Towards Management of Machine to Machine Networks

Suman Pandey, Mi-Jung Choi*, Myung-Sup Kim, and James W. Hong

Suman Pandey
Dept. of Computer Science and Engineering, POSTECH, Korea
suman@postech.ac.kr

Myung-Sup Kim
Dept. of Computer and Information Engineering, Korea University, Korea
tmskim@korea.ac.kr

Mi-Jung Choi
Dept. of Computer Science, Kangwon National University, Korea
mjchoi@kangwon.ac.kr

James W. Hong
Division of IT Convergence Engineering, POSTECH, Korea
jwkhong@postech.ac.kr

Abstract— **Abstract: Machine to Machine (M2M) technology has the potential to increase the revenue, decrease the costs and improve the customer services of an organization. We have analyzed the management requirements of M2M systems, which are based on existing M2M network use cases and services. The most important characteristics including sleeping devices, low power lossy area networks, heterogeneous networks, device intelligence, mobility, two way communication, network dynamics, time sensitivity of data and data volume of M2M systems have been comprehensively investigated and reflected in management requirements discussed in this paper. The main management functionalities are fault, configuration, mobility, QoS and security management.**

Keywords- M2M; Network Management; Standarization; Network Characteristics

I. INTRODUCTION

M2M is a technology that enables devices such as computers, embedded systems, sensors, mobile devices, etc. to communicate with each other and make decisions with minimal human intervention. In short, M2M connects our assets with communication networks and hardware to provide valuable services. These assets are referred to as smart devices in M2M networks.

With the increasing intelligence of devices and networks, M2M technology has also evolved very rapidly. The concept of cloud computing of embedded smart devices has widened the range of M2M applications [1]. Table I shows some of the future M2M applications and the important services provided by them. Even a small enterprise network requires all kinds of management tools such as antivirus, spam blockers, firewalls and software delivery tools. Similarly, M2M networks also need strong management tools and frameworks. This paper focuses on requirement gathering for M2M network management. We first elaborate activities from standard organizations towards network management of M2M. Several standardization bodies are working in defining architecture and services for M2M applications. They are also focusing on Network management as a part of their activities. However there is a need to identify the characteristics of the M2M applications which will effect M2M network management. In this paper, we analyze common characteristics of these different M2M networks. We then discuss specific characteristics of M2M networks, which differ from application to application. Based on these characteristics we derive the common set of network and device management requirements for M2M applications.

TABLE I. TABLE I M2M APPLICATIONS AND SERVICES

M2M applications	**Services provided**
Automotive [18]	Breakdown calls, Stolen vehicle tracking, Remote diagnosis, Insurance services, Navigation, Registry of delivered goods and payment received
Connected Consumer [19]	Photo upload from camera, Content download to eBook, Surveillance data upload, Remote control of home appliance
Smart Metering [20]	Manage electricity distribution network, Obtain meter reading, Management of power quality and outage, Tariff setting and payment, Theft protection
City Automation [21]	Traffic flow management, Dynamic Traffic light control, Surveillance and security
eHealth [22]	Monitoring of patient health and fitness, Triggering alarms on critical conditions, Remote control of medical treatments
Monitoring (Person/ Animal/Objects) [17]	Track and trace, Monitor, Theft protection
Point of Sale [17]	Secure transaction
Controlling (vending machine/Production machine) [17]	Monitoring for stock (vending machine), Update pricing (vending machine), Identify faults, damages, malfunctioning remotely

This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (20110020518) and WCU (World Class University) program through the National Research Foundation of Korea funded by the Ministry of Education, Science and Technology (R31-2010-000-10100-0).

* Correspondence to Mi-Jung Choi, Dept. of Computer Science, KNU, Chuncheon, Republic of Korea

The remainder of the paper is organized as follows. Section II provides an overview of M2M systems. Section III details related work in the field of M2M network management. Section IV describes the specific characteristics of M2M systems, which distinguish them from other systems. Section V details the management requirements of M2M systems. Then Section VI provides concluding remarks and proposes future work.

II. Overview of M2M Systems

The most important concept which any M2M service provider needs to understand is the set of different technology components required to work together to provide a particular M2M solution. In this section, we give an overview of M2M networks and their logical divisions. We also discuss the possible devices in each divisions and how data flows from one part of the system to another.

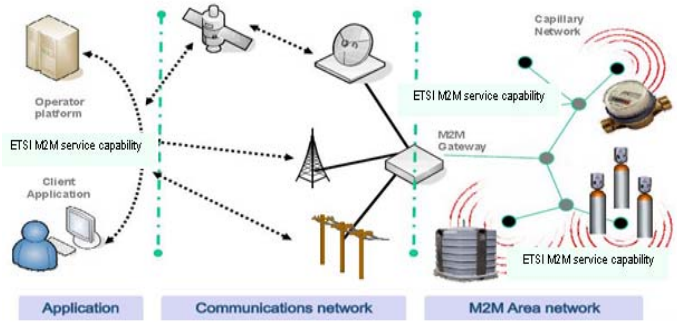

Fig. 1 ETSI M2M Network Architecture

The European Telecommunications Standards Institute (ETSI) [2] has divided M2M systems into three parts including area networks, communication networks and applications as shown in Fig. 1. An area network is composed of data end points, which are usually sensors, compact microprocessors, subscriber identification module (SIM) cards and smart meters. These end points could be subsystems connected via special interfaces. The area network could be based on standards including PLC, ZigBee, M-BUS, wireless M-BUS, or IEEE 802.15. If the area network is composed of sensors via a wireless communication channel, then in this logical division the data flows from sensors to a radio module. Sensor data (usually an alert) is sent to microprocessors via a communication circuit. Microprocessors then deliver these alerts to a radio module, which converts the instructions into packets and sends them over the communication network. The intelligence of these microprocessors and radio modules depends on vendor implementation and application needs.

Data in M2M systems travel from an area network to a communication network. When data leaves the area network and arrives to communication network, its first destination is usually a gateway. The gateway is a device which decides the communication protocols and converts the incoming data into legacy system format. A middleware layer that routes data and converts the format of the data could also be part of the communication network. Middleware layer could also perform network management tasks such as logging, notification, auto-configurations, etc. Some parts of the business logics could also be applied in these middleware's and gateways. Communication network can be of any type including wireless LAN, telephone lines, Ethernet, satellite or cellular networks. Finally, the data gets integrated into a business process at the M2M application layer such as, eHealth, smart metering etc.

The data flow explained above is not standard; it varies from application to application. Some components will merge with others as time passes and M2M systems mature.

III. Related Work

M2M network management is a relatively new area of investigation. In this section, we will first describe the efforts of standards organizations related to M2M network management. The details of each standard with their date of establishment, target network, supported management functionalities, communication protocol and current status is explained in Table II. The discussion of standards here is independent of the underlying transport layer and focused only on the management approaches from application layer. Later we will discuss industry's efforts in this area as well.

A. Standards for M2M Network Management

ETSI TC M2M members are working on standardizing M2M service requirements by analyzing various use cases. Fig. 1 shows the network architecture of M2M, and the requirements of ETSI M2M service capabilities at each level including area network, communication network and application. The members have published stage one documents related to requirements-gathering based on several M2M use cases including those on smart meters, eHealth, city automation, connected consumers and automotives. In stage two (by the third quarter of 2011), they will work on defining end-to-end architecture and identifying key capabilities, message flows and interfaces. In stage three (by the fourth quarter of 2011), they will define protocols for various interfaces. The ETSI M2M service capabilities as shown in Fig. 1 will also address management tasks. The network management functionalities are supported in the framework through Network Remote Entity Management (NREM), Gateway Remote Entity Management (GREM) and Device Remote Entity Management (DREM). The application data is referred to as resources. Resources are defined in a tree structure. The standard describes management resources as MgmtObj. The resources are handled with the RESTful [3] style of data exchange. The four basic methods in the RESTful architecture are Create, Retrieve, Update and Delete.

Another standardization body, the Telecommunications Industries Association (TIA), has established the working group TR 50 for Smart Device Communication (SDC) [4]. Fig 2. provides the protocol layering diagram discussed within TIA TR-50.1 [5]. The SDC protocol layer can execute over different transports by means of convergence or adaptation layers (the presence of applications on the gateway device is still under discussion). Their framework will make its functionality available to applications through a well-defined Application Programming Interface (API). Their work is in a very preliminary stage.

ETSI and TIA are establishing standards from scratch and independent of the underplaying transport layer. However, there are alliances such as IPSO [6], the Open Mobile Alliance (OMA) [7] and Energy Services Network Association (ESNA) [8], which are focusing on reusing and enhancing existing standards to fit M2M requirements in converged networks. These alliances are working on enhancing their existing standards to map ETSI and TIA standards for M2M. IPSO is promoting Internet Protocol (IP) for smart objects. OMA is focusing on wireless and mobile network services specifications. The ESNA is focusing on making Network Energy Services (NES) based standards as the de facto standards for smart grid networks.

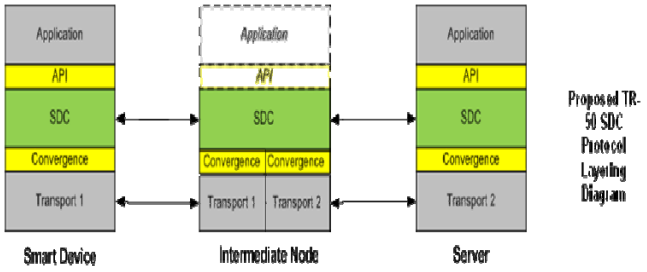

FIG. 2. TIA M2M PROTOCOL LAYERING DIAGRAM

B. IP Based Standards for Smart Devices

IPSO supports IP for smart objects. This alliance was formed to promote IEEE and IETF standardization bodies. Standards established by the 6lowpan, Roll and CoRE working groups under IETF can provide complete M2M solutions. 6lowpan provides an adaption layer for IPv6 over IEEE 802.15.4. Their technique includes packet fragmentation, reassembling, header compression and optimized neighbor discovery for Low power and Lossy Networks (L2Ns). The Roll working group defines the routing solutions for L2Ns. The first draft of the Roll group's IPv6 Routing Protocol for L2N (RPL) is almost stable. The CoRE working group specifies a framework to monitor and control smart objects intended to run on L2N. They will define a RESTFull style of API and specify the proxy handling mapping between CoAP and REST APIs. CoAP will also support cashing for sleepy devices.

C. Converged Mobile and Personal Area Network Based Standards for Smart Devices

OMA focuses on specifications related to interoperable mobile services. OMA claims that their standards can provide building blocks that map into the ETSI M2M framework [9]. The Managed Objects (MO) that can be used for M2M services include Firmware Update MO (FUMO), Scheduling MO (Sched MO), Diagnostic and Monitoring MO (DiagMon MO), Connectivity MO (ConnMO), Gateway Management Object MO (GwMO), Smartcard Management MO (SC MO), Software Component Management MO (SCOMO), Lock and Wipe MO (LAWMO), and Device Capability MO (DCMO). FUMO will control the process of firmware updates. Sched MO will interact with a scheduling agent on the device to have DM commands occur at scheduled times. DiaMon MO will allow a server to monitor a device's performance and diagnose problems. ConnMO will provision connectivity for 3GPP, 3GPP2, and WLAN. GwMO will enable management of devices, when there is no direct communication between DM Server and DM Client. SCMO will read and write data on smart cards. SCOMO will manage software components on devices. LAWMO will enable remote locking and wiping of a device (e.g. to disable a stolen device). DCMO will enable selective enabling/disabling of device capabilities (such as a camera). The OMA initiative for Converged Personal Network Services (CPNS) will enable an M2M area network. CPNS will provide a protocol for the converged network which includes both cellular and wireless personal area networks (WPAN). OMADM client server architecture uses XML for a data exchange format and SyncML for a data exchange protocol. To fulfill M2M service requirements, OMA is currently working on developing and extending lightweight DM protocols for M2M devices and gateways. They are continuing to collaborate with ETSI TC M2M and to produce white papers to identify M2M services. OMA activities for M2M are very promising; however, they are still in the initial stage.

D. Converged Smart Grid Standard

Smart grid technologies have been in existence for decades. ETSI and TIA have also identified it as M2M network. Smart grid is more than just smart meters; it includes smart meters, smart sensors, smart switchgears and other smart equipment working together to make the grid more reliable, robust, and efficient. A U.S. government organization, the National Institute of Standards and Technology (NIST), has finalized a roadmap for smart grid interoperability standards [10]. They have identified security, status monitoring, fault detection, recovery, address capability, routing capability and QoS support as the most important management tasks for smart grids. The management architecture which NIST and the Electric Power Research Institute (EPRI) are considering for the future of smart grid management include 1) SNMP vX - data communication networking, routing, addressing, multihomein, fault, configuration, accounting, performance, security and other management, and 2) Internet-based management standards (DMTF, CIM, WBEM, ANSI, INCITS).The word "data" is plural, not singular.

The European Alliance ESNA is another organization which is specifying standards for smart grids. They are promoting the NES communication and application protocols for smart grids. Their primary standards are the Open Smart Grid Protocol (OSGP) and NTA8150. OSGP defines how application messages are exchanged among data connectors and utility meters and other devices. It will add an application layer of security and authentication as well. It will cover all OSI layers (1-7). The NTA8150 protocol provides the AMI API Interface for application and service layers. It is XML based. The focus of smart grid management in past was mostly service management of electricity distribution. However, clear standards for network and device management in smart grids are essential.

E. Industry Efforts for M2M Network Management

Several industries provide various services and applications based on the M2M concept, and they are actively participating in standardization activities as well. iDigi [11] provides smart devices and services. They also provide management support for devices including authentication, account management, configuration, software updates and group updates. They are leveraging the possibility of M2M applications by introducing cloud computing and providing their server platform as PaaS and services as SaaS. However, they use proprietary protocols to communicate between gateways and server platforms. Numerx [12] is also providing PaaS for the M2M market. Their services are related to security, remote monitoring and asset tracking and recovery. Inilex' Apprize [13] provides SaaS based middleware which could provide communications between any type of application and any type of M2M network. MWA Intelligence [14] provides remote asset and service management for M2M; however, they merely focus on office equipment and utility management. Recowireless [15] and Silentsoft [16] provide remote management of SIM and telemetry services to a limited extent. Most of these industry projects are intended to certain types of applications. There is a need to identify a common set of management tasks applicable to all M2M applications.

TABLE II. TABLE II. M2M STANDARDS WHICH COVERS MANAGEMENT FUNCTIONALITY

Standards	Establish-ment date	Target network	Support management functionality	Communica-tion protocol	Current status
ETSI (TS M2M)	Jan. 2009	All	Fault Management, Configuration Management, Account Management, Performance Management, Security Management	RESTful APIs	Drafts are available TS 102 690 - Architecture specification [23] TS 102 689 - Service requirement [17] TR 102 691 - Smart meter [20] TR 102 732 – eHealth [22] TR 102 897 - City automation [21] TR 102 875 - Connected consumer [19] TR 102 898 - Automotive[18]
TIA (TR 50 WG)	Dec. 2009	All	Security, Performance, Network management/Operations, Device Management (discovery and identification)	Not yet defined	Preliminary stage. Defined the focus and established the groups
IPSO IETF (6LowPAN + ROLL + CORE WG)	Sept. 2008	IP	CoAP protocol will support – Congestion control, multicast, caching, resource discovery, monitoring, security, create, read, update and delete resources.	CoAP, will also define binding with HTTP REST API	rfc's drafts are available rfc4919 - Problem statement for 6lowpan [24] rfc4944 - Basic specification for 6lowpan [25] 6lowpan nd – Neighbor discovery in L2Ns. [26] RPL - IPv6 Routing protocol for L2Ns [27] CoAP – Application layer protocol to monitor and control smart devices. [28]
OMA DM M2M initiative	Pipeline	Mobile and Personal area network	Firmware updates, Software updates, Provisioning, Diagnostics, Monitoring	SyncML, binding with HTTP REST and SOAP	Not available
ESNA (OSGP + NTA8150)	Sept. 2010	Smart Grid network	Installation Maintenance, Meter-to-data assignment, Configuration, Performance monitoring, System-level diagnostics	XML and SOAP.	NTA8150 - Provides AMI API Interface for application and service layer [8] OSGP – Communication and data model [8]

IV. M2M APPLICATION CHARACTERISTICS AND ITS IMPACT ON NETWORK MANAGEMENT

The standardization bodies are working on defining the service requirement and architecture for M2M networks and applications. Network management of M2M is also part of their focus. However none of them have identified the characteristics of M2M applications which will effect network management and other service provisioning. In this section, we describe some specific characteristics of M2M networks and devices. While designing a network management system for M2M networks, it is important to consider these specific characteristics. Some characteristics are common for all M2M networks including Sleeping devices, Low power lossy area networks, Heterogeneous networks and Device intelligence. Certain characteristics including Mobility, Two way communication, Network dynamics, Time sensitivity of data and Data volume will differ from application to application. Table III shows the relative study of the applications, which are sensitive to these characteristics. Here we elaborate each characteristic and how they affect network management of M2M systems.

1) Sleeping devices – Battery operated M2M devices will have long sleep times. M2M network management systems shall be able to buffer and deliver the management requests to the devices when they are awake. Management system shall not be overburdened by keeping track of the sleeping devices beyond the gateways. Sleeping devices also require time synchronization for efficient message handling.

2) Low power lossy area networks (L2Ns) – Some of the M2M network can be made up of devices which will have low performance processor, small memory, low bandwidth and high loss rate, especially in M2M Area Network. M2M management system shall save power consumption for these

un-powered M2M Devices. Powered objects such as gateways should assist the un-powered objects such as sensors to take care of management functions. Reliable delivery of critical management messages shall be ensured in such network with the help of gateways.

3) Heterogeneous networks – M2M networks can use different communication media including wired and wireless media. Moreover, there is a possibility for M2M application to use multiple vendor equipments; hence there can be multiple management protocols and data representations of managed objects. M2M network management system shall be capable of interfacing heterogeneous M2M Area Networks management approaches. This may be achieved at the M2M gateway.

4) Intelligence - M2M devices may have more computing power and memory compared to sensors. M2M devices, specifically gateways, are more intelligent and have more autonomy compared to sensor gateways. Intelligence could help M2M network management system to provide several management tasks including intelligent power management, authentication, encryption, embedded security, dynamic ip handling, network registration, interfacing for GPRS/CDMA and SMS, plug and play, exception based reporting, scheduling etc.

5) Mobility – Multiple M2M devices can be embedded in vehicles for various service provisioning, safety and convenience. Medical care and disaster relief applications will also have embedded devices with patients who need high mobility. While designing network management system for such M2M applications, considering various management aspects of mobility including location identification, navigation and roaming is essential.

TABLE III. TABLE III SENSITIVITY OF M2M APPLICATIONS TO SPECIFIC CHARACTERISTICS

	Mobility	Two way com	Time sensitivity of data	Network dynamics	Data volumes
Automotive / Track and Trace	High	High	High	High	Medium
Connected consumer	Low	Medium	Medium	Low	High
Smart metering	Low	High	Medium	Low	High
eHealth	High	High	High	High	High
Monitoring (Person/Animal/Objects)	High	Medium	Medium	High	low
Point of Sale	High	Low	High	Medium	Medium
Controlling (Vending machine/ Production machines)	Low	Medium	Medium	High	Medium

6) Two way communication – Certain M2M applications have higher data communications and signaling from both, server to client and from client to server. For example in case of automotive, client to server data communication can include events based or periodic reports, emergency reports or non emergency reports, set of data consisting of the position of the vehicle, its velocity and a time tag etc. Server to client data communication can include provisioning information, such as reporting intervals, reporting schedule, position requests and a set of triggering events under which the M2M device is to establish a communication link and contact the M2M server. Higher two way communication will require better upload and download bandwidth and QoS provisioning.

7) Time sensitivity of data – Certain M2M applications are time sensitive, i.e. the data delivery should have minimum latency and high responsiveness. Time critical data includes eHealth data and accidental data from automotive applications. For designing network management for such systems better QoS provisioning and SAL monitoring is essential.

8) Network dynamics – M2M networks with higher network dynamics will have higher dropped packets, dying nodes, nodes becoming disconnected, powering on or off, new nodes joining the network, etc. Such networks shall have robust failure and fault notification mechanisms. Devices and gateways shall be able to return to fully operational state autonomously if possible. Reliable delivery of a message shall be supported.

9) Data volume – Certain M2M applications such as surveillance data uploading in home security system, continuous health monitoring in eHealth, and smart metering systems, will have higher data communication. In such systems, guaranteed QoS is required. Another general characteristics of M2M application data is that, M2M applications will have bursty traffic at regular intervals or on the trigger of certain events such as fault events, accidental events etc.

As we see that the characteristics of M2M networks vary from application to application. They also impact certain aspects of network management tasks.

V. REQUIREMENTS FOR M2M NETWORK MANAGEMENT

In this section we will elaborate the network management functionalities required for M2M networks and applications. We are not focusing on the specific techniques required to achieve the management tasks. This will be part of our future work. Our focus here is on requirement gathering for M2M network management only.

1) Fault Management – Fault management is essential part of all types of M2M networks and applications. Fault management could be periodic, on demand or event driven. M2M network management shall support periodic, on demand or event driven reporting of faults with specific parameters (i.e. time, date and fault data). Event driven reporting shall be supported on events including power outage, communication outage, node failure, link failure, congestion, protocol failures, service failure and unsuccessful installation attempts. Apart from these general event driven faults, accidental,

environmental and theft related context information can also be triggered as an event in fault management of M2M. M2M network management shall also support preventions from faults by reconfigurations, reinstallations, rebooting and firmware updates. M2M network managment shall log the faults with diagnostic information, so that it could be retrieved upon request.

2) Configuration Management and Software Upgrade – Gateway and core shall support configuration management, auto-configuration, and registration to M2M services. Time synchronization shall also be provided by gateways and devices. M2M network management shall be able to change the state of a M2M Device remotely e.g. enable or disable. It shall be able to configure for reporting with the specific parameters and rate, events or alarm trigger rates. M2M network management shall support downloading and securely installing new software updates. Device shall be able to accept, deny or defer the updates. Both type of update shall be provided, i.e. automatic update and prompted update. Pre provisioning of all these network management services on M2M gateways and devices shall be possible, even when communication path is unavailable or device is in sleeping mode.

3) Mobility Management – Mobility management is critical requirement in M2M applications with high mobility as shown in Table III. Mobility management will include location awareness, navigation support, vertical-horizontal handoff and roaming facilities depending on the application needs. GPS-based systems are popular for location management. A GPS-based system shall support intelligent network selection and intelligent GSM and GPRS registration. It shall also support intelligent PDP context (GPRS data session) management, so as to avoid too many short sessions or a very long sessions with little data. Mobile nodes have higher possibility of residing beyond the reachable area; in such situation application might try to connect to the nodes aggressively. M2M network management shall try to avoid such aggressive behavior to reduce signaling and power overhead.

4) QoS and SLA monitoring – Certain applications have characteristics such as high two way communication, high time sensitivity of data and high data volume as shown in Table III. QoS and SLA monitoring will be an essential management task in such mission critical applications. The parameters which should be monitored can include bandwidth utilization and latency. If bandwidth utilization or latency exceeds the threshold value defined in SLA then blocking of the services or graceful degradation of the service shall be supported. In future multiple M2M services can be provided in single M2M network. The service provider will need to provide better QoS for certain services to certain customers. In such scenarios, traffic classification is essential for service providers to manage and configure various services for different customers. Resource allocation based on the priority of the services shall be supported.

5) Account management – Charging scheme for M2M service usage can be prepaid or postpaid. M2M account management shall provide support for both type of charging schemes. Automotive application shall support provide pay as you drive and auto insurance facilities. eHealth system shall also support auto health insurance support. Smart metering systems can support prepaid scheme and alerts to the customers about recharging of the account. Faults management and QoS management system shall directly communicate with account management to provide compensations for the power outage and critical faults.

6) Security Management – As M2M networks are interoperable networks, the data travels from one type of networks to another. Therefore, all the actors involved in the M2M system should collaborate to provide end to end security. Authentication, data confidentiality and integrity, authorization, treat and virus attack protection, a trusted and secure environment, and secure software upgrades are important security management features for M2M systems [17]. M2M systems shall support authentication of M2M cores, gateways and devices. When there is a request for M2M gateway/device or service access, then M2M gateways and devices shall be able to authenticate the M2M applications from which the request was received. In M2M systems, there are multiple services; each service shall be able to perform separate authentication. The strength of authentication shall be chosen by the customer. M2M systems shall protect the privacy of the user and the data. When data gets exchanged, it shall be confidential. The appropriate encryption algorithm shall be applied to ensure the confidentiality of the data. M2M systems shall also provide secure updates of application security software for M2M devices and gateways remotely. The security keys and algorithms shall also be securely distributed among M2M devices and gateways.

VI. Conclusion and Future Work

This paper has described the characteristics and management requirements of M2M systems. The focus of the study is on network and device management. By analyzing existing M2M applications and their service requirements, we proposed a common set of management functionalities for M2M systems.

The management requirements were gathered and analyzed considering certain characteristics of M2M systems including sleeping devices, low power lossy area networks, heterogeneous networks and device intelligence, mobility, two way communication, network dynamics, time sensitivity of data and data volume. Considering these characteristics, we proposed a common set of management functionalities for M2M systems, which include fault management, configuration management, software upgrade, location management, QoS and SLA monitoring and security management.

For our future work, apart from network and device management functionalities we will also analyze management functionalities for M2M services management. We will compare different management paradigm including distributed, centralized, peer to peer, agent-based management and

management by delegation. After comparing these management approaches we will propose the suitable management paradigm for M2M network and services management. We will also define management policies and expressive languages or metadata for information exchanged between M2M nodes pertaining to these management functionalities.

REFERENCES

[1] "Digi launches major M2M initiative with easy, out-of-the-box cloud connectivity for embedded development", http://www.digi.com/news/pressrelease.jsp?prid=703, April 2010. (last access May 10 2011)

[2] "ETSI M2M", http://www.etsi.org/Website/Technologies/M2M.aspx.

[3] Roy Thomas Fielding, "architectural styles and the design of network-based software architectures", http://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm, 2000.

[4] "TIA TR-50", http://www.tiaonline.org/standards/committees/committee.cfm?comm=tr-50.

[5] Jeff Smith, Joint coordination activity on internet of things, Geneva, 15-16 March 2011 (http://ftp.tiaonline.org/TR-50/TR-50_main/Public/20110318_Teleconference/TR50-20110318-004_JCA%20IoT%20March%202011%20Meeting%20-%20TIA%20TR-50_Jeff_Smith_rev1.0.ppt).

[6] "IPSO", http://ipso-alliance.org/.

[7] "Device management working group", http://www.openmobilealliance.org/Technical/DM.aspx.

[8] "ESNA", http://www.esna.org/.

[9] Ileana Leuca,"OMA M2M activities", ETSI M2M Workshop, Sophia Antipolis,19-20 October 2010 (http://docbox.etsi.org/Workshop/2010/201010_M2MWORKSHOP/06_M2MGlobalCollaboration/LEUCA_OMABOARDx.pdf).

[10] "NIST framework and roadmap for smart grid interoperability standards release 1.0", http://www.nist.gov/index.html.

[11] "iDigi", http://www.idigi.com/.

[12] "Numerx",http://www.numerex.com/News-and-Events/Press-Releases.aspx.

[13] "Inilex Apprize M2M communication platform", http://www.inilex.com/Apprize/Apprize.html#.

[14] "MWA Intelligence", http://www.mwaintel.com/index.html.

[15] "Omega management suite", www.racowireless.com.

[16] "Silentsoft 7Days telemetry", www.silentsoft.com.

[17] "ETSI TS 102 689 V1.1.1 (2010-08)", http://www.etsi.org/Website/Technologies/M2M.aspx.

[18] "Draft ETSI TR 102 898 V<0.4.0> (2010-09)", http://docbox.etsi.org/M2M/Open/Latest_Drafts/00008v040.pdf.

[19] "ETSI TR 102 857 V0.3.0 (2010-06)",http://docbox.etsi.org/M2M/Open/Latest_Drafts/00006v030.pdf.

[20] "ETSI TR 102 691 V1.1.1 (2010-05)", http://www.etsi.org/deliver/etsi_tr/102600_102699/102691/01.01.01_60/tr_102691v010101p.pdf.

[21] "Draft ETSI TR 102 897 V<0.1.1> (2010-01)", http://docbox.etsi.org/M2M/Open/Latest_Drafts/00007v011.pdf.

[22] "Draft ETSI TR 102 732 V0.3.1 (2010-03)", http://docbox.etsi.org/M2M/Open/Latest_Drafts/00005v031.pdf.

[23] "Draft ETSI TS 102 690 V0.10.3 (2011-01)", http://docbox.etsi.org/M2M/Open/Latest_Drafts/00002v0103.pdf.

[24] "6LoWPANs", http://tools.ietf.org/html/rfc4919.

[25] "Transmission of IPv6 packets over IEEE 802.15.4 networks", http://tools.ietf.org/html/rfc4944.

[26] **"**Neighbor discovery optimization for low-power and lossy networks", http://tools.ietf.org/html/draft-ietf-6lowpan-nd-15.

[27] **"**RPL: IPv6 routing protocol for low power and lossy networks", http://tools.ietf.org/html/draft-ietf-roll-rpl-19.

[28] **"**Constrained application protocol (CoAP)", http://tools.ietf.org/html/draft-ietf-core-coap-01.