A Smart Home Application based on the Internet of Things Management Platform

Mahmoud Elkhodr, Seyed Shahrestani, and Hon Cheung
University of Western Sydney
Sydney- Australia

***Abstract*—The Internet of Things is an emerging research area promising many interesting solutions to various problems encountered in various domains. The ever-expanding networks of sensors, actuators and smart devices on the Internet of Things, will raise interesting challenges for service and network management. This paper explores these challenges and expands on an already proposed management platform for the Internet of Things. The platform offers a management solution for things, specifically constrained things that suffer from limited computation and power resources. Also, this work introduces and demonstrates some of the monitoring and control management capabilities provided by the proposed platform. The results of a smart home experiment conducted to show the advantages of this platform are also reported.**

Keywords—component; Internet of Things; Management; Platform; Smart Home, M2M

I. INTRODUCTION

A primary aim of the Internet of Things (IoT) is to bring connectivity to every physical object. This evolvement in communications, specifically things to things communications, promises to revolute many industries, ranging from supply chains to e-health. Currently, a number of research on the IoT is aimed at facilitating and enabling the anticipated ubiquitous communications between things with minimal human interventions [1]. In the very near future, societies and businesses will shift from being interested in the IoT technologies to becoming more dependent on the IoT. This dependency is rising as time goes by and as more automation becomes increasingly integrated into the IoT services and applications.

In their basic fundamentals, IoT applications enable the sending of information sensed by things or actuating the physical environment of things remotely over the Internet. Combining these basic sensing and actuating services with other services provided by smart things and other IoT applications will ultimately lead to the automation of the various IoT tasks on the Internet. Accordingly, automated services will eventually sustain things-to-things and people-to-things communications, not only within local area networks but also distributed over heterogeneous communication networks.

This rapid revolutionary development of communications pose some serious challenges to the widespread adoption of the IoT [2]. The IoT is a complex interconnected system of sensors, actuators, smart devices, e.g. smart fridge, and software applications that communicate together to perform some tasks or respond to an event. However, the heterogeneity of such communications is challenged by the lack of a shared infrastructure and common standards for the IoT [3]. In addition, until unconventional power sources are developed to recharge things' battery or prolong their life, power consumption remains a restriction and forms a strong limitation that challenges things in the IoT. Consequently, these limitations pose significant challenges to the management of the IoT.

Therefore, the requirements needed to manage things in the IoT need to be addressed. This is necessary to determine the suitable control, monitoring and processing capabilities for managing the IoT. Reliable security and privacy solutions for the management of things and IoT networks need to be considered as well. Thus, current network and service management protocols need to be explored and investigated. Such investigations should help in determining if existing management solutions can be used or adapted for the management of the IoT; or whether a whole new set of management protocols are needed for managing the IoT.

To address these management challenges, the Internet of Things Management platform (IoT-MP) is proposed. Previous work in [4] introduced the architecture and the major components of the proposed platform. This work is a continuation of the previous work. It shows how the IoT-MP is used to support partially some fundamental management functions, including those needed for the proper monitoring and control of things. Also, this work demonstrates the IoT-MP communications capabilities as well.

The remainder of this paper is structured as follow: Section II describes the management challenges facing the IoT. Section III introduces the proposed Internet of Things platform. Some control and management operations provided by the proposed platform are described in this Section as well. Section IV introduces a Smart Home experiment implemented based on the proposed platform. The results collected from these experimental works are also reported in this section. Conclusions remarks and future works are given in Section V.

978-1-5090-0214-6/15 $31.00 © 2015 IEEE
DOI 10.1109/DSDIS.2015.23

II. MANAGEMENT CHALLENGES

With the evolvement of the IoT, comes the need for management. Traditionally, network management is needed to manage network equipment, devices, and services. However, with the IoT, there is a need to manage not only these traditional devices but also a completely new range of things that simply has the communication capability. Therefore, management solutions are needed because a large number of various things connected to the Internet will communicate with each other, generating a large amount of traffic [5]. With billions of tiny things equipped with sensors and actuators entering the digital word, powering devices like lights, electric appliances, home automation systems and a vast number of other integrated machinery devices, transport vehicles, and equipment; management of things becomes vital.

A. Maintenance and Control Challenges

For the successful deployment of the IoT, obvious management functionalities such as remote control, monitoring and maintenance are needed [6]. These management functionalities enable managers to perform many maintenance tasks remotely over the Internet. Also, they help in reducing errors and accelerating response time. The ability to turn things on and off, disconnecting things from specific networks, and monitoring the statuses of things are amongst the essential tasks that a management system should support. On the other hand, having a management system deployed in an IoT network helps in eliminating travel's and staff training's costs. Also, it helps in accelerating the response to failure events. For example, a management system that supports the remote monitoring, via the Internet, of sensors and smart objects deployed in remote locations such as in healthcare [7] or a busy city is highly beneficial. Such system allows managers to control remotely, diagnose errors, and troubleshoot things in real time, reducing costs and accelerating many maintenance tasks [8].

B. Performance Challenges

Monitoring the performance of things and the IoT network is among the requirements needed for the management of the IoT [9]. Nevertheless, performance becomes extremely significant in IoT applications that deploy things in remote locations where accessibility is an issue. Performance is also considered important in emergency applications where failures can be catastrophic [10]. Thus, management solutions should provide the capabilities needed to monitor the performance of things and the IoT network as well. This includes the functionalities that allow the early detections of errors, diagnosis of problems, and resolution of network issues before the occurrence of failures. Performance statistics related to response time, availability, up and down time, and others are also considered highly advantageous.

Other performance requirements relate to the things' hardware. This is because, providing insights into the health of things and their networks is an important performance activity. For instance, monitoring, reporting and alerting the change in things' state (e.g. the status of an actuator whether it is on or off), the ambience's temperature, hardware's temperature, battery's levels, among others, are important for the performance management of the IoT.

C. Security and Privacy Challenges

There are obvious security concerns in the IoT such as authorization, authentication and access control which need to be addressed [11]. For instance, data control is one of the most significant barriers to the adoption of many IoT applications. While, it is important to solve the problem associated with data ownership, it can be left to regulatory and policy makers. However, it is significant to provide ways to control access to things' data which allow users to decide to whom, when and to which extent, their private information are revealed.

The fully-connected IoT smart home, for example, offers many benefits to users. Controlling accesses to doors, lighting, and appliances are a desirable technology for households. However, there is a tradeoff between the control privileges versus the management counterparts. This includes issues such as ongoing maintenance, interaction control and, significantly, security. Given that things are mostly accessible via unsecured networks such as the Internet, security plays a central role in the appropriate management of the IoT. Therefore, controlling accesses to data such as the date, time, location, and who has access to things and the data they produce, are examples of the security, and even privacy, requirements needed in the IoT.

In regards to privacy, things have their users and owners. Thus the information they collect and know about a user's environment, or/and the user, in general, are always at a risk of exposure. Therefore, traditional privacy risks associated with the used of sensitive or private data such as payment information, social security numbers, energy consumptions and others need to be considered in the IoT. A second exposure relates to the fact that the more the IoT systems become interconnected, the greater these systems are at risk of disclosing private information, such as location information, to unauthorized entities [12].

Interestingly, in the IoT, security and privacy impact on the personal safety of users as well. The unauthorized accesses to private information, remote controls and modifications of things, and their statuses could harm the physical safety of users. For example, securing the IoT vehicular networks is important for the personal safety of drivers. In [13], some security and privacy threats in the IoT are reported.

III. THE INTERNET OF THINGS MANAGEMENT PLATFORM

The Proposed platform is based on a distributed architecture adapted from the Simple Network Management Protocol (SNMP) architecture. It utilizes agents and managers to provide the

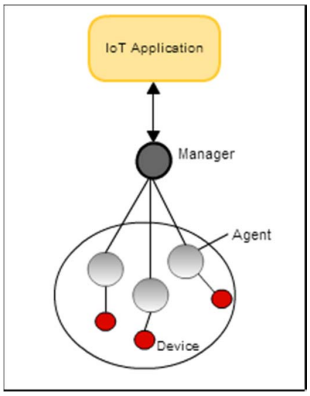

Figure 1- IoT's two-tier Architecture

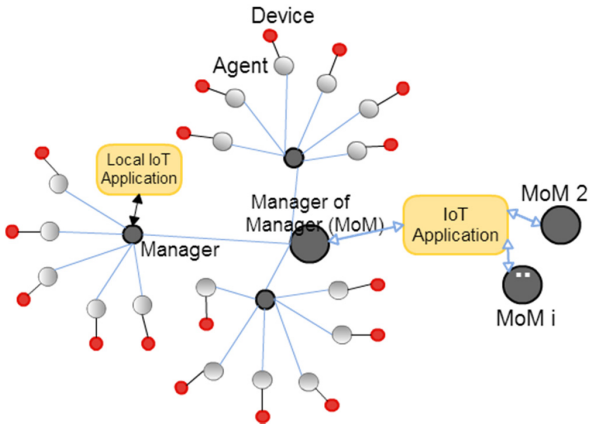

Figure 2- Hierarchal Architecture

Management functionalities needed for monitoring, controlling and managing location privacy of things. The IoT-MP is a simple two-tier model, as shown in Fig 1, consisting of an agent which could be residing on the managed thing, or in its local area network. And a manager that resides somewhere on the communication network. Multiple agents can interact with a manager, and multiples managers can interact with an agent. Managers can interact with other managers as well. A manager can act as an agent for other managers, and a manager can act as a manager of managers.

Figure 2 shows how managers communicate via a Manager of Manager (MoM). In this case, the manager acts as an agent to the MoM. Therefore, the IoT-MP model architecture varies from a simple two-tier model to a sophisticated hierarchal structure of multiple agents, managers and MoMs. The IoT-MP uses an extensible design where things are defined using attributes on the management database located at the manager.

These attributes carry the management information of things supplied by agents. In addition to providing management information, agents perform the operational role of processing requests received from managers, and sending responses to these requests. Agents send notification alerts to managers when an event occurs as well. Consequently, this management information, which are supplied by agents and stored in the management database in the form of attributes, are used by management applications to manage, monitor and control things. Things' information, such as sensory data are exchanged between the agents and managers using a defined messaging scheme. The manager uses messages to request management information from the agent. Each message sent to the agent, and the manager makes reference to a particular managed thing. An agent can supervise only one thing at a time.

This approach provides the manager, using a management application, with the capabilities of monitoring and controlling things using agents. Some of the current supported messages by the IoT-MP are *GetUpdate()*, *GetLocation()* and *GetStatus()*.

These messages are sent by managers to agents. The IoT-MP agent responds with a *Response ()* message. Agents can also be configured to send alert messages to managers. For example, if a specific event or condition occurs, such as a failure in the network, agents send an alert message to the manager. Table I shows the descriptions of some of the messages exchanged between the manager and agent.

Two important messages designed specifically to work with things that have sensing and actuation capabilities are the *GetUpdate()* and *Actuate()* messages. The message format of these messages is described in [4].

TABLE I MESSAGES EXCHANGED AND THEIR FORMATS

Message	Description
Message Get()	This message is initiated by the manager in order to retrieve some information from an agent. For example, GetSatus () will retrieve the status of the managed thing.
Message Set()	This message is initiated by the manager to perform an operational change on things. For example, the management application could change the status of an actuator from on to off.
Message Alert()	This message is initiated by an agent and sent to the manager as an alarm. For example, an agent could send a message to the manager advising that one of the managed thing's status has changed (an appliance is turned off, an actuator status has changed from off to on etc…).

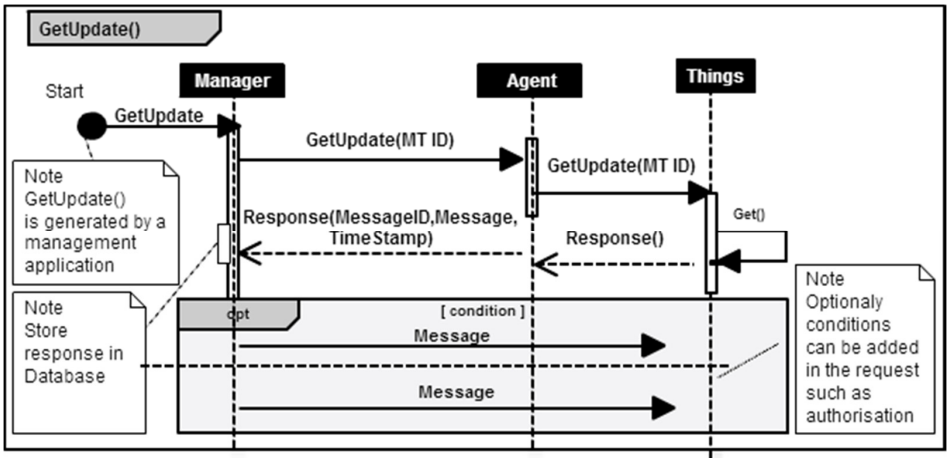

Figure 3- Sequence Diagram

A manager initiates the GetUpate() message and send it to an agent requesting an update on the data sensed by a sensor. While *Actuate ()* is a message sent from the manager to an agent initiating an actuation mechanism on an actuator. An actuator is a device with an actuation capability. The sequence diagram of the message *GetUpdate()* is given in Fig. 3.

IV. The Experimental Works

This section describes the experimental works and analyzes the collected results. To evaluate and validate the proposed platform, an experiment is developed. The experiment aims to demonstrate the management capabilities of the proposed IoT-MP in an IoT setup. The experiment involves several software and hardware implementations.

A. IoT Scenario

In order to implement the IoT-MP, an IoT scenario was first setup. Fig 4 shows the Smart Home demo. In this demo, Bluetooth low energy enabled sensors developed by Texas Instrument were used [14]. The sensors have the following sensors: temperature, humidity, pressure, accelerometer, gyroscope and magnetometer. The sensors use Bluetooth Smart, also known as Bluetooth 4.0, as a medium of communication. According to the manufacturer, the onboard battery attached to these sensors should last up to one year in operation.

To create a Smart Home system, we attached the sensors to a number of household appliances. The sensors are configured to send the collected information to the user using a mobile application. For example, the sensor attached to the Microwave collects the following information: the ambiance temperature, the object temperature (the microwave in this example) and pressure information.

In addition to temperature information, the sensor attached to the lamp provides accelerometer and magnetometer sensors' readings as well. These additional readings can be used to extract location information. They help in determining whether the location of the lamp has changed or if the lamp is mobile.

The user can view this information using a mobile application developed and supplied by Texas Instrument. The mobile application displays in real-time the data collected by the sensors.

B. Implementing the IoT-MP

The mobile application, developed by Texas Instrument, provided a way to view the data collected from the sensors over Bluetooth. However, the setup remains in the form of a local area network. Therefore, further developments which involved several software and hardware implementation took place in order to bring this Bluetooth communication model to the Internet. The purpose behind these implementations is to create a more reasonable IoT environment. Ultimately, this will provide the work with a more realistic IoT scenario for the proper application of the proposed IoT-MP. Thus, enabling to evaluate and validate efficiently the management capabilities of the IoT-MP.

Consequently, the components of the IoT-MP were implemented as part of this IoT experiment. Figure 5 shows how the experiment used the IoT-MP's agent-manager architecture in order to make the information available on the Internet. The agents are software applications that could even run on mobiles, tablets or computers. This software has Bluetooth functionalities implemented allowing them to establish a communication with Things. On the other hand, the manager is implemented as part of a server application that resides on the Internet. The implementations of the manager include a web service (API). This API is implemented specifically for the purpose of establishing a communication between the manager and the agents. Communications between agents and managers are secure and encrypted using the SSL3.0 protocol. The Bluetooth communication between things and the mobile device are encrypted using 128 bit AES.

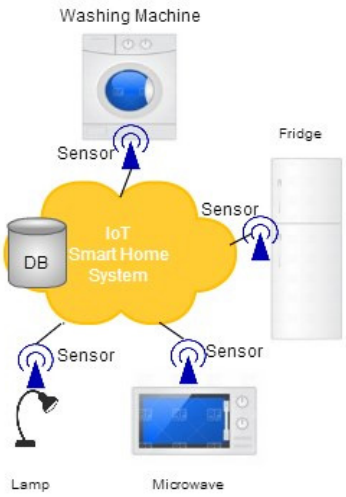

Figure 4- The IoT Demo Scenario

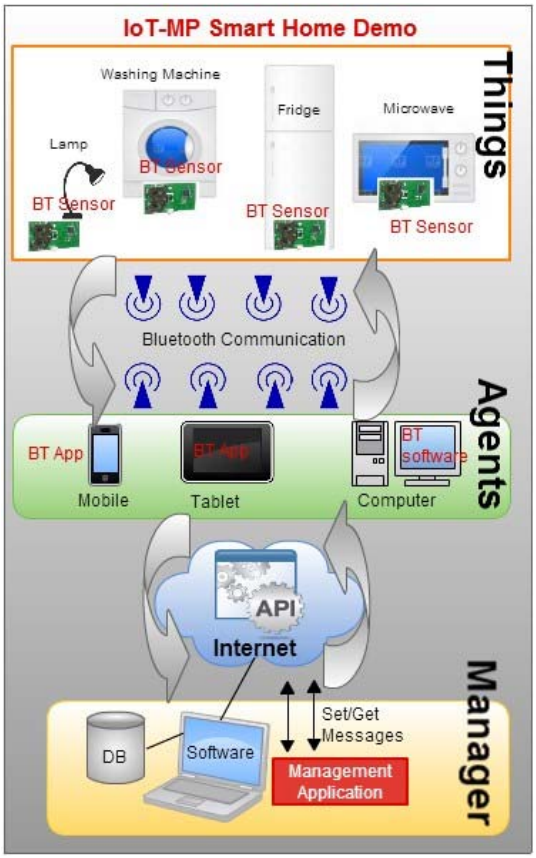

Figure 5- Smart home application based on the IoT-MP

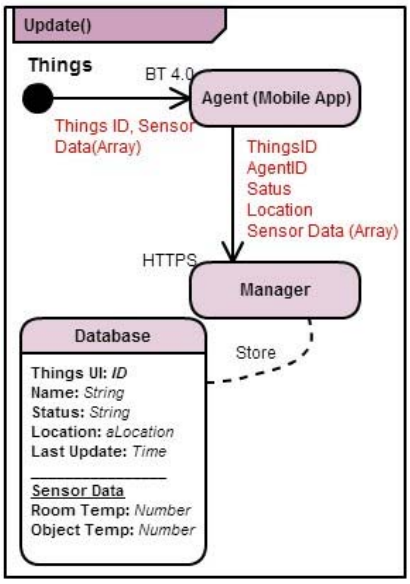

Figure 6- Update () Message Flowchart

The manager relies on the IoT-MP messaging scheme described in Section III, for all aspects of communications with agents.

To this end, the IoT-based Smart Home system is implemented and put into operation. Fig. 6 shows a periodic message called *Update ()* which makes the sensors' data available on the Internet using the IoT-MP. Also, Fig 6 shows some management information (last received update, location, status) provided by an agent to a manager.

This information is used by management applications in order to perform management functions on things. Consequently, the IoT-MP's functions allow the user, using the management application, to initiate management activities on things remotely over the Internet. For instance, the message *GetStatus()* shown in Fig.7, is used to retrieve the latest status of a thing e.g. the lamp. The response for this message include information on the current state of the sensor (on, off), the Bluetooth connection status (connected/disconnected), location of the lamp, and how long the lamp has been running. Therefore, these management messages provide important monitoring and control capabilities necessary for the proper management of things in the IoT.

The experiment conducted in this work offers an example on how the IoT-MP can be used to support management over services such as control and monitoring of things, remotely over the Internet. Also, the experiment demonstrates the IoT-MP's communications capabilities. It shows that the IoT-MP incorporates a systematic model of communications which allow

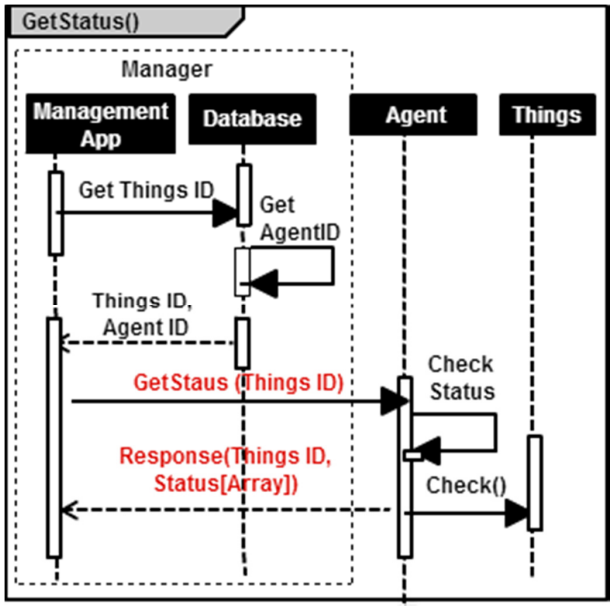

Figure 7- GetStatus () Sequence Diagram

the receipt of things' data and the requesting of these data, remotely over the Internet. It also shows how things with low resources, such as sensors, can rely on agents to supply management information, e.g. location information. Further developments on the Smart Home experiment are currently planned. Future works will implement additional management capabilities, specifically, those needed for managing the security and privacy of things on the IoT.

V. Conclusions

The Internet of Things technology offers a new communication approach that enables connecting a large number of sensors, actuators, and smart objects together. Nonetheless, the diversity of things that can be part of such an infrastructure can pose serious problems from a management point of view. This paper explored such problems and proposed a management platform, referred to as the IoT-MP. The IoT-MP partially addresses some of these management problems. The platform offers some fundamental management functions, including those needed for proper monitoring, control, and communications. Also, in this study, an IoT Smart Home system has been deployed using the IoT-MP. The use of IoT-MP has enabled point to point communication and made sensors' data available on the Internet. Furthermore, the IoT-MP provided the necessary management functions needed to control and manage things in this Smart Home setup. The results collected from the experiment demonstrated the successful deployment of the IoT-MP and validated its management capabilities. Our future works will expand the IoT-MP by incorporating our previous results on Location Privacy Management Model in the management platform

References

[1] A. Zanella, N. Bui, A. P. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things Journal,* vol. 1, pp. 22-32, 2014.

[2] R. H. Weber, "Internet of Things–New security and privacy challenges," *Computer Law & Security Review,* vol. 26, pp. 23-30, 2010.

[3] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks,* vol. 54, pp. 2787-2805, 2010.

[4] Mahmoud Elkhodr, Seyed Shahrestani, and H. Cheung, "Managing the Internet of Things," presented at the The 8th International Conference on the Internet of Things (iThings 2015), Sydney, Australia, 2015.

[5] J. Cooper and A. James, "Challenges for database management in the internet of things," *IETE Technical Review,* vol. 26, pp. 320-329, 2009.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems,* vol. 29, pp. 1645-1660, 2013.

[7] C. Doukas and I. Maglogiannis, "Bringing IoT and cloud computing towards pervasive healthcare," presented at the Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), Palermo, Italy, 2012.

[8] L. Yang, S. Yang, and L. Plotnick, "How the internet of things technology enhances emergency response operations," *Technological Forecasting and Social Change,* vol. 80, pp. 1854-1867, 2013.

[9] O. Vermesan and P. Friess, *Internet of things: converging technologies for smart environments and integrated ecosystems*: River Publishers, 2013.

[10] J. Zaldivar, C. T. Calafate, J. C. Cano, and P. Manzoni, "Providing accident detection in vehicular networks through OBD-II devices and Android-based smartphones," presented at the IEEE 36th Conference on Local Computer Networks (LCN), Bonn, Germany, 2011.

[11] M. Elkhodr, S. Shahrestani, and H. Cheung, "A Semantic Obfuscation Technique for the Internet of Things," presented at the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 2014.

[12] M. Elkhodr, S. Shahrestani, and H. Cheung, "A contextual-adaptive Location Disclosure Agent for general devices in the Internet of Things," presented at the 2013 IEEE 38th Conference on Local Computer Networks, Sydney, Australia, 2013.

[13] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks,* vol. 57, pp. 2266-2279, 2013.

[14] T. Instruments, "Texas Instruments CC2540/41 Bluetooth® Low Energy Software Developer's Guide v1. 4.0," *SWRU271F Version,* vol. 1, 2013.