I J A B E R, Vol. 14, No. 2 (2016): 1317-1326

AN ADVANCED PLATFORM FOR M2M DEVICES AND GATEWAYS

Sardorjon Vakkosov[1]

Abstract: *M2M communication is viewed as a new era of communication. A lot of devices are connecting to each other resulting new opportunity for vendors and new business. M2M communications are defined as the automotive communication between remote devices and central management system. It means that the real-time applications for monitoring the specific environment can operate without human intervention. One of the examples of environmental monitoring applications is smart metering which is defined to gather data from the environment using sensor nodes and forward the data through gateways and sink nodes. Storing data that received from sensor nodes, processing them and transmitting it using proper communication technology is very challenging. In this paper, we propose a platform that provides solutions for M2M devices and gateways for making them operate more accurately and efficiently. Besides, we present the implementations of communication protocols.*

Key Words: *M2M, M2M platform, M2M architecture, M2M technologies, Protocol, CoAP.*

AN ADVANCED PLATFORM FOR M2M DEVICES & GATEWAYS

Machine to Machine (M2M) is defined as a communication for devices such as tablets, mobile phones, computers and any other asset which operates with or without human intervention. In other words, M2M communications provide a large-scale connection of heterogeneous networks (*A cellular-centric service architecture for machine-to-machine (m2m) communications*. Lo, Y. W. Law, and M. Jacobsson).

The number of connecting M2M devices is growing dramatically. On one hand, this growth brings opportunity for industry and provides advantages for M2M applications. On the other hand, it causes new challenges to solve for both industry and research initiatives. While the growth of the number of M2M devices increases the verticality of M2M applications in the different business domains, there is a lack of interoperability between two different applications of two distinct

1. Jung-Il Namgung, Soo-Hyun Park Ubiquitous System Lab, Graduate School of FIS, Kookmin University, Seoul, South Korea *{svakkosov, greenji, shpark21}@kookmin.ac.kr*

business domains; that is one of the major problems which M2M is facing today. In order to solve the problem, applications should exchange general infrastructure, ecosystems, and system components.

M2M applications should assure that its components perform interoperability and the system itself has a highly qualified network structure; devices and gateways are supplied with sufficient software in order to provide cost-efficiency and less power consuming. One of the significant problems is the weakness of devices that employed in the system. The devices and gateways are fixed and they might run multiple applications at the same time.

In order to address these problems, ETSI defined a technical specification for the M2M platforms that implemented RESTful architecture. There are several applications which developed with the accordance to the specification. In order to actualize M2M devices and gateways, ETSI M2M architecture presents Remote Entity Management service. Remote Entity Management advances controlling by increasing the confidentiality of a device and offers various management functions.

In this paper, we purpose a comprehensive platform that takes into account the major requirements of any kind of M2M devices. Our intention is to describe the operating of M2M platform on the devices and gateways with the accordance to official standards which issued by standardization organizations. Specifically, we review the architectures of M2M applications that deployed to constrained environment and represent some solutions that can be applied into M2M scenarios.

The remainder of this paper is organized as follows. Section II outlines the overview of architectures of some M2M scenarios. System model is described in Section III. The implementation of protocols using our test-bed is described in Section IV. Finally, Section V concludes and highlights directions for future work.

System Model of M2M Applications

As mentioned above M2M can be implemented by various types of applications. Commonly applied use cases of M2M are as follows: metering, environmental monitoring and etc,. The utilized devices in these types of applications are mainly resource constrained and environment also has some limitations.

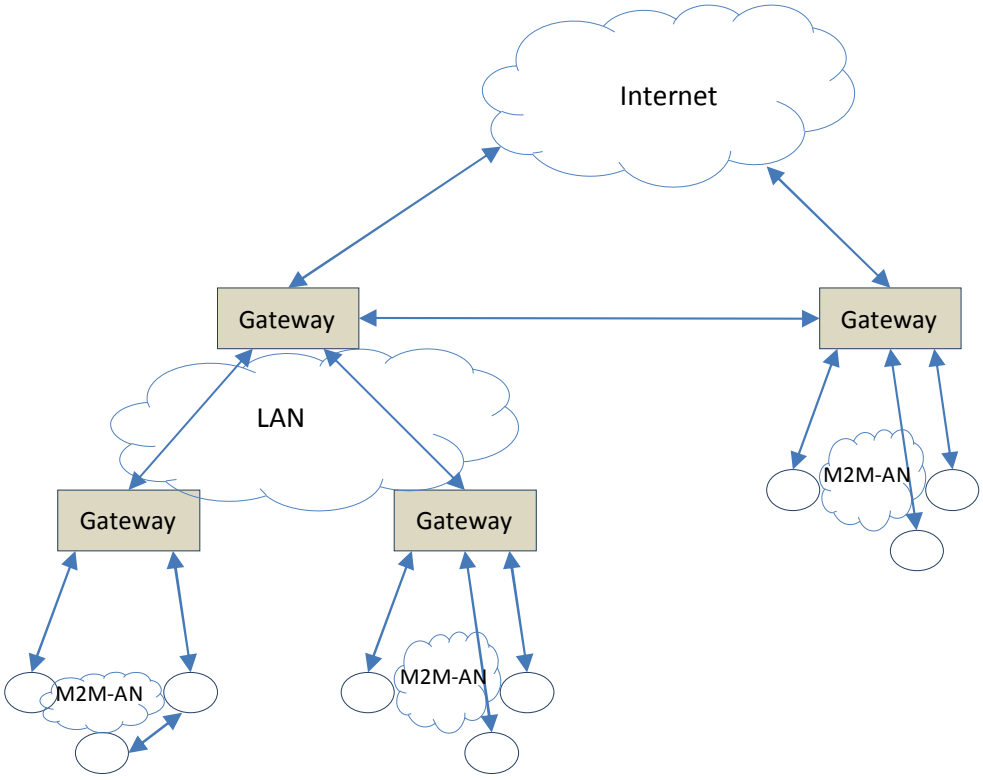
The resource constrained environment for M2M application is indicated by Constrained Environment term, those consists of two domains: network domain, gateway domain. Several constrained devices are deemed a suitable device for M2M applications like metering, home automation.

Low-power networks include constrained devices forwarding their collected data to a sink node. The method of forwarding might fail to sustain within two

device clusters. Herein, the real performance of M2M services is obtained as data that one node can pass to another (*Standardized Protocol Stack For The Internet Of (Important) Things*. M.R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, M. Dohler). The benefit of this communication is that the gathered data can be transmitted to base station using high level communication of clusters without any data loss.

Energy effective communication should be enabled for individual nodes in limited environment. Besides, gateways which concentrate communication traffic from terminal nodes should be used and provided connections to IP networks (*M2M: From mobile to embedded internet*. G. Wu et al).

Figure 1: M2M-AN architecture



The diagram showing the hierarchical M2M Area Network architecture is in Figure 1.

The gateways provide the following functions:

- Aggregate communication traffic from multiple terminal nodes
- Perform translations between communications protocols used in external networks (IP networks)
- Serve as a higher layer device for lower layer devices
- Serve as a platform for controlling terminal nodes and introducing value-added services

Implementing the integration of M2M-ANs with the Internet connects such devices in a cascade, allowing multiple M2M-ANs to get connected to a Wide Area Network (WAN). Nowadays, a new approach is being introduced to the market; gateways provide IP network connection utilizing a specific wireless technology (e.g., ZigBee)(http://www.digi.com/products/ wireless-routers-gateways/ gateways). But, still gateways are unable to make IP-based access to individual nodes in M2M-ANs, or to nodes in M2M-ANs which utilize different wireless technology.

IP-based communication requires the investigation of the network architecture that represents the nodes and network of an M2M-AN as an IP network.

Architecture of the Proposed Platform

The advanced platform aims to ease the development of new M2M services by supporting their devices and gateways with advanced functions. This chapter reviews the platform's design and usage, and some attention-worthy aspects are also discussed.

Operational Architecture of the Platform

Developing platforms for management and maintenance of devices and gateways are utmost important. Having a platform that provides the common functionality of any devices and gateways would simplify the development of M2M systems in terms of development time and cost. On one hand, developing software for communication, security, and data storing takes much effort and time. On the other hand, utilizing previously created software is not the proper way all the time. Seamless integration of connected devices into other services along with bypassing the regularly received appeal in M2M service platforms can be enabled by improving platform's design and architecture. Effective device control, acceleration of the ecosystem of various domains for M2M services and development of new and productive applications are targeted by such platforms.

Figure 2: Operational Architecture of the platform.

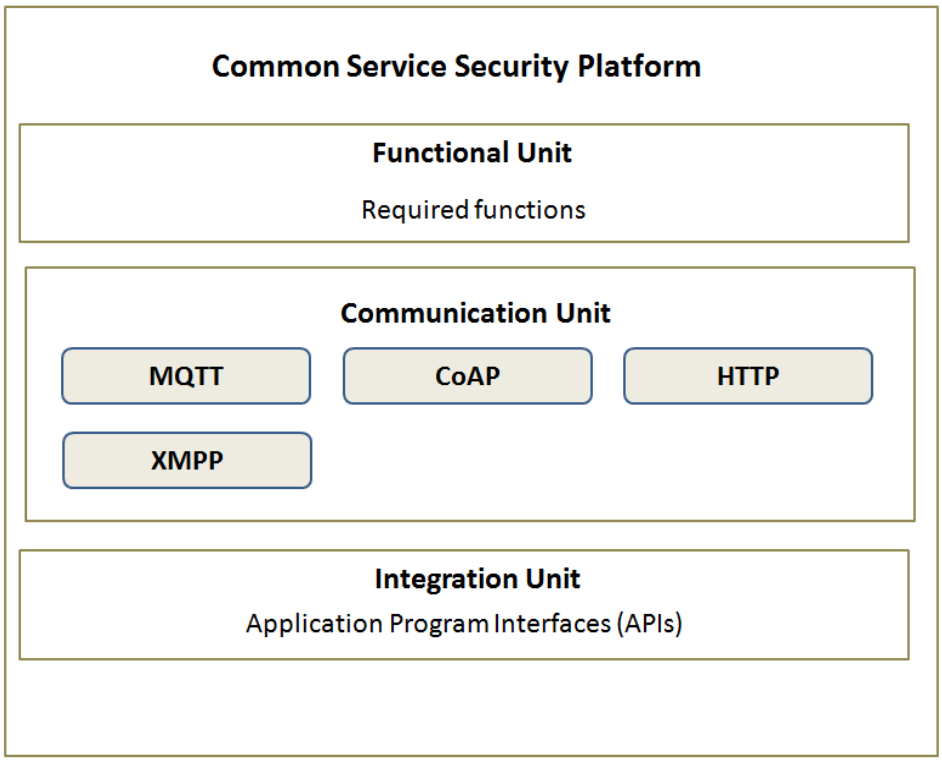


Figure 2 illustrates operational architecture of the platform including 3 unites:

1. **Functional unit:**

   Functional unit promotes administrative and security services with functions that can be defined as basis foundations.

2. **Integration unit:**

   M2M application can use several communication APIs that perform as a role of bridge to other ready services; that provides overall functionality of the device and gateways.

3. **Communication unit:**

   Communication unit includes several protocols to provide overall communication. It is needed to ease utilization of the platform and for secure communication.

Functional unit functions are classified as: Authorization, Authentication, and Accounting.

Integration unit implements several security capabilities such as data encryption/decryption, key derivation, signature generation/verification, security credential and etc.

Communication on the device/gateway domain and network domain are provided by the Communication Unit with lightweight communication protocols.

Overall architecture of the platform

The security platform applies various ways of storing and managing security in M2M systems to diversify scenarios in M2M applications.

Our suggested platform for M2M service is in Figure 3. One M2M standards and interface are used in order to deploy it M2M applications, which can utilize our Common Service Security Platform for common functionality of constrained M2M devices. M2M devices and Sensors/Actuators utilize various networks for inte rexchange of messages by CSSF on a communication stage.

1. Data Functionality

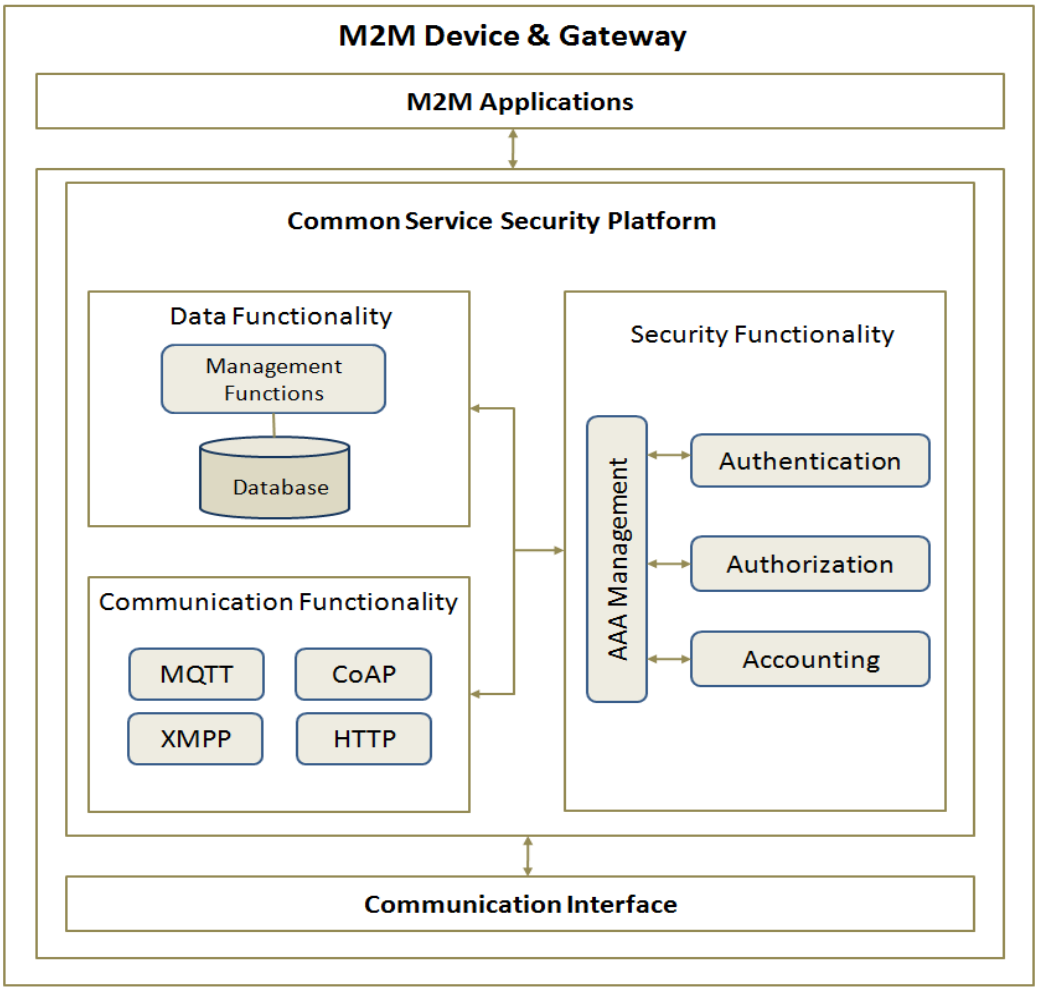
M2M applications utilize lots of devices and gateways in order to perform expected manner. In some scenarios, sensor devices gather data and they should store the date in order to keep confidentiality of the system. According to the implemented mechanism, device store the date for some time and forward it to gateways; gateways also store the date that transmitted from several nodes and forward it to a base station or end user. Mostly, devices and even gateways might not have enough resources and thus it is important to implement lightweight techniques. Our platform provides functionality for storing date and offer lightweight solutions to achieve that.

2. Communication Functionality

Communication functionality is important as proper wireless technologies enable protocols and M2M applications to conduct better performance and efficient energy usage. Decreasing interference and expanding spectral effectiveness and widening network capacity is in central focus now. Recently, new techniques for a better effective energy network explication were introduced, concentrating on maximizing the cell size. Of the network architecture methods, cooperative relaying is under special attention and problems of expanding and widening network capacity and effectiveness are to be solved soon.

After an absence of wired access to the application domain, interconnected nodes' connection is delivered by cellular networks, but there are unreliable high packet loss rates. Therefore, on the basis of several M2M protocols, lossy channels simplify the styling and the procedure of M2M applications by determining features.

Figure 3: Overall architecture of the platform



The platform includes the Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP) and the Message Queuing Telemetry Transport (MQTT) protocol as the protocols of Communications Functionality. Besides, the platform also includes Hypertext Transport Protocol (HTTP) to offer for gateways in order to present its full communication functionality.

3. Security Functionality

The Security functionality is a one of the main entities within the platform, because of its capability to contain necessary functions and resources for providing a trusted condition for the implementation of software and receiver of sensory data

in M2M gateway. The Security functionality provides secure communication for the devices and gateways, thus it protects the devices from unauthorized access. It consists of three main mechanisms:

- Authentication
- Authorization
- Accounting

Implementation of the Platform

Some open source implementations, eclipse IDEA are used for the accomplishment of the proposed platform components in pervious chapter. Open source tools help CSSF to achieve full functionality of the platform.

Figure 4: Real test bed with Ubiquitous board

The test-bed environment is in Figure 4. Full functionality of the system is shown by two Ubiquitous gateway boards. A VM with Ubuntu installed is used as a server for testing. Ethernet communication helps us to connect experimental nodes and base station (in this case Linux installed VM). WiFi, ZegBee, 3G can be used in real M2M systems. Our platform offers communication protocols that can be applied for IP networks too.

Implementing Protocols

Exchanging requests and responses are available by the Constrained Application Protocol (CoAP). CoAP with the UDP protocol and transport layer security (DTLS) provides a notable secure communication.

The header followed bites are parts of message body - the length of the datagram defines the payload and its size. The whole message should match a single datagram as in the User Datagram Protocol (UDP).

Our experiment uses FreeCoap that includes several features of the protocol; and the size of the implementation is comparatively small. The FreeCoAP source code easily modifiable, so are Client + Server and DTLS features.

Sockets based client server program is used for conducting other two protocols.

Communication of the two targets is based on Socket, as of layman's term. IP-address and port are usually included in the socket.

The client-server architecture is conducted by the binding with the TCP / IP model. The client - server architecture allows client-server connection to be set up after client's initiation of the communication and server's observation,

Although Sockets are manageable in Java, C++, but we prefer C language in our experiment.

Being quite simple, Http is application layer protocol that uses TCP/IP stack for transferring the date. Herein, packages are delivered to the destination by TCP protocol.

Conclusion and Future Works

The number of the connecting devices is grooving dramatically. As the result, new deployments of M2M applications are appearing. Besides, this grows is creating new opportunities for the market. However, it is also creating new requirements to the M2M solutions. The adaptation of M2M applications into constrained environment requires lightweight mechanisms because of its resource limited devices. Constrained M2M devices have low capabilities in terms of both energy and computing resources. Hence, they cannot implement complex security schemes. In this paper, we offer our lightweight platform that proposes advanced functionality for M2M devices and gateways. Our future work will be focused on the improving functionality of the platform and presenting performance evaluation. Specifically, evaluation of the implemented protocols will be presented.

Acknowledgments

This research was supported by Department of Financial Information Security (BK21+ Future Financial Information Security Specialist Education Program Group), Kookmin University.

The work is a part of the results of the research "Development of the wide-band underwater mobile communication systems" supported by Ministry of Oceans and Fisheries, Korea.

References

Wireless Communications, IEEE, vol. 20, no. 5, pp. 143–151 (2013). *A cellular-centric service architecture for machine-to-machine (m2m) communications*. Lo, Y. W. Law, and M. Jacobsson.

IEEE Commun. Surveys and Tutorials, DOI 10.1109/SURV.111412.00158 (2012).*Standardized Protocol Stack For The Internet Of (Important) Things*. M.R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, M. Dohler

IEEE Commun. Mag., vol. 49, no. 4, pp. 36–43, Apr. (2011). *M2M: From mobile to embedded internet*. G. Wu et al

Digi International Inc. (2011) Connectport(R) X2 for Smart Energy. [Online].

Available: http://www.digi.com/products/ wireless-routers-gateways/gateways/