A Green and Secure IoT Framework for Intelligent Buildings based on Fog Computing

Ying-Si Zhao[1], Han-Chieh Chao[2,3,4]

[1] School of Economics and Management, Beijing Jiaotong University, China
[2] College of Mathematics and Computer Science, Wuhan Polytechnic University, China
[3] Department of Electrical Engineering, National Dong Hwa University, Taiwan
[4] Department of Computer Science & Information Engineering, National Ilan University, Taiwan
yszhao@bjtu.edu.cn, hcc@niu.edu.tw

Abstract

The Internet of Things (IoT) provides an opportunity to connect plethora devices and make them capable of serving the cities better in a collaborative manner. However, energy-efficiency and security problems are the two hugest chanllenges that severely hinder the development of IoT-based smart cities. In this article, we attempt to provide a green and secure IoT framework for Intelligent Buildings which are basic elements in smart cities. Specifically, a smart agent node is installed for each Intelligent Building to make it an autonomous region. The IoT data are divided into different categories according to their application domain, priorities, meanings and potential value. The resources of IoT are precisely controlled and managed to satisfy the data users under the strictly limitation. Simulation results illustrate the effectiveness of our framework in terms of quality of service (QoS). We believe that this is a meaningful and initiatory explonation to make the smart cities more practical. Finally, some research challenges are highlighted.

Keywords: IoT, Intelligent building, Fog computing

1 Introduction

One of the IoT's inherent responsibilities is moving the society, especially the cities, forward to make it green, efficient, convenient and secure [1]. Consequently, IoT has been widely employed and researched in many fields [2-4] including smart grid, smart metering, smart cameras, smart waste management, intelligent transportation system (ITS), smart home appliances, e-healthcare, smart disaster monitoring, et al. According to the IDC forecast, the worldwide IoT market will reach 1.7 trillion US dollars in 2020 which is tremendous. Though several simple paradigms of smart cities based on IoT have been presented worldwide, it is severe to research how to immerse extremely complex IoT into the big cities properly to make a better use of the public resources, increasing the QoS offered to the citizens, while reducing the operational cost of the public administrations.

At present, the Internet of Things industry has penetrated into many fields such as construction, home, transportation, medical care and automobile. Besides, along with the development of science and technology, Internet of Things, which becomes increasing connected with architecture, plays an important role in smart homes, security and other areas, thus constituting a prominent feature in the development of the intelligent building industry. Intelligent Building, as a new product appearing in the late 1980s, comprehensively integrates and interlinks structure, system, service, operation to achieve the optimal combination, thereby acquiring an energy-saving, efficient, convenient and comfortable living and working environment. The first internationally-recognized smart building was born in Hartford, United States in January 1984, and its successors achieved rapid development worldwide. In China, intelligent build firstly appeared in 1990. With the development of its national economy and technological advancement, people have increasingly high requirement for housing; while intelligent building, through an organic combination of intelligent building and information technologies, provides people with an efficient, comfortable and convenient humanistic building environment. Meanwhile, intelligent building is also a major node on the future "information highway". Intelligent buildings implements optimal design relying on four basic elements, i.e. building structure, system, service and management, which involves the comprehensive application of various technologies such as computer technology, network communication technology, and monitoring technology. In particular, integrated cabling, equipment automation, system integration, intelligent communication network

*Corresponding Author: Ying-Si Zhao; E-mail: yszhao@bjtu.edu.cn
DOI: 10.3966/160792642018051903019

systems, access network environments, and 4C convergence (Computer, Communication, Consumer Electronics, and Content) have become the top priorities of smart buildings.

A complex sketch of smart city ecosystem is presented in [5]. It can be observed that an Intelligent Building is a relative independent and simple part of the whole city and it is natural to inelligentize the buidings first as the foundation of the smart cities. In addition, the Intelligent Buildings are of very clear return on investment and they indeed act as catalyzers of other added value services [6] in the smart cities. Therefore, perfectly integrating the IoT into a building is of great influence to the development of smart cities.

An Intelligent Building with smart meters, smart lamps, e-healthcare and quite many smart electric apparatus is presented. It can be observed that the whole network can be divided into two layers. The smart devices in a building comprise a small network whose responsibility is monitoring the locally building and all the small networks are the first layer. The fog computing servers among the Intelligent Buildings comprise a large network and this is the second layer. Different to the first layer, the second layer is the backbone of the whole network and it is responsible for transmitting and processing data from a higher level.

Though quite many research efforts have been made to seamlessly integrate the IoT with the cities, energy-efficiency and security problems of IoT serevely hinder the development of the smart cities. In this paper, we use the fog computing framework to make the Intelligent Buildings green and secure. Specifically, a fog computing server is employed by each building and most generated data are preprocessed locally before being outsourced to the external region of the buiding.

The main contributions of this study are presented as follows:

- We summarize the communication protocols in smart cities and emphasize the challenges in designing the routing algorithms for intra-building data.
- We propose a set of principles to divide the data of an Intelligent Building into different categories which greatly affects the behaviors of the fog computing servers.
- Based on the properties of the data, the tasks of the fog computing server are classified and properly scheduled to improve the QoS.
- Several basic services and possible approaches of the fog computing servers are discussed.
- Haven processed all the collected data, a secure and efficient scheme is proposed to store the valuable data which can be analyzed and mined to discover valuable rules and knowledge.

2 Taxonomy of the Generated Data

2.1 Data Category Priciples

Based on different principles, the generated data of various sources can be divided into different categories. In this paper, the designed principles are presented as follows:

Application region. The region where the data need to be further processed and used is defined as the application region of the data. Note that, the data are classified from the fog computing servers' view. This is reasonable considering that the fog computing servers are the main entities to process the data.

Priority level. The data of different services have totally different urgencies and the delays of the data lead to different damages. The priority level is employed to indicate the important degrees of the data and the data with a higher privacy level are more impotant. In general, the priority levels of the data are assigned by the network operators.

Confidentiallity. The condidentiallities of the data are defined by the data owners. If a data owner agrees to publish his data to the public, the data is public. Otherwise, the data are private and they can be accessed only by the data owner.

Potential. Whether the generated data can be widely analyzed and mined to discover valuable knowledge in the predictable future is defined as the potential of the data. Apparently, most useless data will be dropped to save storage space and energy.

2.2 Data Classification

Based on the application region of the data, the data can be classified into internal data and external data whose definitions are presented as follows:

Internal data. For a fog computing server S_i of an Intelligent Building B_i, the data processed and used in the building B_i is internal data for S_i.

External data. For a fog computing server S_j of an Intelligent Building B_j, the data processed and used outside the building B_j is internal data for S_j.

Based on the priority level of the data, the data can be classified into high priority data and low priority data whose definitions are presented as follows:

High priority. The data whose delays lead to great damages to the data owner or users are defined as high priority data.

Low priority. The data whose delays don't have obvious affection to the data owner or users are defined as high priority data.

Based on the confidentiallity of the data, the data can be classified into internal data, external data and processable data whose definitions are presented as follows:

Private data. The data which can be accessed by the data owner and authorized data users.
Public data. The data which can be accessed by all the publics without any limitations.

Based on the potential of the data, the data can be classified into internal data, external data and processable data whose definitions are presented as follows:

High potential. The data which will be widely employed in the predictable future by the researchers are of high potential.
Low potential. The data which will be ignored in the future are of low potential.

A summarization about the classification priciples and examples is presented in Table 1.

Table 1. Taxonomy of the intelligent building data

Principles	*Application region*		*Priority level*		*Confidentiality*		*Potential*	
Categories & examples	*Internal*	Lighting, home appliance	*High*	E-healthcare, disaster monitoring, emergency	*Private*	E-healthcare, smart control, home appliance	*High*	E-healthcare, smart metering
	External	Smart control, e-healthcare, disaster monitoring, emergency, smart metering	*Low*	Smart cotrol, smart home appliance, smart metering, smart lighting	*Public*	Smart metering, lighting, Disaster monitoring	*Low*	Smart cotrol, disaster monitoring, emergency, home appliance, lighting

3 Communication and Routing in Intelligent Buildings

3.1 Communication Protocols

IoT networks are data-centric and efficiently gathering the data to the fog computing server is the base of the whole framework. In different application scenarios, many communication protocals have been designed including 802.15.4, WiFi, Bluetooth, Ethernet, GPRS, 3G and 4G. For instance, the electronic appliances in a room can communicate with each other by Bluetooth; the smart lamps in a corridor can communicate with each other by ZigBee; and the mobile devices in a buiding can communicate with eath other by WiFi. As a consequence, to manage all the smart devices, the agent node needs to support all the possible communication protocols in an Intelligent Building. An alternative approach is employing a middleware between the end devices and the fog computing server.

The most important responsibility of IoT networks are collecting and processing data. Specifically, the main functionalities of the fog computing servers are transmitting the packages, analyzing and storing the collected data. Consequently, it is reasonable to divide the tasks of the fog computing servers into different categories based on the properties of the data. Based on the application regions, the package transmission tasks can be further divided into three types: transfer packages between other buildings, receiving packages for the devices in the building and transmitting the packages of the devices in the building to other buildings.

3.2 Intra-Building Routing

Another challenge is how to successfully deliver the packages generated by the smart devices to the agent node. In general, the agent node is deployed on the roof of the bulidings to conveniently commucate with external devices such as communication base stations and neighbor buildings. All the smart devices in a building comprise a 3-dementional wireless networks named smart buiding network (SBN). Though quite many routing algorithms for wireless sensor networks (WSNs) and ad-hoc networks, most of them cannot perfectly suit the SBNs because of the following reasons:

- The nodes in SBNs are randomly scattered in 3-dementional and traditional routing algorithms assume that the network is nearly deployed in a plane. Apparently, the network structures are totally different. As an example, location-based routing algorithm GPSR performs very well in plane networks, however, extending GPSR to the 3-dementisonal space is extremely difficult.
- The devices in SBNs are various. Some of them are static such as smart meters and home appliances and some others are dynamic such as the monitoring devices of the patients. As a conseqence, the topologies of the networks are very complicated which greatly improve the difficulties of data routing.
- The data in SBNs are of very differnet sources and priority levels and in traditional networks, all the packages are equal with each other. Though this difference doesn't greatly affect the routing process when the network is unoccupied, how to deliver the packages according to their priorities is a difficult problem when the workload is heavy.

3.3 Inter-Building Routing

Apparently, the Intelligent Buildings together comprise an Intelligent Building network which shares some similar properties with the static wireless sensor networks (WSNs). First, each building is static and they are wirelessly connected. Second, each building can communicate with its neighboring buildings considering the radio range of the fog computting server. Third, each building is capable of transmitting, storing and processing data. However, the fog computing servers are of much richer resources compared with the nodes in WSNs. As a consequence, most techniques designed for WSNs such as data routing, data aggregation, data fusion, data query and data collection can be directly employed to the SBNs. In conclusion, we should focus on the data routing and process techniques in a building rather than the techniques between the buildings.

4 Task Identifying and Scheduling

Except for directly delivering the packages to different destinations based on the address, the fog computing server is also responsible for processing the data and responsing the requests. For example, we may employ the smart cameras to monitor the public area to protect the people from being stolen, robbed or threated.

Although the tasks are very different with each other, we can simplify a task T_k to the vector (P_k, L_k), where P_k, L_k are the priority level and processing time of T_k, respectively. Then, we propose a new measurement to evaluate the performance of the task schedualing scheme. Assume that a set of tasks $\{T_1, T_2, ..., T_m\}$ are processed in order. The weighted average data processing delay WD of the tasks is defined as follows:

$$WD = \frac{(\sum_{i=1}^{m} L_i * D_i)}{m}, \quad \textbf{(1)}$$

where D_i can be calculated as follows:

$$D_i = \sum_{j=1}^{i} P_i. \quad \textbf{(2)}$$

Mathmatically, we need to minimize WD by properly arrange the processing order of the tasks in $\{T_1, T_2, ..., T_m\}$. Considering that m is a constant number, we just need to minimize $WD' = \sum_{i=1}^{m} L_i * D_i$. Assume that the ordered tasks are $(T_1', T_2', ..., T_m')$ and hence the corresponding WD' can be represented in the following form:

$$\begin{aligned} WD = {} & P_1' * (L_1' + L_2' + \cdots + L_m') + P_2' * (L_2' + \cdots + L_m') + \cdots \\ & + P_i' * (L_1' + \cdots + L_m') + P_{i+1}' * (L_{i+1}' + \cdots + L_m') \\ & + \cdots + P_m' * L_m' \end{aligned} \quad \textbf{(3)}$$

For each pair of contiguous tasks T_i' and T_{i+1}' in $(T_1', T_2', ..., T_m')$, we can switch their order and the updated WD'' can be represented as:

$$\begin{aligned} WD'' = {} & P_1' * (L_1' + L_2' + \cdots + L_m') + P_2' * (L_2' + \cdots + L_m') + \cdots \\ & + P_{i+1}' * (L_1' + \cdots + L_m') + P_i' * (L_{i+1}' + \cdots + L_m') \\ & + \cdots + P_m' * L_m' \end{aligned} \quad \textbf{(4)}$$

Then, $WD'' - WD'$ can be calculated as:

$$WD'' - WD' = P_{i+1}' * L_i' - P_i' * L_{i+1}' \quad \textbf{(5)}$$

Apparently, if $WD'' - WD' < 0$, i.e., $\frac{L_{i+1}'}{P_{i+1}'} > \frac{L_i'}{P_i'}$, we need to switch T_i' and T_{i+1}' to decrease WD. We continuously iterate the switch operation until the order of the tasks keep stable and the ordered tasks can be represented as $(T_1'', T_2'', ..., T_m'')$. In this casetab, it can be inferred that $\frac{L_1''}{P_1''} \geq \frac{L_2''}{P_2''} \geq \cdots \geq \frac{L_m''}{P_m''}$. We can prove that WD is minimized if the order keeps stable considering that switching any pair of tasks makes the order of the tasks unstable and it can be further optimized.

In practical, the tasks are pushed into a fog computing server dynamically. A fog computing server organizes the tasks in ordered based on $\frac{L_i}{P_i}$ to minimize WD. When a new task T_n arrives, we just need to insert the task in to the ordered tasks based on $\frac{L_n}{P_n}$.

5 Secure Data Storage and Efficient Data Retrieval

To save energy, each fog computing server S_i is responsible for analyzing and storing the data generated by the building B_i. The collected data in an Intelligent Building, in real life, are of different confidentialities. The public data can be accessed by all the data users in the building and conversely, the private data can be accessed by the data owner only. Based on the potential and confidentiality, the data need to be stored through different policies. Apparently, the useless data in the future can be directly dropped after a period. For the data which are of great potential and can be leaked to the public, they need to be outsourced to the cloud server where the data can stored properly.

To protect the document privacy, quite many

attribute-based document encryption schemes have been proposed in the literatures. Recently, hierarchical document encryption schemes have been widely researched and employed. In the following we discuss the general flowchart of these schemes. We first describe the system model of hierarchical attribute-based document encryption scheme as shown in Figure 1. The data owner first selects a set of content keys $ck = \{ck_1, ck_2, \cdots, ck_n\}$ which are used to encrypt the documents in F F symmetrically. Then, the content keys are hierarchically encrypted by the attributes assigned by the data owner. The encrypted documents, access structure and encrypted content keys are outsourced to the cloud server. In addition, the index structure of the document collection is also stored in the cloud server to support document search. Once the encrypted search results are sent to the data users, they decrypt the content keys by their secret keys and further decrypt the documents based on the decrypted content keys. In the following, we mainly discuss how to encrypt the content keys in detail.

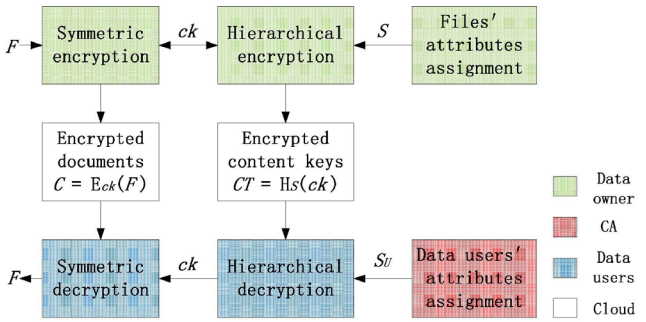

Figure 1. The flow chart of document encryption and decryption

Except for the the flow chart, some common conceptions including bilinear map and Lagrange interpolation are involved in most existing schemes scheme. Let $\mathbb{G}_0$ and $\mathbb{G}_1$ be two multiplicative cyclic groups of prime order p. Let g be a generator of $\mathbb{G}_0$ and e be a bilinear map, e: $\mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_1$ with the following properties:

(1) Bilinearity: For all $u, v \in \mathbb{G}_0$ and $a, b \in \mathbb{Z}_p$, , $e(u^a, v^b) = e(u, v)^{ab}$.

(2) Non-degeneracy: $e(g, g) \neq 1$.

(3) Distributivity: For $u, v, w \in \mathbb{G}_0$ and $a, b, c \in \mathbb{Z}_p$, $e(u^a, v^b, w^c) = e(u^a, v^b)e(u^a, w^b)$..

In addition, $\mathbb{G}_0$ is a bilinear group if the group operations in $\mathbb{G}_0$ and the bilinear map e: $\mathbb{G}_0 \times \mathbb{G}_0 \to \mathbb{G}_1$ are both efficiently computable. The Lagrange Coefficient $\Delta_{i,s}$ for $i \in \mathbb{Z}_p$ and a set, S, of elements in $\mathbb{Z}_p$ is defined as $\Delta_{i,s}(x) = \prod_{j \in S, j \neq 1} \frac{(x-j)}{(i-j)}$. In addition, a hash function $H: (0,1)^8 \to \mathbb{G}_0$ is employed to map the string attributes to a random group element in $\mathbb{G}_0$.

Another challenge is how to sotoring the private data which are accessed only by the internal data users. To improve the data access efficiency and decrease data transmission in the network, a good stretagy is stroing the data locally in the fog computing server. An accompanying challenge is how to improve the search efficiency without leaking the data to the fog computing server and the public. Privacy-preserving document search schemes [7-8] can inspire us to solve the above problem. As presented in our former work [9], the private data are first symmetrically encrypted before being outsourced to the fog computting server. Meanwhile, an index structure is constructed for the data which can be employed to search the interested data without knowing the plaintext of the data.

6 Data Publishing and Access Control Mechanism

Although the private data cannot be directly outsourced to the public, it is likely that the data owner may want to share the data with a set of data users with soecific properties. For example, a tumour patient should provide the personal health record (PHR) to his attending physician and in some case he is also glad to share his PHR with the tumour researchers. Apparently, this is of great significance to the medical science and it is accompanied with two challenges: publishing data without leaking private information and access control of the data users.

Apparently, data generated or collected by individulas and organizations are a key resource in today's information age. However, the disclosure of those data poses serious threats to individual privacy and a fundamental challenge is to balance privacy and utility in data sharing. The notation of k -anonymity [10] has been widely researched. A table satisfies k-anonymity relative to a set of quasi-identifier attributes if and only if when the table is projected to include only the quasi-identifier attributes, every record in the projected table appears at least k times. However, Researchers have observed that k -anonymity does not prevent attribute disclosure, i.e., information about sensitive attributes can still be learned, perhaps due to the uneven distribution of their values.

Over the last decade, differential privacy (DP) has emerged as an important standard privacy notion for research in privacy-preserving data publishing. The DP notion offers strong privacy guarantee and has been applied to many data analysis tasks. A survey of the field from a theoretical point of view is given in [11]. In the DP schemes, the key problem is how to define the "ideal worlds" for privacy. One natural choice is to accept the "privacy as control" conception, and define the ideal worlds to be the ones where "control over personal data" is exercised. Interestingly, instead of

having one ideal world, we have many ideal worlds, one for each individual, in which the individual's data is removed.

Another challenge is designing the access control mechanism. Fortunately, many attribute-based encryption (ABE) schemes have been designed. Key-policy ABE (KP-ABE) schemes and cipher-policy ABE (CP-ABE) schemes are two important branches of existing ABE schemes. It has been widely accepted that CP-ABE schemes are more flexible and suitable for general applications and many varieties of CP-ABE schemes have been proposed in the literatures [12-14]. However, most existing schemes are designed for cloud computing and assume that the cloud server is of great computing capability. Considering that the fog server is much weaker than the cloud server, it is severe to propose light-weight ABE schemes for the IoT framework. Moreover, combing the fog computing and cloud computing [15-17] to further improve the QoS of the networks is also a challenge.

7 Conclusion and Future Work

In this paper, we describe an IoT framework for green Intelligent Buildings and focus on designing the universal model to schedule the tasks based on different properties. A new delay measurement is proposed in which the priorities of the transmitted packages are taken into consideration. Then, we propose an algorithm to minimize the delay measurement. How to securely store the private data in the fog computing server while maintain the searchability is also detailedly discussed. In addition, some difficulties and open issues in the field of SBNs are also presented. Specifically, designing light-weight data routing algorithms and integrating the artificial intelligence into SBNs are very promising and challenging.

Acknowledgements

This work was supported by the Fundamental Funds for Humanities and Social Sciences of Beijing Jiaotong University (2015jbwj009).

References

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of Things for Smart Cities, *IEEE Internet of Things Journal*, Vol. 1, No. 1, pp. 22-32, February, 2014

[2] R. Morello, C. D. Capua, G. Fulco, S. C. Mukhopadhyay, A Smart Power Meter to Monitor Energy Flow in Smart Grids: The Role of Advanced Sensing and IoT in the Electric Grid of the Future, *IEEE Sensors Journal*, Vol. 17, No. 23, pp. 7828-7837, December, 2017.

[3] J. Ni, K. Zhang, K. Alharbi, X. Lin, N. Zhang, X. S. Shen, Differentially Private Smart Metering with Fault Tolerance and Range-based Filtering, *IEEE Transactions on Smart Grid*, Vol. 8, No. 5, pp. 2483 - 2493, September, 2017.

[4] P. Papadimitratos, A. De La Fortelle, K. Evenssen, R. Brignolo, S. Cosenza, Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation, *IEEE Communications Magazine*, Vol. 47, No. 11, pp. 84-95, November, 2009.

[5] Y. Mehmood, F. Ahmad, I. Yaqoob, A. Adnane, M. Imran, S. Guizani, Internet-of-things-based Smart Cities: Recent Advances and Challenges, *IEEE Communications Magazine*, Vol. 55, No. 9, pp. 16-24, September, 2017.

[6] C. E. A. Mulligan, M. Olsson, *Architectural Implications of Smart City Business Models: An Evolutionary Perspective, IEEE Communications Magazine*, Vol. 51, No. 6, pp. 80-85, June, 2013.

[7] N. Cao, C. Wang, M. Li, K. Ren, W. Lou, Privacy-preserving Multi-keyword Ranked Search over Encrypted Cloud Data, *IEEE Transactions on Parallel & Distributed Systems*, Vol. 25, No. 1, pp. 222-233, January, 2014.

[8] Z. Xia, X. Wang, X. Sun, Q. Wang, A Secure and Dynamic Multi-keyword Ranked Search Scheme over Encrypted Cloud Data, *IEEE Transactions on Parallel & Distributed Systems*, Vol. 27, No. 2, pp. 340-352, February, 2016.

[9] J-S. Fu, Y. Liu, H-C. Chao, B. K. Bhargava, Z.-J. Zhang, Secure Data Storage and Searching for Industrial Iot by Integrating Fog Computing and Cloud Computing, *IEEE Transactions on Industrial Informatics*, doi:10.1109/TII. 2018.2793350, January, 2018.

[10] L. Sweeney, K-anonymity: A Model for Protecting Privacy, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 10, No. 5, pp. 557-570, October, 2002.

[11] C. Dwork, A. Roth, *The Algorithmic Foundations of Differential Privacy*, Now Publishers, 2014.

[12] J. Bethencourt, A. Sahai, B. Waters, Ciphertext-Policy Attribute-Based Encryption, *IEEE Symposium on Security and Privacy, Berkeley*, California, America, 2007, pp. 321-334.

[13] B. Waters, Ciphertext-policy Attribute-based Encryption: An Expressive, Efficient, and Provably Secure Realization, in: D. Catalano, N. Fazio, R. Gennaro, A. Nicolosi (Eds.), Public Key Cryptography– PKC 2011, PKC 2011, *Lecture Notes in Computer Science*, Vol. 6571, Springer, 2011, pp. 57-70.

[14] V. Goyal, A. Jain, O. Pandey, A. Sahai, Bounded Ciphertext Policy Attribute Based Encryption, *35th International Colloquium on Automata, Languages and Programming*, Reykjavik, Iceland, 2008, pp. 579-591.

[15] W. Zhang, Z. Zhang, H.-C. Chao, Cooperative Fog Computing for Dealing with Big Data in the Internet of Vehicles: Architecture and Hierarchical Resource Management, *IEEE Communications Magazine*, Vol. 55, No. 12, pp. 60-67, December, 2017.

[16] H. Gao, C. H. Liu, W. Wang, J. Zhao, Z. Song, X. Su, J. Crowcroft, K. K. Leung, A Survey of Incentive Mechanisms for Participatory Sensing, *IEEE Communications Surveys &*

Tutorials, Vol. 17, No. 2, pp. 918-943, January, 2015.

[17] Z.-J. Zhang, C.-F. Lai, H.-C. Chao, A Green Data Transmission Mechanism for Wireless Multimedia Sensor Networks Using Information Fusion, *IEEE Wireless Communications*, Vol. 21, No. 4, pp. 14-19, August, 2014.

Biographies

Ying-Si Zhao was received the B.S. and M.S. degrees in communication engineering from Beijing Jiaotong University, Beijing, in 2007 and 2009, and the Ph.D. Degree in Management from Beijing Jiaotong University, Beijing, CHINA, in 2014. Since 2014, she has been a teacher with the Business Administration Department, Beijing Jiaotong University, School of Economics and Management. Her research interests mainly include Marketing, Innovation & Entrepreneurship, Cloud Computing & its Applications, Network Public Opinion and so on.

Han-Chieh Chao is a Chair Professor of the Department Computer Science & Information Engineering and Electronic Engineering of National Ilan University, I-Lan, Taiwan (NIU). He was serving as the President since August 2010 to January 2016 for NIU as well. Now, he is serving at National Dong Hwa University, Hualien, Taiwan also as the President. He was the Director of the Computer Center for Ministry of Education Taiwan from September 2008 to July 2010. His research interests include High Speed Networks, Wireless Networks, IPv6 based Networks, Digital Creative Arts, e-Government and Digital Divide. He received his MS and Ph.D. degrees in Electrical Engineering from Purdue University in 1989 and 1993 respectively. He has authored or co-authored 4 books and has published about 400 refereed professional research papers. He has completed more than 100 MSEE thesis students and 4 PhD students.
Dr. Chao has been invited frequently to give talks at national and international conferences and research organizations. Dr. Chao is the Editor-in-Chief for Journal of Internet Technology, and IET Networks. Dr. Chao has served as the guest editors for Mobile Networking and Applications (ACM MONET), IEEE JSAC, IEEE Communications Magazine, IEEE Systems Journal, Computer Communications, IEE Proceedings Communications, the Computer Journal, Telecommunication Systems, Wireless Personal Communications, and Wireless Communications & Mobile Computing. Dr. Chao is an IEEE senior member and a Fellow of IET (IEE).