This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

Recent Advances in Industrial Wireless Sensor Networks Towards Efficient Management in IoT

Zhengguo Sheng, *Member, IEEE,* Chinmaya Mahapatra, *Student Member, IEEE,* Chunsheng Zhu, *Student Member, IEEE,* and Victor C. M. Leung, *Fellow, IEEE*

***Abstract*—With the accelerated development of Internet-of-Things (IoT), wireless sensor networks (WSN) are gaining importance in the continued advancement of information and communication technologies, and have been connected and integrated with Internet in vast industrial applications. However, given the fact that most wireless sensor devices are resource constrained and operate on batteries, the communication overhead and power consumption are therefore important issues for wireless sensor networks design. In order to efficiently manage these wireless sensor devices in a unified manner, the industrial authorities should be able to provide a network infrastructure supporting various WSN applications and services that facilitate the management of sensor-equipped real-world entities. This paper presents an overview of industrial ecosystem, technical architecture, industrial device management standards and our latest research activity in developing a WSN management system. The key approach to enable efficient and reliable management of WSN within such an infrastructure is a cross layer design of lightweight and cloud-based RESTful web service.**

***Index Terms*—Internet-of-Things, device management, IEEE 802.15.4, RESTful, error correction coding (ECC), cloud.**

I. Introduction

With the development of IoT technologies, a wide range of intelligent and tiny wireless sensing devices will be deployed in a variety of application environments. Generally, these sensing devices are constrained by limitations in energy resources (battery power), processing and storage capability, radio communication range and reliability, etc., and yet their deployment must satisfy the real-time nature of applications under little or no direct human interactions. In order to well maintain these sensor devices, for example, monitoring the performance or sending commands to a sensor node, it is essential to design reliable and efficient communication protocol to remotely manage sensor devices without consuming significant resources.

According to the definition in [1], the term of management generally consists of configuration, monitoring and administration of managed entities, including network elements, system resources, applications and services. Hence it can be hierarchically divided into three major domains: 1) Network management where the elements making the network connected are managed, such as routers and servers, etc. 2) System management where system elements (usually networked) are managed, such as operating system and information system, and 3) Application management where applications built on system are managed, such as web applications and J2EE applications. In most cases, there are no clear boundaries between these domains and even in some scenarios they can be exchangeable. Different from the above management domains, we consider the sensor device management that is an integration of network, system and application managements. In essence, it includes provisioning and management, configuration of network parameters, firmware upgrades and performance monitoring, etc.

Traditional device management solutions used to target devices such as computer, mobile phone, set-top box and gateway, etc. In order to address the interoperability of connected devices, a number of industry standards have been developed and recognized by international communities, for example OMA Device Management (OMA DM) [2] for management of small mobile devices and TR-069 [3] of Broadband Forum for automatic configuration of internet access devices such as gateways and set-top box, etc. However, these solutions are not optimized for WSN-based IoT applications, because of missing features that should be considered for sensor device management, such as limited resources of devices, distributed network environment and real time nature of applications, etc.

In order to cope with new challenges for designing IoT[1] device management, there are some key characteristics that should be taken into account, such as limited resources of wireless sensor devices, distributed network environment and massive data collected from a variety of applications, etc. Particularly, there is a considerable need to understand the new requirements imposed by IoT, and its inter-dependence with networking protocols and functions. To be specific, it is of fundamental importance to understand: (1) what is the current status of industrial IoT development, (2) what are the technical architecture and key elements of IoT to perform device management and (3) how to utilize efficient communication protocols and the emerging cloud computing infrastructure to assist IoT device management in future massive WSN deployment, which are the major motivations of this paper.

The following summarizes our key contributions:

- We give an overview of IoT ecosystem covering the recent industry development in the context of main areas

Z. Sheng is with School of Engineering and Informatics, University of Sussex, UK. (E-mail: z.sheng@sussex.ac.uk)

C. Mahapatra, C. Zhu and V. Leung are with the Department of Electrical and Computer Engineering, University of British Columbia, Canada. (E-mail: {chinmaya, cszhu, vleung}@ece.ubc.ca)

[1]In this paper, we focus on WSN based IoT (or M2M) applications and techniques. In order to simplify the presentation and align with industry terminology, we use IoT to represent a system level description of WSN, and should be treated in equal means throughout the paper.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

of application, challenges and key players. By identifying the key characteristics of IoT development, we summarize the major areas of applications into smart city, smart home and smart transportation.
- We focus on the main verticals of IoT ecosystem by describing the IoT architecture into three main layers, namely sensor device, data connectivity, cloud management platform. For each of these layers, we provide a survey of technical solutions and identify the importance of device management from a system level.
- We identify the importance of IoT management and its positions in the IoT architecture, outline new research trend towards efficient management, and propose a framework of cloud based management system for WSN. Specifically, we take a cross layer approach to extend the Representation State Transfer (REST) paradigm, in which a reliable and efficient management protocol can be embedded in resource constrained sensor devices, and connect WSN to the IoT cloud management platform using CoAP methods.

The remainder of this paper is organized as follows. We provide an overview of IoT ecosystem in Section II, and introduce the IoT architecture and its key technologies in Section III. The management protocol standards, new research direction and our proposed cross layer design are reviewed and discussed in Section IV. The IoT cloud management platform features, out-of-shelf solutions, and our contributions are introduced in V. A prototype IoT management system is built and evaluated in Section VI, and future work and conclusion are then given in Section VII and VIII.

II. Overview of IoT Ecosystem

In this section, we provide an overview of global industrial IoT ecosystem, including the main characteristics, key application scenarios to technical visions, and players.

A. Major Characteristics

The development of industrial IoT has following major characteristics:

1) Ecosystem formed by industrial alliances: Industrial associations are early founded and often funded by the government authority and academy for the purpose of enhancing the development and cooperation, and providing services to government and more importantly its industrial ally. Currently, major driving forces behind the IoT industry alliances include manufacturers, vendors, service providers, telecom operators and government, etc.

With the development of WSN technologies in the past few years, a number of major standardization alliances are gradually formed based on their interests in technology selections and commercial markets. Technically speaking, current WSN solutions can be categorized as non-IP based and IP based solutions. Most of off-the-shelf solutions belong to the former, especially for some well-known standard alliances, such as ZigBee [4] and WAVE2M [5] for office and manufacturing automation, and WirelessHart [6] and PROFIBUS [7] for real-time industrial control systems, etc. However, most of these non-IP solutions are isolated within their own verticals, which hinders the IoT development due to the incompatible nature across heterogeneous communication systems.

For the IP based solutions, IETF[2] takes the lead to standardize communication protocols for resource constrained devices and develop a number of Internet protocols, including IPv6 over Low power wireless personal area networks (6LoWPAN) [8], Routing Protocol for Low Power and Lossy Network (RPL) [9] and Constrained Application Protocol (CoAP) [10], etc, to tackle the technical challenges, such as extensive protocol overheads against memory and computational limitations of sensor devices [11]. Meanwhile, IP Smart Object Alliance (IPSO) [12] actively promotes IPv6 embedded devices for Machine-to-Machine (M2M) applications. PROFINET, a promising real-time Ethernet standard, also adapts Ethernet to the next generation of industrial automation [13]. Today, many non-IP based technical alliances are evolving toward a protocol translation gateway model to better cope the interoperability with the dominated IP networks, e.g., ZigBee IP.

Although a number of intelligent and tiny devices have been deployed in a variety of application verticals, they all require similar functions (e.g., device management, discovery, registration) and share common infrastructure and network elements. This provides a motivation to recent global IoT/M2M related standardisations from applications' perspective.

In particular, the European Telecommunication Standards Institute (ETSI) Technical Committee (TC M2M) [14] is to standardize the application layer which is independent of the underlying communication networks. The goal of ETSI TC M2M includes the specifications of service requirements, functional architecture, interfaces and use cases. The oneM2M Global Initiative [15] has been formed in order to develop one globally agreed specifications for common service layer, which can be the basis of horizontal IoT platforms. The IoT-Architecture project [16], which is an European research project addressing the Reference model of IoT, is to develop IoT architectures in an interoperable manner. The project has derived entities and resources, which are subject for management functions, and provides various functions to orchestrate and manage collaboration of IoT devices.

2) Government plays an important role in IoT deployment: Although the industry is accelerating the pace of IoT development, we should admit that there are still significant obstacles for its growth, such as fragmented solutions, and interoperability across vertical applications, etc. Moreover, existing IoT solutions are not fully accepted by customers due to security and privacy concerns which are caused by the fact that the IoT development is on its early stage in which

[2]The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors and researchers concerned with the developments and promotions of Internet standards of the Internet protocol suite (TCP/IP).

[3]The nominative use of a logo is recognized only for purposes of description and identification of the product or service of the company it represents.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

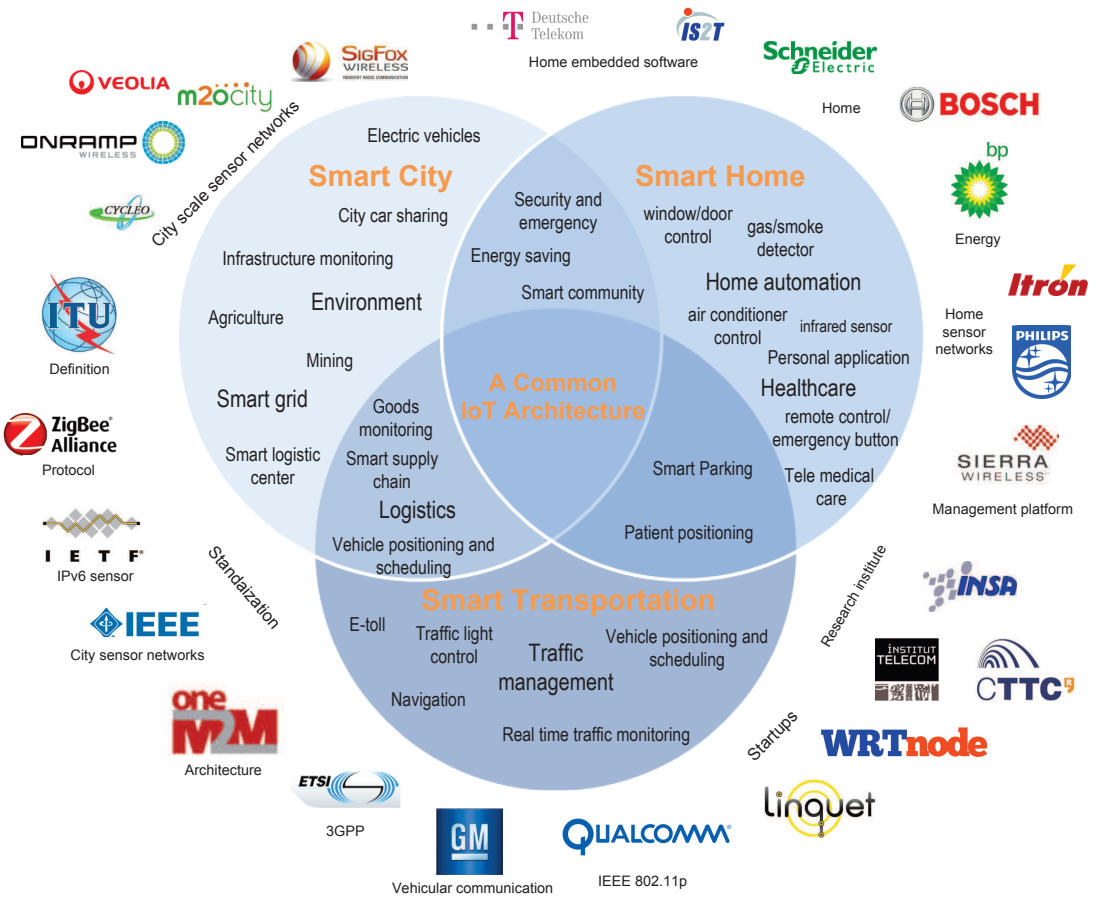


Fig. 1. Industrial IoT ecosystem, including major applications and players.[3]

standardizations of IoT architecture, model and application are still under way. Today, governments or regulation authorities are aware of the challenges in the IoT ecosystem that cannot be addressed by the industry alone, and have started to play an important role in IoT market development by investing IoT applications and introducing incentive programs to improve public security and welfare. For example, since 2009, the US regulation authority has issued an action plan for standards governing the development of a smart grid, which stimulates regional potential for research and innovation [17]. In Europe, intensive standardization and regulatory efforts are made to deploy a universal eCall service as a mandatory vehicle fitment by 2016 [18]. In China, the government has also designated a great importance to the development of IoT and strategically fostered it in China's 12th five-year plan [19].

3) Limited market drive, few significant applications: Although the industry is optimistic about the future IoT development, e.g., Cisco forecasts of 50 Billion Internet-Connected Things by 2020, and also governments are vigorously advancing many demonstration projects, e.g., European "20-20-20" [20] target to achieve 20% reduction in emissions, 20% renewable energies, and 20% improvement in energy efficiency, the current progress remain under proof-of-concept and there is a lack of spontaneous needs from industries and customers. According to one latest consulting report [21], nearly three-fourths of enterprises express interest in adopting IoT solutions to reduce expenditures and increase efficiency. However, only 13% of IoT use cases between 2009 and 2013 targeted revenue growth or innovation.

This is suggested that we are still early in the adoption of the IoT and a mature market is not yet formed. Current implementations mainly focus on solution optimization without highly developed intelligent system. Pilot projects tend to be presented as proof of concept in limited areas without a large scale commercialization. Given the lack of successful references, IoT is not ready to bring substantial business for large scale operations in a short term.

B. Main areas of application

According to IDC report [22], the global market for IoT (or M2M) shows a huge long term potential with over 100 billions things could be turned into machines by 2020. For example, in Europe, the market value will reach to 11 billion Euro by 2015 for IoT related projects, including sensor devices, integration, application development and service management, etc. Another example in China shows that IoT applications are rapidly developed and widely deployed in a number of areas, ranging from personal devices to industrial automations. According to the information from the 2nd IoT EXPO China, the market size in 2011 is 30 billion Euro. This number is

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

TABLE I
KEY IOT AREAS, APPLICATION REQUIREMENT AND CHALLENGES.

Key development areas	Application requirement	Challenges
Smart grid	– Sensor monitoring of power generation, – Warning of power transmission, – Management of power supply automation, – Metering of power usage.	Lack of core technologies, including reliable communications, MANET, gateway, middleware, electromagnetic compatibility and security.
Smart transportation	Development of RFID technology on intelligent transport system (ITS).	Information island on transportation managements from different administration departments; Low level of system integration.
Intelligent logistics	Development of RFID, GPS, GIS, smart container and smart tracking etc.	Less developed value chain and standards are the bottleneck; Information based application needs to be further promoted in greater scope and depth.
Smart home	– Industry consolidation, – Development in multi-access, energy saving and cross application integration, etc.	In short of standard, core component, industry collaboration, security, privacy protection, support of policy and funding.
Environment protection	– Environment monitoring includes population, atmospheric sciences, geographic research, – Monitoring of flood and fire.	Limited number of monitoring stations and lack of well developed management platforms; Less developed on manufacturing of high precision sensor chips; No unified industry standard.
Industrial automation	– Intelligent of industry raw material and product supply chain, – Manufacture management and safety, – Energy saving and low carbon economy.	Limited scope and depth of industry application; Lack of technology breakthroughs and industry standards.
Intelligent health care	– Telemedicine, visualization of remote treatment, – Information sharing and management of patient treatment, drug and medical stuff, – Computerized physician order entry (CPOE).	No clear industry planning; High cost and lack of secure and privacy; Limited manufacture ability on medical and biomedical sensors, large scale data mining.
Agriculture	– Real-time access and information sharing of agricultural resources, – Intelligent management of products circulation and safety.	Lack of low cost sensing technology and devices; Lack of communication infrastructures in countryside.
Financial services	Development of mature technology and safer security.	Lack of technology standard, secured and effective identification mechanism; Problem of user privacy loss.
Public security	Need fully support and financial investment from government.	Lack of public security standard; Uncoordinated development of value chain and lack of intellectual property rights.

expected to be increased by 30% per year and reaching to 90 billion Euro in 2015. Hence it is impossible to envisage all potential IoT applications having in mind. In Fig. 1, we present some of the major applications on the market, and categorize them into smart city, smart home and smart transportation.

1) Smart city: Technically speaking, smart city is very much like a conceptualized blueprint, rather than actual services that have been implemented and put in use in people's everyday life. However, the development of the concept is booming while the urban population has expanded rapidly in recent years. By 2025, with more than 60% of the world population expected to live in urban cities. By 2023, there will be 30 mega cities globally, with 55% in developing countries, such as China, India, Russia and Latin America [23].

Because the rapid growth of population naturally demands the innovation or development of a better way to provide public services to its citizens, cities and their services represent an almost ideal platform for IoT research, taking into account city requirements and transferring them to solutions enabled by IoT technology. In the following, we provide some examples of the recent development in some regions and countries.

1) Europe definitely has the strong willing to develop smart cities, since cities tend to be denser, have better public transit, a stronger focus on sustainability and low-carbon solutions, and perhaps most important, a culture and citizenry more engaged in the journey towards more sustainable and smarter cities. There are many successful examples and projects are going on. European commission plays a leading role in the smart cities development, such as FP7 Smart Santander project [24] which aims at deploying an IoT infrastructure with thousands of sensor devices across several cities, and the recent call from Horizon 2020 on Low Power Computing, Internet of Things and platforms for smart objects. Also, major European telecom operators, energy companies, car manufactures and financial institutes have been involving in different level of collaborations to delivery smart cities services.
2) According to 2011 China's urban development report, there are almost 660 million people living in cities,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

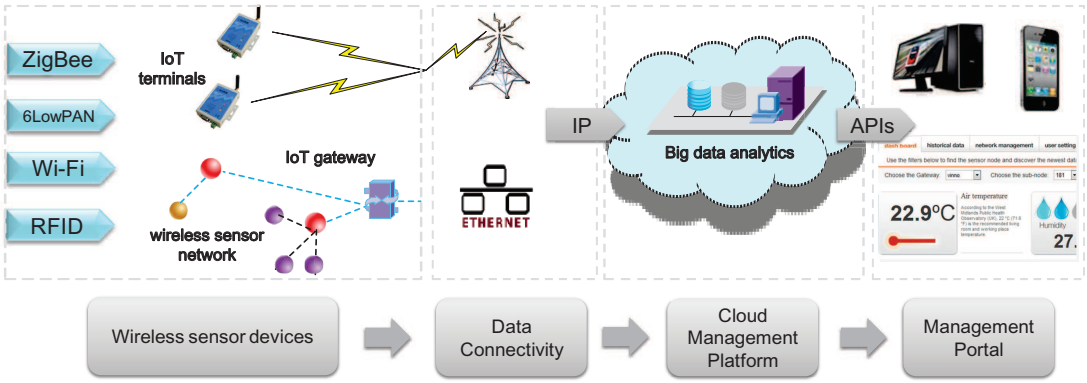


Fig. 2. End-to-end IoT architecture

which counts for 49.68% of Chinese population. This ratio will be increased to 51% by the end of 2015. Moreover, more than 220 Chinese cities will have a population of over one million people (there are currently only 35 in Europe). Many cities have announced their smart city plans to provide public services, e.g., grid management system, building management, water monitoring, security video surveillance, smart traffic (information, parking management and e-toll) and telematics, including two of the biggest cities like Beijing and Shanghai, and a number of medium-size cities, like Wuxi, Ningbo, Chengdu, Wuhan, Kunming, Fujian, Shenzhen and Guangzhou.

3) The smart city concept is less commonly used in North America than in Europe and Asia, but North American cities are looking to technology to improve the quality of public services and boost local economies. U.S and Canadian cities are also matching their counterparts around the world in setting ambitious sustainability targets. Major innovation activities include building smart grid and water infrastructures, adopting new business model to improve the efficiency of city transportation, promoting electric vehicle and charging facilities, and sharing public sector data for open innovations.

2) Smart Home: The concept of smart home has existed for over 10 years. Although the related technologies are well mature, there are still barriers to populate a large scale adoption, such as expensive unit price, exaggerated advertising, fancy ideas but not practical, and lack of industry standards. The existing applications can be categorized into following areas:

1) Home security and monitoring: The applications include window/door control, gas/smoke detector, infrared sensor, remote control/emergency button and air conditioner control. It also provides alternative method to take care of children and elderly.
2) Community security: These applications include property management, community monitoring, electric patrol, security intercom and entrance guard.
3) Multi-service home gateway: The applications include broadband service, home multimedia system, IPTV and remote health monitoring.
4) Home devices connectivity and control: including intelligent home appliances, such as smart bulb, high-end wash machine and refrigerator, which are already available on the market.
5) Energy and water use: The application includes monitoring energy and water supply consumption to obtain advice on saving cost and resources.

3) Smart Transportation: The development of smart transportation is generally led by governments or transportation authorities. Successful examples include real time traffic and public transportation information sharing, intelligent traffic control systems, incentive program to regulate transportation, largely promotion of electric vehicle and charging facilities, and dedicated short-range communication (DSRC) enabled vehicular communication system, etc. Typical application scenarios are presented as follows [25].

1) Navigation and safety: Utilizing the vehicles (e.g., cars, buses, trains) along with the roads and the rails equipped with sensors, actuators and processing power, important traffic information could be offered to the drivers or passengers of the vehicles to achieve better navigation and safety. Main functions include collision avoidance systems and monitoring of transportation of hazardous materials.
2) Road planning and route optimization: Benefiting from the more accurate traffic information about road patterns, governmental authorities could better plan and design the roads. Particularly, intelligent roads can be performed, with warning messages based on climate conditions and unexpected events (e.g., accidents or traffic jams). In addition, enterprises (e.g., freight companies) could perform route optimization for energy savings.
3) Guided delivery: Regarding the vehicles transporting goods, integrating the information about the vehicle movement and the information about the type and status of the goods, guidance about the delivery time, the delivery delays and faults could be obtained. With the status of the warehouses, automatic refilling of the magazines could be achieved further.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

To provide a better vision of IoT applications, we highlight in Table I some key IoT development areas, including application requirements and challenges.

III. IoT ARCHITECTURE

It is clear from Fig. 1 that although a wide range of intelligent and tiny sensing devices have been massively deployed in a variety of application verticals, they all share a common architecture and network elements. Generally, the IoT characteristics with their challenges can be summarized as follows:

1) No direct human interaction: It is necessary to ensure a reliable communication via remote device and communication managements.
2) Fragmented IoT services with distinct service requirements and customers needs: It is necessary to unify the service capabilities on a single horizontal platform and open platform application programming interfaces (APIs) to satisfy customization.
3) Massive connections into a IoT network: It is necessary to address problems of insufficient address resources and access congestion, etc.
4) Heterogeneous networks access: It is necessary to address the naming and addressing of heterogeneous access to guarantee QoS requirements.
5) Sensing device management and control: As fundamental issues to enable IoT services, it is necessary to provide reliable and efficient mechanisms to remotely monitor and control sensor devices.
6) Massive information processing: It is necessary to address massive information storing, sharing and mining.

Looking into IoT architectures proposed and discussed in various organizations, we come up with a IoT architecture as shown in Fig. 2:

A. Sensor device

It lays a foundation of the IoT architecture. IoT uses various wireless sensor devices to capture events or monitor status of different things, such as temperature or inventory level, which are relayed through gateways to upper layers via wireless, wired, or hybrid networks. Table II shows a list of short range radio technologies that are currently being used in IoT applications.

B. Data connectivity

It actually behaves as a gateway to translate the captured event from the sensor devices into a standard format and deliver it through broadband or wireless networks to the cloud platform. According to the technologies used in realizing the communication between the sensing networks and carrier's networks, the existing solutions for data connectivity are summarized in the following two domains.

1) 3G/4G subscriber identification module (SIM) module: With the advantages of well developed telecom operators 3G/4G wireless networks, it is straightforward and relatively low cost to develop SIM card based IoT applications. The SIM based solutions are primarily used in low dense wireless sensor networks or rural area where Internet access is impossible.

2) IoT gateway: It primarily relies on the Ethernet connection to deliver reliable Internet access for WLAN. Especially for those WSN running incompatible radio or communication protocols with the gateway, it is important to integrate the proxy implementation into the IoT gateway and allow any wireless sensor devices to talk to end users via Internet. In our previous work [26], we integrate IEEE 802.15.4 connectivity into an open source gateway and implement the Hypertext Transfer Protocol (HTTP)-CoAP proxy to realize remote access from any IP terminal to IPv6 sensor devices.

C. Cloud management platform

It is a horizontal platform that forms the kernel of the IoT architecture by providing a unified set of common operation functions such as device management, protocol conversion, route forwarding, to application verticals. Moreover, the additional feature of big data analytics is needed to cope with massive IoT applications.

In fact, due to the complex deployment and the stringent requirements imposed by various services, it is a challenge to maintain a large scale IoT system across different layers. The emerging IoT management can thus play an important role in providing reliable and efficient method to monitor and control wireless sensor devices in a unified manner, which can show clear advantages: (1) it can abstract the common IoT components and reuse, thereby reducing the application development cost and ensuring quick deployment through reduction in development time; (2) it can provide efficient data collection, semantically inter-operable data exchange across verticals, and an easy-to-use application development environment to IoT service providers; (3) it can minimize the system costs (e.g., device energy and network congestion), while maximize the utilization of computing resources in an integrated manner.

In order to successfully operate IoT device management in such an architecture, two essential management entities are particularly important and discussed in details in the following sections:

- Management protocol: It is necessary to develop an efficient and reliable management protocol for WSN without consuming extensive resources. In essence, it includes provisioning and management, configuration of network parameters, firmware upgrades and performance monitoring, etc.
- Management data analytics on cloud platform: It works on the top of the sensor device and is designated to integrate and elaborate diverse sensing data from multiple source of edge devices by using big data analysis tools, so as to deliver intelligent and customized services to users in the pervasive world.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

TABLE II
SHORT RANGE RADIO TECHNOLOGIES AND APPLICATIONS MAPPING IN INDUSTRIAL WSN

	Technical Summary	Typical Radio Band	Transmission Range	Data Rate	Applications
Wi-Fi	It is probably the most widely used wireless local area network (WLAN) technology based on the IEEE 802.11 series of standards.	2.4 GHz, 5GHz	150m	54Mbps	Video and monitoring based applications, smart home
Bluetooth	Bluetooth low energy technology is a global standard, which enables devices with coin cell batteries to be wirelessly connected to standard Bluetooth enabled devices and services.	2.4GHz (v1.x,v4), 5GHz (v3.0)	10-150m	1Mbps, 24Mbps	Remote access, Sports & Fitness, Indoor positioning (HAIP), smart phone based applications
ZigBee (IEEE 802.15.4)	A well-defined protocol stack for WSN with features of self-deployment, low complexity, low data rate and low cost, etc, based on IEEE 802.15.4 standards.	780MHz (China), 868MHz, 915MHz, 2.4GHz	100-300m	20Kbps, 40Kbps, 250Kbps,	Smart Energy, Home Automation, Building Automation, Health care, Remote Control, Retail Services, etc.
RFID	A fast developing radio technology used to transfer data from an electronic tag, which includes identification, information collection, etc.	125KHz (LF), 13.56MHz (HF), 433MHz (UHF) 2.4GHz (MW),	<10cm, <1m, 4-20m, 60-100m	1-5Kbps 6.62-26.48Kbps 40-640Kbps 200-400Kbps	Logistic, E-car license, one pass card
433MHz enabled proprietary solutions	Proprietary solutions by using one of the most commonly used ISM (industrial, scientific and medical) radio band in China.	433MHz	300-1500m	<10Kbps	Home security, environment monitoring, etc.

IV. SENSOR DEVICE MANAGEMENT PROTOCOL

The IoT must excel not only in terms of offering constantly evolving application development and management environments, but also in terms of supporting a communication protocol to deliver semantics efficient management functions.

A. Industry standards in device management

Traditionally, device management solutions used to target devices such as computer, mobile phone, set-top box and gateway, etc. In order to address the interoperability of connected devices, a number of standards have been developed and recognized by international communities. There are two widely used DM solutions for networked devices:

OMA Device Management (OMA DM) is for management of small mobile devices, offering platform scalability and horizontality. Essentially, the first step before a device can communicate with an OMA DM server is the bootstrap configuration called provisioning. OMA client provisioning specifications define the OMA client provisioning object as an SyncML[4] document containing the initial provisioning parameters for end devices. This document includes configuration parameters for proxy servers, network access points and access rules. Once the device is provisioned, it can be remotely managed by the OMA DM server according to the configured and verified relationship with management servers.

TR-069 is a Wide Area Network (WAN) management protocol defined by the Broadband Forum for managing an increasing number of Internet access devices such as modems, routers, gateways, set-top box and VoIP-phones. It is a bidirectional Simple Object Access Protocol (SOAP)[5]/HTTP-based protocol for remote management of end-user devices. TR-069 provides the communication between customer-premises equipment (CPE) and auto configuration servers (ACS). It includes both safe auto configuration and control of other CPE management functions within an integrated framework.

Although these solutions are not optimized for emerging IoT applications, their recent efforts have started to investigate the IoT device management, i.e., OMA DM starts to address the M2M device management (LWM2M) by extending the OMA DM through a gateway to sensor devices using a lightweight M2M protocol. Moreover, BBF TR-069 recent IoT activities include use cases study to verify extended vertical scenarios impact to TR-069, and identification of new constraints from IoT (local) area networks and new objects including data modelling and protocols.

There are also proprietary solutions from industry players, such as wireless M2M Protocol (WMMP) [27] proposed by telco operator and iDigi Device Cloud, and traditional solutions, such as Simple Network Management Protocol (SNMP) and command line interface (CLI) [28], as well as emerging solutions, such as Message Queue Telemetry Transport Protocol (MQTT) [29] and Extensible Messaging and Presence Protocol (XMPP) in supporting M2M device management. However, we should admit that unlike traditional networked devices, IoT devices usually come with new features, such as low cost and power, limited processing capability, heteroge-

[4]Synchronization Markup Language (SyncML) is an XML-based, industry-standard protocol for synchronizing mobile data across a variety of multiple networks, platforms and devices.

[5]SOAP is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

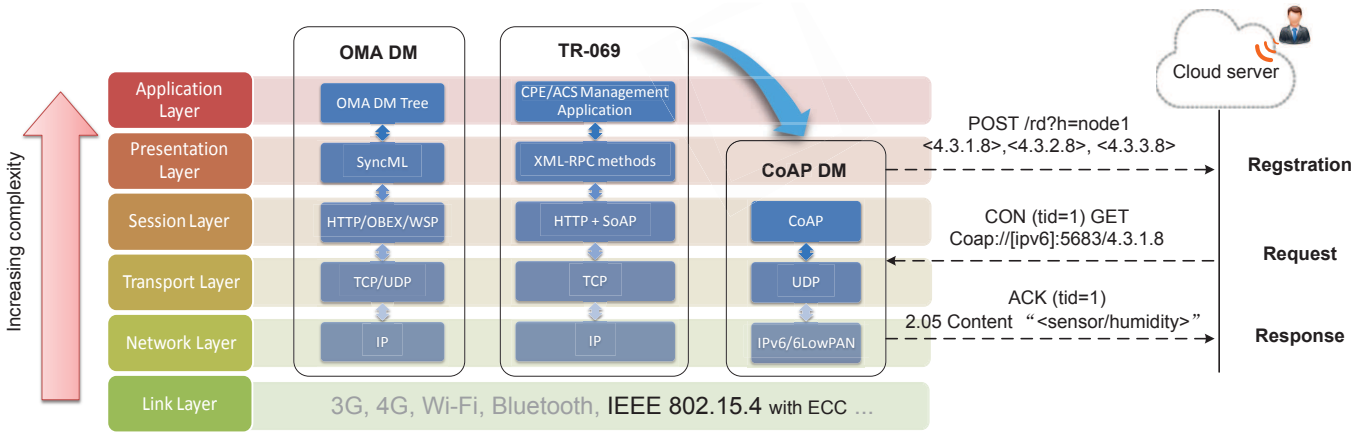


Fig. 3. Comparisons of RESTful management protocol with OMA and TR-069, and its interaction with cloud platform

neous and intelligence. With increasing amount of different type of these devices being connected over Internet, it is essential to maintain and control wireless sensor devices in a lightweight, open and universal method.

B. New research trend

So far the enterprise level solutions are more preferable to use the Big Web Services (or WS-*) architecture which may bring extensive overheads for resource constrained devices. More recent works are dedicated for creating a loosely coupled system by developing Representation State Transfer (REST) style IoT systems which is better suited for simple and flexible integration scenarios [30]. REST, a design concept that all the objects in the Internet are abstracted as resources, is a lightweight web service implementation to provide sharable, reusable and loose coupling services.

Motivated by the fact that the TCP/IP protocol is the de-facto standard for computer communications in today's networked world, IP based solution could be the future for IoT networks [31], e.g., IP Smart Object Alliance (IPSO) actively promotes IPv6 embedded devices for IoT applications. In order to tackle the technical challenges, such as extensive protocol overheads against memory and computational limitations of sensor devices, IETF[6] takes the lead to standardize communication protocols for resource constrained devices and develop a number of Internet protocols, including the Constrained Application Protocol (CoAP)[7] [10] for pervasive IoT applications.

Although considerable research has been done on the implementation of CoAP in various resource constrained sensor devices, the system level management is not well explored. [32] proposes dedicated application protocol on top of CoAP to map all application functions in building automation, and [33] proposes the latest integration of CoAP with SNMP (draft-vanderstok-core-comi-04), however, they all either build management capabilities on top of CoAP or need to support multiple protocols simultaneously, which may bring extra overheads to resource constrained devices. To promote organic-growth of IoT systems, open technologies are preferred for IoT management and the RESTful approaches are promising. Specifically, we propose software platforms using CoAP method directly for managing sensor devices. Moreover, the proposed real-time big data analysis engine is able to elaborate diverse management data from multiple sources and directly map management functions into CoAP methods. In essence, the proposed method not only integrates WSN into the Internet, but also manages them via the "web".

In Fig. 3, we mainly compare the complexity of management protocol stacks among three solutions. Regarding to the RESTful approach, we propose efficient naming and addressing solutions based on CoAP Uniform Resource Identifier (URI) such that each onboard resource can be represented and traced in a more compatible format.

C. Management functions

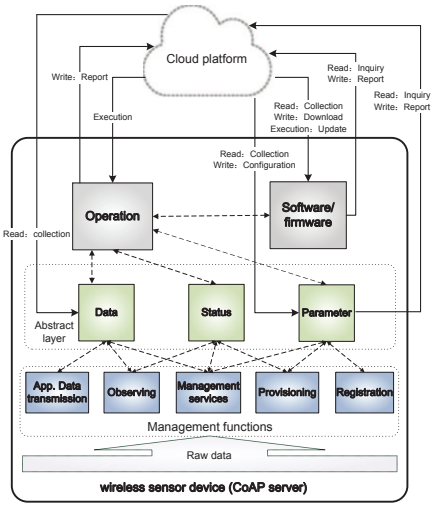
We propose the management functions in Fig. 4 (a) which shows the interactions between a wireless sensor device and cloud platform. Due to the requirements imposed to IoT services, such as no direct human interaction, reliable remote control and scalable features of applications, we define five major management functions which are essential to WSN:

1) **Registration**: It is a primary function to allow a sensor device to register/de-register with a remote cloud platform, maintain and update registration information.
2) **Provisioning**: It is to initialize and synchronize essential information (e.g., setup or configuration) of a sensor device with the cloud platform.
3) **Management services**: Once the sensor device is registered with the cloud platform, a number of essential management services should take in charge to maintain

[6]The Internet Engineering Task Force (IETF) is a large open international community of network designers, operators, vendors and researchers concerned with the developments and promotions of Internet standards of the Internet protocol suite (TCP/IP).

[7]The CoAP is based on the exchange of short messages which, by default, are transported over UDP. The protocol has a registered scheme of $<$ coap : // $\sim>$ with a default port of 5683. CoAP messages are encoded in a simple binary format.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access



(a) The proposed management functions on WSN

Class Name	ID	Resource Name	ID	Sub-Resource Name	ID	Method Name	ID
Hardware information							(Hex->bit)
HW	1	CHIP ID	1	Null	0	Get	8->1000
HW	1	SRAM	2	Null	0	Get	8->1000
HW	1	FLASH	3	Null	0	Get	8->1000
HW	1	MAC addr	4	Null	0	Get	8->1000
HW	1	RADIO	5	Frequency	1	Get	8->1000
HW	1	RADIO	5	Channel	2	Get	8->1000
HW	1	USART0	6	Baudrate	0	Get	8->1000
Operating system information							
SYS	2	CONTIKI_v	1	Null	0	Get	8->1000
SYS	2	NAME	2	Null	0	Get/Put	c->1100
Network protocol information							
NET	3	PANID	1	Null	0	Get	8->1000
NET	3	RDC	2	Null	0	Get	8->1000
NET	3	MAC	3	Null	0	Get	8->1000
NET	3	NETWORK	4	Null	0	Get	8->1000
NET	3	IPv6	5	Prefix	1	Get	8->1000
NET	3	CoAP_v	6	Null	0	Get	8->1000
Onboard resources information							
RES	4	ACTUATOR	1	leds	1	Get/Put/Post	e->1110
RES	4	SCREEN	2	Null	0	Get/Put/Post	e->1110
RES	4	SENSOR	3	Humidity	1	Get	8->1000
RES	4	SENSOR	3	Illumination	2	Get	8->1000
RES	4	SENSOR	3	Temperature	3	Get	8->1000

(b) Resources naming and addressing assignment

Function	Direction	Logical operation	CoAP method	Uri-Path Opt.	Location-Path Opt.
Registration	Uplink	Register	POST	√	√
	Uplink	De-register	DELETE	√	√
	Uplink	Update	PUT	√	√
Provisioning	Down/uplink	Configuration	GET	√	
Management services	Down/uplink	Read	GET	√	
		Write	PUT	√	
		Execute	POST	√	
		Creat	POST	√	
Observing	Downlink	Observe	GET with observe opt.	√	
	Uplink	Notify	Response to observe	√	√
App. data transmission	Downlink	Collect	GET	√	

(c) CoAP methods mapping to management functions

Fig. 4. The proposed RESTful management protocol for WSN based on CoAP

IoT services, such as parameter configuration, connection diagnose, status inquiry and remote control, etc.

4) **Observing**: It is the unique feature of CoAP to allow the cloud platform to "observe" resources on IoT devices, i.e., to periodically update a resource to the remote cloud over a period of time.
5) **Application data transmission**: It includes any other dedicated or proprietary applications based above CoAP.

Although the management functions can be defined in different manners, they all share common resources on one sensor device and we abstract these resources as parameters, status and data, which are defined as abstract layer. The interactions with the cloud platform (i.e., operations and software/firmware updates) can be directly triggered with these resources via `GET`, `PUT`, `POST` and `DELETE` methods provided by CoAP.

D. Naming and addressing of resource identities

It is necessary to define efficient naming and addressing solutions such that each resource can be represented and traced in a compatible format. We define a simple resource model in which resources are logically organized into class. A class defines a group of resources, for example the Hardware class contains all the resources that can be used for provisioning purposes. A resource is identified by the path:

$$\sim /\{\text{Class ID}\}.\{\text{Resource ID}\}.\{\text{Sub-Resource ID}\}.\{\text{Method ID}\}$$

where the Class ID, Resource ID and Sub-Resource ID are with size of 1 byte. The Method ID is to represent access methods available to a resource. It is 4 bits and each bit from the Most significant bit (MSB) represents an authorized operation in a sequence of `GET`, `PUT`, `POST` and `DELETE`. The value "1" means authorized and "0" means non-authorized. The Method ID provides an efficient way of informing cloud/users the access methods of a resource. Furthermore, the CoAP server may assign different method IDs to a same resource as long as users' access levels are different. Fig. 4 (b) shows the detailed naming and addressing assignment on our sensor testbed.

E. CoAP-based management protocol

The CoAP is based on the exchange of short messages which, by default, are transported over UDP. The protocol has a registered scheme of $<$ `coap` : // $\sim>$ with a default port of 5683. CoAP messages are encoded in a simple binary format.

Fig. 4 (c) shows the detailed CoAP methods mapping to management functions. Each management function can be abstracted as a recall process to conduct with resources on sensor device, thus the RESTful approach provided by the CoAP protocol can be adopted as a lightweight method to access from application servers to sensor devices. Especially, the `Uri-Path` Option is to indicate management resource identities and the `Location-Path` Option is to indicate the address of remote registration server for future update and delete operations.

It is worth noting that each management function can be abstracted as a recall process to conduct with resources of sensor device, thus the RESTful approach provided by the CoAP protocol can be adopted as a lightweight method to access from application servers to sensor devices. The RESTful interactions illustrated in Fig. 3 also gives an example of registration and retrieval process of onboard resources, i.e., humidity, illumination and temperature (defined in Fig. 4 (b)), using the proposed management method.

F. A cross layer approach to ensure reliable WSN management

In [34], we have shown the simplicity and efficiency of the proposed device management solution for WSN. The performance evaluation results tell that the overhead imposed by CoAP protocol is negligible and thus the CoAP based device management is a promising solution for future IoT.

To further evaluate the efficiency of the proposed CoAP based management solution, we compare it with the standard CoAP method in terms of packet length. Fig. 7 (b) shows

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

the onboard resources defined by both standard CoAP method (human-readable string) and the proposed method. The URI length is calculated from the space occupied in the RAM. It is clear that the proposed URI representation takes far less memory space than the standard URI representation in which the main space are consumed by "`Attributes`". Through the resource discovery, we can receive a list of available resources and the total length of transmission packets for both methods are 420 bytes and 109 bytes, respectively. Since the CoAP is transmitted in a block-wise fashion (6 blocks for the standard method, only 2 blocks for the proposed method), the memory saving of 311 bytes is composed of URI savings and 4 extra CoAP block headers. The total transmitting packets can be reduced by 74%, which shows promising for resource constrained sensor devices.

Although the proposed application protocol can help manage IoT sensor devices in an efficient way, we should admit that there are still challenges in providing a reliable communication channel to fulfill management tasks, especially for a large scale WSN deployment. It is well known that packet size directly affects the reliability as larger packets suffer higher loss rates [35]. In our previous study in [34], we have shown that the proposed device management protocol can significantly reduce packet overheads, which in turn improves the packet loss rate of the management communication by nearly 20%. However, in most of industrial WSN applications, wireless sensor devices are deployed in a large scale and communications are convoyed in a multi-hop fashion. In our experiment, we have shown that the proposed management protocol leads to a packet loss rate of 44.21% for a maximum number of 6 hops, because of severe environmental interference in an open office area with strong Wi-Fi background noise and co-channel congestions, etc.

Errors in the packet transmissions occur due to channel variations such as fading and interference from adjacent sensor nodes [36]. For reliability concerns, the traditional transmission of a message is initiated by marking the message as "confirmable" in the CoAP header. It requires an end-to-end ACK and retransmission strategy, which can result in a poor throughput and longer transmission time. This concept lacks proactive means for error correction as well as results in increased communication latency. Therefore, a fundamental approach to reduce the packet loss of IoT communication is necessarily to be integrated together with upper layer protocols to deliver reliable WSN management.

We propose to use the approach of Error Correction Coding (ECC) to improve transmission reliability. ECC adds redundancy in the system to improve the transmission reliability. Although additional redundancy reduces the efficiency, it is still a more preferable solution, because it helps to improve both reliability and latency. ECC, such as Bose-Chaudhuri-Hocquenghem (BCH) and Reed-Solomon (RS), are well known in wireless local area networks (WLANs). However, they are yet to be implemented in IoT systems. Hence, we further evaluate the performance of the WSN in terms of the packet error rate and energy efficiency, and compare it with the state of the art Automatic Repeat reQuest (ARQ) scheme that is widely used in IEEE 802.15.4 radio.

1) Analysis of packet error in ARQ scheme: In ARQ scheme, data is decoded by $cyclic\ redundancy\ check$ (CRC) codes and the erroneous data is re-transmitted from the sender. Here we consider stop and wait ARQ method. Assuming the ACK bits are received without error, the packet error rate of the ARQ scheme is given by

$$PER_{ARQ} = 1 - (1 - P_b)^l \,, \tag{1}$$

where l is the packet length of the payload transmitted in a single transmission, P_b is the bit error rate. P_b for IEEE 802.15.4 based sensor motes is given in [37].

2) Analysis of packet error in ECC schemes: In [38], a MAC layer ECC scheme was proposed and its flexibility and compatibility with IEEE 802.15.4 is shown. We use the same framework for showing the validity of our ECC schemes. For BCH and RS codes, we use a (n, k, t) t-error control method with $n - k$ redundant bits appended to the k-data bits. We further assume that the transmission of the packets between the sensor node and sink node/gateway is in bursts of n-bit data. Therefore, the packet loss rate at the sink node is given as

$$PER_{ECC} = 1 - \left(1 - \sum_{i=t+1}^{n} \binom{n}{i} P_b^i (1 - P_b)^{n-i}\right)^{\lceil \frac{l}{k} \rceil} , \tag{2}$$

where $\lceil . \rceil$ is the ceiling function. The expected number of retransmissions is given by

$$E(T) = \frac{PER_{ARQ/ECC}}{\left(1 - PER_{ARQ/ECC}\right)} \,. \tag{3}$$

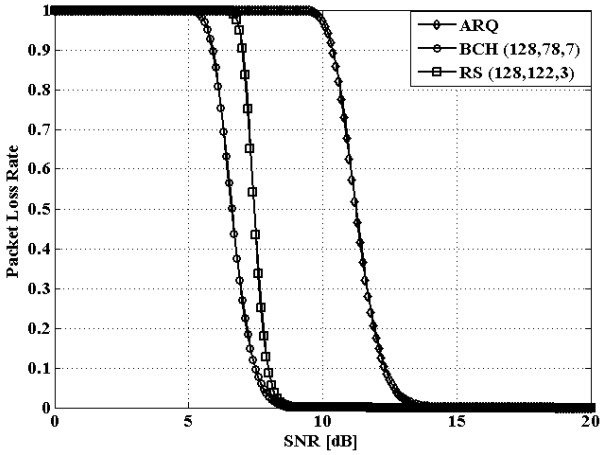
3) Energy Efficiency: One of the major overheads for ECC is the energy consumption during its transmission and reception, which is also known as its communication energy. Let P_{RX} and P_{TX} be the receiver power and the transmitted power, respectively, during reception and transmission. Given the encoding energy for block codes is negligible [39], the total energy consumed is

$$P_{avg} = (P_{TX} + P_{RX}) + E(T) \times (P_{TX} + P_{RX}) \,. \tag{4}$$

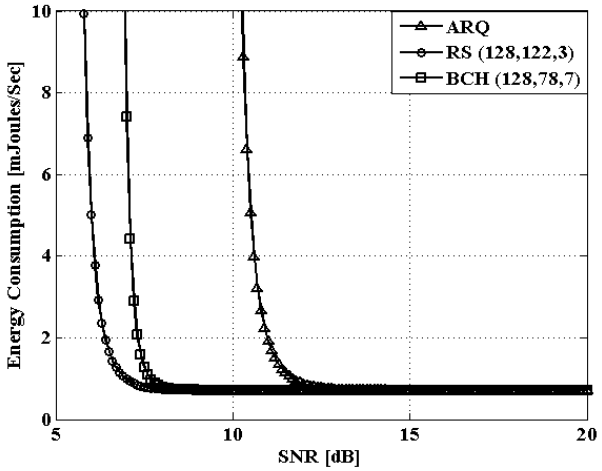
We perform a theoretical analysis to find out the packet loss rate of the MICAz mote[8]. The systems signal to noise ratio is varied from 0dB to 20dB. The packet error rate is generated for BCH (128,78,7) and RS (128,122,3). These values of n are taken to correlate with the packet load of 133 bytes (payload of 127 bytes and 6 bytes of header). The power consumption of MICAz mote is taken as 721.5mW [37]. From Fig. 5(a), it can be inferred that ECC schemes provide approximately a gain of 4 dB in SNR as compared to ARQ scheme for the same packet loss rate. This is equivalent to a power gain of around 2 watts, which is essential savings in case of energy

[8]The MICAz is a 2.4 GHz Mote module used for low power wireless sensor networks. It runs the TinyOS operating system with a TI CC2420 radio module.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access



(a) Packet loss versus SNR for MICAz Mote at different coding schemes.



(b) Energy Consumption with respect to SNR for MICAz Mote at different coding schemes.

Fig. 5. Analytical results of different coding schemes for MICAz Mote.

constrained IoT systems. BCH code provides slightly better gain of around 0.5dB, owing to its better error correction capability compared to RS code. In terms of energy efficiency in Fig. 5(b), ECC schemes are approximately 6dB more energy efficient as compared to ARQ scheme. RS code is more energy efficient due to its better coding rate (k/n) as comparison to BCH code.

We further analysis its performance in the same multi-hop wireless sensor network [34]. The sensor platform is equipped with CC2530 MCU with 8051 CPU core running at 32MHz, 8KB SRAM and 256KB flash block to support IEEE 802.15.4-compliant radio transceiver. To support CoAP, all sensor devices are running Contiki v2.6 operating system with implementation of 6LoWPAN, IPv6 and RPL protocols based on IEEE 802.15.4. Given the limited memory size, we can configure a maximum number of 6 hops by optimizing the communication system. The test is carried out in an open office area with strong Wi-Fi background noise and lowest possible WSN radio frequency output power to ensure a multi-hop

TABLE III
PACKET LOSS RATE IN A MULTI-HOP NETWORK

Protocol	Packet Loss Rate				
	Hop 2	**Hop 3**	**Hop 4**	**Hop 5**	**Hop 6**
Standard CoAP mgmt with ARQ	7.38%	21.76%	46.09%	48.9%	56.65%
The proposed mgmt with ARQ	5.91%	17.30%	36.18%	39.69%	44.21%
The proposed mgmt with ECC (analysis)	3.73%	9.09%	14.76%	24.42%	32.71%

fashion, which makes a sensor device can only communicate to each other within around 30 cm.

Table III shows the packet loss rate, where the values of packet loss rate for the proposed management method and the standard CoAP method using ARQ scheme are taken from [34]. It shows that the ECC can achieve better performance for multiple hops. Specifically, ECC schemes combined with the proposed management method provides acceptable packet loss rate till 5 hops transmissions, whereas methods not using ECC have acceptable packet loss rate till 3 hops only.

V. MANAGEMENT DATA ANALYTICS ON THE CLOUD

With the fast penetration of IoT technologies in a variety of vertical industry domains, plethora of data are expected to be generated from diverse applications that is aggregated at a very high-velocity, thereby increasing the need to better index, store and process such data. In order to foster the rapid deployment of IoT applications by overcoming the incompatible architecture across industry domains, the latest industrial research & development trend indicates a favor of building open and horizontal platform for future IoT [40], [41].

The motivation behind a horizontal model is to foster rapid growth and innovation in the industry by allowing multiple providers to work with a common framework, such that users can concentrate their efforts on creating devices and services. Furthermore, by working on a common framework, those devices and services can more easily share information and resources.

One fundamental aspect of the IoT system is the tight connection with cloud computing which provides great benefits for applications hosted on the web with flexible computational and storage requirements. Therefore, it is reasonable to build IoT platforms based on existing cloud infrastructures in order to provide great scalability and interoperability through open access and direct interfaces for communication and data management.

In the following, we summarize the key benefits of open cloud platform for IoT:

1) Low cost for deploying a IoT service: Due to the large scale deployment of IoT, it is desirable to maintain low development and maintenance costs during the entering operation of the service. With cloud platforms, there is no need to setup or maintain the entire software and hardware infrastructures, e.g., operation system,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

TABLE IV
EXAMPLES OF FREE OPEN CLOUD PLATFORMS FOR IOT MANAGEMENT

Service provider	Supporting language	Web service	Open source	Features
Xively (former Cosm)	Android, Arduino, mbed, C/C++, Electric Imp, JavaScript, Java, PHP, Python, Ruby	RESTful API supports JSON, XML & CSV data formats	No	Real-time, visualizations, online store sensor data
Nimbits	Arduino, JavaScript, HTML, Nimbits.io, Java	RESTful API supports simple textual and JSON formats	Yes	Sensor data processing, customized rules
ThingSpeak	Integratable with Arduino, Raspberry Pi, ioBridge / RealTime.io, Electric Imp, Data Analytics with MATLAB	Using HTTP protocol with support of JSON, XML and CSV data formats	Yes	Open API, Real-time data, Geolocation data, Data processing, visualizations Device status messages, Plugins
Yeelink	Node.js, JavaScript	RESTful API supports JSON, XML & CSV data formats	No	High concurrency access, two way communication and control, social networks

management software, servers and routers, for hosting online IoT applications and storing sensor data.

2) Scalability on resource utilization: It is flexible to reuse much of the existing software and hardware for hosting different IoT services. Furthermore, depends on the scale of the application, extend storage or web server resources can be directly purchased from the cloud service providers.
3) Interoperability across application domains: It is easier to manage and share data across different IoT applications, and allow service providers to compose a new service from existing services, i.e., IoT Mashups [42].
4) Quick and easy implementation: It is not a necessary condition of expertise in setting up a web-based application, configuring webserver and database system, and making connections to launch IoT services, but a focus on the data and application that need to be hosted on the cloud platform [43].
5) Quality of service (QoS) guarantee: The cloud service provider can ensure the availability of the software and hardware with minimum system failures and power interruptions, e.g., Microsoft Azure guarantees at least 99.9% availability of its cloud services.
6) Anywhere access: The IoT data is accessible from any kind of computational device that has access to the cloud platform over Internet.

Table IV lists some of the most popular free open cloud platforms ideally for managing wireless sensor devices.

In the following, we introduce our latest work in design an efficient and effective management cloud platform for IoT. The platform works on top of the wireless sensor networks. It is designated to integrate and elaborate diverse sensing data from multiple source of edge wireless sensor devices, so as to deliver intelligent and customized services to users in the pervasive world. Also, it provides the development environment to support the development of different personalized IoT applications. Fig. 6 shows our management platform on the cloud, which adopts a hierarchical architecture with the following three layers.

A. Cloud gateway layer

This layer works as a bridge between WSN and the management platform of IoT cloud, so as to form a seamless management platform across wireless sensor nodes and cloud. For instance, the communications between these two sides can employ the standard web service format based on the HTTP protocol and Extensible Markup Language (XML) data format. In addition, although most of the current service interactions on the cloud are SOAP based which is a protocol specification for exchanging structured information in the implementation of web services in computer networks, the RESTful based web services are more preferable to management of lightweight wireless sensor devices, hence the SOAP-REST transformation can be achieved using additional adapters. This adapter can receive the REST service invocation request, and transform it into the SOAP service invocation request [44].

B. IoT management layer

Beyond the basic management services like data storage, visualization and failure handling, we propose the real-time big data analysis as a key service in this layer.

Consider the limited resource of sensor devices, diverse management (or contextual) data need to be uploaded to the IoT cloud platform for further processing. Such data collected from independent IoT sources often have implicit but disparate assumptions of interpretation. For example, data standard about temperature collected from a sensor device in the US (Fahrenheit) is different from that collected in Europe (Celsius). Such implicit assumptions of data interpretation have to be addressed before the services can be dynamically composed and delivered. Thus, to make the management data from different sources be context-aware, one possible way is to require service providers to pre-specify the context definition for their sensor devices and register them to the cloud. Further, as introduced in our earlier works, we use a lightweight ontology which contains a modifier using to capture additional information that affects the interpretations of generic concepts [45]. Specifically, the generic concept in the ontology can have multiple modifiers, each of which indicates an orthogonal dimension of the variations in data interpretation. The data analysis engine can understand the context of data sources

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access

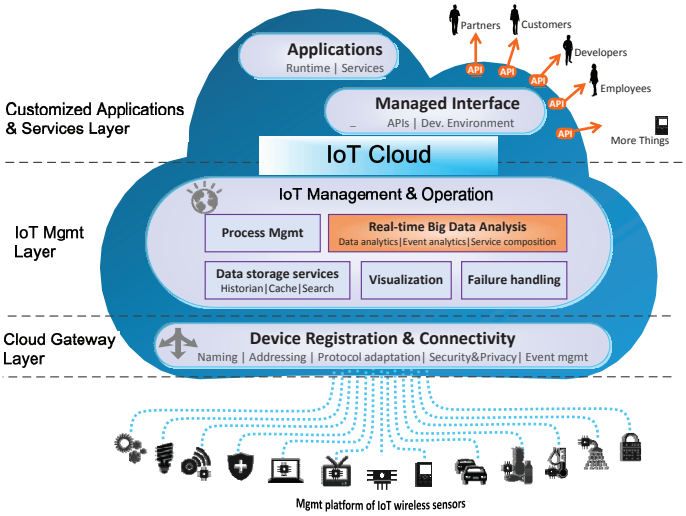


Fig. 6. Architecture of the management platform on the Cloud

and therefore know how to interpret the data based on the values of the modifiers associated with the corresponding context, which is more flexible and adaptable to the dynamic IoT environment. More details about the setting of the cloud platform, e.g., the BPEL engine presented in Fig. 7, can be found from our previous work [44].

C. Customized application and service layer

This layer is built upon the specifications and methodologies of RESTful web services and provides the managed interfaces which consists of development environment and APIs to support customized IoT applications and services. Similar to our prior work [44], the managed interface can be implemented by integrating the Apache ODE (http://ode.apache.org/) management interface, the JBoss jBPM (http://jbpm.jboss.org/) management interface and series of open source packages.

During a sensor device's run-time, once this layer receives a web service request from a user, it can automatically analyze the requested URI and the related parameters encapsulated by HTTP, so as to determine the specific class (e.g., JAVA class) to invoke the corresponding web services based on the configuration files. After the operation of the related web services, the IoT cloud will return the results to the user in the form of REST-style data through HTTP.

Thus, compared to traditional service-oriented architecture (SOA) based solutions, the advantage of the proposed architecture is that developers can focus on developing the functions of IoT applications without concerns of transforming raw data to contextual information, and the mapping between specific service request and the corresponding context information in run-time. Fig. 7 shows the user-cloud-sensor interactions in the proposed M2M system.

VI. IoT Management System Evaluation

We develop a prototype system to connect sensor devices via the cloud platform using the proposed CoAP based management protocol. The snapshot of the management portal is shown in Fig. 7 (a). Through the pre-defined CoAP APIs, interactions with application data can be easily managed and retrieved in a unified manner without remembering all string URIs.

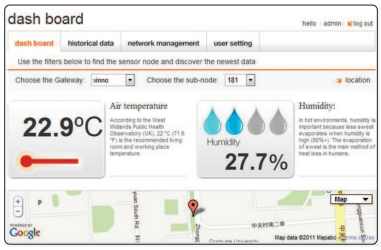
By integrating the proposed management protocol into the IoT cloud system, we evaluate the system performance in terms of time efficiency by setting up a test environment in which 5 sensor devices are used to upload computing tasks to the cloud platform with a total average rate of $E = 5/\text{min}$. The ε£-GALEN ontology [46] is adopted as benchmark, and the computing tasks are to index and calculate the similarities of concepts on this ontology under the condition of four different size assertions (1000, 1500, 2000, 36000). We take 5 tests and each lasts for 30 minutes. The average results are shown in Fig. 7 (c). The time delay when performing the task via cloud consists of: (1) response and communication time between the remote IoT cloud platform and the sensor device; and (2) processing time of the task. The results show closed performance of response time with an average of 4.5s, while the process time mostly depends on the size of the data set. As a comparison, we replace the cloud server with a Nexus 4 smart phone, which is a reasonable example to illustrate local processing capability, and it shows that the cloud platform can better achieve communication and computation efficiently and widely support large data IoT applications in real-world. It is worth noting that depends on specific scenarios of IoT applications and computing capacities of wireless sensor devices, we can choose different size of dataset for real-world deployments.

VII. Future Work

In the future work, a more robust and reliable device management system for IoT needs to be built. Especially, the following research issues need to be considered with higher priorities:

1) *Real-time management* is a challenging issue for resource constrained sensor networks. In this case, the IoT system needs to rely on efficient service gateway design to minimize the amount of data to be sent by constantly reviewing the data from users, and intelligent data oriented middleware design to only transmit real time information when a reading is out-of-threshold.
2) *Security, trust and privacy* are also important issues to be considered in practical applications. There are both hard way and soft way methods to achieve different degrees of security. In our case, the CoAP based management principle can utilize the transport layer bindings of UDP or SMS protocols. Thus, the security mechanisms of these channel bindings can be utilized to implement access control and policy enforcement for M2M systems. For example, the UDP channel security defined by the Datagram Transport Layer Security (DTLS) can support multiple key models, i.e., pre-shared or public key, depending on the system requirements. Also the encryption key exchanges through SMS can also provide an alternative to establish a secure channel. These

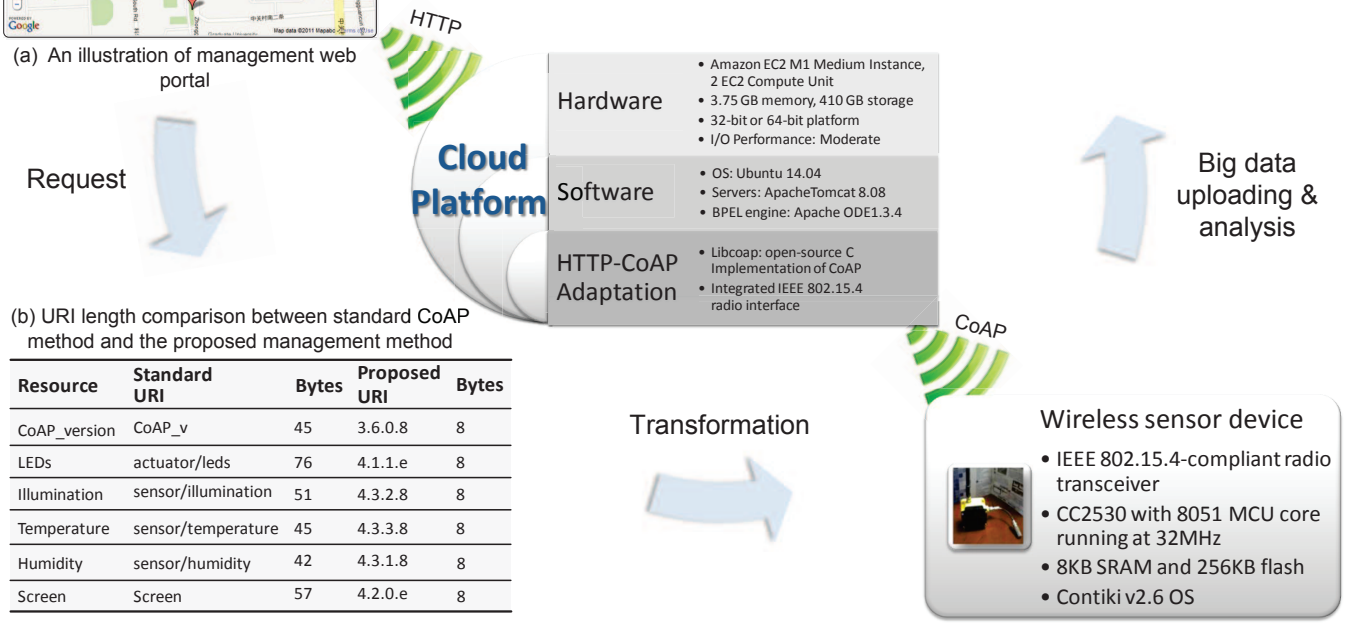
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2015.2435000, IEEE Access



(a) An illustration of management web portal

(c) Overall system performance of the IoT cloud

Average time delay (ms)		Data set 1 (1000)	Data set 2 (1500)	Data set 3 (2000)	Data set 4 (36000)
Cloud platform	Response time	4683	4475	4626	4395
	Process time	40	461	702	2483
Smart phone platform	Total time	2234	4736	7445	136073



(b) URI length comparison between standard CoAP method and the proposed management method

Resource	Standard URI	Bytes	Proposed URI	Bytes
CoAP_version	CoAP_v	45	3.6.0.8	8
LEDs	actuator/leds	76	4.1.1.e	8
Illumination	sensor/illumination	51	4.3.2.8	8
Temperature	sensor/temperature	45	4.3.3.8	8
Humidity	sensor/humidity	42	4.3.1.8	8
Screen	Screen	57	4.2.0.e	8

Fig. 7. User-cloud-sensor interactions and its performance in the proposed IoT system

security methods are appropriate for M2M deployments where there is an existing trust relationship between the devices and server.

3) *Dynamic registration, bootstrap and management* will be particularly considered for a large scale deployment with devices coming in and out and changing their characteristics and functionalities. The IoT device management should be suitable to develop an open and universal ecosystem with sustainable interactions and interoperability among things.

VIII. Conclusion

In this paper, we have introduced the IoT ecosystem and key technologies to support IoT communications, and described the essential management mechanisms for IoT system. Specifically, we have introduced a cross layer design of a lightweight and scalable RESTful web service based infrastructure to enable efficient and reliable management of wireless sensor networks. Through performance evaluations, we have shown the simplicity and efficiency of the proposed solution, which is promising to drive the new IoT device management standardization. In our view, these benefits will enable future IoT to effectively and efficiently combat network complexities while meeting the requirements of high-quality services.

References

[1] L. Gurgen and S. Honideni, "Management of networked sensing devices," in *Proc. International Conference on Mobile Data Management: Systems, Services and Moddleware*, 2009.

[2] Open Mobile Alliance, *http://technical.openmobilealliance.org/Technical/*.

[3] Broadband Forum, "CPE WAN management protocol," *http://www.broadband-forum.org/technical/download/*.

[4] ZigBee Alliance, "ZigBee home automation public application profile," *IEEE J. Select. Areas Commun.*, Oct. 2007.

[5] A.-B. García-Hernando, J.-F. Martínez-Ortega, J.-M. López-Navarro, A. Prayati, and A. P. L. Redondo-López, "Problem solving for wireless sensor networks," *Springer*, Jul. 2008.

[6] J. Song, S. Han, A. Mok, D. Chen, M. Lucas, and M. Nixon, "WirelessHART: Applying wireless technology in real-time industrial process control," in *Proc. IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS).*, April 2008, pp. 377–386.

[7] J. Kjellsson, A. Vallestad, R. Steigmann, and D. Dzung, "Integration of a wireless I/O interface for PROFIBUS and PROFINET for factory automation," *IEEE Trans. Ind. Electron.*, vol. 56, no. 10, pp. 4279–4287, Oct 2009.

[8] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15.4 networks," in *Internet Engineering Task Force, RFC 4944*, 2007.

[9] T. W. (Ed.), P. T. (Ed.), A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, "RPL: IPv6 routing protocol for low-power and lossy networks," in *IETF, RFC 6550*, 2012.

[10] Z. Shelby, K. Hartke, and C. Bormann, "Constrained application protocol (CoAP)," *Internect Draft, Available at: http://datatracker.ietf.org/wg/core/charter*.

[11] Z. Sheng, S. Yang, Y. Yu, A. V. Vasilakos, J. A. McCann, and K. K. Leung, "A survey on the IETF protocol suite for the internet of things: standards, challenges, and opportunities," *IEEE Wireless Communications Magazine*, vol. 20, no. 6, pp. 91–98, 2013.

[12] I. S. O. A. (IPSO), *Available at: http://www.ipso-alliance.org*.

[13] J. Jasperneite and J. Feld, "PROFINET: an integration platform for heterogeneous industrial communication systems," in *Proc. 10th IEEE Conference on Emerging Technologies and Factory Automation (ETFA)*, vol. 1, Sept 2005, pp. 8 pp.–822.

[14] European Telecommunication Standards Institute (ETSI), *http://www.etsi.org/technologies-clusters/technologies/m2m*.

[15] J. Song, A. Kunz, M. Schmidt, and P. Szczytowski, "Connecting and managing M2M devices in the future internet," *Mobile Networks and Applications, Springer*, vol. 19, pp. 4–17, 2014.

[16] IoT-Architecture, *http://www.iot-a.eu/public*.

[17] D. Katusic, M. Weber, I. Bojic, G. Jezic, and M. Kusek, "Market, standardization, and regulation development in machine-to-machine communications," in *20th International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, Sept 2012, pp. 1–7.

[18] eCall: Time saved = lives saved, *http://ec.europa.eu/digital-agenda/en/ecall-time-saved-lives-saved*.

[19] Internet of Things: Innovation with Chinese Characteristics, *http://www.hoganlovells.com/internet-of-things-innovation-with-chinese-characteristics-09-12-2013/*.

[20] European Commission: The EU climate and energy package, *http://ec.europa.eu/clima/policies/package*.

[21] The Internet of Things Ecosystem: Unlocking the Business Value of Connected Devices, *http://www2.deloitte.com/us/en/pages/technology-media-and-telecommunications/articles/internet-of-things-iot-enterprise-value-report.html*.

[22] J. Gole and M. Cansfield, "M2M moves center stage: Where telcos fit into the m2m ecosystem," *IDC report, available at: http://www.idc.com/getdoc.jsp?containerId=LM04U*, 2012.

[23] The New Mega Trends, *http://www.gilcommunity.com/docs/new-mega-trends-sarwant-singh-frost-sullivan/*.

[24] Smart Santander, EU FP7 project, Future Internet Research and Experimentation, *http://www.smartsantander.eu/*.

[25] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[26] Z. Sheng, C. Zhu, and V. C. M. Leung, "Surfing the internet-of-things: Lightweight access and control ofwireless sensor networks using industrial low power protocols," *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 14, no. 1, 12 2014.

[27] Z. Su, Q. He, J. Zhang, and H. Li, "Research of single sign-on in mobile rfid middleware based on dynamic tokens and wmmp," in *IEEE 16th International Conference on Computational Science and Engineering (CSE)*, Dec 2013, pp. 1191–1194.

[28] A. Sehgal, V. Perelman, S. Kuryla, and J. Schonwalder, "Management of resource constrained devices in the internet of things," *IEEE Communications Magazine*, vol. 50, no. 12, pp. 144–149, December 2012.

[29] C. Zhou and X. Zhang, "Toward the internet of things application and management: A practical approach," in *IEEE 15th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, June 2014, pp. 1–6.

[30] C. Bormann, A. Castellani, and Z. Shelby, "Coap: An application protocol for billions of tiny internet nodes," *IEEE Internet Computing*, vol. 16, no. 2, pp. 62–67, March 2012.

[31] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, and M. Dohler, "Standardized protocol stack for the internet of (important) things," *IEEE Communications Surveys Tutorials*, vol. 15, no. 3, pp. 1389–1406, Third 2013.

[32] M. Jung, J. Weidinger, W. Kastner, and A. Olivieri, "Building automation and smart cities: An integration approach based on a service-oriented architecture," in *Proc. 27th Int'l Conf. on Advanced Information Networking and Applications Workshops (WAINA)*, March 2013, pp. 1361–1367.

[33] P. van der Stok and B. Greevenbosch, "CoAP management interfaces (draft-vanderstok-core-comi-04)," in *IETF, available at: https://datatracker.ietf.org/doc/draft-vanderstok-core-comi/*, 2014.

[34] Z. Sheng, H. Wang, C. Yin, X. Hu, S. Yang, and V. C. M. Leung, "Lightweight management of resource constrained sensor devices in internet-of-things," *IEEE Internet of things Journal*, 2015.

[35] T. Savolainen, J. Soininen, and B. Silverajan, "Ipv6 addressing strategies for iot," *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3511–3519, Oct 2013.

[36] K. Yu, F. Barac, M. Gidlund, and J. Akerberg, "Adaptive forward error correction for best effort wireless sensor networks," in *IEEE International Conference on Communications (ICC)*, June 2012, pp. 7104–7109.

[37] M. C. Vuran and I. Akyildiz, "Error control in wireless sensor networks: A cross layer analysis," *IEEE/ACM Transactions on Networking*, vol. 17, no. 4, pp. 1186–1199, Aug 2009.

[38] K. Yu, M. Gidlund, J. Åkerberg, and M. Bjorkman, "Reliable and low latency transmission in industrial wireless sensor networks," *Procedia Computer Science*, vol. 5, pp. 866–873, 2011.

[39] S. Lin, *Error control coding: fundamentals and applications*, vol. 114.

[40] J. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, Feb 2014.

[41] H. Schaffers, N. Komninos, M. Pallot, B. Trousse, M. Nilsson, and A. Oliveira, "Smart cities and the future internet: Towards cooperation frameworks for open innovation," in *The Future Internet*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2011, vol. 6656, pp. 431–446.

[42] J. Im, S. Kim, and D. Kim, "Iot mashup as a service: Cloud-based mashup service for the internet of things," in *IEEE International Conference on Services Computing (SCC)*, June 2013, pp. 462–469.

[43] C. Doukas, *Building Internet of Things with the Arduino*. USA: CreateSpace Independent Publishing Platform, 2012.

[44] X. Hu, T. Chu, H. Chan, and V. Leung, "Vita: A crowdsensing-oriented mobile cyber-physical system," *IEEE Trans. Emerging Topics in Computing*, vol. 1, no. 1, pp. 148–165, June 2013.

[45] X. Hu, X. Li, E.-H. Ngai, V. Leung, and P. Kruchten, "Multidimensional context-aware social network architecture for mobile crowdsensing," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 78–87, June 2014.

[46] A. Rector, J. Roger, P. Zanstor, and E. Haring, "OpenGALEN: open source medical terminology and tools," *American Medical Informatics Association*, 2003.