Identifier (ID) based Enhanced Service for Device Communication and Control in Future Networks

Muhammad Khan and DoHyeun Kim
Computer Engineering Department, Jeju National University, South Korea

Abstract: *Enablement of the future smart devices to interact with each other for the provision of intelligent and useful services to users is the focus of research towards the realization of future networks. The conventional static nature of networks is not feasible for the future networks which require scalability and device mobility at its core. The usage of Identifier (ID) in conjunction with a physical address supports mobility of the devices and the scalability of the overall network. This paper presents ID based device communication and control service in future networks. The study is performed using the test bed for indoor environment management, which utilizes the data from indoor and outdoor sensing devices to provide and optimum indoor environment (temperature, humidity, light etc.) by controlling the indoor actuating devices. The test bed implementation has been modified in order to execute the proposed ID based device communication and control scheme and compare the results with the IP only implementation of the test bed. The comparison reveals that ID based device communication and control scheme can be as efficient as IP based routing while providing the added advantages of coping with heterogeneity, scalability and mobility in the future networks.*

Keywords: *Future networks, identifier, ID, device control, service, efficient.*

Received November 21, 2015; accepted August 8, 2016

1. Introduction

The field of networks is evolving with tremendous pace. New strategies and technologies are being adopted to handle the issues associated with extremely large numbers of devices connected to the internet. Especially with the concept of things connected to Internet forming an Internet of Things (IoT) [8, 10, 11], the traditional IP based solutions are already falling short [7]. As specified in the MobilityFirst project [6], the current Internet is focused on connecting machines across different networks by providing the network address as identity for each machine in the global Internet. This scenario, of connecting machines which are fixed, does not support the vision of the future networks where the devices are highly mobile. The mobility of devices means that these devices will be changing their location and connecting to different networks at different time using different technologies. The stream-based connectivity provided by current internet thus cannot efficiently support such mobile devices. In the current internet, whenever a device changes its network, a new address (new identity) must be assigned to it thus re-initiating the stream based connection.

According to [1], an IoT is required in which the device identity is separate from its network address. Several approaches have been proposed introducing a separate Identifier (ID) layer to provide device identifiers which are different from their network address. Such approaches are normally based on overlay ID layer along with the network layer [3, 6], integrating ID layer into the network layer [2] or providing ID based routing at the application layer with distributed databases [5] to provide ID based routing in IoT system. This paper presents the implementation of ID based device communication and control service using a test bed for indoor environment control in order to compare the efficiency of the proposed approach to the IP based approach in the same system. The IP based control and communication service has been presented in [4]. The authors believe that the ID based device communication and control service can provide not only better performance in the overall operations of the system but it can also assist in a better information binding scheme when devices are needed to be associated with locations or users.

The rest of the paper is organized as follows: The next section provides a brief overview of the related work focusing on the major approaches for the utilization of device ID in the future network scenarios. Section 3 presents the control platform for indoor environment management and based on this architecture the ID registration, resolution and message forwarding scheme has been described. Section 4 describes the message format and brief details related to the message structure for the ID based device communication and control approach. Section 5 illustrates the execution scenario for the ID based control service. Section 6 provides the brief description of the experimental setup for testing the efficiency of the proposed scheme and the comparison with the IP based scheme results. Finally, the conclusions and future work have been presented in section 7.

2. Related Work

There are several issues which come in conjunction with the vision for future networks. One such issue is that the things connected to internet may not always be fixed and the mobility of connected devices along with other concerns are the main focus of future networks technologies.

Many solutions have already been suggested and several strategies have been applied to the existing networking technologies in order to solve the mobility and scalability issues for the future networks. ID based routing is one of such solutions and it has been suggested by many studies in different forms to solve the inherent issues for IoT. As specified in Mobility First [6], the requirement for the future networks and IoT is devices which have identities separate from their network address, allowing communication between identities instead of network addresses. It also suggests that by implementing the identity/address table at the network layer, the mobility issues for the things can be overcome. Like MobilityFirst [6], Veil [3] also proposed an ID layer to support the network of devices below the network layer. The network of devices was assumed to have large number of devices connected based on IP and Non-IP physical addresses. The IP enabled devices means the Ethernet enabled devices while Non-IP devices include blue-tooth enabled devices and Zigbee based sensors etc.

Virtual Id based Routing (VIRO) [9] proposes the mechanism for Virtual Id (vid) based routing in the Veil architecture. It utilizes the structured virtual id space to separate routing from addressing (namespace-independence). VIRO routing mechanism is based on the mapping of this structured vid space on both low level physical addresses (MAC) and IP addresses at the network level. VIRO utilizes a routing algorithm similar to Distributed Hash Tables (DHT) routing for the creation and maintenance of the routing tables as well as for the vid's, addresses mapping and data forwarding.

The assignment of identifier to the objects in the Mobility First [6] project is performed using the Global Unique identifier (GUID). The mapping of the GUID and the respective object's physical address is achieved through the proposed Global Name Resolution Service (GNRS). So the data forwarding in MobilityFirst is performed by the routers either using the GUID only or by consulting the GNRS to find the physical address associated with the specific GUID.

Another approach called as the Ucodes based on uID architecture [5], uses the ID based routing and information retrieval using distributed databases. The Ucodes for things (tagged objects) are implemented at the application layer. The things only contain tag with Ucode and the rest of the information associated with that ucode is stored on a separate Application Information Server. The Ucode resolution server acts as a DNS to resolve the Ucode read from a thing via a user terminal (mobile device etc.,) along with the thing's context. The resolution server provides the address of application information server based on the Ucode and context information provided. The user terminal then interacts with the Application Information Server using the address provided by the ucode resolution server to get the related information and services for the specific thing.

The ID based solutions described above implements an overlay or layer and treats the ID as an application level identifier. While these approaches have their own merits and demerits, the authors believe that utilizing the device IDs at every layer of the system may provide additional benefits in terms of device associations with data or resources at all the layers of the network, improving mapping table updates and improving the overall performance of the system. This paper provides the implementation of ID based device communication and control service in a local IoT system for indoor environment control. The device identification and communication scheme for the proposed service has been illustrated. Finally, the performance of the proposed service is compared with the IP based solution and the results have been presented.

3. Control Platform

As described earlier, the main platform for the implementation of the proposed ID based device communication and control service has been presented in [4]. The control platform is shown in Figure 1.

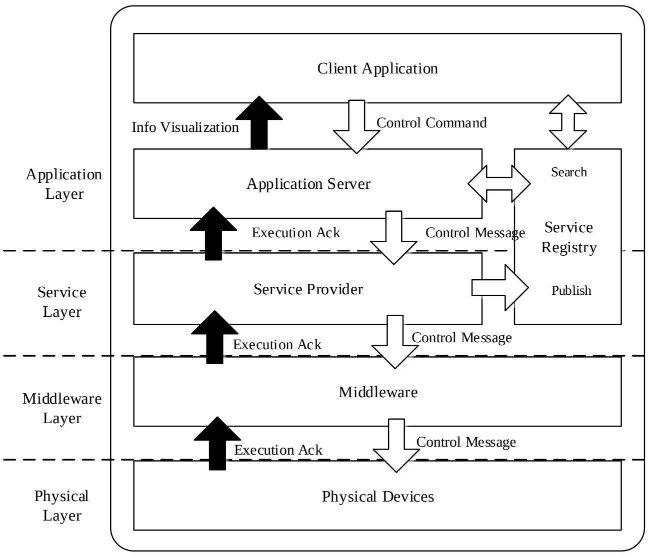

Figure 1. IoT platform for device control.

The ID based device communication and control service has been implemented as shown in Figure 2. The ID registration for devices connecting to the system via a gateway takes place at the middleware layer. At the middleware layer a routing table is maintained containing the device ID and Physical address for all the devices connected to the gateway. The Gateway implements the adapter modules for various communication technologies to enable interactions with heterogeneous devices. Gateways share the ID registration information with the Service Provider at the service layer. The service providers maintain all the information about devices connected to it via the gateways. This distributed storage of information helps in easy provisioning of information and services related to the devices. It also provides for the in network storage of sensing and state data so every time the state or sensing data is required by services, no communication with the devices is needed. This is an efficient way to reduce communication traffic below the service layer. At the application layer, the information from the service layer is used to create binding information for the virtual devices. The binding information include relation among devices, space (building, floor, room) and client (user) using the respective IDs. The space and client information binding details are out of the scope of this paper. The resolution of the device ID is required for the forwarding of control messages from application layer to the devices. For this purpose, the mapping tables at the provider and middleware layer are utilized to route the message to the appropriate physical device.

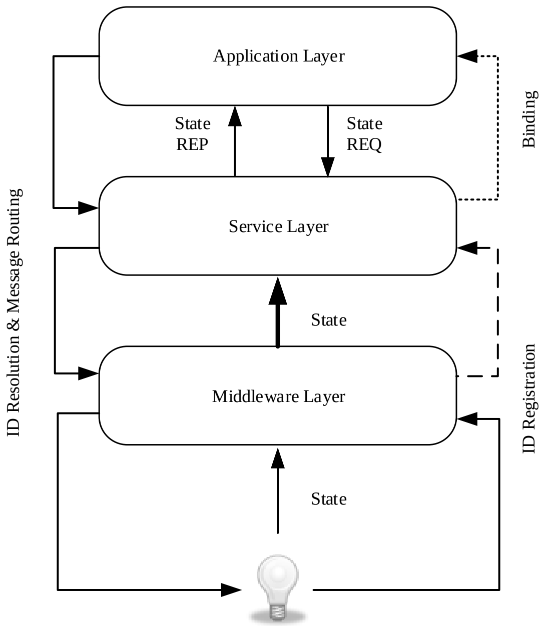

Figure 2. ID based device registration, resolution and control.

4. Communication Scheme

The section describes the message format for the ID based communication scheme. The message consists of 4 fields as shown in Table 1. The first field is specified as the message code which is two characters wide. The description of each message code is presented in Table 2. The next field in the message format is the Message type. Message type is a string value describing the type of activity intended by the message. Device ID field indicates the device for which the message is intended and command field contains the actual control command for the thing i.e., (Power on/off etc.,). The details of message types and commands are left out intentionally to avoid extra details.

Table 1. Message format in terms of data fields.

Message Code	Message Type	Device Identifier (ID)	Command

Table 2 describes the codes for messages exchanged in the implementation of the proposed ID based scheme. The '00' code indicates that the message is connection related message so it should be handled by the ID registration module to establish or terminate a connection. '01' indicates a message intended to update the mapping table. These messages are exchanged to let the provider layer of be aware of the things being connected or disconnected at the middleware layer of the system. '10' indicates a control message which can be either a request to execute a command on some device (thing) or a response after the execution of the command by the device. '11' indicates a message regarding the state of the device.

Table 2. Message codes description.

Message Code	Description
00	Connection message
01	Mapping table management message
10	Control message
11	Multi-step state message

Table 3 below presents example messages from the implementation of the proposed scheme. The first example shown by the first row of Table 3 is a connection message indicated by the code field. The message type field indicates that the message is intended for the establishment of connection and the ID specifies the device from which the message is being sent. The command field in this instance is left blank.

Table 3. Sample messages.

Message Code	Message Type	Device Identifier (ID)	Command
00	Connect	#DS00001	
10	Request	#DS00001	POW_OFF

The second example message (second row of Table 3) is a control message as specified by the code field. These messages are normally forwarded from the Application layer to the intended thing/device. This instance is a request message as indicated by the message type field. The ID field contains the identifier of the destination thing/device. Command field contains the actual command to be executed by the device.

5. Control Service Execution Scenario

Figure 3 illustrates the execution scenario for the ID based control device control service. The Figure shows that mapping tables are maintained at three layers of the system. A physical address to ID mapping table is maintained at the Gateway (middleware layer) level, a device ID and Gateway IP mapping table is maintained at the Provider (Service Layer) and the third table for device ID to Provider IP mapping is maintained at the App Server (Application Layer). When the Application server wants to send message to a specific device, the message with the intended device ID is first routed to the appropriate Provider from the application server. At the provider, the appropriate Gateway IP is obtained from the mapping table based on the device ID and the message is forwarded to the specific Gateway. At the gateway again, the device ID is used to search the mapping table to get the physical address of the device and the message is communicated using the appropriate driver or communication adapter. The response from the device is then routed backwards.

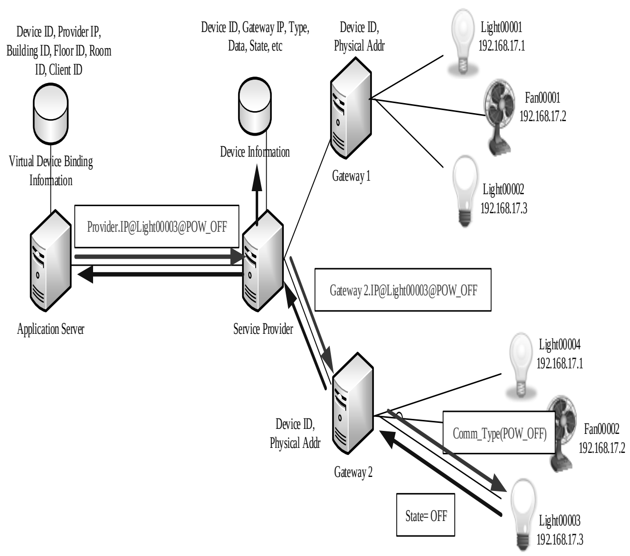

Figure 3. ID based message transmission to control actuator.

Table 4. Hardware and software specifications.

	Server 1 (mcl-12)	Server 2 (mcl-16)	ControlRequester (mcl-11)
Operating System	Microsoft Windows 7(X64)	Microsoft Windows 7(X64)	Microsoft Windows 7(X64)
Development Environment	.Net Framework 3.5, 4.0	.Net Framework 3.5, 4.0	.Net Framework 3.5, 4.0
DBMS	Microsoft SQL Server 2012 express	Microsoft SQL Server 2012 express	-
Hardware	CPU: Intel® Core™ W3503 @ 2.39GHz	CPU: AMD® Athlon™64 X2 Dual Core Process 6000+ @ 3.1GHz	CPU: Intel® Core™ i5-3570 @ 3.40GHz
	RAM: 4GB	RAM: 5GB	RAM: 4GB
	Graphics: NVIDIA GeForce FX 580	Graphics: Standard VGA Graphics Adapter	Graphics: NVIDIA GeForce GT 440

Using the reverse routing process as shown in the Figure.

Figure 3 also shows the distributed database for the storage of information at different layers of the network. The service layer database holds the information about the devices connected to it via gateways. The information consists of type, model and state of the connected devices. Similarly, at the application layer, device IDs can be bound with any other information related to the devices and stored as virtual objects. For example, data from a geographic information provider such as room, floor and building IDs can be bound with the device ID. This binding information can be used by the application layer to provide location based services to the client. This information is also used to associate things and spaces to the client and hence providing the multicast functionality to the system based on space and/or client association. One such service can be to turn off all the lights associated room number 423. Similarly, client ID can be used to identify the user without the concern of the device through which he/she are connected or the communication technology used by the client. Thanks to service oriented architecture such a scenario can easily be implemented by exposing multiple endpoints of a single service to accommodate heterogeneous communication channels.

The gateways shown in Figure 3 are the implementation of communication modules to cater for the heterogeneity of the connected devices. The gateways only maintain a mapping table at runtime to keep track of the connected devices IDs and their communication channels. Using the mapping table, the destination device and the communication adapter is decided to deliver the message.

6. Performance Evaluation and Comparison

In order to analyse the efficiency of the ID based system, the performance of the system was analysed in comparison with the performance of the same system's operation based on IP addresses. The IP based evaluation of the same system has been presented as part of [4]. The performance analysis for the ID based device communication and control service was performed using the experimental setup as shown in the Table 1. The same setup as in [4] has been used in order to compare the system based on the same parameters and to provide as much accurate comparison as possible. For this experiment, an actuator emulator has been used to emulate the functionality of actuating devices such as Fan, Light, AC and Boiler/heater. A snapshot of the device emulator is shown in Figure 4. A specialized client application called as the Control Requester is developed for the experiment to act as multiple clients and generate control messages for devices simultaneously. This specialized multithreaded client uses the control service exposed by the application server to issue control requests to the connected devices. The Control Requester simulates the number of clients requesting the control for the connected devices and to record the delay associated with each control message generated.

The experimental setup shown in Table 4 was used to compare the performance of both the ID and IP based approaches for device communication and control in the same test setup. As shown in Figure 4, the average delay for the transmission of a control messages generated at the application layer intended for 1, 5 and 25 devices simultaneously. The delay in milliseconds is the time for the control message to reach the intended device and the acknowledgement message received back at the application layer. The average delay generated by the IP based control service [4] is plotted with the new ID based solution to compare the performance. It is evident from the results that the performance of both the implementations is almost the same. The slight increase in the average delay for the ID based solution can be attributed to the string based IDs used to represent the devices.

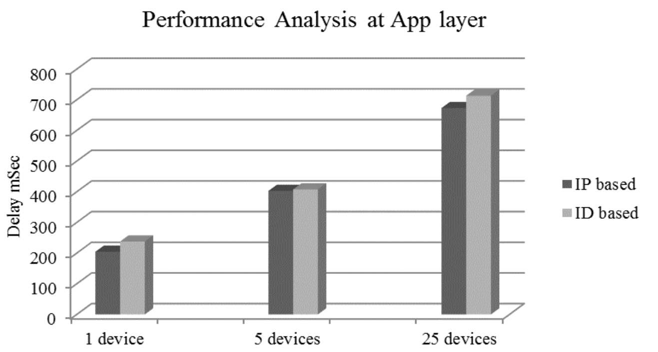

Figure 4. Device control delay comparison.

Although, the new ID based solution exhibits same performance as its previous IP based solution when tested from the perspective of the control service, however, as mentioned earlier, the other benefits of using IDs to represent the devices instead of their physical addresses outperforms the IP based solution in terms of scalability as well as from the perspective of the mapping table management when moving devices are considered as part of the system. When a moving device leaves the area of one network and enters another network, the assigned address changes. This change in the address triggers the mapping table update event. To compare the performance of both the IP and ID based solutions, the device emulator was modified to simulate devices which are on the move between multiple networks. This emulation was performed by changing the physical addresses of devices during the operation of the system and assigning them addresses associated with different Gateways. This simulates that idea of a device IP change in the same local network (same Gateway), Moving of the device to another network (different Gateway) associated with the same Provider and moving of the device to a network associated with another Provider (different Gateway & different Provider). In Figure 5, these three entries are specified as Same GW, Diff GW and Diff GW and PR respectively and show the average delay for mapping table update messages in all the three scenarios for both the IP and ID based Implementations.

In an all IP based system, the change in IP address must be propagated throughout the system as that is the only parameter which uniquely identifies the device and to associate a device with its respective Gateway and Provider. Hence, even an IP change in the local network (same Gateway) must be propagated all the way to the mapping table at the Application layer. This is the reason for the same delay for all the entries based on IP change in Figure 5. On the contrary, in the ID based solution, the physical address is only used at the Gateway level mapping table. Thus a local address change needs an update in the Gateway level mapping table only and hence the significantly less delay for mapping table update as compared to IP based solution. The mapping Table update delay is same for both the solution only in case a device moves from the network of one Provider to another Provider's network.

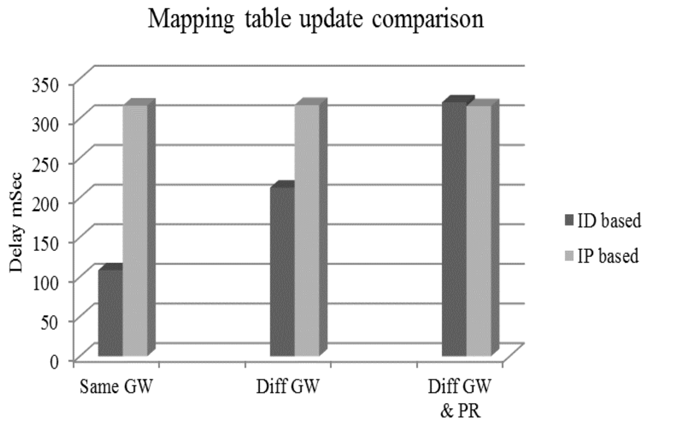

Figure 5. Mapping table update delay comparison.

The results of the performance evaluation and comparison shows that the proposed ID based device communication and control solution exhibits same performance in terms of the device control service but it outperforms the IP based solution when overall operational performance of the system is considered.

7. Conclusions

ID based device communication and control is a viable solution for overcoming the issues associated with future networks of devices or things. The idea presented in this paper suggests that ID based communication and control scheme can be utilized in Wireless Sensors and Actuators Network (WSAN) and IoT implementations as efficiently as an IP based scheme while providing extra benefits of scalability and mobility in the system. The comparison of performance for both the IP and ID based implementations on a local test bed shows the feasibility of the presented idea. This study is part of an on-going project which further plans to study the utilization of ID for UserID based multicast control message transmission and UserID based intelligent service provisioning.

Acknowledgments

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT)(No.2018-0-01456, AutoMaTa: Autonomous Management framework based on artificial intelligent Technology for adaptive and disposable IoT), and this research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2019-2016-0-00313) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation). Any correspondence related to this paper should be addressed to DoHyeun Kim; kimdh@jejunu.ac.kr.

References

[1] Atzori L., Iera A., and Morabito G., "The Internet of Things: A Survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, 2010.

[2] Batalla J. and Krawiec P., "Conception of ID Layer Performance at the Network Level for Internet of Things," *Personal and Ubiquitous Computing*, vol. 18, no. 2, pp. 465-480, 2014.

[3] Jain S., Yingying C., Chen Y., Zhang Z., and Jain S., "VEIL: A ''Plug-&-Play'' Virtual (Ethernet) ID Layer for Below IP Networking," *in Proceedings of IEEE Globecom Workshops*, Honolulu, pp. 1-6, 2009.

[4] Khan M. and Kim D., "Service-Oriented Process Modelling for Device Control in Future Networks," *The International Arab Journal of Information Technology*, vol. 14, no. 5, pp. 691-697, 2017.

[5] Koshizuka N. and Sakamura K., "Ubiquitous ID: Standards for Ubiquitous Computing and the Internet of Things," *IEEE Pervasive Computing*, vol. 9, no. 4, pp. 98-101, 2010.

[6] Li J., Shvartzshnaider Y., Francisco J., Martin R., and Raychaudhuri D., "Enabling Internet-of-Things Services in The Mobilityfirst Future Internet Architecture," *in Proceedings of the IEEE International Symposium on A World of Wireless, Mobile and Multimedia Networks WoWMoM*, San Francisco, pp. 1-6, 2012.

[7] Li J., Zhang Y., Nagaraja K., and Raychaudhuri D., "Supporting Efficient Machine-To-Machine Communications in the Future Mobile Internet," *in Proceedings of the IEEE Wireless Communications and Networking Conference Workshops WCNCW*, Paris, pp. 181-185, 2012.

[8] Li S., Da Xu L., and Zhao S., "The Internet of Things: A Survey," *Information Systems Frontiers*, vol. 17, no. 2, pp. 243-259, 2015.

[9] Lu G., Jain S., Chen S., and Zhang Z., "Virtual Id Routing: A Scalable Routing Framework with Support for Mobility and Routing Efficiency," *in Proceedings of the 3rd International Workshop on Mobility in the Evolving Internet Architecture*, *MobiArch'08 Co-Located with SIGCOMM*, Seattle, pp. 79-84, 2008.

[10] Misra G., Kumar V., Agarwal A., and Agarwal K., "Internet of Things (IoT)-A Technological Analysis and Survey on Vision, Concepts, Challenges, Innovation Directions, Technologies, and Applications (An Upcoming or Future Generation Computer Communication System Technology)," *American Journal of Electrical and Electronic Engineering*, vol. 4, no. 1, pp. 23-32, 2016.

[11] Whitmore A., Agarwal A., and Da Xu L., "The Internet of Things-A Survey of Topics and Trends," *Information Systems Frontiers*, vol. 17, no. 2, pp. 261-274, 2015.

Muhammad Khan is an Assistant Professor at the Department of Computer Software Engineering, University of Engineering & Technology Peshawar, Pakistan. He received his M.S. degree from Computer Software Engineering Department, University of Engineering and Technology Peshawar in 2012 and completed his Ph.D. studies from Jeju National University South Korea in 2016. The major focus of his work is the application of alternate programming strategies to enable the involvement of masses in Internet-of-Things application design and development. End-User Programming and Human-Computer Interactions are also included in his research interests.

DoHyeun Kim received the B.S., M.S. and P.D degrees in Electronics Engineering from Kyungpook National University, Taegu, Korea, in 1988 and 1990, 2000 respectively. He joined the Agency of Defence Development (ADD), Korea, in 1990. Since 2004, he is currently a professor at the Department of Computer Engineering at Jeju National University, Korea. His research interests include sensor web, optimization algorithm and context prediction.