M2M Service Platforms: Survey, Issues, and Enabling Technologies

Jaewoo Kim, Jaiyong Lee, *Member, IEEE*, Jaeho Kim, and Jaeseok Yun, *Member, IEEE*

***Abstract*—Machine-to-Machine (M2M) refers to technologies with various applications. In order to provide the vision and goals of M2M, an M2M ecosystem with a service platform must be established by the key players in industrial domains so as to substantially reduce development costs and improve time to market of M2M devices and services. The service platform must be supported by M2M enabling technologies and standardization. In this paper, we present a survey of existing M2M service platforms and explore the various research issues and challenges involved in enabling an M2M service platform. We first classify M2M nodes according to their characteristics and required functions, and we then highlight the features of M2M traffic. With these in mind, we discuss the necessity of M2M platforms. By comparing and analyzing the existing approaches and solutions of M2M platforms, we identify the requirements and functionalities of the ideal M2M service platform. Based on these, we propose an M2M service platform (M2SP) architecture and its functionalities, and present the M2M ecosystem with this platform. Different application scenarios are given to illustrate the interaction between the components of the proposed platform. In addition, we discuss the issues and challenges of enabling technologies and standardization activities, and outline future research directions for the M2M network.**

***Index Terms*—Machine-to-Machine, Service Platform, Architecture, Identification, Addressing, Communication and Networking, Peer-to-peer, Management, Standardization.**

I. Introduction

MACHINE-to-Machine communication occurs among machines (some objects or devices) with computing/communication capabilities without human intervention [1]. Existing Human-to-Human communications are expanding to Human-to-Machine, or Machine-to-Machine Communications. M2M uses machines to monitor certain events with sensors and to instruct actuation [2]. The captured events are relayed through wired or wireless networks to servers, which extract and process the information gathered and automatically control and instruct other machines. The network provides end-to-end connectivity between machines.

Industrial supervisory control and data acquisition (SCADA) systems [3], introduced in the 1980s, may be regarded as early forms of M2M. While M2M and SCADA focus on similar functionality, SCADA consists of isolated systems based on proprietary technologies, which make the solution expensive. SCADA has begun to open up its proprietary protocols and publish its protocol specifications. It is transitioning from proprietary system to low-cost, standardized technologies. Currently various concepts similar to M2M have been introduced including the Internet of Things (IoT) [4], M2M communication [1][5], Smart Device Communications [6], Machine-Oriented Communication (MOC) [7], Machine-Type Communication (MTC) [8], and Ubiquitous Sensor Networks (USNs) [9].

M2M networks have various applications (services), such as environmental monitoring, civil protection and public safety, Supply Chain Management (SCM), energy & utility distribution industry (smart grid), Intelligent Transport Systems (ITSs), healthcare, automation of building, military applications, agriculture, and home networks [1][9]. These innovative M2M applications and services create an array of new business and market opportunities

The characteristics of M2M networks are quite different from those of conventional wired or wireless networks [1][5][8]. M2M networks are composed of large numbers of nodes, since the main subject participating in M2M communication is a machine or object, or indeed it can be everything around us. To give such a large number of objects (millions or billions) the ability to communicate, the cost must be low. Because most machines are battery operated, energy efficiency is the most important aspect. As the machine senses itself or its surrounding physical environment, the traffic per machine is very small. However, data are generated from a large number of objects, and because the data generation period, amount, and format are all different, a large quantity of data is generated. While M2M communication can occur without human intervention, operational stability and sustainability are also required.

Many M2M research activities and solutions do not address some of the main issues of application and service development necessary for the realization and dissemination of M2M services, as they are focused on energy efficiency, wireless networking, and protocols [14]. M2M service platforms are a relatively new area of interest. [15] provided an initial analysis and comparison of the several M2M platforms. The authors compared according to their main focus the platform's aims among people, objects, environments, and enterprise systems. They also compared how much the platforms fulfilled the requirements of the M2M platform they defined: standard based, versatility, scalability, and IoT oriented. In contrast, we surveyed more platforms including those in [15], our focus for survey being the functionality and ecosystem the platform provides. The following topics need to be dealt with M2M service platforms: addressing, naming, identifying, peer-to-

Manuscript received October 1, 2012; revised May 28, 2013.

Jaewoo Kim and J. Lee are with the Department of Electrical and Electronics Engineering, Yonsei University, 50 Yonsei-ro, Seodaemun-gu, Seoul 120-749, Korea (e-mail: {kimjw064,jyl}@yonsei.ac.kr).

Jaeho Kim and J. Yun are with Embedded Software Convergence Research Center, Korea Electronics Technology Institute, 68 Yatap-dong Bundang-gu, Seongnam, Korea.

Digital Object Identifier 10.1109/SURV.2013.100713.00203

peer (P2P) interaction (communication), communication and networking, mobility, and the management of devices and networks for sustainability. Platform design and architecture need to be developed to enable the seamless integration of Internet-connected objects into services and important real-life stakeholder applications, thus avoiding the commonly heard complaint in M2M service platforms that there are too many silos [38]. The main purposes of such platforms are (i) to facilitate the development of new and creative applications, (ii) to manage devices and users efficiently, and (iii) to accelerate the ecosystem of different domains for M2M services.

In this paper, we present a survey of recent M2M issues. In classifying M2M devices and their applications, we first highlight the application profiles of these devices. With these features in mind, we discuss the necessity of and requirements for M2M platforms. We then propose an M2M service platform (M2SP) architecture and compare it with other M2M platforms. After this, we present a service scenario based on this architecture. Then we discuss the key technologies enabling the M2M service platform: the addressing, naming, and identification of M2M devices; communication and networking protocols; P2P communication; and the management of devices and networks. We also discuss the standardization activities of international organizations.

The remainder of this paper is organized as follows. In Section II, we review the features of M2M applications and traffic. In Section III, we give a brief background of M2M and comparison of existing M2M platforms. In Section IV, we propose an M2M service platform architecture with service scenarios. In Section V, The key technologies enabling the M2M service platform and standard activities in international standard organizations are presented. Finally, Section VI offers a conclusion and discusses future research directions.

II. Features of M2M Applications and Traffic

A. M2M Classification and Applications

As mentioned above, M2M has various applications, all of which require devices with different characteristics and functions [1][8]. There are public applications such as environmental protection and ITS, as well as non-public applications such as home network, asset management, and bio and medical applications. There are also location-based services, which require localization techniques, such as ITS and asset management. Some applications require the mobility of devices, such as mobile robots. Finally, some portable devices have fewer energy efficiency restrictions since charging batteries is easy. Thus, depending on the application, there can be M2M machine devices from dummy and simple nodes to intelligent and powerful capability nodes. Network technologies must be designed taking into account the various characteristics and applications.

We classified M2M nodes from low-end sensor nodes to mid-end and high-end sensor nodes, according to their hardware capabilities, and linked node types with applications, characteristics, and required functionalities (functions); the summary of this classification is shown in Table I. In the Table I, if a node type requires/does not require a function, the corresponding table entry is marked with O/X, respectively. If a node type may or may not require a function depending on the application, then the corresponding entry is marked with "△".

Low-end sensor nodes are cheap and have low capabilities. They are static, energy efficient, and simple. These nodes are deployed by spraying them in the region of interest. They have a high density in order to increase the network lifetime and survivability. Their resources are too constrained to have IP support. They have basic functions such as data aggregation, auto configuration, and power saving, and they are applicable to environmental monitoring applications.

Mid-end to high-end sensor nodes are more expensive than low-end sensor nodes, and may have mobility depending on the applications. They are subject to fewer constraints with regard to complexity and energy efficiency, and may have additional functionalities such as localization, Quality of Service (QoS) support, TCP/IP support, power control or traffic control, and intelligence. Mid-end sensor nodes can be applied to home networks, SCM, asset management, and industrial automation.

High-end sensor nodes can be applied to ITS and military or bio/medical applications. High-end nodes have a low density and are able to handle multimedia data with QoS requirements, such as video streaming. Mobility is an essential function for mobile robots. This category includes mobile devices such as smart phones.

B. Traffic Features of M2M Applications

M2M devices generate various traffic patterns, including periodic, event-driven, and multimedia streaming patterns, depending on their applications. These various traffic patterns are generated by the massive number of nodes, which have different patterns, generation periods, and generated amounts. This will create big data [16] which is a collection of data sets so large and complex that M2M traffic becomes difficult to process.

Figure 1, reconstructed based on [17] and [18], shows an example of daily M2M traffic patterns from M2M nodes in the different applications. In Figure 1, $S_1 \sim S_4$ is an example of the continous/event-driven/periodic traffic pattern generated from the node of applications such as surveillance camera/emergency report/metering, respectively. When these various data traffics from a large number of sensors are gathered through IP network, an unpredictable pattern is created at the core network, as seen at the right side of Figure 1, S. The accumulated traffic in the core network may cause network congestion and outage of network resources [18]. The core network must handle these large volumes of data to guarantee the QoS and reliability for applications.

III. M2M Platforms

A. Necessity for M2M Platforms

Because of the different standards that device manufacturers use, application services based on machine devices are difficult to manage and expand. Application services need to implement different interfaces to communicate with different types of machines. As these interfaces provide the same functions and develop the same applications, supporting

TABLE I
M2M NODE PROFILES

		Low-end	Mid-end	High-end
Application services		Environment protection	Home networks, SCM, Asset management, Industrial automation	ITS, Military, Bio/Medical
Characteristics	Density	High	Mid	Low
	Complexity	Low	Mid	High
	Energy efficiency	High	Mid	Low
	Cost	Low	Mid	High
	Scalability	High	Mid	Low
	IP	Non-IP	IP	IP
	Mobility	Low, almost static	Low mobility	Mobility
	Hop count	High	Mid	Low
	Intelligence	Low	Mid	High
Functions	Data aggregation	O	△	X
	Auto configuration	O	O	O
	Power saving	O	O	O
	Localization	X	△	O
	QoS support	X	△	O
	TCP/IP	X	△	O
	Power control	X	△	O
	Traffic control	X	△	O

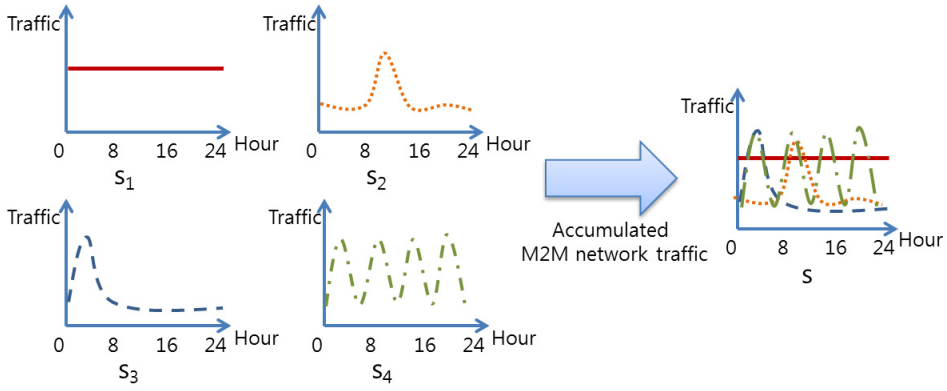

Fig. 1. An example of an M2M network traffic pattern

different interfaces is a redundant process, which slows down the development of service applications and devices, as well as the activation and growth of M2M services. Figure 2, revised from [11], shows the current vertical M2M deployments together with the horizontal M2M deployments based on an M2M service platform. Current M2M markets are highly fragmented. Various vertical M2M solutions have been designed independently and separately for different applications, which inevitably impacts or even impedes large-scale M2M deployment [10]. To realize the vision and goals of M2M services, horizontal M2M deployments with an open M2M service platform, which enables inter-industry convergence services by sharing data and establishes the M2M ecosystem, are essential.

An open M2M service platform will connect with one another all the ecosystems of the contents (services), platform, network, and device (CPND) domains, which were previously independent, and establish the M2M ecosystem. The M2M ecosystem, which consists of the stakeholders, including device providers, Internet service providers (ISPs), platform providers, service providers, and service users [4], can substantially reduce deployment costs and improve time to market of M2M services. The device provider is responsible for devices providing raw data and/or content to the network provider and application provider, according to the service logic. The ISP provides their infrastructures for M2M device communications. The platform provider provides integration capabilities and open interfaces, as well as data storage, data processing, or device management. The application provider utilizes capabilities or resources made available by the network provider, device provider, and platform provider, in order to provide M2M applications to customers. The service user is an individual or company what utilizes M2M applications provided by an application provider. This M2M ecosystem with an open M2M service platform encourages the stakeholders to develop and realize their innovative services, and stimulates

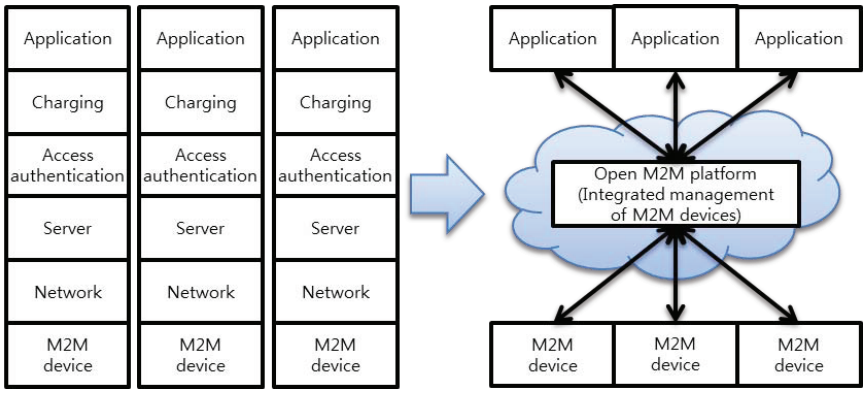

Fig. 2. The necessity for the M2M service platform

rapid and organic growth of CPND domains of the M2M market.

B. Comparisons of Existing M2M Platforms

Existing platforms for M2M services can be devided into three categories: 1) commercial M2M platforms that currently provide M2M services; 2) M2M hardware platforms for M2M devices; and 3) research on M2M platforms that deals with the architecture and functions of such platforms. By analyzing these platforms, we can model the existing M2M platforms and compare them. We may then derive the ideal M2M platform.

1) Commercial M2M Platforms: The European Telecommunication Standards Institute (ETSI) Technical Committee M2M (TC M2M)provides an M2M architecture with a generic set of capabilities for M2M services. ETSI M2M defines the Service Capability Layer (SCL) as providing functions that are shared by different applications, and the reference points between M2M devices, gateways, and the network. ETSI M2M adopted a representational state transfer (REST) architecture style [36] and standardizes the resources structure that resides on an M2M SCL and the procedures for exchanging information by means of the resources over the reference points. This standard can be referred to when implementing an M2M service platform that adopts the ETSI M2M standard interface for communications. Many commercial M2M platforms are compliant with the ETSI M2M standard.

Current commercial M2M platforms include Cosm [19], ThingSpeak [20], Nimbits [21], EVERYTHNG [22], Sensinode [23], OnePlatform [24], Axeda [25], SensorCloud [26], NeuAer [28], and iDigi [29]. The characteristics of these platforms can be summarized as follows:

- Application protocol and interface: Existing platforms use REST architecture or Simple Object Access Protocol (SOAP) for interfaces and they operate on Hypertext Transfer Protocol (HTTP), Constrained Application Protocol (CoAP), or HTTPS protocols. Most platforms use RESTful architecture based on the HTTP protocol. Some use lightweight CoAP, and others use HTTPS for security.
- Registration: Devices and users have to be registered to the platform.
- Open source: Application developers and users can develop new services themselves by using the software developer's kit (SDK) provided by the platform.
- Data processing: Platform can process and analyze the information collected from devices, such as the maximum, minimum, and average values of the data or perform other customized function.
- Account: The platforms provide differentiated accounts according to privacy, storage, service type (SMS, web service, cloud), and the number of available devices.
- User access: The platforms support mobile devices (applications), web portals, or application programs.
- Business model: 1) Individual users install devices and share them; in this case, a user's device provides information to other users. 2) Some platforms are aimed at enterprises or for public purposes and require a large number of nodes, for example, industrial automation or environmental monitoring.
- M2M network support: Some platforms allow gateways to connect devices that cannot directly connect to the Internet.

Table II shows the existing commercial platforms and indicates the main characteristics of each. The corresponding characteristics of a platform are marked with "O" and the final column briefly states some features of the platform or hardware related to them.

2) M2M Hardware Platforms: There are two types of hardware platforms that can be connected to commercial service platforms. One is off-the-shelf commercial products that are related to certain platforms, for example, Cosm consumer products [30], ioBridge [31], NanoRouter [23], MicroStrain Sensors [32], and Digi routers [29] (see the last column of Table II). The second type is a development/hackable platform that users can develop themselves, such as Arduino [33], mBed [34], or Nanode [35].

3) M2M platform architecture: INOX [38] is an M2M service architecture. The authors propose a new platform architecture for M2M services. They regard M2M/IoT networks as a combination of an M2M/IoT application environment in which there are applications talking directly to the sensors and things, and the common services and management architectural model. In INOX, the platform functionalities provided are the registry and discovery of things, monitoring, virtualization of objects, networking and computational resources, service enablers and self-functionalities (self-management,

TABLE II
COMMERCIAL M2M PLATFORMS

Platforms	Application protocol	Application interface	User access		Device sharing	User management	Business model	Data analysis	M2M area network support	Features
			Web	Mobile App						
Cosm	HTTP	RESTful	O	O	O	O	B2C, C2C	O		Open source API, realtime-data, control, monitor, analyze
ThingSpeak	HTTP	RESTful		O	O	O	B2C, C2C	O		
Nimbits	HTTP	RESTful		O	O	O	B2C, C2C			Sharing data points, Google cloud, ioBridge
EVERYTHNG	HTTP	RESTful	O	O	O	O	B2C, C2C			Active digital identity
Sensinode	HTTP/ CoAP	RESTful	O			O	B2B		O	6LoWPAN, ZigBee, Nano Stack
OnePlatform	HTTP	RESTful		O		O	B2B	O	O	Cloud service
Axeda	HTTPS	RESTful/ SOAP	O	O		O	B2B	O	O	Cloud service Axeda Wireless Protocol
SensorCloud	HTTPS	RESTful		O		O	B2B	O	O	MathEngine, MicroStrain sensors
Bugswarm	HTTP	RESTful	O		O		B2C			Linux based, support 3G, WiFi
NeuAer	HTTP	RESTful		O	O		B2C			Tag and Rule, NFC, WiFi
iDigi	HTTP	RESTful	O	O			B2B	O	O	ZigBee, WiFi, iDigi product

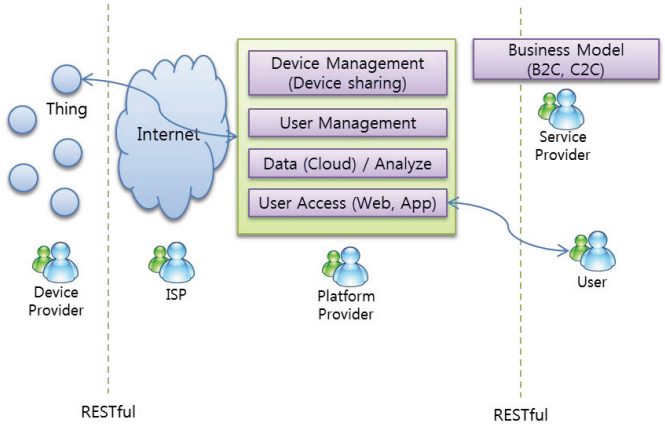

Fig. 3. Model 1: Commercial platform without M2M area network

self-organization, etc.), and orchestration capabilities for controlling and managing services. This model is closer to the ideal platform than are commercial platforms.

The authors in [39] designed an M2M platform that bridges business applications and machines based on the Java 2 Enterprise Edition (J2EE) framework and service oriented architecture (SOA). Web service is used to communicate with the external components. This can reduce their dependence on one another and allows for quick responses to changes in the industry chain. Internal design uses J2EE, which consists of a presentation layer, a business layer, and a data access layer.

BOSP [40] focuses on carriers' demands to construct a business operation support platform for M2M. BOSP is the architecture of an M2M platform formed by an access layer, a device management layer, and an ability formation layer. The access layer provides multi-networking capability over ubiquitous networks. The device management layer offers convenient methods to monitor and control massive devices. The ability formation layer creates the ability to quickly build networks and fulfill applications.

In [41], the authors proposed e-DSON, which is a distributed M2M service platform architecture using a service overlay network. The authors describe functions, object structure, and service flow of service composition process using their platform for M2M services. Although the platform has the same layer as [39], e-DSON has more detailed functionality in the service component of business layer. The e-DSON platform gathers various information such as users, services, contents, and resources, through interaction with other e-DSON platforms, then composes a service overlay network that satisfies the requirements of users and the network.

The work conducted in [42] adopted the IP Multimedia Subsystem (IMS) to integrate the M2M devices and services. It can take advantage of the legacy 3GPP network and coordinate MTC communications of 3GPP to communication management, such as congestion and overload control. Also,

experimental results of the retractable bollard management case study were presented.

C. M2M Platform Model

M2M service platform architecture can be divided into three categories: Model 1 is a commercial platform without M2M area networks, Model 2 is a commercial platform with M2M area networks, and Model 3 is a platform from the research areas. Figure 3 shows the platform of Model 1. Model 1 has a Business to Customer (B2C) and Customer to Customer (C2C) business model. The targets of the platform with the B2C and C2C models are individual users who have a small number of different devices. All devices are registered to the platform and shared with different users. Devices send their data to the platform periodically or when events or requests occur. These collected data are analyzed and converted into meaningful knowledge for users. Users who have subscribed can use the services by accessing the Web portal of the platform or using an application (app) on their personal mobile devices through a RESTful interface. In Model 1, M2M area networks, such as a sensor network, in which many connected sensors and objects cooperate with one another to accomplish complex tasks, are not supported.

Model 2 in the Figure 4 is also from the commercial platform. Unlike Model 1, Model 2 supports M2M area networks that collect data from many connected sensors and objects and are retrieved from an access gateway. This model has a Business to Business (B2B) model aimed mainly at companies that want to provide M2M services with M2M area networks or industrial automation rather than individual users.

Figure 5 shows Model 3. In Model 3, devices are also registered to a platform, as in Model 1 and 2. However, not only authorized personal user devices, but also authorized public devices or those of industrial domains are all shared with one another. Model 3 provides user access to M2M services via the Web service using user's PC or mobile phones. However, mobile apps which are optimized to mobile devices, are not considered. In contrast with Model 1 and 2, Model 3 does not have a concrete business model and does not consider the stakeholders involved in the M2M platform. Model 3 shares smart object resources with virtualization, and provides search and discovery for shared resources. It also supports an M2M area network. However, in addition to device management, M2M area network management functionalities, such as sensing coverage area management and network lifetime management, which is used to decide the replacement time of battery powered objects or sensor nodes [43], are not provided.

Figure 6 shows the ideal model for an M2M platform. It provides all the functions of Models 1, 2, and 3. The ideal model manages the devices, users, data, services, user access, and the network. It supports all business models (B2C, C2C, B2B, business to government (B2G)) and M2M area network management. For mobile devices, a mapping function between appropriate devices and apps is provided. It also offers P2P communication between end device and users or between end devices. The interface of device and users can utilize the RESTful architecture to follow the M2M standard. In addition to the stakeholders - the service users, device providers, platform providers, ISPs, and service providers mentioned in Section III - software developers who develop and release softwares such as app or Web applications to provide particular services using the devices, are involved in this model to sustain the M2M ecosystem.

D. Requirements of the M2M Platform

Based on Section III. C, we can derive the following requirements for an M2M platform:

- M2M device profile management: To access objects or devices connected to the Internet, they should be registered to a platform. The platform should be able to search and modify the registered M2M devices, and query a list of registered M2M devices. The platform should also be able to authenticate and control devices and support their management. M2M area network management is also required.
- M2M user profile management: The platform should be able to manage the user access restrictions to devices and services. It should be able to support profile registration and modification of service users, user authentication, user access, and manager information. It should be able to determine who is allowed to use which devices or services.
- M2M data management: The platform should be able to collect data from objects or devices. Smart device users should be able to access the platform, query the list of the collected data, and control the devices. Different data from different services should be able to provide mash-up services. Also, the platform should be able to react to the collected data by automatically controlling and instructing devices or actuators.
- App/Web access: Owing to the proliferation of smart devices, M2M services should be provided by mobile smart devices. Users should be able to access M2M services by using an app or the web. To support app access, the platform should manage the application store. To support Web access, the platform should provide a Web page for the M2M services. There are pros and cons to both access methods. Apps take time to download and install, but are optimized to smart devices(smart phones, tablets), and interoperation with device modules such as camera and sensors is possible. On the other hand, although access via the Web does not require anything to be downloaded, it is not optimized to devices, it is slower than an app, and interoperation with modules is restricted.
- Cloud services: The platform should be able to store data from objects and sensors. These data can be accessed anywhere and at anytime by users accessing the platform through the Internet.
- P2P communications: The platform should be able to support direct communication through the Internet without having to go through the platform between user devices and objects. P2P communication can reduce delay and prevent the storing of unnecessary traffic in the platform.
- M2M area network management: In addition to individual device management, the platform should provide network

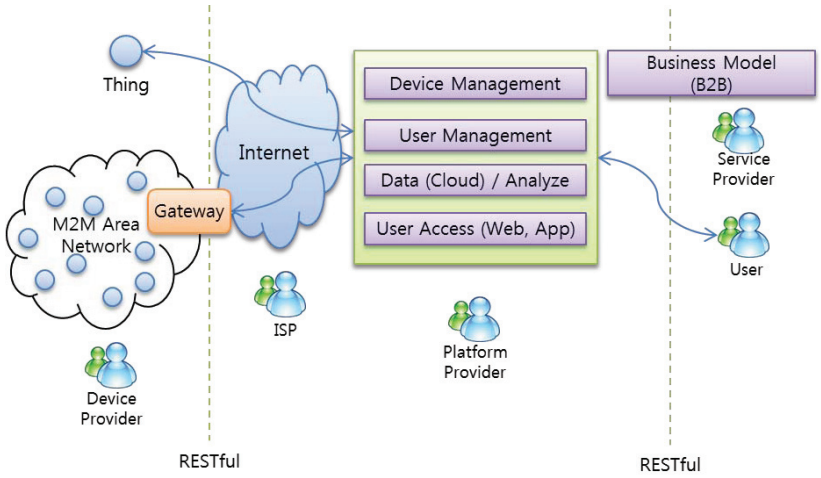

Fig. 4. Model 2: Commercial platform with M2M area network

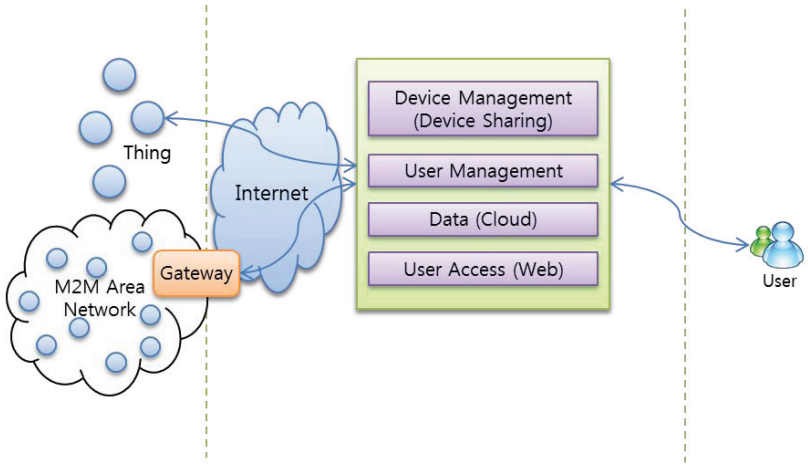

Fig. 5. Model 3: Platform architecture from research areas

management functionality for M2M are networks such as a sensor network.

- Connection management: The platform should be able to manage the interoperation and connection of the M2M devices, when the devices can be reached through various networks or communication methods.

IV. M2SP: M2M Service Platform

A. M2SP Architecture

Figure 7 shows the architecture of the M2SP and network. The M2M network is composed of M2M area networks, access networks, and a core network. Objects have communication modules and create M2M area networks. M2M area networks include various heterogeneous networks such as RFID, fixed WSNs, mid-end intelligent WSNs, high-end mobile WSNs, and wired sensor networks. A sink or gateway node collects information from these networks and connects to the core network through various access networks, such as WCDMA, LTE, Wi-Fi, or wired Ethernet. There are various types of traffic in the core network, generated from billions of objects, such as real-time traffic, periodic traffic, and streaming. The core network must be able to guarantee the QoS and reliability of this traffic. The objects and users connected through the core network are managed, and services can be provided via an M2SP. The M2SP consists of four entities.

- M2M Device platform: To access objects or devices connected to the Internet anywhere and at any time, these M2M devices must be registered. Registered M2M devices create a database of objects. From this, managers, users, and services can easily access information from M2M devices. The Device-platform manages device profiles, such as location, device type, address, and description. It is available to register, modify, and query devices. It provides devices with the functionality of authentication and authorization key management. It also performs the management functions of the devices and M2M area networks. It monitors the status of devices and M2M area networks, and controls them based on their statuses.

- M2M User platform: The User-platform manages M2M service user profiles and provides functionalities such as user registration, modification, charging, and inquiry. The User-platform interoperates with the Device-platform, and manages user access restrictions to devices, object networks, or services. Service providers and device managers have administrative privileges on their devices or networks. Administrator users can use an additional functionality that manages the devices through device monitoring and control.

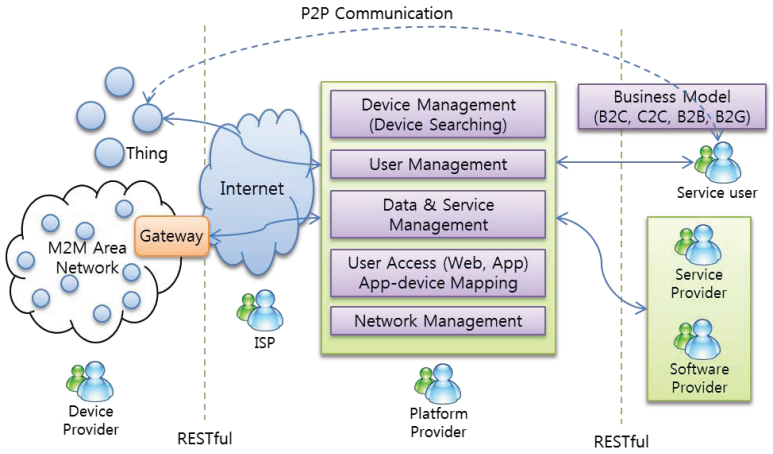

Fig. 6. The ideal platform model

- M2M Application platform: The Application-platform provides new integrated services based on the data sets collected from the devices. By providing an open API of the platform, different data from different devices can be blended and used to create new services. Open API developers can register developed open APIs to the Application-platform so that they can be operated in it. The Application-platform also collects control processing log data for the management of the devices by working with the Device-platform. For seamless services, connection management with the appropriate network is provided.

- M2M Access platform: The Access-platform provides an app or Web access environment for users. It contains apps or links to web sites that provide services. The service is actually provided through the Application-platform or M2M devices. For smart device apps, the Access-platform provides an app management function that manages app registration by developers and a mapping relationship between apps and devices. The mapping function provides an app list for appropriate devices.

In addition to these components, the platform uses RESTful architecture for app interfaces between the devices and platforms.

B. M2M Service Scenarios

Scenarios of M2M service based on the M2SP are now presented. They illustrate the interaction of the different components and stakeholders of the M2SP.

1) Low-End M2M Devices: An environmental monitoring application is shown in Figure 8. M2M nodes are deployed in the areas of interest in order to monitor various aspects of the environment, including temperature, humidity, water pollution, and air pollution. Service users can monitor the environment of the areas, and the M2M service provider manages the M2M area network for service maintenance. An M2M area network is formed by the low-end M2M devices and a sink node. A sink node is a gateway that provides the connection between the low-end devices and the service platform.

An M2M service provider buys sensor nodes from the device provider and installs them in physical areas. They are

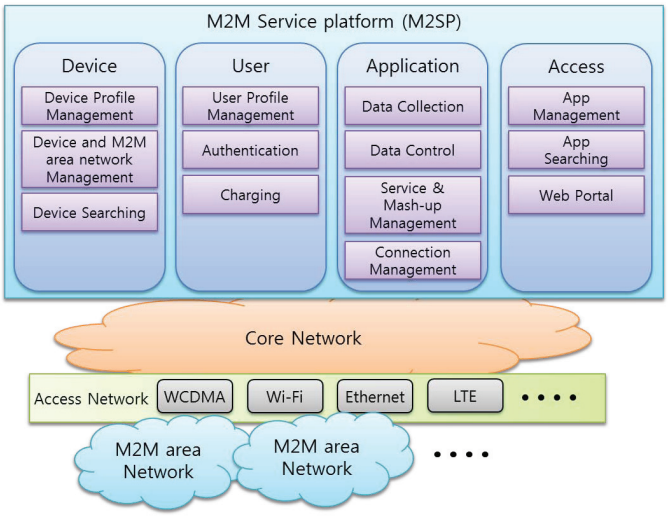

Fig. 7. The proposed M2M platform architecture

then registered to the Device-platform which is operated by a platform provider. The services provided by the devices are also registered to the Application-platform. A software/app provider registers apps for the devices to the Access-platform. The M2M service user and the M2M service provider register their authority to the User-platform as a user and administrator, respectively. They also register their mobile devices with the Device-platform. Then, they download the appropriate app for the environmental monitoring services by searching from the Access-platform.

The sensor nodes periodically send environmental information and information on its own status to the Application-platform. Using a personal device, the manager can access the machines through an app or on the Web. In this scenario, the service provider can also be a service user. The environmental data can be used to remotely monitor the environment of various areas for public purposes. The data can be made available to the general public. Additionally, mash-up with other devices or services is possible. The platform (Application-platform) can also automatize the control of other related devices. For example, an alarm message can be sent if certain conditions

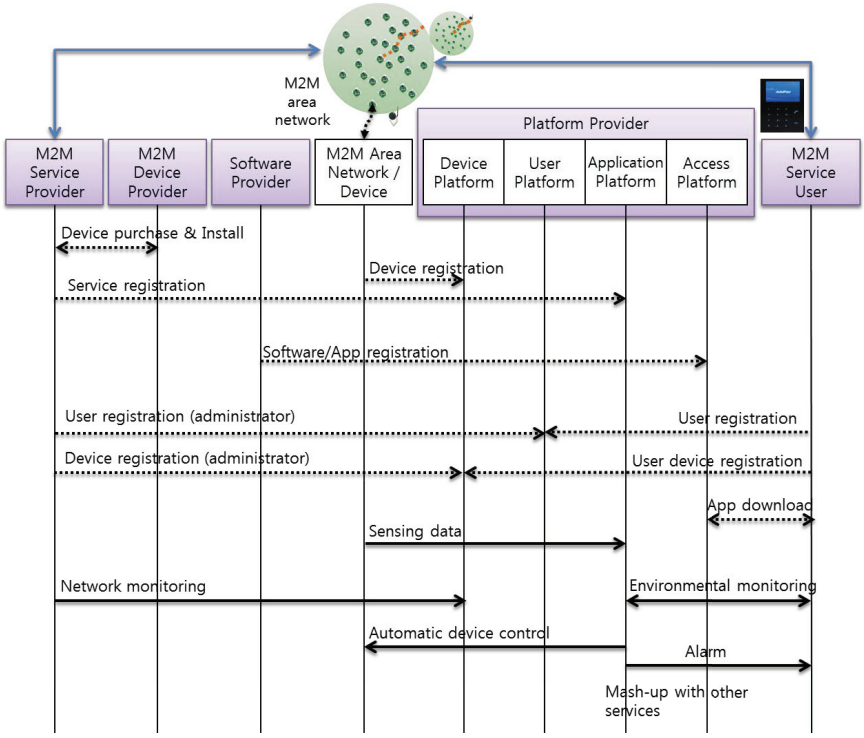

Fig. 8. Environmental monitoring service scenario

are met and it is possible to automatically control temperature or humidity for agricultural use. All the communications are provided by the ISP which is not presented in this figure.

The service platform can integrate the RFID. The handling of the RFID is not significantly different from the sensor devices. Basically, the RFID tag ID and related information are registered in the device platform. If the tag reader (including smartphones) transmits the tag ID to the device platform, the product information is returned. For further handling of the RFID and its application using the proposed platform, Application-platform can be involved. A tag reader can be considered as a sensor device that periodically check around RFIDs and transmits the RFID tag IDs, with other related information (such as location), to the Application-platform. The Application-platform sends an alarm message if some condition met, or commands other devices, depending on the application services. Application-platform can mash-up the RFIDs and other sensor devices to create a new service.

2) Mid-End M2M Devices: In this scenario, people use their smart devices to use the vending machine that is registered to the M2SP, as shown in Figure 9. Users can find the location of a vending machine that has the particular product they would like to purchase by searching for the product and stock information relating to surrounding vending machines. M2M service provider manages the vending machine by monitoring the stock, providing product information, and advertising products.

An M2M device provider manufactures a vending machine that has M2M communication capabilities. An M2M service provider buys these vending machines and installs them in physical places. The service provider then registers these machines to the Device-platform. The services provided by the devices are also registered to the Application-platform. A software/app provider registers apps for the devices to the Access-platform. The M2M service user and the M2M service provider register their device and authority with the User-platform. They also download appropriate apps for the environmental monitoring services by searching from the Access-platform.

The vending machine periodically sends information about product stock and its own status of the Application-platform. Using a personal device, the manager can access the machines through an app or on the Web. The manager can monitor the stock, provide product information, and advertise products using the vending machine's display. The manager can control the machine, including performing a reset or profile updating with Device-platform and the Application-platform. M2M users registered to the M2SP can access the vending machine through the Application-platform. Users can find a vending machine that has a particular product they would like to purchase. Mash-up with mobile payment is also supported in this scenario.

V. Enabling Technologies and Standardization Activities

A. Identification and Addressing

Owing to the proliferation of M2M services, it is expected that the large number of M2M devices will produce data that should be retrievable by authorized users. These M2M devices need to be uniquely identified and addressed. M2M devices and area networks must also interwork with IP core networks. Identification technologies must be able to handle the following issues [44]:

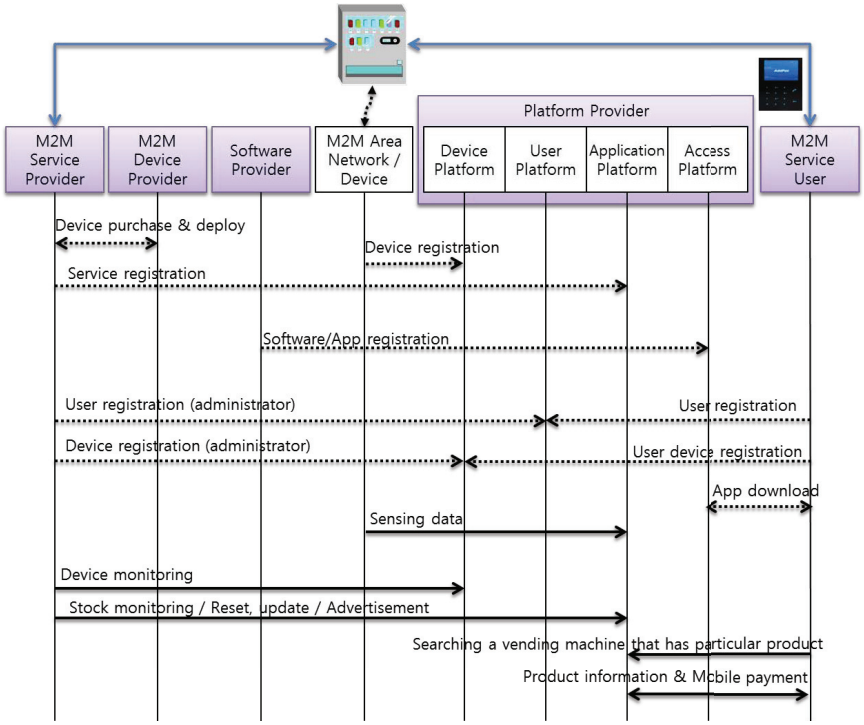

Fig. 9. Vending machine service scenario

- Uniqueness: A unique identifier must be assigned to one object.
- Consistency: A unique identifier must have the same meaning everywhere.
- Persistency: The lifetime of an identifier should be longer than the lifetime of the object.
- Scalability: An identifier has to support an unlimited number of identifier.

We first review the existing identifiers and addressing schemes. A Media Access Control (MAC) address is a unique identifier assigned to network interfaces for communication. MAC addresses are most often assigned by the manufacturers of devices. Currently, there are three address spaces for MAC addresses, MAC-48, Extended Unique Identifiers (EUI)-48, and EUI-64. EUI-64 was introduced to solve the MAC address exhaustion problem. It is made of a 24-bit organization unique identifier (OUI) and a 40 bit organization-specific identifier.

In the network layer, the IPv4 address scheme does not provide scalability. To solve this problem, IPv6 [45] was introduced. The IPv6 address is a 128-bit identifier that consists of 64 bits of the network prefix and 64 bits of the interface identifier. Connectivity, interoperability, and compatibility with heterogeneous networks must be provided. Internet Engineering Task Force (IETF) IPv6, over low-power wireless personal area networks (6LoWPAN) [46], provides a set of protocols that can be used to integrate resource-limited devices into IPv6 networks by simplifying IPv6.

TCP/IP cannot be supported in resource-constrained M2M devices. However, as mentioned above, depending on the M2M application, various kinds of capability nodes exist. For high-end M2M devices that are less resource constrained, TCP/IP based network protocols can be considered.

Figure 10 shows the IP-interworking architecture and protocol stack for the M2M network. Figure 10 (a) is the IP interworking architecture for the non-IP based M2M area network. In this case, a separate addressing scheme for the M2M area network is needed, as is the gateway that translates this packet into an IP packet. Figure 10 (b) [47] shows the IP-interworking architecture of the 6LoWPAN enabled M2M network. The 6LoWPAN adaptation layer over the IEEE 802.15.4 protocol stack performs header compression, and fragmentation is defined between the IP and link layers. Figure 10 (c) shows the IP-interworking architecture of M2M device nodes that support an existing TCP/IP. In this case, objects can establish end-to-end connection with one another.

Additionally, there are identifiers and naming for higher layers. A Uniform Resource Identifier (URI) [48] is a string of characters used to identify a name or resource. It can be classified as Uniform Resource Name (URN) or a Uniform Resource Locator (URL). A URN provides a globally unique, persistent identifier of a resource or a unit of information, regardless of location. A URL identifies the network location of an instance of a resource to find the resource identified by a URN and contains a physical path for finding the resource. An Object Identifier (OID) is a URN scheme used by a wide variety of computer applications and systems, including ISO applications such as X.500 directory schemes, the Simple Network Management Protocol (SNMP), and communication systems.

The Electronic Product Code (EPC) is designed as a universal identifier that provides a unique identity for every physical object anywhere in the world, for all time. Its structure is defined in the EPCglobal standard [49]. EPCglobal's main vision is the universal, unique identification of individual items using EPCs encoded in inexpensive RFID tags.

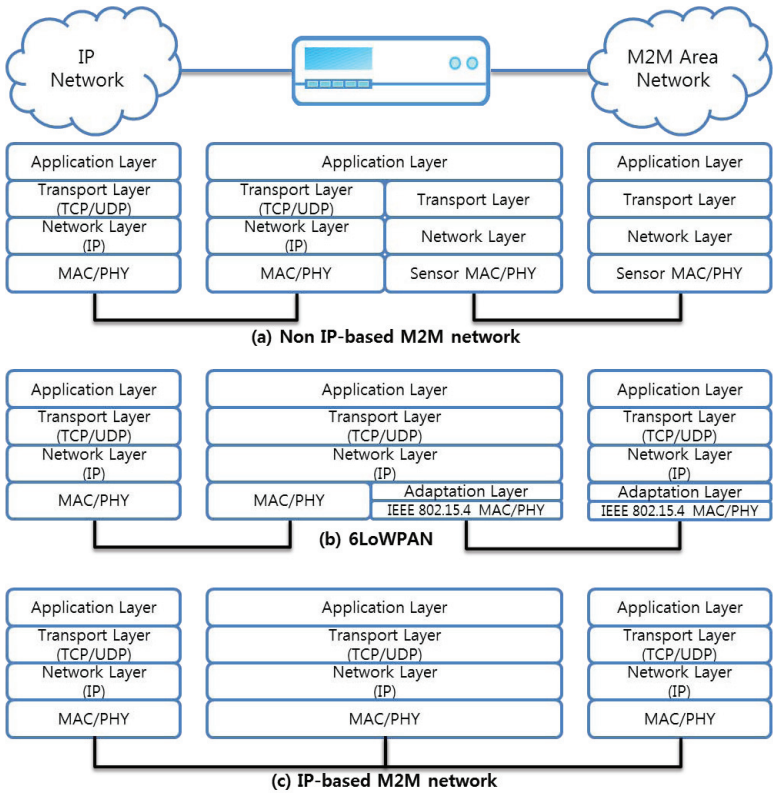

Fig. 10. IP interworking with M2M area network

The way in which addresses are obtained presents an issue. The Domain Name Service (DNS) is designed to provide a mechanism for mapping names into IP addresses. By querying the DNS, a host address can be identified. In the M2M network, the Object Name Service (ONS) [50] translates the RFID tag identifier into a URL, identifying where information about the object resides.

The addressing scheme would finally be unified to IPv6 at the core network connected to the service platform. However, there are addressing systems already used in various industrial domains. As in Figure 10, these non-IP based local addressing systems and 6LoWPAN would also coexist and interoperate with IPv6 through gateways. URI is designed to accommodate the existing identifiers, including not only the aforementioned OID, EPC, and EPC global, but also international standard book number (ISBN), digital object identifier (DOI), and so on. Therefore, it is expected that the naming would be unified into the URI to identify the various resources in M2M services.

B. Communication and Networking Protocols

Communication and networking protocols enable things to transmit the information obtained from the physical environment and receive commands from the users and services. There are two approaches to M2M communication. One is the infrastructure-based approach which utilizes cellular networks (Cellular M2M), and the other is the infrastructure-less based approach (Capillary M2M), such as wireless ad-hoc networks. Capillary M2M protocols have the advantage of minimal configuration at low cost. They should maintain connectivity and service for different applications, even with user mobility.

WSNs are generally powered by a battery with limited power, and thus protocols are primarily designed to be energy efficient [53]. While early research on WSN protocols has mainly focused on monitoring applications based on low-rate delay tolerant data collection, current research is considering various applications, such as industrial automation, military, ITS, and healthcare. These applications have different QoS requirements: delay, reliability, priority, throughput; and different traffic patterns: periodic, event-driven, streaming. To support these different kinds of M2M applications, network QoS parameters and traffic patterns must be considered during the network design as well as the energy efficiency. Since a protocol cannot support all the different kinds of M2M applications, extensive MAC/Routing protocols for different goals have been proposed.

A lot of MAC protocols for WSNs have been proposed in the literature, and numerous surveys on WSN MAC protocols can be found in [53], [52], and [51]. MAC protocols can be classified according to the targeted application scenarios of delay, reliability, and traffic patterns, for which they are suitable [51], [53]. Scheduled protocols are optimized for high-load traffic such as multimedia applications; protocols with common active periods intend to decrease delay are suited for medium-load traffic; preamble sampling protocols are convenient for delay tolerant rare reporting events such as metering applications; some hybrid protocols combine the benefits of several protocols.

Routing protocols are mainly devided into three categories: data centric, hierarchical, and location based [54]. Data centric protocols are not designed to handle the QoS requirements.

Hierarchical protocols are useful for heterogeneous networks where there are cluster heads that have more resources and computational power than other nodes. The location based approach is useful when the application requires location awareness. Location awareness yields a reduction in latency and energy consumption.

Despite the long history of MAC/Routing protocols, Problems remain and others keep emerging with regard to the rapid growth of M2M applications [52], [53], [51], [54], [55], [56]. These issues include mobility of sensors and sinks, multi-channel access, cross-layer awareness, the energy harvesting environment, multi-constrained QoS, and scalability.

In the industrial domain, Object Linking and Embedding (OLE) for process control (OPC) [57] from the OPC Foundation enables interaction between control systems and PC-based application programs in industrial control systems such as SCADA. The OPC Unified Architecture (UA) is the most recent OPC specification which can be implemented with Java, Microsoft .Net, or C, eliminating the requirement of earlier OPC versions to use only a Microsoft Windows. OPC-UA [57], [58] combines the existing functionality of OPC with service-oriented architecture for process control, while enhancing security and providing an information model. OPC and OPC-UA contribute to the evolution from proprietary systems in the industrial control domain to open, less expensive, standardized systems.

M2M applications can be built using REST architecture [36]. The REST-style architecture consist of clients and servers. Clients initiate requests to servers; servers process requests and return the appropriate responses. These requests and responses access and manipulate the resources. A resource can be any thing that can be identified by URIs (e.g., documents, images, and files). REST uses the GET, PUT, POST, and DELETE operations of HTTP to access resources. However, the protocols used for RESTful architecture are not appropriate for resource constrained networks and devices [37]. A large overhead of HTTP implies packet fragmentation and performance degradation of M2M devices. Also, TCP flow control is not appropriate for M2M devices and the overhead is too high for short transactions. To extend the REST architecture for resource constrained M2M devices, constrained application protocol (CoAP) has defined. CoAP is an application protocol intended to be used in simple devices allowing them to communicate over the Internet. CoAP includes a subset of the HTTP functionalities, optimized for M2M applications. It also supports multicast, very low overhead, and asynchronous message exchanges over a user datagram protocol (UDP) for M2M devices.

C. Network Management

M2M area networks can consist not only of many devices acting alone but also of sensor networks, in which nodes in large numbers cooperate with one another to accomplish complex tasks. For this large number of nodes, it is impossible to manage each node individually [43],[59].

Network management includes the process of managing, monitoring, and controlling a network. Using network management, the state and operation of M2M area networks must be monitored. In the face of unexpected problems based on collected information, M2M applications and network parameters, such as a switching node (on/off), controlling wireless BW, and a sensing period, will need to reconfigure and adapt themselves, based on the information from the network [60]. It is also possible to tracing low network performance areas and predict future network statuses [61].

Traditional network management methods are designed to manage wired networks whose characteristics are different from those of M2M networks. Existing network management protocols, including the widely used SNMP, do not support the characteristics of WSNs that have limited resources. Sensor nodes may not support full TCP/IP, and polling the management messages in WSNs causes a huge amount of traffic, because WSNs consist of hundreds or thousands of nodes and management requests, and responses are delivered through the network in a multi-hop fashion. This management overhead consumes WSN resources and has a negative effect on the performance of the network.

The M2M area network management system design requirements are summarized from [59] and [60] as follows:

- Fault tolerance: Manage dead nodes (run out of energy, physical damage)
- Scalability: Dense, large number of nodes
- Cost and complexity: Low cost, low complexity
- Application dependence: Data-centric application, emergency, or real-time application
- Energy efficiency: Limited battery; recharge is difficult or impossible
- Dynamic configuration: Dead nodes, new nodes, and mobile nodes
- Minimize management traffic: Management traffic can affect the network performance

There are some studies on network management architecture, framework for ad-hoc networks [62], [63], and WSNs [60], [61], [64], [65], [66], [59] that comprise M2M area networks.

MANNA [60] introduces a management architecture for WSNs. It includes functional, informational, and physical architecture to manage and control WSN entities. The authors propose several types of functional architecture and suggest both locations for managers and agents and the functions they can execute. sNMP [61] proposes a topology discovery algorithm for WSNs, with its applications to network management. The constructed topology is used for efficient data dissemination and aggregation, duty cycle assignments, and network state retrieval. LiveNCM [64] proposes a new management tool that provides a subset of functionalities of SNMP. It reduces network traffic and energy consumption by estimating some data using linear models or by interpreting data message exchanges. MARWIS [65] proposes management architecture for heterogeneous WSNs. They propose subdividing WSNs into smaller sensor subnetworks. A wireless mesh network operates as a gateway to building communication between these subnetworks. Cooperative management [66] attempts to reduce management request and response messages, which create additional traffic, in addition to the application data of the nodes. Sending management data and application data together rather than separately can reduce the energy usage

of the management system. The authors discuss different models for cooperation between the management system and the sensing application and estimate the trade-off between the number of packet transmissions and the delay of management data.

Another research issue is how to use the collected network management information to manage the network [43]. Although M2M operates with distributed characteristics, centralized decision making and management with the data collected are essential. Because of the dead nodes, the performance of the M2M area network degrades as time goes on. For these M2M area networks, it could be possible to minimize network performance degradation and extend the network lifetime by processing the collected management information and applying some algorithms. The WSN management information collected could be used not only for monitoring the network but also for network maintenance, for example, by deploying relay nodes to maintain connectivity [67], or by deciding on a node replacement policy when deploying additional nodes to maintain network performance [68], [69], [70]. These studies are based on network information such as network connectivity, coverage, location, and residual energy. Such types of information can be obtained from WSN management protocols. Management using mobile nodes can also be considered. Mobile nodes can explore the area that network coverage does not reach, and can connect isolated nodes that cannot access the network or communicate with the sink node. However, these studies do not consider the network management system of an M2M area network. Technologies that enable the M2M area network to work with the management system are required; these technologies can support the sustainability of M2M area networks.

D. Peer-to-Peer Communication

As stated in Section II.2, enormous M2M data make big data, which is then sent to an M2M service platform. Users and devices communicate through the platform to access the stored data; they cannot connect directly without having to go through the platform. However, this type of communication is not the most efficient in terms of delay, system resource usage, and load distribution of data servers for locally processable M2M traffic, when devices that are close to one another exchange messages, and when users send and receive data constantly over a period of time. Many M2M applications require connectivity between end devices that communicate directly through the Internet without having to go through the platform. This includes direct device-to-device communication between end devices. P2P communication can reduce delay and prevent the storing of unnecessary traffic in the platform. This effect will increase with the rise in the number of M2M devices and applications requiring P2P communication.

Existing research on P2P communication is about clients sharing content. The research issues are congestion control and P2P localization. However, to support the P2P communication between devices or users and devices in an M2M network, a signaling process is required for resource allocation and authorization between end devices. Based on the device profile and user profile of the platform, authorization and redirecting of signaling are required. Further, existing analyses and comparisons of load distribution and delay reduction performance through P2P communications. [71], [72], [73], [74], [75], [76] deal with device-to-device communication, which is a kind of P2P communication, in the cellular infrastructure. These are the main research issues of P2P communication in an M2M network.

E. Standardization Activities

M2M is correlated with many technologies across multiple industries. Consequently, the required scope of standardization is significantly greater than that of any traditional standards. The scope of various standard organizations active in M2M ranges from communication and networking layers (M2M area network (IETF, IEEE, ISO/IEC, ZigBee) and wide area network (3GPP, 802.16p, WiMAX Forum)), to application layer standardization (ETSI, CoRE, oneM2M), and to other IoT related standards (ITU-T, EU FP7). Collaboration among these standards organizations across different industries is therefore essential.

1) Application Layer Standardization: The scope of the European Telecommunication Standards Institute (ETSI) [77] Technical Committee (TC M2M) is to develop and promulgate the standardization of the application layer that is independent of the underlying communication network. The goal of ETSI M2M includes the specifications of use cases, M2M service requirement, functional architecture, and interface standardization. The IETF Constrained RESTful Environment (CoRE) working group has defined the Constrained Application Protocol (CoAP) [79], which provides an application protocol to manipulate the resource of the constrained M2M devices networks and offers features for M2M applications, such as very low overheads, multicast support, and asynchronous message exchanges. To reduce standardization overlap and to avoid the creation of competing M2M standards, the seven standard organizations (SDOs), including ETSI, set up the oneM2M [80] standardization launched by the Association of Radio Industries and Businesses (ARIB) and the Telecommunication Technology Committee (TTC) of Japan; the Alliance for Telecommunications Industry Solutions (ATIS) and the Telecommunications Industry Association (TIA) of the USA; the China Communications Standards Association (CCSA); the European Telecommunications Standards Institute (ETSI); and the Telecommunications Technology Association (TTA) of Korea. The goal of oneM2M is to develop one globally agreed-upon M2M specification, which meets the need for a common M2M service layer. With an access independent view of end-to-end services, oneM2M will also develop globally agreed-upon M2M endtoend specifications using common use cases and architecture principles across multiple M2M applications.

2) Wide Area Network Standardization: SDOs of wide area networks including 3GPP, IEEE 802.16p, and WiMAX Forum are aim to standardize enhancements to 3GPP or 802.16 networks for enabling M2M applications. The objective of the 3GPP Machine Type Communication (MTC) standard is to accommodate M2M in the existing 3GPP cellular network. It identifies the service requirements for M2M [8], and standardizes the network and system improvements for M2M

network communication [78]. The main standardization items are identifiers, addressing, device triggering, congestion and overload control of the system. The aim of IEEE 802.16p [81] is to standardize enhancements to 802.16 networks to enable a range of M2M applications in which device communications require a wide area of wireless coverage in licensed bands for purposes such as observation and control. 802.16p defines system requirements, reference architecture, and air interface for low power consumption, mass devices, and short-burst transmissions in WirelessMAN for M2M. WiMAX Forum [82] specifies M2M requirements, network system architecture, usages, deployment models based on IEEE 802.16 protocols, and a performance guide line for an end-to-end M2M system.

3) M2M Area Network Standardization: IEEE run the 802.15.4 [83] working group, whose objective is the standardization of the PHY/MAC layer of wireless personal area networks (WPAN), which consists of low-power devices. 802.15.4 is adopted as a PHY/MAC layer of ZigBee. As already mentioned in section V. A, in the IETF, 6LoWPAN [46] defines the simplified IPv6 protocol over the 802.15.4 protocol stack. The main protocols in 6LoWPAN have been specified and implemented in some commercial products. Another IETF working group, Routing Over Low power and Lossy networks (ROLL), developed routing protocol for Low power and Lossy Networks (LLNs) [84], which is made up of many embedded devices with limited resources and interconnected by a variety of links, such as IEEE 802.15.4, Bluetooth, and low power WiFi. ZigBee [85] is a cost-effective, low-power, wireless network standard that can be applied to wireless monitoring and application control. The ZigBee specification is defined by the nonprofit organization ZigBee Alliance. It defines from network layer to application layer based on the 802.15.4 PHY/MAC including networks, application profiles, and software solutions such as commission. The ISO/IEC JTC1/WG7 Working Group on Sensor Networks defines general requirements, sensor network reference architecture, interfaces for sensor networks, application profiles, and interoperability guidelines. Sensor networks in order to support Smart Grid technologies are also being standardized.

4) Other Relevant Activities: Other relevant standardization activities are progressing with regard to the IoT. The aim of the ITU-T Joint Coordination Activity on Internet of Things (JCA-IoT) [86] is to standardize the IoT, including network aspects of tag-based identification of things and networking and service aspects of sensor information. The Internet of Things Global Standards Initiative (IoT-GSI) [87] promotes a unified approach in ITU-T for the development of technical standards enabling the IoT on a global scale. The IoT-GSI aims to develop a definition of the IoT, provide a common working platform by collocating meetings of IoT-related rapporteur groups, and develop the detailed standards necessary for IoT deployment, taking into account the work done in other SDOs. IoT-A's [88] objective is to create the architectural reference model of the Future Internet of Things, together with the definition of an initial set of key building blocks, allowing seamless integration of heterogeneous IoT technologies into a coherent architecture and their federation with other systems of the Future Internet. The IoT at Work [89] project has the aim of designing an IoT architecture that takes the industry and factory automation system and their networking and communication needs into account, while focusing on the auto configuration, security, and service-oriented application architecture to allow true flexibility and reliability.

VI. Conclusion

M2M is a hot topic for the future of computing and communication networks. Not only is it a technological revolution that has a profound impact on our daily lives by enabling communication with and among objects, but it also creates a new ecosystem with an M2M platform.

In this paper, we presented a survey of M2M service platforms and explored some research issues and challenges to enabling an M2M service platform. We first classified M2M applications and nodes from low-end sensor nodes to mid- and high-end sensor nodes by considering their hardware capabilities, applications, characteristics, and functionalities (functions). These various sensor nodes generate different traffic types and create a large amount of data. With this in mind, we discussed the necessity of an M2M platform to substantially reduce development costs and improve time to market of M2M devices and services.

We compared and analyzed existing approaches and solutions to the issues with M2M platforms. The service platforms reviewed were considered under three categories according to business models and functionalities. We also compared specific functionalities and features of existing commercial platforms. By comparing and analyzing existing platforms, we identified the requirements and functionalities of the ideal M2M service platform. Based on these, we proposed an M2SP architecture consisting of a Device-, User-, Application-, and Access-platform. These entities interact with each other and provide M2M service platform functionalities. Application scenarios of low-end devices and mid-end devices are presented to illustrate the interaction between the components of the proposed platform, from the deployment stage to the service providing stage. This platform will encourage the M2M ecosystem.

In addition, we discussed the issues and challenges of network technologies that enable M2M services and platforms: identification and addressing, communication and networking protocols, network management of M2M area networks, and P2P communication. The standardization of various M2M related technologies is necessary to resolve these technological issues.

In the future, some issues need to be explored and considered to realize M2M. One of the issues is the auto registration process of devices. For large networks such as WSNs, it is impossible to register every device manually. One approach is to register only a sink node and leave the inside of the WSNs to the auto configuration process of WSNs. The platform collects only aggregated information processed from the sink node and controls the sink node. Even so, auto registration is required for the large number of M2M devices. An M2M service platform can be combined with a cloud computing service. Thus, the implementation of M2M platforms in distributed cloud data centers can be considered. In this case, it is necessary to optimize and analyze M2M

platform performance according to the locations and number of distributed cloud data centers. Another direction is to handle big data generated by M2M. Software defined network, such as OpenFlow, can be considered in the Future Internet for the integrated management of M2M traffic.

ACKNOWLEDGMENT

This work was supported by the IT R&D program of MKE/KEIT. [10041262, Open IoT Software Platform Development for Internet of Things Services and Global Ecosystem]

REFERENCES

[1] ETSI TS 102 689, "Machine-to-Machine communications (M2M); M2M service requirements," Aug. 2010.
[2] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, M. Guizani, "Home M2M networks: Architectures, standards, and QoS improvement," *IEEE Commun. Mag.* , vol.49, no.4, pp.44,52, April 2011.
[3] K. Stouffer, J. Falco, K. Kent, "Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security," National Institute of Standards and Technology, Tech. Rep, Sept. 2006.
[4] Pre-published Recommendation ITU-T Y.2060, "Overview of Internet of Things," Jun. 2012.
[5] WMF-T31-127-v01, "Requirements for WiMAX Machine to Machine (M2M) Communication," WiMAX Forum, Apr. 2011.
[6] TIA TR-50, "Smart Device Communications," Feb. 2010.
[7] Pre-published Recommendation ITU-T Y.2061, "Requirements for support of machine oriented communication applications in the NGN environment," Jun. 2012.
[8] 3GPP TS 22.368, "Service requirements for Machine-Type Communications (MTC); Stage 1 (Release 11)," Mar, 2013.
[9] ITU-T Y.2221, "Requirements for support of ubiquitous sensor network (USN) applications and services in the NGN environment," Jan, 2010.
[10] "Standardized M2M Software Development Platform," http://www.interdigital.com/wp-content/uploads/2012/08/Standardized_M2M_SW_Dev_Platform.pdf
[11] E. Scarrone and D. Boswarthick, "Overview of ETSI TC M2M Activities," March 2012.
[12] CASAGRAS, "RFID and the Internet of Things: Enablers of Ubiquitous Computing and Network,".
[13] ISO/IEC 29182-2, "Sensor Network Reference Architecture (SNRA) Part 2: Vocabulary and Terminology," Draft.
[14] I. F. Akyildiz, W. Su, Y.Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey," *Computer Networks*, vol. 38, no. 4, pp. 393-422, 2002.
[15] M. Castro, A. J. Jara, and A. F. Skarmeta, "An Analysis of M2M Platforms: Challenges and Opportunities for the Internet of Things," *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, 2012 6th Int. Conf. July 2012, pp.757-762.
[16] MIKE2.0, Big Data Definition: http://mike2.openmethodology.org/wiki/Big_Data_Definition
[17] Y. Nie and Y. Ma, "A First Look at AMI Traffic Patterns and Traffic Surge for Future Large Scale Smart Grid Deployments," *The 2nd Int. Conf. on Advanced Communications and Computation(INFOCOMP 2012)*, Oct. 2012, pp. 120-124.
[18] M. Z. Shafiq, L. Ji, A. X. Liu, J. Pang, and J. Wang, "A first look at cellular machine-to-machine traffic: large scale measurement and characterization," *Proc. 12th ACM SIGMETRICS/PERFORMANCE joint int. conf. on Measurement and Modeling of Computer Systems (SIGMETRICS '12)* New York, USA, 2012, pp.65-76.
[19] Cosm: https://cosm.com/
[20] ThingSpeak: https://www.thingspeak.com/
[21] Nimbits: www.nimbits.com/
[22] Evrythng: http://evrythng.com/
[23] Sensinode: http://www.sensinode.com/
[24] Oneplatform by Exosite: http://exosite.com/
[25] Axeda Platform: http://www.axeda.com/
[26] SensorCloud: http://www.sensorcloud.com/
[27] Bugswarm: http://www.buglabs.net/bugswarm
[28] NeuAer: http://www.neuaer.com/
[29] iDigi Device Cloud: http://www.digi.com/
[30] Cosm Consumer Product: https://cosm.com/support/hardware
[31] IoBridge: http://iobridge.com/
[32] MicroStrain Sensors: http://www.microstrain.com/
[33] Arduino: www.arduino.cc/
[34] mBed: http://mbed.org/
[35] Nanode: http://www.nanode.eu/
[36] R. T. Fielding and R. N. Taylor, "Principled Design of the Modern Web Architecture," *ACM Trans. on Internet Technology (TOIT)*, Vol. 2, Issue 2, May 2002, pp. 115-150.
[37] W. Colitti, K. Steenhaut, N. D. Caro, B. Buta, V. Dobrota, "REST Enabled Wireless Sensor Networks for Seamless Integration with Web Applications," *2011 IEEE 8th Int. Conf. on Mobile Adhoc and Sensor Systems (MASS)*, Oct. 2011, pp.867-872.
[38] S. Clayman and A. Gali, "INOX: a managed service platform for interconnected smart objects," *Proc. of the workshop on Internet of Things and Service Platforms 2011 (IoTSP '11)*, pp. 1-8.
[39] S. Zhang, J. Zhang, and W. Li, "Design of M2M Platform Based on J2EE and SOA," International Conference on E-Business and E-Government, pp. 2029-2032, *2010 Int. Conf. on E-Business and E-Government*, 2010.
[40] Q. Xiaocong and Z. Jidong, "Study on the structure of "Internet of Things(IOT)" business operation support platform," *2010 12th IEEE Int. Conf. Commun. Technology (ICCT)*, Nov. 2010, pp.1068-1071.
[41] Y. J. Kim, E. K. Kim, B. W. Nam, I. Chong, "Service composition using new DSON platform architecture for M2M service," *Information Networking (ICOIN), 2012 Int. Conf. on*, Feb. 2012, pp.114-119.
[42] L. Foschini, T. Taleb, A. Corradi, D. Bottazzi, "M2M-based metropolitan platform for IMS-enabled road traffic management in IoT," *IEEE Commun. Mag.* , vol.49, no.11, November 2011, pp.50-57.
[43] J. Kim, H. Jeon, and J. Lee, "Network management framework and lifetime evaluation method for wireless sensor networks," *Integrated Computer-Aided Engineering*, vol. 19 no.2, April 2012, pp. 165-178.
[44] K. Sollins, L. Masinter, "Functional Requirements for Uniform Resource Names," *IETF, RFC 1737*, December 1994. http://www.ietf.org/rfc/rfc1737.txt
[45] R. Hinden and S. Deering, "IP Version 6 Addressing Architecture," *IETF, RFC 4291*, February 2006. http://www.ietf.org/rfc/rfc4291.txt
[46] M. Gabriel, K. Nandakishore, H. Jonathan, and C. David. "Transmission of IPv6 Packets over IEEE 802.15.4 Networks." *IETF, RFC 4944*, September 2007. http://www.ietf.org/rfc/rfc4944.txt
[47] T. ECH-CHAITAMI, R. MRABET, H. BERBIA, "Interoperability of LoWPANs Based on the IEEE802.15.4 Standard through IPV6," *Int. J. of Computer Science Issues (IJCSI)*, Vol. 8 Issue 2, Mar. 2011, pp.315-323.
[48] URI Planning Interest Group, W3C/IETF (21 September 2001), "URIs, URLs, and URNs: Clarifications and Recommendations 1.0". July 2009.
[49] F. Armenio et.al. "The EPCglobal Architecture Framework Version 1.3," March 2009.
[50] EPCglobal, Inc. "EPCglobal Object Name Service (ONS) Version 1.0.1," May 2008.
[51] A. Bachir, M. Dohler, T. Watteyne, and K. K. Leung, "MAC Essentials for Wireless Sensor Networks," IEEE Commun. Surveys Tutorials, Vol. 12, No. 2, 2010, pp. 528-550.
[52] M. A. Yigitel, O. D. Incel, C. Ersoy, "QoS-aware MAC protocols for wireless sensor networks: A survey," *Computer Networks*, Vol. 55, No. 8, June 2011, pp. 1982-2004.
[53] P. Suriyachai, U. Roedig, and A. Scott, "A Survey of MAC Protocols for Mission-Critical Applications in Wireless Sensor Networks," *IEEE Commun. Surveys & Tutorials*, Vol. 14, No. 2, 2012, pp. 265-278.
[54] P. Huang, L. Xiao, S. Soltani, M. W. Mutka, and N. Xi, "A Survey on Energy-Efficient Routing Techniques with QoS Assurances for Wireless Multimedia Sensor Networks," *IEEE Commun. Surveys & Tutorials*, Vol. 15, No. 1, 2013, pp. 101-120.
[55] T. Watteyne, A. Molinaro, M. G. Richichi, and M. Dohler, "From MANET To IETF ROLL Standardization: A Paradigm Shift in WSN Routing Protocols," *IEEE Commun. Surveys & Tutorials*, Vol. 13, No. 4, 2011, pp. 688-707.
[56] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey," *IEEE Commun. Surveys & Tutorials*, Vol. 15, No. 2, 2013, pp. 551-591.
[57] OPC Foundation: http://www.opcfoundation.org/
[58] W. Mahnke, S. Leitner, "OPC Unified Architecture - The future standard for communication and information modeling in automation," ABB Review, Mar. 2009, pp.56-61.
[59] W.L. Lee, A. Datta, and R. Cardell-Oliver, "Network Management in Wireless Sensor Networks," http://www.csse.uwa.edu.au/~winnie/Network_Management_in_WSNs.pdf
[60] L.B. Ruiz, J.M. Nogueira, and A.A.F. Loureiro, "MANNA: A Management Architecture for Wireless Sensor Networks," *IEEE Commun. Mag.* 41(2) (2003), pp. 116125.

[61] D. Budhaditya, S. Bhatnager, and B. Nath, "A Topology Discovery Algorithm for Sensor Network with Application to Network Managemtn," *Technical Report DCS-TR-441*, Department of Computer Science, Rutgers University, 2001.
[62] W. Chen, N. Jain, and S. Singh, "ANMP: ad hoc network management protocol," *IEEE J. Sel. Areas Commun.* 17(8) (1999), pp. 15061531.
[63] C.C. Shen, C. Srisathapornphat, and C. Jaikaeo, "An adaptive management architecture for ad hoc networks," *IEEE Commun. Mag.* 41(2) (2003), pp. 108115.
[64] A. Jacquot, J.-P. Chanet, K.M. Hou, X. Diao, and J.-J. Li, "A New Approach for Wireless Sensor Network Management: LiveNCM," *New Technologies, Mobility and Security NTMS 08* (2008), pp. 16.
[65] G. Wagenknecht, M. Anwander, T. Braun, T. Staub, J. Matheka, and S. Morgenthaler, "MARWIS: a management architecture for heterogeneous wireless sensor networks," *WWIC'08 Proc. 6th int. conf. Wired/wireless internet commun.*, 2008, pp. 177-188.
[66] J. Furthmuller, S. Kessler, and O.P. Waldhorst, "Energyefficient management of wireless sensor networks," *Wireless On-demand Network Systems and Services (WONS), 2010 7th Int. Conf. on* (2010), pp. 129136.
[67] A.S. Ibrahim, K.G. Seddik, and K.J.R. Liu, "Connectivity-aware network maintenance and repair via relays deployment," *IEEE Trans. Wireless Commun.* Vol. 8, No. 1, 2009, pp. 356366.
[68] S. Misra, S.V. Rohith Mohan, and R. Choudhuri, "A probabilistic approach tominimize the conjunctive costs of node replacement and performance loss in the management of wireless sensor networks," *IEEE Trans. Netw. Service Manage.* Vol. 7, No. 2, 2010, pp. 107117.
[69] S. Parikh, V.M. Vokkarane, L. Xing and D. Kasilingam, "Node-Replacement Policies to Maintain Threshold-Coverage inWireless Sensor Networks," *Computer Commun. and Networks (ICCCN), Proc. 16th Int. Conf. on* 2007, pp. 760765.
[70] H. Zhang and J.C. Hou, "Maintaining sensing coverage and connectivity in large sensor networks," *Wireless Ad Hoc Sensor Networks* Vol. 1, No. 1-2, 2005, pp. 89-123.
[71] H. Min, W. Seo, J. Lee, J. Lee, S. Park, and D. Hong, "Reliability Improvement Using Receive Mode Selection in the Device-to-Device Uplink Period Underlaying Cellular Networks," *IEEE Trans. Wireless Commun.*, vol.10, no.2, February 2011, pp.413-418.
[72] M. Zulhasnine, C. Huang, and A. Srinivasan, "Efficient resource allocation for device-to-device communication underlaying LTE network," *IEEE 6th Int. Conf. on Wireless and Mobile Computing, Networking and Communications*, 11-13 Oct. 2010, pp.368-375.
[73] C. Yu, K. Doppler, C. Ribeiro, and O. Tirkkonen, "Resource sharing optimization for device-to-device communication underlaying cellular networks," IEEE Trans. Wireless Commun., vol.10, Aug. 2011, pp.2752-2763.
[74] T. Chen, G. Charbit, and S. Hakola, "Time Hopping for Device-To-Device Communication in LTE Cellular System," *in Proc. IEEE Wireless Communications and Networking Conf. (WCNC)*, April 2010, pp.18-21.
[75] F. H. Fitzek, M. Katz, and Q. Zhang, "Cellular controlled short-range communication for cooperative P2P networking," *in Proc. Wireless World Research Forum* 17, Nov. 2006. pp.141-155.
[76] P. Janis, C.-H. Yu, K. Doppler, C. Ribeiro, C. Wijting, K. Hugl, O. Tirkkonen, and V. Koivunen, "Device-to-device communication underlaying cellular communications systems," *Int. J. Commun., Network Syst. Sciences*, vol. 2, no. 3, June 2009. pp.169-247.
[77] European Telecommunications Standards Institute (ETSI): www.etsi.org/
[78] 3GPP TR 23.888, "System Improvements for Machine-Type Communications; (Release 11)".
[79] Z. Shelby, K. Hartke, C. Bormann, B. Frank, "Constrained Application Protocol (CoAP)," draft-ietf-core-coap-11; July 2012.
[80] oneM2M: http://www.onem2m.org/
[81] IEEE 802.16's Machine-to-Machine (M2M) Task Group: http://www.wirelessman.org/m2m/index.html
[82] WiMAX Forum: www.wimaxforum.org/
[83] IEEE 802.15 WPAN Task Group 4 (TG4): http://www.ieee802.org/15/pub/TG4.html/
[84] T. Winter, Ed., P. Thubert, Ed. A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, JP. Vasseur, and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *IETF, RFC 6550*, March 2012. http://tools.ietf.org/html/rfc6550
[85] ZigBee Alliance: http://www.zigbee.org.
[86] Joint Coordination Activity on Internet of Things (JCA-IoT): http://www.itu.int/en/ITU-T/jca/iot/Pages/default.aspx
[87] Internet of Things Global Standards Initiative (IoT-GSI): http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx
[88] Internet of Things - Architecture: http://www.iot-a.eu/public
[89] IoT-at-Work: https://www.iot-at-work.eu/

Jaewoo Kim received the B.S. degree from the Yonsei University, Korea in 2007. He is currently a Ph.D candidate in Electrical and Electronic Engineering at Yonsei University, Korea. His research interests are network management in wireless sensor networks, IoT/M2M Platform design, QoS and mobility management for supporting next generation mobile network architecture, 3GPP LTE technology.

Jaiyong Lee received Ph.D degree in Computer engineering from Iowa State University, USA in 1987. He has been with ADD(Agency for Defense Development) as a research engineer from 1977 to 1982, and with Computer Science Dept. of POSTECH as an associate professor from 1987 to 1994. Since 1994, he is a professor in School of EE, Yonsei University. He has been a president of OSIA(Open standards and Internet Association), editor of JCN(Journal of Communication and Networks) and ETRI journal, and served as a chair and steering/organizing committee member in many conferences such as Wibro Developers Forum(2006), world communication forum(2006) and APCC(2012).

He has been actively involved in RFID/USN research activities in many positions such as chairman of Korean Mobile RFID Forum, and Vice chair of USN Convergence Forum, and Korean standard representative of ISO/IEC JTC1/WG7. Since 2004, hes been a director of CARUT(Center for Advance RFID/USN Technology).

His research interest areas are IoT/M2M platform design, future network architecture for IoT and SNS, Network Management, and Wired/Wirelss TCP protocol design.

He was the president of the association of IACF(Indusry-Academic Cooperation Foundation)of Korean Universities. Also, he was dean of college of engineering and graduate school of engineering, Yonsei university.

Jaeho Kim received the BS and MS degrees in computer science and engineering from the Hankuk University of Foreign Studies, South Korea, in 1996 and 2000, respectively. Currently, he is a Ph.D. candidate in the electrical & electronic engineering from the Yonsei University, South Korea. He is also working as a managerial researcher in the Embedded Software Convergence Research Center at the Korea Electronics Technology Institute (KETI), Seongnam, South Korea from 2000. His research interests are in the areas of wireless sensor networks, medium access protocols, and Internet of Things.

Jaeseok Yun received the MS and PhD degrees in mechatronics from the Gwangju Institute of Science and Technology, South Korea, in 1999 and 2006, respectively. Currently, he is working as a senior researcher in the Embedded Software Convergence Research Center at the Korea Electronics Technology Institute (KETI), Seongnam, South Korea. He was a research scientist/ postdoctoral researcher with the Ubiquitous Computing Research Group in the College of Computing and the GVU Center at the Georgia Institute of Technology from 2006 to 2009. His research interests are in ubiquitous computing, wearable computing, human-computer interaction, and Internet of Things. He is particularly interested in human activity sensing and its applications.