sensor
	Vibration Sensor
	Humidity Sensor
Power Supply	220ACV/60Hz to 5DCV/2A Adapter

(b)

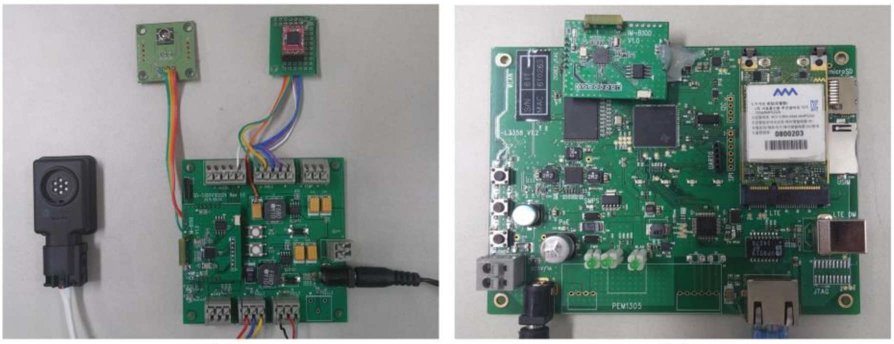
4.3. Data Transmission

4.3.1. Messages for Data Transmission in TCP

The message for data transmission in monitoring gas facilities between the gateway and the monitoring server in the TCP consists of two types of main fields—a common header field and a body field. The structure and size of the common header field are fixed, while those of the body field depend on the message type. Figure 4 demonstrates the message format for the data transmission in TCP.

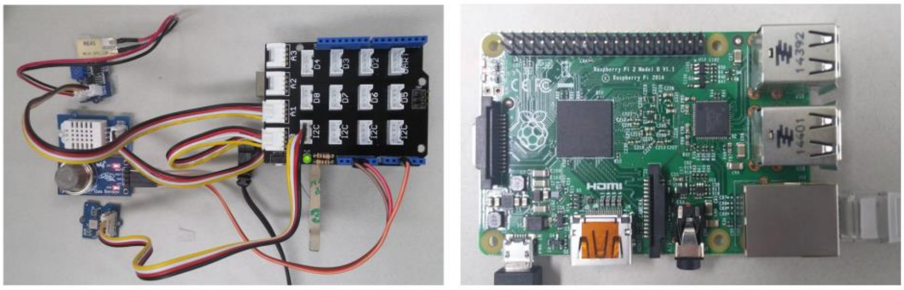
A common header field should be placed in front of a body field, regardless of the message type. The common header field in the message provides the receiver with the sender's various data, such as the message length, message type, encryption key size, OID, MAC address, IP address, and header divider.

A body field follows a header field in the message. The structure of the body field is transformed, depending on the message type. In the case of the sensor data message in the TCP, the gateway sends to the monitoring server the gas and environment data obtained from the sensor. The monitoring server, which receives the sensor data message, can track the identity of the data through its OID. The sensor data message contains the common header, timestamp, gas, temperature, pressure, corrosion, vibration, weight, wind velocity, and body tail. In the case of the gas isolation valve action message, the monitoring server sends the device control data to the sensor node through the gateway in an exceptional situation. The monitoring server designates and controls the gas isolation valve connected to a specific sensor node, using the OID. This message type contains the common header, action, timesta mp, and body tail, and it is used for controlling the gas isolation valve.



(a) (b)

Figure 2. A-type: (a) Gateway (b) Sensor Node



(a) (b)

Figure 3. B-type: (a) Gateway (b) Sensor Node

Common Header Field (74 bytes)

Message Length	Message Type	Encryption Key Size	OID	MAC Address	IP Address	Header Divider
4 bytes	4 bytes	2 bytes	26 bytes	18 bytes	16 bytes	4 bytes

Sensor Data Message (154 bytes)

Common Header	Timestamp	Gas	Temp	Pressure	Corrosion	Vibration	Weight	Wind Velocity	Humidity	Body Tail
74 bytes	14 bytes	8 bytes	6 bytes	8 bytes	8 bytes	8 bytes	8 bytes	8 bytes	10 bytes	2 bytes

Gas Isolation Valve Action Message (94 bytes)

Common Header	Action	Timestamp	Body Tail
74 bytes	4 bytes	14 bytes	2 bytes

Figure 4. Message Format for the Data Transmission in TCP

4.3.2. Messages for Data Transmission in HTTP

In the HTTP, real objects, such as gateways, sensor nodes, sensors, and gas isolation valves, can be transformed into RESTful resources. A message for data transmission between the gateway and the monitoring server in the HTTP takes advantage of the URI for RESTful resources by means of the POST method. When the message is transmitted by the HTTP, an additional common header is unnecessary. The response to the received message is sent by using the JavaScript Object Notation (JSON) format. In the case of the sensor data message in the HTTP, the gateway sends the gas and environment data to the monitoring server by using the URI. This message type contains the OID, timestamp, gas, temperature, pressure, corrosion, vibration, weight, wind velocity and humidity. In the case of the gas isolation valve action message in HTTP, it contains OID, timestamp, and gas isolation valve action.

5. Conclusion

This paper has presented the implementation of two kinds of gateways and sensor nodes that apply an OID to monitor gas facilities. The proposed gateways and sensor nodes collect gas and environment data and take action by communicating with a monitoring server in an emergency situation. They also apply our proposed OID, as an identification system, to the message for transmission, so gas facilities and related devices can be provided with a unique identification and be accurately and safely managed. To validate the proposed gateways and sensor nodes, we installed devices near the gas station and gas storage tanks in operation and verified the collected data from the sensor nodes at the remote site. We expect that our proposed gateways and sensor nodes that apply an OID could be widely utilized in a monitoring system for gas facilities.

Acknowledgments

This work was supported by the Energy Technology Development Program (2013T100200078, development of integrated demand response system technology for co-residential resources and demonstration of business model) funded by the Ministry of Trade, Industry &Energy (MOTIE, Korea).

References

[1] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A Survey", Computer Networks, vol. 54, no. 15, **(2010)**, pp. 2787-2805.
[2] S. Karpischek, F. Michahelles, F. Resatsch and E. Fleisch, "Mobile sales assistant-an NFC-based product information system for retailers", Proceedings of the First International Workshop on Near Field Communications (NFC'09), **(2009)**, pp. 20-23.
[3] H. Park, S. Song, and Y. Kwak, "Design the Middleware of Intelligent Monitoring System for Vehicles", International Journal of Control and Automation, vol. 8, no. 3, **(2015)**, pp. 423-430.
[4] D. Niyato, E. Hossain, and S. Camorlinga, "Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization", IEEE Journal on Selected Areas in Communications, vol. 27, no. 4, **(2009)**, pp. 412-423.
[5] A. Mainwaring, D. Culler, J. Polastre, R. Szewczyk, and J. Anderson, "Wireless sensor networks for habitat monitoring", ACM International Workshop on Wireless Sensor Networks and Applications, **(2002)**, pp. 88-97.
[6] K. Martinez, J. K. Hart, and R. Ong, "Environmental sensor networks", IEEE Computer Society, **(2004)**, pp. 50-56.
[7] R. Cardell-Oliver, K. Smettem, M. Kranz and K. Mayer, "A reactive soil moisture sensor network: Design and field evaluation", International Journal of Distributed Sensor Networks, vol. 1, no. 2, **(2005)**, pp. 149-162.
[8] H. Kim, J. Shin, H. Shin, and B. Song, "Design and Implementation of Gateways and Sensor nodes for Monitoring Gas Facilities", The 4th International Conference on Information Science and Industrial Applications (ISI 2015), **(2015)**.

[9] I. Hwang, D. Lee, and J. Baek, "Home network configuring scheme for all electric appliances using ZigBee-based integrated remote controller", IEEE Transactions on Consumer Electron, vol. 55, no. 3, **(2009)**, pp. 1300-1307.
[10] Z. Shunyang, X. Du, J. Yongping, and W. Riming, "Realization of home remote control network based on ZigBee", Proceedings of International Conference on Electronic Measurement and Instruments (ICEMI'07), **(2007)**, pp. 4-344-4-348.
[11] Q. Zhu, R. Wang, Q. Chen, Y. Liu and W. Qin, "IoT Gateway: Bridging Wireless Sensor Networks into Internet of Things", Proceedings of the International Conference on Embedded and Ubiquitous Computing, **(2010)**, pp. 347-352.
[12] D. Bimschas, H. Hellbrück, R. Mietz, D. Pfisterer, K. Römer and T. Teubler, "Middleware for Smart Gateways Connecting Sensornets to the Internet", Proceedings of the International Workshop on Middleware Tools, Services and Run-Time Support for Sensor Networks, **(2010)**, pp. 8-14.
[13] S. Guangming, Z. Yaoxin, Z. Weijuan, and S. Aiguo, "A multiinterface gateway architecture for home automation networks", IEEE Transactions on Consumer Electron, vol. 54, no. 3, **(2008)**, pp. 1110-1113.
[14] Union, Internation Telecommunication, "Information Technology-Abstract Syntax Notation One (ASN. 1): Specification of Basic Notation", ITU-T Recommendation X.680, **(2002)**.
[15] OID Repository, http://www.old-info.com
[16] Health Level Seven International, http://www.hl7.org
[17] C. Bisdikian, "An Overview of the Bluetooth Wireless Technology", IEEE Communications Magazine, vol. 39, no. 12, **(2001)**, pp. 86-94.
[18] Raspberry Pi 2 Model B, https://www.raspberrypi.org/products/raspberry-pi-2-model-b.
[19] Arduino Uno, https://www.arduino.cc/en/Main/arduinoBoardUno.

Authors

Hojoong Kim, he received the BS and MS degrees in electronic engineering from Inha University, Incheon, Republic of Korea, in 2011 and 2015, respectively. He is currently working as a researcher at Korea Electronics Technology Institute. His research interests include computer network, embedded system, and parallel and distributed systems.

Hyunjune Shin, he received the BS degrees in electronic engineering from Kwangwoon University, Seoul, Republic of Korea, in 2015. He is currently working as a researcher at Korea Electronics Technology Institute. His research interests include Internet of Things, embedded system, and serial communication.

Junho Shin, he received the BS and MS degrees in electronic engineering from Ajou University, Suwon, Republic of Korea, in 1998 and 2000, respectively. He is currently working as a managerial researcher at Korea Electronics Technology Institute. His research interests include Internet of Things, embedded system, and sensor network.