Journal of The Institute of Electronics and Information Engineers Vol.53, NO.3, March 2016 http://dx.doi.org/10.5573/ieie.2016.53.3.076
ISSN 2287-5026(Print) / ISSN 2288-159X(Online)

논문 2016-53-3-9

보안 표준 지원 M2M 공통 서비스 플랫폼

(Common Services Platform for M2M Supporting Security Standards)

사도르존 와코소브*, 남궁 정 일*, 박 수 현*

(Sardorjon Vakkosov, Jung-Il Namgung, and Soo-Hyun Park©)

요 약

사물통신(M2M)은 사람의 개입이나 간섭 없이도 2개 이상의 단말 간에 통신을 가능하게 하는 기술이다. M2M 통신은 환경 모니터링, 헬스 케어 등과 같은 다양한 유즈케이스에 적용될 수 있다. 대부분의 유즈케이스에서 M2M은 관심 있는 환경으로부터 데이터를 수집하기 위해서 센서 노드를 활용하며 데이터는 다른 기기(즉, 게이트웨이, 싱크 노드)를 거쳐 M2M 응용으로 전송된다. 어떤 유즈케이스에서는 M2M 단말들이 서비스의 신뢰성을 향상시키기 위해서 센서 데이터를 저장하고 처리할 수 있도록 설계되어진다. 게이트웨이와 싱크노드 또한 센서 노드들로부터 수집된 데이터를 저장 및 처리할 수 있다. 이러한 형태의 접근방법은 학계 및 산업계 모두에 매우 도전적으로 받아들여지고 있다. 이러한 접근방법의 성능을 개선하기 위해 본 논문에서는 M2M 단말과 게이트웨이를 위한 공통 서비스 보안 플랫폼(CSSP)를 제안한다. CSSP 플랫폼은 단말과 게이트웨이를 보다 정확하고 효율적으로 만들기 위한 솔루션을 제공한다. 게다가, 통신 프로토콜간의 비교 및 선정된 메트릭스에 따른 프로토콜들의 성능 분석을 제시한다.

Abstract

Machine to Machine (M2M) is a technology that presents communication between two or more devices with or without human intervention. M2M communications can be applied for various use cases such as environmental monitoring, health care, smart metering and etc. In most use cases, M2M utilizes sensor nodes to collect data from the intended environment and the data is transmitted back to M2M application through other devices (gateways, sink nodes). In some use cases, M2M devices are being designed to store and process sensor data for improving the reliability of the service; Gateways and sink nodes are also intended to store and process the gathered data from sensor nodes. This kind of approach is very challenging for both academy and industry. In order to enhance the performance of this approach, in this paper, we propose our Common Service Security Platform (CSSP) for M2M devices and gateways. CSSP platform presents solutions for the devices and gateways by making them operate more accurately and efficiently. Besides, we present a comparative analysis of communication protocols and present their performance in accordance with selected metrics.

Keywords : M2M, M2M platform, M2M architecture, M2M technologies, Protocols

Ⅰ. Introduction

Machine to machine (M2M) is a technology that creates various opportunities for both vendors and new business sectors. M2M communication is considered to be one of the succeeding boundaries in cordless communication[1]. In connection with the introduction of recent models for low-energy wireless communications and mobile operators set a goal finding new sources of profit, it is relatively new occurrence that wireless M2M communications are obtaining higher attention[2].

The growing number of the connected M2M devices will create challenges for mobile network operators (MNO). The total amount of devices and mobile network traffic will supposedly manageable

* 정회원, 국민대학교 금융정보보안학과
(Department of Financial Information Security, Kookmin University)
© Corresponding Author(E-mail: shpark21@kookmin.ac.kr)
※ This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2012461).
Received ; January 13, 2016 Revised ; February 16, 2016
Accepted ; March 7, 2016

with M2M is only 19% of connections and 4% of the traffic. However, conventional telephones, tablets, and mobile broadband connections are relatively similar with their requirements in terms of use, geographical location, safety and many other criteria. M2M devices are quite different. As a consequence, M2M devices are considered with different demands on the network.

The increasing number of M2M devices will be essential to cellular communication. It will grow from 250 million to 2.3 billion over the next decade. Traffic will continue to grow even faster from 200 pet bytes in 2014 to 3.2 Exabyte's in 2024.M2M devices do not behave the same as telephones, tablets, and other more specified mobile devices. This may result in less control traffic at certain times and in certain areas. For example, the review of the joint car market displays that at the peak point of the busy traffic hours in specific cells would double due to the sum of interconnected machines. On the other applications are equally diverse requirements, which could create issues for MNOs such as, health and supply chain applications that require a more reliable connection for crucial applications. Distributed applications for farming have a higher need for rural coverage. Besides, some other applications require a reduction of round trip time to enable real-time analytics. The growth of M2M requires intelligent network design and maintenance. MNOs should reconsider their method to the management of their networks to cope with the growth of M2M. These include the implementation of quite dynamic management and the network optimization, supporting heterogeneous networks, taking more sophisticated planning tools, and taking a more balanced approach to the spectrum reforms.

M2M growth has caused to apply different approaches in terms of supporting devices on mobile networks. Mobile Network Operators should plan and work according to the requirements of the M2M. Otherwise, they might suffer from the side effects that may create unpleasant user experience from their networks. On the other hand, it might cause to be being out of the new revenue opportunities.

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 the standardization organizations and represent some technologies that can be applied into M2M scenarios.

Today several M2M research activities and solutions fail to discuss a number of major arguments of application and service development, due to the fact that they often focus on energy capacity, protocols, and wireless networking. Besides, the study is not paying attention enough for following aspects: addressing, identifying, assigning, peer to peer transmission and networking, managing and mobility of appliances and systems. In order to address those arguments the architecture and platform design must be improved. Furthermore, many M2M platforms are in practise in market but most of them intended to specific devices or require much device resources. Common Service Security Platform (CSSP) provides flexible architecture and deployment for any kind of M2M devices. One of the impact of utilizing the platform for M2M systems is that: the platform does not require much device resources; It provides lightweight protocols in order to support either client-server and peer-to-peer communication.

The remainder of this paper is organized as follows. Section II outlines the overview of architectures of some M2M scenarios. Section III surveys different types of technologies that can provide communication for M2M applications. Detailed information about M2M applications as well as their security issues summarizes in this chapter. The proposed architecture and system model of the platform along with its respective functionalities are detailed in section IV. The performance evaluation of the platform is described in section V. Finally,

Section VI concludes and highlights directions for future work.

Ⅱ. ARCHITECTURE OF M2M APPLICATIONS

Constrained Environment term indicates the environment that M2M application applied for. In that environment devices and actuators are mainly resource constrained. According to ETSI's high level architecture for M2M, application consists of two domains: network domain, device domain. Low power constrained devices make low power networks in the device domain. Several constrained devices can operate unattended for a long time, therefore, they are deemed a suitable device for M2M applications like building automation, where numerous devices must be stationed and managed in accordance with cost-efficiency.

Low-power networks contain a set of constrained devices forwarding their collected data to a sink node that distributes the message to the back server. The method may not accurately obtain M2M connections within any cluster that contain two devices. In the context of adaptation of internet protocols into constrained devices, the real performance of M2M services can be recognized as knowledge that the nodes can discover and address another single M2M node in the same network[3]. Therefore, M2M applications that reside in the resource constrained networks supports communication for devices and one of those devices considered as a constrained device that acts locally without a requirement to report its state to delegate nodes. Allowing applications where sensors and gateways can transmit their data to the back ends or making a state of access for other devices is one of the benefits of this kind of communication. Besides, it creates comprehensive, globally available businesses for constrained devices.

Fig. 1. illustrates hierarchical M2M networks. Regionally associated devices can be linked with a cluster head. The nodes cluster head and sink nodes make child-parent associations. The nodes attempt to

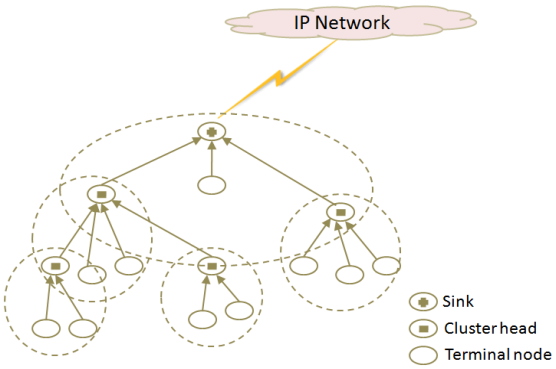


Fig. 1. Hierarchical architecture of M2M networks.

connect to the cluster head or sink node in order to send their data. By this context, the cluster head or sink node also can behave as a child node. Information that gathered from child nodes is transferred to the cluster heads. Each cluster head or sink node also might have its own data to transfer. In such cases, all data accompanies by the sender cluster head and transmit to parent cluster head.

In an environment in which there are numerous terminal nodes and these nodes have severe limitations in their processing power, communication distance, and power consumption, it is necessary to enable individual nodes to communicate efficiently without consuming much power. To achieve this, some studies have investigated using gateways, which concentrate communication traffic from terminal nodes and provide connections to external networks such as IP networks[4].

A conceptual diagram of this hierarchical constrained network architecture is shown in Fig. 2. The gateways provide the following functions:

- Aggregate communication traffic from multiple terminal nodes
- Perform translations between communication protocols used within the constrained network and those used in external networks (IP networks)
- Serve as a higher layer gateway for lower layer gateways
- Serve as a platform for controlling terminal nodes and introducing value-added services

An effective way of implementing the integration

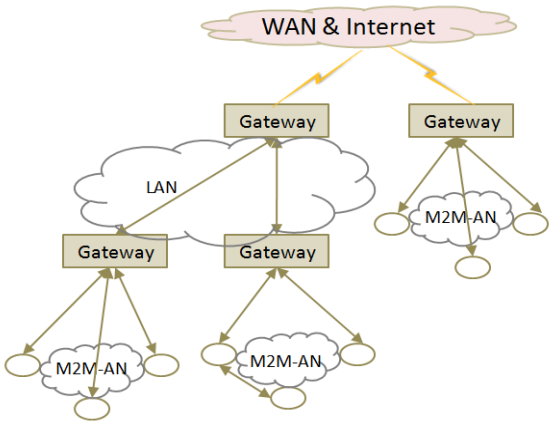


Fig. 2. Hierarchical M2M-AN architecture.

of M2M Area Networks (M2M-ANs) with the Internet is to connect such gateways in a cascade. This allows multiple M2M-ANs to be connected to a Local Area Network (LAN), which covers a relatively small area, and the LAN to then be connected to external networks, such as a Wide Area Network (WAN) and the Internet. Some gateways that use a specific wireless technology (e.g., ZigBee) for providing a connection to an IP network have begun to appear in the market[5]. However, such gateways can be used in a situation in which only the parent node of a single sensor network is connected to IP networks. Thus, it is not possible for nodes in external networks to make IP-based access to individual nodes in M2M-ANs, or for nodes in different M2M-ANs that use different wireless technologies to communicate with each other directly. In order to achieve direct IP-based communication, it is necessary to study the network architecture that represents the nodes and network of an M2M-AN as an IP network with granularities appropriate for a node and a network, respectively.

Ⅲ. TECHNOLOGIES FOR M2M APPLICATIONS

Sensors are the cornerstone of any M2M service. These are the devices gathering information, to be relayed further up in the system. Put simply, a sensor is a device that measures some physical quantity which is converted into a digital signal. Sensors are mostly realized by integrated circuits. One main goal for sensors if they are to be used for M2M is that they are extremely power efficient. A sensor will do no good, if the batteries have to be recharged constantly. Therefore the ideal sensor is one that can run on power from its surroundings, for instance sun or warmth.

For M2M, sensors are the first step in the system that records the data to be transmitted. The different types of sensors are too numerous to be counted and includes Radio-Frequency Identification (RFID) tags, wireless modules, embedded sensors and so on. Ideally these should obtain information and do certain tasks without human intervention. This is the ground idea of M2M, that the machines are communicating to each other, in order to ease the lives of humans.

1. IEEE 802.15.4

IEEE 802.15.4 is one of the standards that produced and supported by IEEE 802.15 working group [6]. This specification is targeted to physical (PHY) and medium access control (MAC) layers and has been designed for the low-rate frequency and low power WPANs. IEEE 802.15.4 is based on the other standards, determine the higher layers to allow a complete network protocol stack. The standards such as ZigBee, WirelessHART, 6LoWPAN, etc utilize IEEE 802.15.4 as a physical layer protocol.

The physical layer is specified including following three distinct frequency ranges:

- 902-928 MHz, originally up to ten channels, enlarged to thirty
- 868-868.8 MHz enables one channel
- 2400-2483.5 MHz allows sixteen channels

Major characteristics of the standard are the utilization of supported time cuts and express function multiplied access with interference delay, to avoid interference, sound immunity utilizing a linear spread order spectrum, also energy efficiency using sleep mode. Guaranteed time slot ensures the transfer of certain types of sensors, if they are critical, for example, in the case of home automation is the fire alarm may desiring to send a notification or security

intruder detection.

From different frames, we expect the default function or model that another device can analyze and recognize. The various structure types have different features and use cases. Several examples of structures in accordance with IEEE 802.15.4 are defined as following: Beacon, ACK, data, and MAC. Expression of them is as follows:

- A beacon frame, used by a coordinator to transmit beacons
- A data frame, used for all transfers of data an acknowledgment (ACK) frame, used for confirming successful frame reception
- A MAC command frame, used for handling all MAC peer entity control transfers[7]

The frames are mainly utilized for the weaker band transmission, for example, to associate with other devices and making transfers adequately reliable for transmission in noisy environments.

IEEE 802.15.4 headers contain the physical and MAC header including a number of selections to be inserted and viewed in transmission. The highest size of the packet for physical layer is 127 octets, and highest overhead is 25 octets. As a result, MAC layer's highest resolution frame is 102 octets. At the Link layer, the security mechanism, which is voluntary, yet much suggested, requires more overhead that is the greatest case (21 octets in the case of AES-CCM-128, compared to 13 and 9 for the AES-CCM-64 and AES-CCM- 32 respectively) transmits 81 octets ready for the upper classes.

2. ZigBee

ZigBee utilizes IEEE 802.15.4 standard as a physical layer protocol and one of the utmost technologies for constrained environment applications with low bandwidth, low-power, and low-cost features. In most scenarios it is utilized for wireless personal are networks or mesh networks that work across large intervals. Despite Wi-Fi, ZegBee is not able to simply talk with others IP protocols. But, the advantage is that the ZigBee devices can remain in sleep, and it dramatically increases energy consumption time.

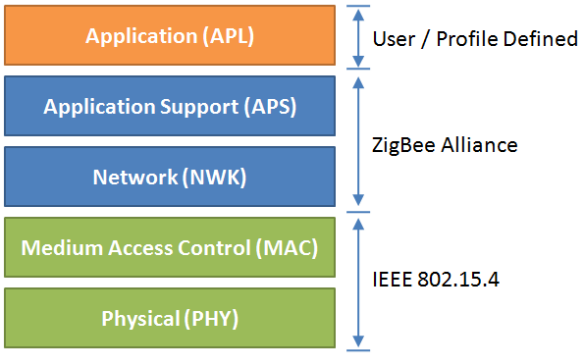


Fig. 3. ZigBee Stack.

To ensure interoperability between technologies that produced from various manufacturers, the ZigBee technology is identified by numerous forms of the devices. Forms that established and included in the technical reports of ZigBee contain home automation, ZigBee Smart Energy, telecommunications applications, and industrial home automation, and etc. These profiles include use cases like industrial control, environmental data gathering, medical data collection, home automation, building automation, etc. The initiative of the technology is an attempt to combine standards ROLL IPv6 and IETF 6LoWPAN in stack ZigBee. The easiest method to make it possible is accommodating ZigBee Application Layer above UDP protocol[8].

As shown in Fig. 3. ZigBee is built using IEEE 802.15.4 as a physical layer protocol and maintains custom application layers and other profiles that defined by ZigBee Alliance. ZigBee represents two kinds of devices: reduced function devices and full function devices. Usually full function devices maintain more resources and hence, can serve as a coordinator, end device or a router if desired. Reduced function devices are oftentimes battery powered devices. For that reason, they can only serve as a terminal device.

3. 6LoWPAN

IP for Low-power Wireless Personal Area Networks (6LoWPAN) is slightly distorted acronym that merges the advanced type of the Internet

Protocol (IPv6) and Low-Power Wireless Personal Area Networks (LoWPAN). This enables IP for the applications that utilize energy constrained and limited computing power devices. 6LoWPAN is recognized as the leading wireless standard for M2M / IoT scenarios.

Although 6LoWPAN has many security challenges and also has many drawbacks to trust that are available with its development. The sensor devices are generally designed for a neglected environment and the packages might simply listen in communication. To succeed vulnerability of 6LoWPAN, many types of research and development clarifications have been offered. In order to stop denial of service (DoS-attack) that is a dangerous threat for M2M networks, attack revelation mechanism with interference discovery system has been suggested[9]. It is shown that it can detect critical threat those attacks for 6LoWPAN networks if attack preventing solutions are utilized. In[10] integrated secure gateway-based 6LoWPAN was proposed and according to the solution, users can interact instantly with the sensor devices or to request sensor information from the internal server.

While developing security protocols it utmost important to take compromising attacks into an account. The simple implementation of Internet Protocol Security (IPsec) which proposed in[11] has capabilities to support integration among the WPAN and the 6LoWPAN. In fact, quite few research on the topic of secure 6LoWPAN using IPsec can be found recent research works. Challenges implementing the IPsec system with limited resources are still open at the stage of discussion. However, some researchers are proposed like SAKES - Secure Authentication and Key Establishment Schemes. SAKES utilize encryption mechanism for messages. The mechanism is a combination of a symmetric key in the authentication stage and a tiny asymmetric key in the state of establishing the key for building a session key between 6LoWPAN devices and the server[12]. In use, the session key is determined utilizing the Diffie-Hellman key exchange method

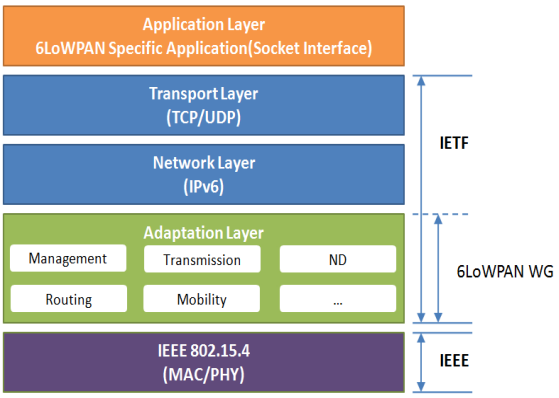


Fig. 4. 6LoWPAN Protocol Stack.

(DH) that enables the both sides to obtain an arrangement of joint secret key by swapping data through a safe channel. But session key utilizing DH have some drawbacks like it is generated on the client side but it is not equal on the server side. SAKES has an opportunity to object against the funnel and canker attacks, however, it might be restricted only if that 6LHs and 6LRs haven't completed. In addition, SAKES has a flaw that only security assurance implemented beside inactive nodes in the 6LoWPAN network. Fig. 4. shows the protocol stack of the 6LoWPAN.

4. Bluetooth

Bluetooth is a standard that managed by Bluetooth standard. Previously, it is maintained by IEEE 802.15.1 and IEEE stopped supporting for today. Formerly, it was intended to utilize for constant, flowing data applications that a large amount of data is transmitted through a short distance.

This makes Bluetooth a higher utilization of energy consumption. On the contrary Bluetooth, the Bluetooth Low Energy (BLE) produces low energy consumption. Bluetooth Low Energy came out to the business in 2011. Bluetooth Low Energy works in the range of 2.4 GHz and an extra major advantage of BLE is as follows: it stays in hibernation mode until the communication is established. Original network communication time equals some milliseconds for BLE while the Bluetooth consumes 100 milliseconds.

Ⅳ. THE SYSTEM MODEL OF PROPOSED PLATFORM

The Common Services Security platform (CSSP) supports its functions in order to simplify the development of M2M applications. M2M devices and gateways can have common functionality utilizing the platform. The design of the platform, its utilization, and some other useful analyzes will be studied in this chapter.

1. Operational architecture of the platform

Various M2M research activities and solutions fail to discuss a number of major arguments of application and service development required in order to understand and distribute of M2M services, due to the fact that they often focus on energy capacity, protocols, and wireless networking. M2M service platforms recently became an area of modern market, but there are several platforms in practice now. Platforms can be distinguished in agreement with the objectives, circumstances, and enterprise systems. In order to distinguish the number of platforms satisfied the M2M platform specifications, we can set following perspectives: standard based, flexibility, and scalability. Additionally, the following issues also must be sold along with the development of the M2M service platforms. Those are addressing, identifying, assigning, peer to peer transmission and networking, managing and mobility of appliances and systems. The architecture and platform design must be improved to allow the seamless connection of objects toward other operations utilizing Application Program Interfaces (API), therefore avoiding the regularly caught criticism in M2M platforms contain too many conditions. The principal objectives of such platforms include promoting and developing new and original applications, for controlling devices efficiently, and for stimulating the various domains' ecosystem for M2M services.

Fig. 5. shows operational architecture of Common Service Security Platform (CSSP). As illustrated in the fig 5, the platform consists of 3 unites:

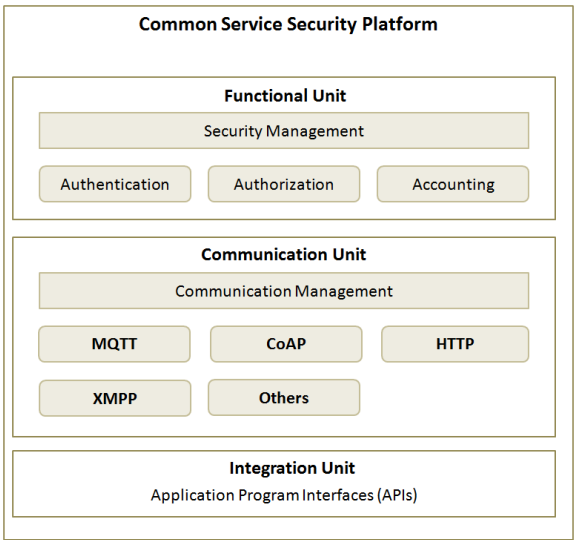


Fig. 5. Operational architecture of the platform.

A. Functional unit

Functional unit contains a set of functions that provide administrative and security services. These functions can be classified into several categories and considered the basis foundations of the platform.

B. Integration unit

Basically, M2M application can use other ready to use services in order to produce its overall potential. This unit includes several communication APIs that perform as a role of bridge to other ready to use services. These APIs can be considered as key functions for providing overall security of the platform.

C. Communication unit

Communication unit includes several communication protocols that are used to provide overall communication. CSSP involves this unit in order to ease utilization of the platform and perform secure communication.

Functional unit functions can be categorized into following sections; they are Authorization, Authentication, and Accounting.

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

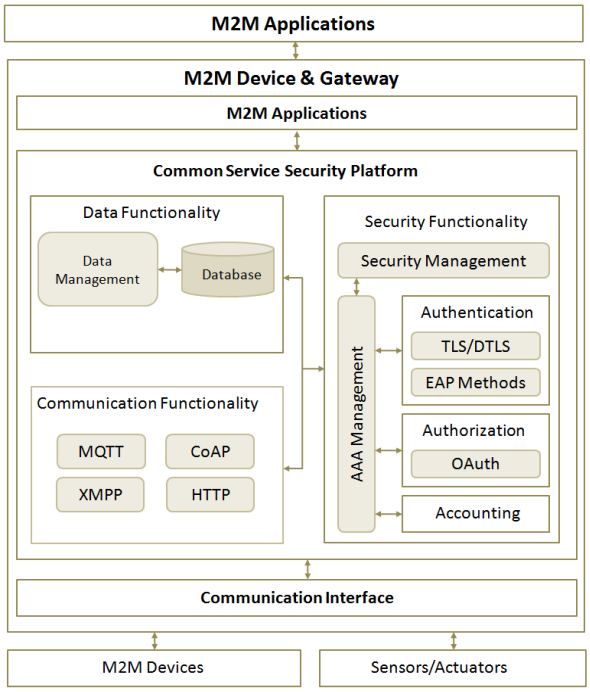


Fig. 6. Overall architecture of Platform.

functional unit request these functions for doing the maintenance concerning secure environments.

Communication unit includes set of lightweight communication protocols in order to provide communication on the device/gateway domain and network domain. Protocols are based on Rest approach.

2. Overall architecture of the platform

To provide the diversity of deployment scenarios that can be found in M2M applications, security platform encourages a variety of methods to store and establish security in M2M systems.

Fig. 6. shows the adaptation of our proposed platform into M2M service scenarios. Our platform has been implementing OneM2M standards and includes interface in order to deploy it M2M applications. In other words, M2M applications can utilize our CSSP in order to achieve common functionality of constrained M2M devices. On communication stage M2M devices and sensors/ actuators utilize different kind of networks in order to send/exchange their messages using CSSP. CSSP has M2M Communication Interface for supporting those network types.

A. Data functionality

M2M applications might contain autonomously working sensors that report central server about the specific parameters. It is important to mention that those parameters could possibly be indicators for patient of the healthcare scenario and smart city, air condition control application, while those utilizations are supposed to form Internet of things by having many sensors connected to each other and to an external network such as internet. The IoT produced traffic that most likely form a significant portion of the future internet traffic; consequently, both internet backbone and the data storage centers can be influenced negatively by the extra amount of traffic. In order to overcome possible data blast influence[13], it should be possible to take an account of internetwork gathering[14] and memory where locally created data is stored in the sensor devices. In this case, the sensor data to the sink node is transported either by a trigger event or by a query from the sink on an event based approach in order to supply the sink node with the transmitted information. In addition, sensor data can have a form for retrieving itself on a charge of reliability. There are two applicable ways, such as:

1. Nodes store multiple replications of sensor data in their internal storage: In this way sensors should have reliable and manageable database system. However nodes are resource constrained thus it is not the proper way to employ more resource consuming database system. On the other hand utilizing a database system which has convenient management and administration can be applied gateways that have more energy and other resources.

2. Distributed storage: By the usage of the shared storage solution which enables data belonging of the node to be stored across numerous nodes; which are later retrieved through the connection of a subset of these nodes.

Adding repetition into network by replication can increase the convenience of sensor data; however, the advantage of increasing the access reliability to sensor data cannot overweight the financial

disadvantage of bandwidth and storage demands of this kind of solution being relatively expensive as compared to a code shared storage system. Moreover, deleting codes could be one possible improvement of the effectiveness in the shared storage system, for instance, one of the widely-known families of deleting codes named Maximum-Distance-Separable (MDS) codes[15], is able to fix utmost number of deletions taking into account the number of exorbitance or parity symbols.

B. Communication Functionality

Communication functionality is considered one of the main factors for building M2M applications. Applying proper wireless technologies enable protocols and architectures of M2M scenarios to allow considerably efficient energy usage and enhance performance.

Despite, the fact that network architecture is stated as the major matters in M2M systems research, much focus in network architecture and deployment is paid to decreasing interference and expanding spectral effectiveness and widening network capacity. Recently, professionals began accepting that making use of the network architecture is one of the most reliable policies for reducing energy consumption. As a result, various techniques were suggested in written works for a better effective energy network explication, concentrating on maximizing the cell size, examining cognitive radio and heterogeneous networks, while allocating both on-cooperative and cooperative relay nodes. Of the network architecture methods, cooperative relaying that still inflicts non-trivial issues and unacknowledged queries in relation to energy consumption issues, is under specific attention and those present problem sere to be solved by considerable research work that concerning various issues of that specialization, including expanding and widening network capacity and effectiveness.

In M2M networks, interconnected nodes are mostly conducted by cellular networks, as they are often allocated in isolated spaces in an absence of wired access to the application domain. The main disadvantage is that: in high packet loss rates such networks are quite unreliable. Therefore, on the basis of M2M several protocols were specially developed on lossy networks, because determined features of these protocols are able oversimplify the design and the procedure of M2M applications.

The CSSP platform includes Communication Functionality, the Constrained Application Protocol (CoAP), Extensible Messaging and Presence Protocol (XMPP) and the Message Queuing Telemetry Transport (MQTT) protocol that is a sample of M2M protocols. As soon as the M2M endpoints are used as a resource for constrained devices, and herein, the lightweight performance's amount determining main criteria for this selection. Besides, CSSP platform also includes Hypertext Transport Protocol (HTTP) in order to offer its full communication functionality for the gateways. In other words CSSP platform offers convenient utilization for both constrained nodes and gateways which have more computing and energy resources

C. Security Functionality

The Security functionality is an important entity of the platform. The functionality contains functions in order to provide secure communication within the M2M network; functions also intended to take into account the safety of the stored date that located in the storage of the devices and gateways. Security functionally consists of following of mechanisms:

- Authentication
- Authorization
- Accounting

Appalling Authentication, Authorization & Accounting in M2M applications guaranties to build trust between the server/user and M2M device.

Due to M2M application's analyzing processes and assimilating large amounts of sensitive sensor data, stringent authentication mechanism gains a notable importance. In order to apply Authentication to the M2M devices CSSP platform implements several security solutions such as, Transport Layer Security

Fig. 7. Real test bed with Ubiquitous board.

(TLS) and Datagram Transport Layer Security (DTLS); there are also other Extensible Authentication Protocol (EAP) methods. Off-the-shelf solution such as TLS is preferable choice if it is required to provide security to M2M applications. However, strict resource tightness of sensor devices makes it hard for TLS and EAP methods to fit ideally in M2M systems.

V. Evaluation of the Platform

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

The test-bed environment is in Fig. 7. Full functionality of the system is shown by two M2M gateway boards. 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.

1. Implementing protocols

Exchanging requests and responses are available by 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 size of the source code is comparatively small. The FreeCoAP source code easily modifiable, and supports Client+Server, DTLS features. Sockets based client-server program is used for implementing other two protocols.

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

The client-server architecture is conducted by the binding with TCP/IP model. 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 data. Herein, packages are delivered to the destination by TCP protocol.

2. CPU usage of protocols

We explain the evaluation of protocols' performance in this section. Firstly, how the measures were set up is explained and obtained results are presented.

The essential metrics including Memory Usage, CPU Usage, and Round trip time delay were installed in the laboratory environment to evaluate the performance of protocols such as CoAP, MQTT, and HTTP. Precise measurements of the certain tests are available in the experiential environment. Due to the difference of receiving and transmitting and path loss or collisions, interactions in a real M2M network are eliminated.

The estimation of the transmission rate among a sensor node and the server/gateway node are doneby the test-bed as of the payload size. While comprising 100 bytes in the every transmission, every

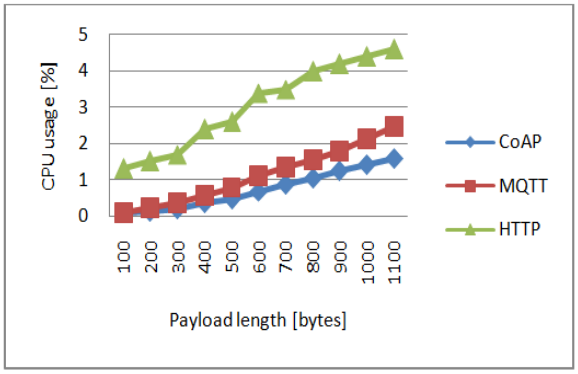


Fig. 8. CPU usage of implemented protocols.

message ranges from 0 to 10,000 bytes.

The result for each payload size is measured 100 times for accurate result. The results obtained by the CPU usage analyzes are in Fig. 8. Through sending 10 sequential messages with an available payload we receive results of the measurement of the CPU usage of a node. Due to the payload's size increase, CPU consumption also grows. For instance: We send 100 bytes and measure CPU usage and will continue sending and measuring 100 times with the same payload. For comparation we take average value of CPU usage. In the second step we will do the same sequence with 200 bytes and in other steps also we increase the payload size by 100 bytes. The dotes in the figure emphasize the average usage of the CPU.

3. Memory usage

Table 1 shows the value of RAM memory usage indicated to assign each protocol. A payload size of 600 bytes is matched by the values of the RAM usage.

Because it designates the memory required for buffering of the packets, most of the RAM memory is used by HTTP.

A way of the complication of each protocol is provided by the ROM memory usage that is a storage containing the compiled code. Improving functionality and more capabilities is possible with the compiled code that utilizes a tiny memory. HTTP uses most of the ROM memory.

C language is the basis of our experiment. The growth of the memory usage and complication for the

Table 1. RAM and ROM memory usage

	CoAP	MQTT	HTTP
RAM	1,288 kB	1,456 kB	3,680 kB
ROM	10,230 kB	13,124 kB	18,755 kB

memory constraint gateways is resulted by the usage of the internal libraries of C language.

Utilizing UDP protocol as a transfer layer protocol, the CoAP implementation succeeds to have the lowest memory consumption and lower intricacy, so that reliability mechanism is not ensured by the protocol. It consequently minimizes the memory utilization and decreases the ROM memory capacity.

3. Round trip time delay

The evaluation of the implementation's performance is conducted by the very important parameter of the round trip time delay on the client while data is detected from a server. The value of round trip time delay should be reduced for intensifying the communication and accomplishing the M2M systems' performance for real-time scenarios. For that reason, time is set for forwarding request to the server; then, as soon as a respond is accepted from the server, the round trip time delay will be calculated.

Every examined protocol's result of round trip time delay is given in Fig. 9. The average round trip time delay of 50 successful transmissions is represented by the dots on the chart. The payload's size spans range from 10 to 1100 bytes; 50 bytes are possible to be supplemented. The context says that right after the server's response is obtained, client is supposed to forward another message.

As of the outcomes, the server's communication with either gateway or sink node can easily be provided by the HTTP protocol. Practically, a barrier is brought by the overhead of the HTTP protocol in M2M area networks. HTTP header size still surpasses 100 bytes, despite the fact that physical world data size can be approximately 100 bytes. Due to MQTT and CoAP protocols' 10-byte header size, overhead level reduction becomes effective.

VI. CONCLUSIONS

The deployment of M2M applications are growing and lead the way to new business cases. It is also creating new requirements to the security solutions. The adaptation of M2M applications into constrained environment requires lightweight mechanisms because of its 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 provides flexible architecture and easy deployment for any kind of M2M devices. CSSP utilizes restful lightweight protocols in order to support communication and proposes lightweight security mechanisms to embed the safety of data on constrained M2M gateways and to prevent eavesdropping. The platform implements the architectures of the standardization organizations hence it is reliable, modular and easy to utilize for any M2M applications. Its pre build API makes applications to interact with external services.

The future work is focused on the adaptation of existing lightweight authentication mechanisms and improving the security features of our platform. Specifically, implementation of OAuth-based Authorization mechanism into our test board is our next work. Furthermore, we planned to implement other lightweight security solutions addressing other components of the proposed platform, in order to provide a comprehensive security approach for constrained M2M environment.

REFERENCES

[1] Chen, Min, et al. “Body area networks: A survey.” Mobile networks and applications 16.2 (2011): 171-193.

[2] M.R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, M. Dohler, ”Standardized Protocol Stack For The Internet Of (Important) Things,” IEEE Commun. Surveys and Tutorials, DOI 10.1109/SURV.2012.111412.00158.

[3] M.R. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, M. Dohler, ”Standardized Protocol Stack For The Internet Of (Important) Things,” IEEE Commun. Surveys and Tutorials, DOI 10.1109/SURV.2012.111412.00158.

[4] G. Wu et al., “M2M: From mobile to embedded internet,” IEEE Commun. Mag., vol. 49, no. 4, pp. 36 - 43, Apr. 2011.

[5] Digi International Inc. (2011) Connectport(R) X2 for Smart Energy. [Online]. Available: http://www.digi.com/products/wireless-routers-gateways/gateways/

[6] IEEE 802.15 WPANTM Task Group 4, http://www.ieee802.org/15/pub/TG4.html

[7] IEEE 802 working group, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs), IEEE Computer Society, Standard specification, [WWW], http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf

[8] A UDP/IP Adaptation of the ZigBee Application Protocol, G. Tolle, October 8 2008, [WWW], http://tools.ietf.org/html/draft-tolle-cap-00

[9] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, “Denial-ofService detection in 6LoWPAN based Internet of Things,” Proceedings of 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 2013, pp. 600- 607.

[10] Y. Zhou, Z. Jia, X. Sun, X. Li, and L. Ju, “Design of embedded secure gateway based on 6LoWPAN,” Proceedings of 2011 IEEE 13th International Conference on Communication Technology (ICCT), 2011, pp. 732-736.

[11] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, “Securing communication in 6LoWPAN with compressed IPsec,” Proceedings of 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011, pp. 1-8

[12] H. R. Hussen, G. A. Tizazu, T. Miao, L. Taekkyeun, C. Youngjun, and K. Ki-Hyung, “SAKES: Secure authentication and key establishment scheme for M2M communication in the IP-based wireless sensor network (6L0WPAN),” Proceedings of 2013 Fifth International Conference on Ubiquitous and Future Networks (ICUFN), 2013, pp. 246-251.

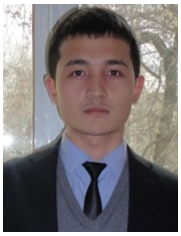
[13] L. Atzori, A. Iera, and G. Morabito, “The

internet of things: A survey," Computer Networks, vol. 54, no. 15, pp. 2787 - 2805, 2010. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1389128610001568

[14] E. Fasolo, M. Rossi, J. Widmer, and M. Zorzi, "In-network aggregation techniques for wireless sensor networks: a survey," Wireless Communications, IEEE, vol. 14, no. 2, pp. 70-87, April 2007.

[15] A. Dimakis, P. Godfrey, Y. Wu, M. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," Information Theory, IEEE Transactions on, vol. 56, no. 9, pp. 4539-4551, Sept 2010.

저 자 소 개



Sardorjon Vakkosov has received his B.S. degree in Information Technologies department at Tashkent University of Information Technologies, Tashkent, Uzbekistan in 2012. He is studying for a master's degree in FIS, Kookmin University. His fields of interest are Machine to Machine (M2M) communications and Internet of things (IoT).

Soo-Hyun Park has received his B.S., M.S. and Ph. D degrees in computer science engineering from Korea University in 1988, 1990 and 1998, respectively. Now, he is a professor in the Department of Information System, Kookmin University, Korea. His current research interests

Jung-Il Namgung has received his B.S. degree in mechanical engineering from Incheon University in 1995, M.S. and Ph. D degrees in Business IT from Kookmin University in 2005, 2011, respectively. Now, he is a BK21+ research professor in the department of Financial Information Security, Kookmin University. His current research interests include IoT (Internet of Things) / M2M (Machine to Machine communication) and Context Awareness / Service Composition / Artificial Intelligence.