ID-based Communications for Future IoT/M2M

Yusuke FUKUSHIMA and Ved P. KAFLE

Internet of Things (IoT) is going to bring a new wave of innovations and revolution in the ICT services to make several aspects of our lives smart. Machine-to-Machine communication (M2M) is the common platform for secure and adaptive communications among heterogeneous devices and network protocols required by IoT services. This paper presents a design and implementation of a mobile sensor network using location-independent ID-based communication technique that enables communications over heterogeneous network protocols, while providing device authentication, discovery, remote control and management.

1 Introduction

Widespread circulation of affordable and low-power consumption wireless communication devices has brought various M2M (Machine-to-Machine) services into reality, in which the devices autonomously exchange information through networks. The total number of hosts used in such services is expected to reach 50 billion by 2020[1]. To address this trend, a framework to ensure safe and secure M2M communications among such enormous number of devices is under discussion at the International Telecommunication Union (ITU)—an international standardizing organization[2]. This framework includes mechanisms to realize such features as: Internet-based management and location detection of the hosts; mutual identification among the hosts for safe starting of communication; uninterrupted communication even in the event of network switching; remote control of the hosts; and support for communication among machines equipped with different network layer protocols. At present, M2M communications are generally unidirectional with relatively small volume traffic at a time—typically, regular data upload from a sensor to a cloud server. However, as M2M technology finds its way into the depth of end-user applications, IoT/M2M in the future will require a much broader spectrum of functions defined in the M2M framework now under discussion in the ITU. Some of the major functions include: remote control of devices from a service and uninterrupted communication to guarantee safe control of devices (i.e. quick and correct response to changes in the environment surrounding the user). To realize these functions, each device must be correctly authenticated before starting the communication and remain correctly recognized during the session. Communication by way of the Internet uses location information (or locator) of the device as a host ID (typically, IP address). This scheme presents a danger of lost identification of the destination device if the locator changes during a session—e.g. switching from a network to another. In addition, a two-way authentication mechanism is required for safe remote control of the devices.

To resolve these problems, studies are underway on network architecture that allows separated use of IDs and locators, i.e. the ID/Locator Split Architecture[3][4]. This architecture generally introduces a new host identifier (hereafter referred to as ID) as the means to identify a host and uses it to separate the host identification function from the network layer. This approach provides a mechanism to secure uninterrupted communication even in the case of changed locators. Among these attempts, we are conducting R&D on the Heterogeneity Inclusion and Mobility Adaptation through Locator ID Separation (HIMALIS)[3] technology. We consider this approach will prove quite effective in the future IoT/M2M environment, as it can provide Internet-based method of locating hosts, as well as a mechanism for two-way mutual authentication among the devices[5][6]. In this report, we describe our experimental approach toward realization of HIMALIS-based IoT/M2M. Our attempt includes construction of an experimental facility that constitutes a part of the Japan-wide Orchestrated Smart/Sensor Environment (JOSE)[7] project.

2 Overview of HIMALIS Network

In this section, we provide an overview of the HIMALIS

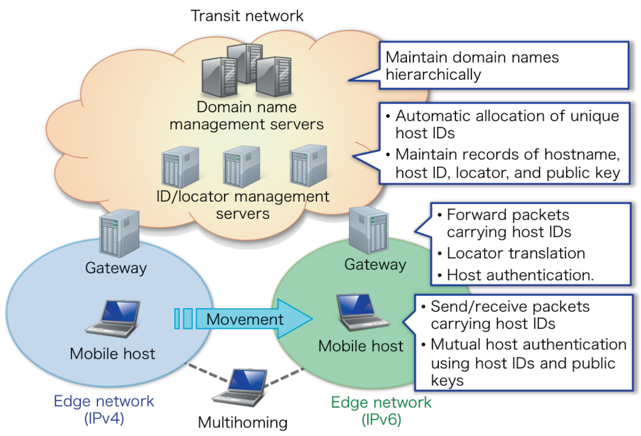

Transit network
Maintain domain names hierarchically
Domain name management servers
• Automatic allocation of unique host IDs
• Maintain records of hostname, host ID, locator, and public key
ID/locator management servers
• Forward packets carrying host IDs
• Locator translation
• Host authentication.
Gateway
Gateway
Movement
Mobile host
Mobile host
• Send/receive packets carrying host IDs
• Mutual host authentication using host IDs and public keys
Edge network (IPv4)
Multihoming
Edge network (IPv6)

Fig. 1 HIMALIS network architecture

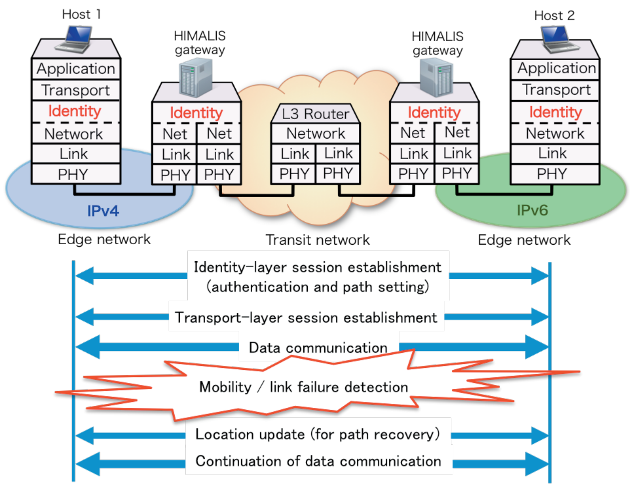


Fig. 2 HIMALIS's protocol stack and ID-based communication

network and ID-based communication.

2.1 Network architecture

The HIMALIS network consists of more than one edge network, and a transit network that connects them (Fig. 1). The transit network connects heterogeneous edge networks using different types of locators by the help of HIMALIS gateways—a HIMALIS gateway dedicated to relay differently configured edge networks using different types of locators (e.g. IPv4, IPv6). The transit network also contains a domain management server and an ID/locator management server. The former has the same hierarchic domain management mechanism with domain name servers (DNS), and the latter provides functions for managing host information (host name, host ID, locator, and public key). The host ID and the key are automatically created during the initial connection process, and are registered, along with the host name and locator, in the ID/locator management server. When a locator is changed because of mobility or other reasons, the host updates its own locator information, enabling other hosts to search.

2.2 Protocol stack and ID-based communication

To realize locator-independent communication, the HIMALIS network uses a new identity layer inserted between the transport layer and network layer, thereby separating the functions that reside in the transport layer completely from those in the network layer. The identity layer has an ID table for managing correspondence relations between host IDs and locators, enabling dynamic continuation of communication through tracking of changes that take place in locators. That is, every time its locator undergoes any change, update request is sent to the communication partners to perform mobility. The HIMALIS architecture provides a two-way authentication mechanism that enables recognizing the counterpart before the communication session begins. This authentication mechanism utilizes the host's capability to decrypt a message if: the message has been encrypted using the communication partner's public key obtainable from the ID/locator management server, and the host possesses the corresponding private key. A session (ID session) is constructed in the identity layer during the initiation process of communication to detect failures (if any) in the communication path and automatically manage any update in the ID table caused by host mobility. In this report, we call such communication mode—.e. communication that takes advantage of the identity layer functions - ID-based communication.

Figure 2 shows the flow of information in ID-based communication. When host 1 (connected to an IPv4 edge network) initiates communication to host 2 (connected to an IPv6 network), host 1 makes inquiries to the domain management server and ID/locator management server to get the information of the destination host (host2 #himalis.net). Through this process, host 1 retrieves the host ID, locator, and public key of host 2. Next, host 1 exchanges a request message to start communication with host 2, then establishes an ID session. This message exchange, as it uses a public key cryptosystem, serves as mutual host authentication as well. Successful establishment of an ID session enables the start of sending and receiving data. In case any changes in the locator take place – for example, by a handover – the hosts exchange latest locator information for updating each ID table.

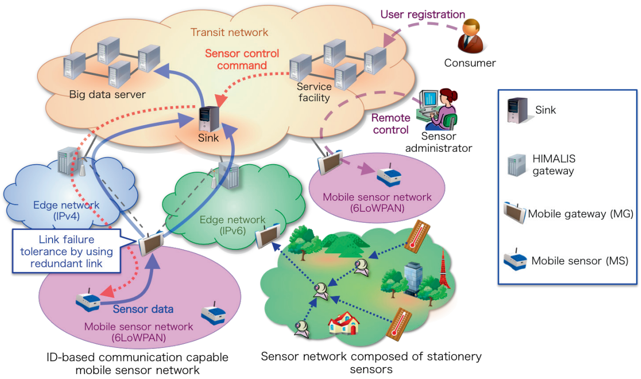


Fig. 3 HIMALIS's protocol stack and ID-based communication

3 ID-based communication network that contains sensor groups

Introduction of ID-based communication enables uninterrupted stable communications via the Internet, even if changes take place in the network layer, thus realizing M2M communication among mobile devices through the Internet and facilitating management after host configuration undergoes any changes. In this section, we describe a HIMALIS network that contains groups of mobile sensors, which represents an illustrative case of M2M communication based on ID-based communication.

3.1 Network configuration

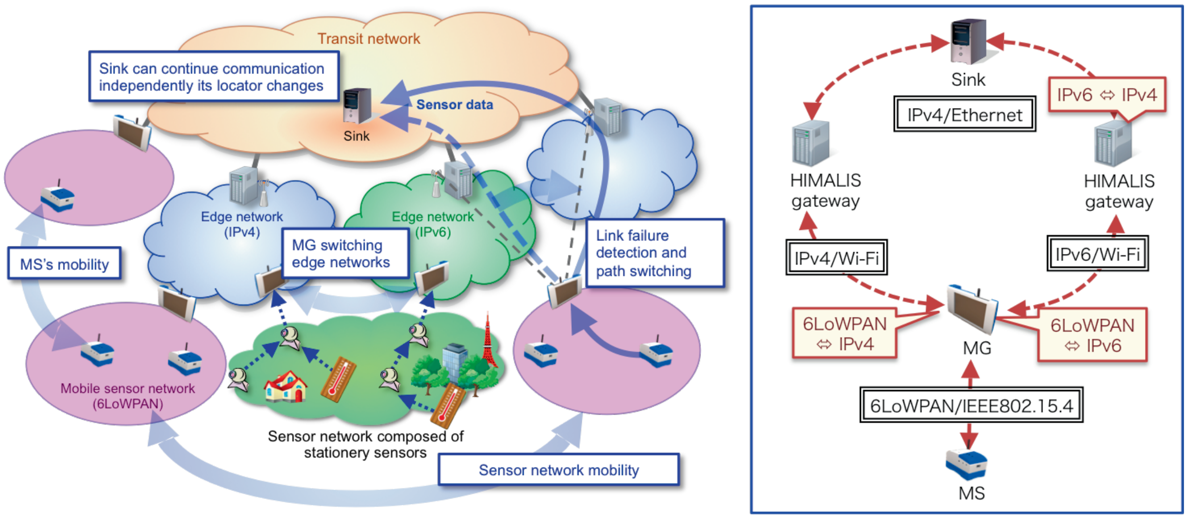
Introduction of ID-based communication into networks connecting sensors enables sensor-to-sensor M2M communications and control from the sensor administrator. These communications are not interrupted even if the sensor switches its network interface from one network to another. In this network, three new hosts (mobile sensors, mobile gateways, and sinks) are connected to a HIMALIS network (Fig. 3).

- A mobile sensor (MS) consists of a small sensor module, wireless communication device, computation module, and battery. An ID communication stack is implemented in the computation module, which transmits sensor data to any destination—by switching networks if needed—and receives data or commands directly from other remotely located ID-communication compatible hosts. The wireless communication module should comply with low-power communication standards such as IEEE 802.15.4, and the choice of communication protocol should be 6LoWPAN (IPv6 over Low power Wireless Personal Area Networks), which is characterized by small communication overhead and connectivity to IPv6 networks. The sensor module should be capable of mounting more than one sensing function, each of which can be switched on/off as needed.

- The mobile gateway (MG) is connected to a sensor network that contains more than one MS. The sensor network can exchange locators with edge networks. The MG itself is implemented with ID-based communication functions, enabling it to support mobility and multihoming. The MG should also provide capability to aggregate handover signaling of connected MS groups, and to switch the entire sensor network to another edge network. In addition, it should allow connection to conventional fixed sensor networks —which may not be compatible with mobile communication. The data collected from the fixed sensors is collectively transmitted to the destination.

- The sink is a mobile host that provides data server functions for storing sensor data. With these functions, the sink can be deployed a transit network or an edge network (or both). Host authentication and direct communication provided by ID-based communication ensure safe reception of sensor data from the MS. The sink also provides a Web-based sensor control interface that allows access from general hosts that do not have HIMALIS communication functions. Using this, remotely located agents (man or machine) can control the MS.

The MS, MG and sink (all with HIMALIS communication functions) can maintain uninterrupted communications even if the connected network is changed during a communication session (Fig. 4). Using this capability, an MS can monitor the situations around by switching to other mobile sensor networks on an arbitrary timing. When MG switches different edge networks, the mobile sensor network accommodating several MSs can also switch the link to the networks without asking MSs to switch the network connection. Introduction of ID-based communication technology enables access to each arbitrary MS even if more than one MS is contained on an MG. This enables deployment of MSs into variety of mobile objects.



Mobility scenarios of HIMALIS sensor network

Communication from MS to Sink

Fig. 4 Mobility scheme of mobile sensors and mobile gateways

3.2 Use case: HIMLAIS network that contains mobile sensor groups

As described above, HIMALIS communication that uses a host specific identifier provides such useful mechanisms as: location management of hosts, and safe and uninterrupted communications. Taking advantage of these features, the HIMALIS-based system can find many applications such as real-time monitoring of the situation around mobile objects and remote control/management of devices mounted on a mobile object. Two major use cases are shown here.

3.2.1 Medical service at any place

Many of the healthcare services that use currently available sensors are generally package types—meaning that the device and service are inseparably bound. Therefore, purchase of the device is a must to receive the service, and after purchase modification of service content is generally difficult. In addition, the sensors mounted on mobile devices (smartphones and watches) can provide only a limited range of bodily measurements (physical restrictions). To realize continuous body monitoring, many sensors should be mounted on the body, and they must be added/removed on an as-needed basis, and they must be properly controlled to transmit required information to the correct. However, such requirement may be unrealistic because of complexity of configuration setup.

Introduction of HIMALIS enables detection, identification and control of each device from a remote location. In such HIMALIS-based system, as the service can handle the burden of controlling devices, dynamic control in response to body conditions—automatic settings of devices and selection of active sensors, adjustment of data acquisition intervals becomes a reality. Such a system is able to monitor body conditions on a 24/7 basis under optimized settings, and also enables the service to provide dynamic feedback to the user. Information from such monitoring can be effectively utilized in a variety of situations: preventive care of lifestyle diseases, warning the patient before his/her chronic disease gets worse, and, in an emergency situation, body information is sent to ambulance/hospital in real-time. Thus, such body information finds wide application for patients under long-term care, as well as for those who need emergency treatment.

3.2.2 Wheelchair support service

The wheelchair is one of the most easily available tools for persons with physical disabilities to move around without a third person's attendance. However, moving around with a wheelchair has its own problems: steps and inclinations on roads, interference with pedestrians, uncomfortable jolting on bumpy roads, difficulty of grasping road situations, congestion on roads that changes every moment, and others. Serious accidents are reported every year, and many users feel unsecure while they are seated in a wheelchair. As an approach to solve these problems, a type of wheelchair with sensors mounted on it has been designed. Information from the sensors is used for tracking moving routes, visual display of hidden danger, and others. Such anticipation information serves as a useful tool for wheelchair users to avoid unknown hazards[8]. To make such system a reality, mechanisms must be designed to upload required information – road surface conditions, positional information, operations taken by the wheelchair

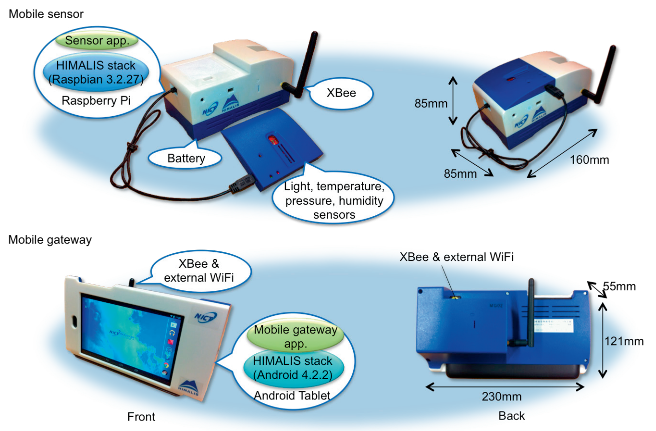


Fig. 5 Implementation of mobile sensors and mobile gateways

user and his/her posture—to the server in a safe and secure fashion, and upload processed data from the server to the user. In general terms, such an IT system can be incorporated into a wheelchair using only currently available technologies. However, what is needed here is a wheelchair with a higher level of flexibility—i.e. a wheelchair that can be easily and flexibly customized to a particular person. Such a wheelchair can be shared by more than one physically disabled person and be available for rent when he/she travels around.

Introduction of HIMALIS enables the server to identify and manage the wheelchairs, each sensor, and the hosts in each person's possession. The remotely-located server can configure the wheelchair to the optimum settings on a person-to-person basis based on the user information (physical strength, driving habits, medical history, and others).

4 System design and implementation

4.1 Implementation of HIMALIS network that contains mobile sensor groups

In the previous section, we gave an account on a HIMALIS network that contains several sensors. This was an example of IoT/M2M that uses ID-based communication. To verify the validity of the system, we implemented MS and MG on it (Fig. 5).

We developed MS based on a Raspberry Pi: this scheme allows to mount a variety of sensor boards on the MS and to deploy MSs on several types of mobile objects. Raspbian OS 3.2.27 (with additional implementation of a HIMALIS stack on it) was installed on a Raspberry Pi, enabling the MS to directly perform ID-based communication. An XBee module (IEEE802.15.4 compatible) was used as the communication module to use the 6LoWPAN protocol that allows IP communications over IEEE802.15.4. Four sensors (temperature, humidity, illumination and atmospheric pressure) were mounted on the sensor board to verify dynamic controllability of the system. The sensor board was connected to a Raspberry Pi using a USB cable—thus easily exchangeable to different sensor boards.

MG was developed based on an Android tablet to ensure easy mounting on to the mobile object, as well as to provide a user-friendly GUI and intuitive operations. An internal wireless LAN interface was basically used for connection with the edge network. Additional installation of an external wireless LAN interface supports make-before-break handover that has a merit of smaller packet loss during the handover process. AndroidOS 4.2.2 (with additional implementation of a HIMALIS stack) was installed on the MG, enabling it to relay MS communication packets and forward the packets appropriately in reference to the ID header. The XBee wireless module (6LoWPAN protocol implemented) was mounted on it to establish connection with the MS. To reduce packet collision instances, CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) was used in place of the XBee's standard communication method, i.e. Digi Mode communication.

The system organization of the HIMALIS network—with mobile sensor groups contained within it—is shown in Fig. 6. MS and MG are connected as shown in the figure. If MG has two wireless LAN adaptors, multihomed connection to more than one edge networks is also available. As this system supports make-before-break handover (smaller packet loss while moving), the system is able to relay MS data even while the MG is switching from one network to another. The 6LoWPAN module (mounted using user land) compresses an IPv6 packet header that was forwarded from the HIMALIS stack via the TUN module. The packet with a compressed header is forwarded to the mobile sensor network by way of the XBee's serial transmission. The sink is implemented for two purposes: as a database server application that gathers data from sensors, and as a mobile host on which a sensor application runs to control MS sensors. The sink is connected either to an edge network or a transit network.

4.2 Mobile sensor's handover support by mobile gateway

To verify implemented communication functions, and to evaluate handover functions, packet loss was measured.

In this examination, the MG switches its link from one edge network to another on an arbitrary timing, and packet loss variations of the MS, caused by the switching, were measured. The networks used for the experiment are shown in Fig. 6 (IPv4 network is shown in blue, and IPv6 network in green). The maximum number of MS's connected to the MG is set to 5, to avoid excessive complexity of evaluation. While the five MSs were sending UDP packets to the sink at a one-second interval, the MG switched between the two edge networks (IPv4 and IPv6). Figure 7 shows the number of successfully received packets by the MG, and the number of those received by the sink. In Figure 7, the horizontal axis represents reception time, and the vertical axis indicates the packet ID (sequentially increasing number allocated by MS when the packet is sent out). The figure clearly illustrates which packet from which MS was successfully received. Despite the complicated situation—i.e. coexistence of IEEE802.15.4 and IEEE802.11b/g—all the packets were successfully received. On the other hand, in the communications between the MG and sink, a certain packet loss was observed starting right after a handover processing. This packet loss was found to be caused by the driver installed in the external wireless LAN interface. The results from the experiment described above clearly indicate that network switching by MG at an arbitrary timing does not exert any negative effect on data transmission from MS.

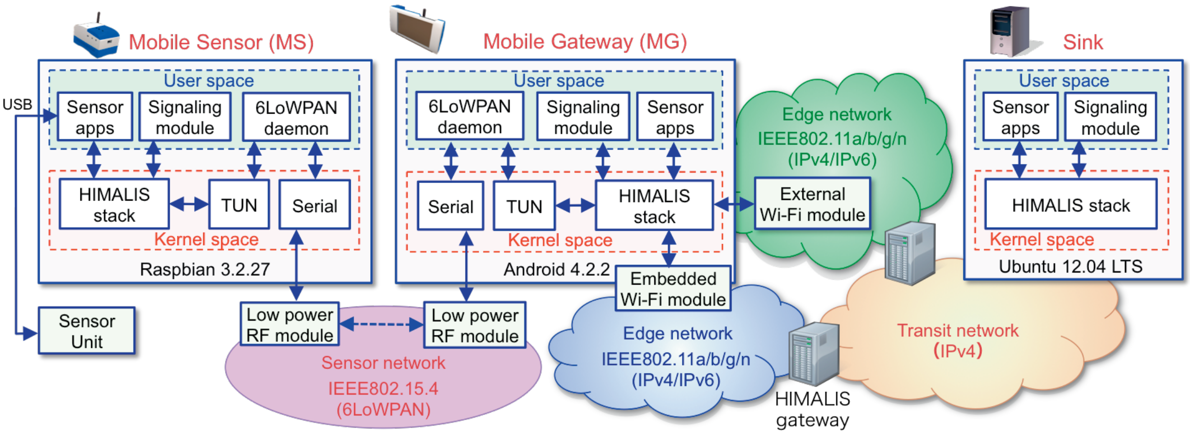


Fig. 6 System organization

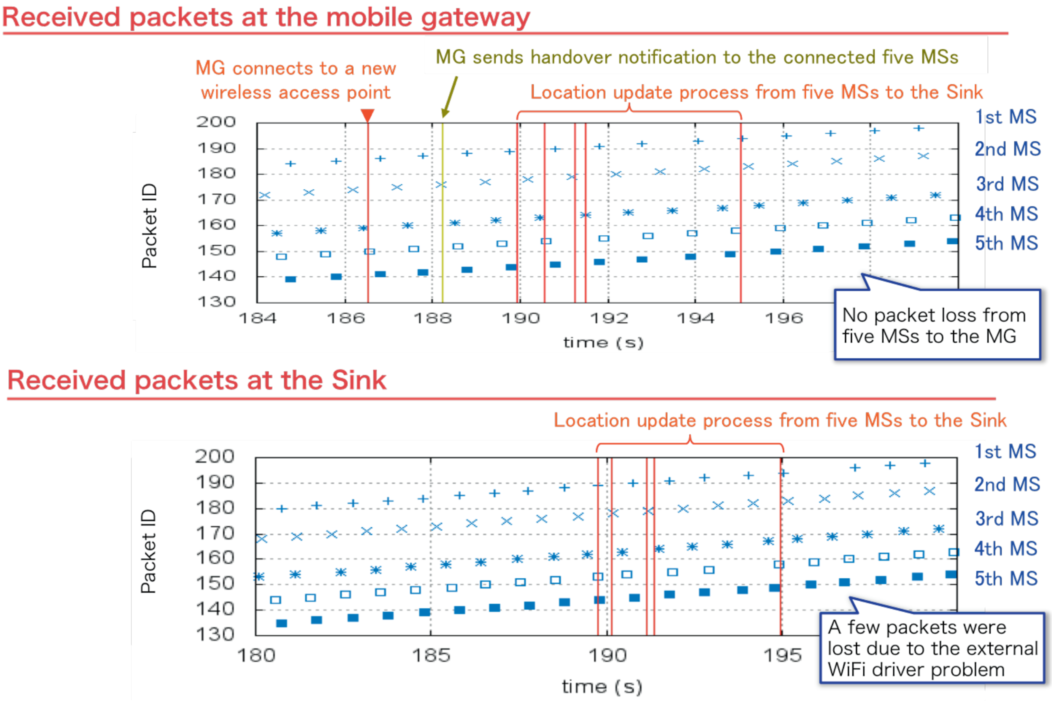


Fig. 7 Packet loss occurrence during a handover: MG is relaying communications of 5 MSs

4.3 Sensor applications

Several sensor applications were developed for use as a common platform to manage/control MS from the sink. Because of the nature of ID-based communication, development of an application that controls direct communication from the sink to MS is relatively easy. However, this application was developed with the objective of providing APIs for M2M communication, with additional features such as optimization of common operations, and starting and stopping of the sensor.

The sensor application for controlling the sink is a Web-based sensor management tool. Any person in charge of MS management has easy access to the sink using a Web browser. In this way, he/she can perform such operations as: searching an MS using ID-based communication, start/stop sending sensor data, and monitoring sensor data being uploaded to the sink. The left pane of Fig. 8 shows the browser based sensor control panel. In this control panel, we can enter an MS host name in the “hostname” field, and select the sensor and the desired sampling rate. In addition, the sampling rate of any particular sensor can be changed as needed, and data acquisition from any redundant sensor can be stopped to reduce power consumption.

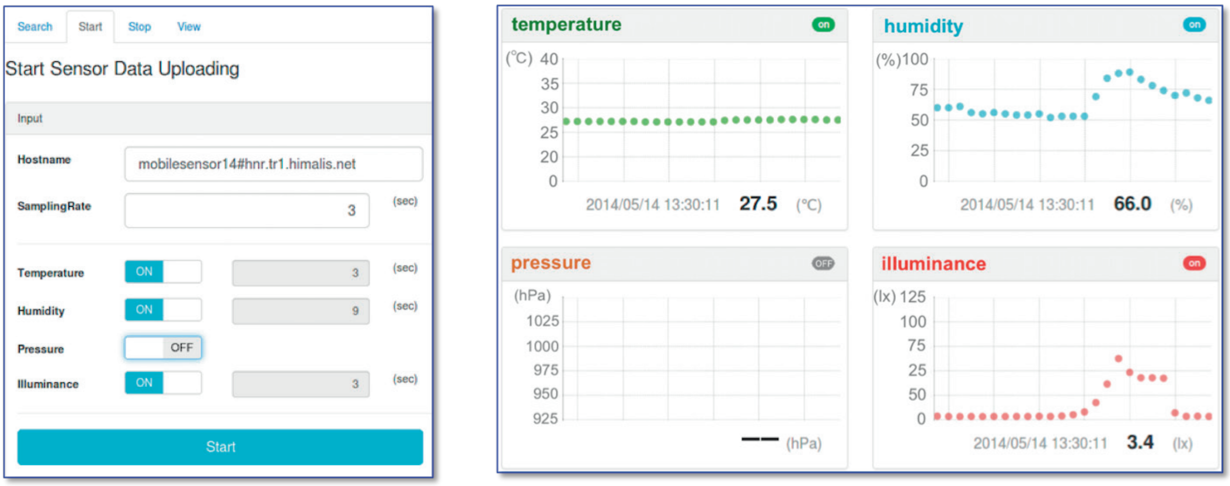
The sensor application for MS notifies the states of the sensors (running/stopped), and controls starting/stopping of data upload from the specified sensor. The data sent from a sensor include acquired data and time stamps. To prevent falsification of data by a man-in-the-middle attack, the data is signed with the shared key (exchanged with the sink beforehand).

The sensor application for MG has a function to add positional information to the sensor data it relays. It also provides a function for an MG to send the sensor data to more than one sink simultaneously. This function is triggered when more than one sink sends an upload request to the same MS, and has an effect of avoiding duplicated sensor data transmissions.

The sensor applications described above were actually implemented in the system for evaluation, and we confirmed that the desired functions—dynamic remote control and monitoring of MSs—work in the sensor applications (Fig. 8, right).

5 Conclusion

In the future IoT environment, where an enormous number of hosts perform M2M communications, a mechanism is required to ensure Internet-based host management and secure remote control. As a preliminary study toward realization of IoT/M2M in the future, we conducted an analysis on such aspects as the host management mechanism and mobile sensor management in an ID/locator split network architecture HIMALIS with an embedded mechanism for safe and dynamic continuation of communication among heterogeneous network layer protocols. In this study, we introduced an ID-based communication scheme of HIMALIS architecture into the two element technologies: gateways that relay mobile sensors and data, and sinks for data storage. Through the study using actual implementation of devices, we demonstrated the viability of M2M communications among mobile devices that connect to each other using different network layer protocols. In the future, we plan to optimize control messages aiming at a viability demonstration of multi-device communication.



Start Sensor Data Uploading

Input

Hostname: mobilesensor14#hnr.tr1.himalis.net

SamplingRate: 3 (sec)

Temperature: ON 3 (sec)

Humidity: ON 9 (sec)

Pressure: OFF

Illuminance: ON 3 (sec)

Browser-based sensor control panel

Sensor data display panel

Fig. 8 Sensor application screen: the sink manages/controls mobile sensors

Acknowledgments

This research was conducted with Dr. Hiroaki HARAI (Director of Network Architecture Laboratory), Dr. Kenji FUJIKAWA (Senior Researcher), Dr. Yuichi TERANISHI (Research Manager), Mr. Tomoji TOMURO (Technical Expert), Mr. Yasunaga KOBARI (Technical Expert) and others. The authors express sincere gratitude to those who helped us during the course of this research.

References

1 Ericsson, "More than 50 billion connected devices," White Paper, Feb. 2011.

2 ITU-T Focus Group Technical Report on M2M Service Layer, "M2M service layer: Requirements and architectural framework," 2014.

3 R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423, May 2006.

4 V.P. Kafle and M. Inoue, "HIMALIS: Heterogeneity inclusion and mobility adaptation through locator ID separation in new generation networks," IEICE Trans. Commun., Vol.E93-B, No.3, pp.478–489, March 2010.

5 V. P. Kafle, Y. Fukushima, and H. Harai, "Design and Implementation of Dynamic Mobile Sensor Network Platform for ID-Based Communication," IEEE Communications Magazine – Communications Standards Supplement, Vol.53, Issue 3, pp.48–57, March 2015.

6 Y. Fukushima, V. P. Kafle, and H. Harai, "ID-based Communication for M2M in Next-Generation Mobile Networks," IEICE Tech. Rep. RCS2014-250, pp.177–182, Vol.114, No.372, Dec. 2014.

7 Large-scale open test-bed JOSE, http://www.nict.go.jp/en/nrh/nwgn/jose.html

8 Y. Iwasawa, H. Suzuki, and I.E.Yairi, "Detecting Exceptional Actions Using Wearable Sensors' Data for Developing Life-Log Database of Visually Impaired People," AAAI Spring Symposium: Data Driven Wellness 2013, pp.6–11, 2013.

Yusuke FUKUSHIMA, Ph.D.

Researcher, Network Architecture Laboratory, Photonic Network Research Institute
Network Architecture, Mobile Network, New Generation Network

Ved P. KAFLE, Ph.D.

Senior Researcher, Network Architecture Laboratory, Photonic Network Research Institute
Network Architecture, Mobile Network, New Generation Network