



Secure Data Access Control with Scattered Forecast Algorithm Based on Exponential Back off Rules Using Internet of Things Environment

Dr.P.Srimanchari¹, Dr.G.Anandharaj²

¹Associate Professor and Head, Department of Computer Applications,
Erode Arts and Science College, Erode, Tamil Nadu – 638001, INDIA.

²Associate Professor and Head, Department of Computer Science,
Adhiparasakthi College of Arts and Science (Autonomous), Kalavai, Vellore, Tamil Nadu – 632506, INDIA.

Abstract: Attribute-based cryptography is a well-known technology to guarantee data confidentiality and fine grained data access control. However, its computational cost in encryption and decryption phase is linear with the complexity of policy. In this paper, we propose a secure and fine grained data access control scheme with cipher text update and computation outsourcing in fog computing for IoT. The sensitive data of data owner are first encrypted using attribute-based encryption with multiple policies and then outsourced to cloud storage. Hence, the user whose attributes satisfy the access policy can decrypt the ciphertext. Based on the attribute-based signature technique, authorized user whose attributes integrated in the signature satisfies the update policy can renew the ciphertext. Specifically, most of the encryption, decryption, and signing computations are outsourced from end devices to fog nodes, and thus, the computations for data owners to encrypt, end users to decrypt, re-encrypt, and sign are irrelevant to the number of attributes in the policies. We measure various metrics such as average residual energy, percentage of composite events processed successfully at the sink, and the average number of hops to reach the sink. Scheduling algorithm based on exponential backoff rule and energy-topology factor, namely EB-ET-distributed randomized (DRAND) algorithm. We analyze the typical DRAND time slot assignment algorithm and the distributed TDMA slot scheduling algorithm based on energy-topology factor, which is proposed in our another work. Then, we introduce the implementation processes of the EB-ET-DRAND scheduling algorithm in various different states. The time slot structure and frame formats of algorithm are designed in detail. Finally, we implement a mesh network simulation system to evaluate the performance of proposed scheme. The experimental results indicate that the EB-ET-DRAND scheduling algorithm greatly improves the performance of time slot allocation and reduces the message complexity, time complexity, and energy consumption.

Keywords: Cryptography, Data access control, Ciphertext, Energy-topology factor.

1. Introduction

The development of Internet of Things (IoT), Cyber Physical System (CPS) and Wireless Sensor Network (WSN) greatly promoted the interconnection and intercommunication of all kinds of things [1], [2]. Physical space is connected into information space by various sensing technologies [3]. The energy supplies of the WSN nodes come from the batteries carried by the nodes, which are not suitable for charging or replacement for cost and ease of use. The energy of the network node is mainly consumed in the data communication module [4]. Therefore, how to improve the communication efficiency and reduce the working time of the communication module can effectively improve the life of network node [5]. The traditional wireless communication protocol cannot be adopted, and the protocol needs to be redesigned. If node wants to access the channel, it needs to be deployed through the Media Access Control (MAC) protocol [6].

In this work, we analyze the DRAND algorithm and E-T-DRAND algorithm in detail. On this basis, by introducing the idea of Lamport's bakery algorithm, we propose the distributed TDMA scheduling algorithm based on exponential backoff rule and energy-topology factor, namely EB-ET-DRAND algorithm. And the priority control algorithm of the EB-ET-DRAND based on exponential backoff rule and energy-topology factor are presented to appropriately adjust the priority of time slot allocation. In addition, we introduce the implementation process of EB-ET-DRAND scheduling algorithm in various different states. The time slot structure and frame formats of algorithm are designed. Although the great benefits brought by fog computing paradigm, security problems including data confidentiality and access control are similar to that in the area of cloud computing and IoT. Moreover, they are more easily compromised and low-trustworthy since fog nodes are deployed at the

network edge and much lower cost than cloud servers [7]. One promising approach to solving such problems is to encrypt data in advance before the upload. The concept of attribute-based encryption (ABE) is a one-to-many cryptographic technique that fulfills these requirements [8]. It features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among private keys and ciphertexts. Especially, the ciphertext-policy ABE (CP-ABE) enables data owner to. Thus, the key point of secure ciphertext update is that the user who renews the ciphertext should be able to prove to the cloud service provider (CSP) that he is a valid user.

The traditional approach is to sign the modified data, which means CSP must simultaneously maintain a public key list of valid users to verify the identities of users. However, it would bring a lot of extra burden to maintain the key list if existing a large number of users, and CSP can know identities of users in this way, which discloses the user privacy. A novel cryptographic technique known as attribute-based signature (ABS) is able to help CSP to verify whether the user is valid [9]–[11]. In an ABS system, user can sign messages with a claim policy and his attributes. Then, with the signature, the CSP can check whether the signer's attributes satisfy the claim policy while remaining completely ignorant of the identity of signer. Therefore, adopting ABE and ABS can achieve data confidentiality, fine-grained access control and user verification, but it also brings high computational cost at the same time in fog computing [12]. The encryption, decryption and signing operations of ABE and ABS require a large number of module exponentiations, which commonly grow linearly with the number of attributes in policies. This presents a significant challenge for users who access and modify data on resource-constrained IoT devices with limited computation and storage capacity.

II. Related Works

The concept of fog computing is proposed by Cisco in 2014, which can be regarded as a layer in the middle of the cloud and end users consisted by fog nodes, such as hardened routers, switches, and etc. [13]. They are much closer to end users than cloud servers, and some of the workloads and services taken in the cloud are moved to the fog nodes. Similar to the cloud servers, fog nodes are not fully trusted as well, data security would raise great concerns from users when they store sensitive data on cloud servers through fog nodes [14]. Thus, a new access control scheme with cloud, fog and users should be considered, since the network structures and system models are different, in which fog nodes should assist user, to make less computational complexity and more flexibility left for users.

The centralized allocation methods mean that there is a central controller in the network, which is responsible for the calculation of the resource allocation scheme of the whole network. It needs to know the information of the whole network and distribute the allocation scheme to every node. The results generated by the centralized allocation of the entire network close to the optimal. But it is not suitable for the frequent changes of network topology. The frequent calculation and distribution of allocation scheme greatly increase additional cost. In the centralized allocation algorithm, graph coloring is used as a common method. However, there are many deficiencies in the case of multi-channel using this scheme, for example, interface constraints, bandwidth constraints, etc. Raniwala *et al.* [28] proposed the Load-Aware Channel Assignment (LACA) method which was a multi-channel heuristic allocation algorithm with multiple constraints. It increases the actual network throughput by restricting the number of channels, the requirements of network traffic and the number of interfaces. The LACA is based on the changes of network load so that it can be applied to multi-channel occasions. According to the estimated network load, the communication links are grouped according to the conflict relation, and then the communication resources are allocated to the nodes in the network. In the scheduling process, LACA algorithm constantly adjusts the channel resource scheduling program according to the network traffic. Because it is a centralized scheme, the algorithm was suitable for static networks. For the distributed resource allocation methods, every node determines the occupancy of time slots and channels according to their own local information to generate allocation strategy in a distributed manner. The distributed allocation method is more suitable for dynamic networks, but the performance of the scheme may be lower than that of centralized allocation. The distributed resource allocation method can arrange the resources reasonably according to the demand, so the wireless channel resources can be used efficiently and the time slots can be multiplexed as much as possible. The dynamic TDMA protocol has a special control frame structure, so the control part and the data part do not interfere with each other. Some researchers have proposed many distributed time slot allocation schemes. The DRAND and DSA-AGGR algorithms are the typical distributed time slot allocation scheme. Based on the centralized randomized time slot scheduling scheme (RAND) [29], Rhee *et al.* [25] proposed the DRAND scheme which was a distributed randomized time slot scheduling algorithm. It implements the RAND algorithm in a distributed way. In this algorithm, the time slot sequence is allocated by coordinating requests among network nodes. It can solve the conflicting node requests to assign the slot sequence of the TDMA. However, the time slot allocation with completely randomness decrease the efficiency, and also result in the high collision rate of the message and the low energy efficiency. The algorithm is suitable for the network with limited mobility which most nodes do not move. Sato and Sakata [30] proposed a distributed TDMA slot scheduling algorithm with prioritized control based on Lamport's bakery algorithm. It can constitute a localized network by measuring the distance to

respective node. This distance measurement-oriented scheme is shown as a possible replacement of DRAND scheduling algorithm. It improves the efficiency of TDMA slot allocation and reduces the time consumption on slot allocation, but increases the number of message required to allocate time slots.

III. Event Model Description

A WSN event is defined as an observable occurrence of a phenomenon or an object during a period of time in a specific area[3]. We distinguish two types of events: *atomic events* and *composite events*.

An atomic event is triggered when a single sensing value (or attribute) exceeds a given threshold. Similar to Ref. [30], we denote an atomic event by $e.t; s; R$ where t is the time when the event occurs and it can be a specific time or an interval, s is the location of the event and it can be a point or a region, and R is a logical expression defining the conditions when the event occurs.

Distributed Algorithms for CEDR in Mobile-Sink WSNs: In this work we assume that only one composite event is requested by the sink at a time. An energy-efficient mechanism to aggregate data or events is using clustering. There are several approaches proposed in literature for clustering in WSNs[9, 13–15, 17]. We distinguish *fixed clustering* and *event-based clustering*.

CEDR for fixed clustering

In this case we assume that the clusters are fixed and they are constructed after the network is deployed, that means before Phase 1 begins. Therefore, in this case, the clustering does not account for the type of event to be monitored. The area is divided into a grid. The grid cell size is at most $R_c = p_5$. In this way any two nodes from neighboring horizontal or vertical cells can communicate directly. The nodes in each grid cell form a cluster. We assume that the network is dense, so that each grid cell has at least one sensor node. Then the nodes are aware of their location. After the nodes are deployed, they can compute their grid cell based on their location. The CH is the node with the largest residual energy and in case of a tie, the one with the smallest ID becomes the CH. After deployment, nodes send a *Hello* message containing their ID, location, and residual energy. The CH node, selected as specified previously, sends a message *JoinCluster* and all the nodes in the cluster reply with an *ACK* message containing their ID. To communicate with the sink within communication range of at least one CH

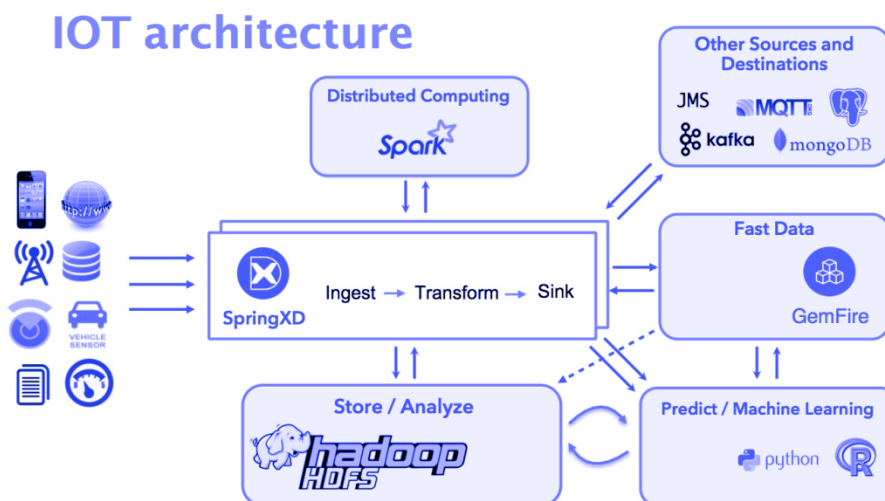


Figure 3.1 IoT Architecture

IV. Communication protocols

We could identify three interaction models of communication between data producers and data consumers in the context of Web applications. The first model is request-reply interaction, which is also referred to as *pull-based data access*, or *synchronous data delivery*, and is typical for a service-oriented architecture. This model assumes that clients issue requests or queries to a service provider for specific data, and the service provider replies with appropriate data. IoT application developers are able to choose one of the following approaches:

Representational State Transfer (REST) _ is an architectural style in which a client issues the standard HTTP request, choosing one of the methods such as GET, POST, PUT, and DELETE, and a server responds with appropriate data. The REST architectural style denotes interaction between a client and a server based on resources that are accessed using the HTTP protocol, addressed by URI, and represented by XML, HTML, or JSON formats. **Standard Web Service** _ a Web service aims to provide communication interoperability among different software platforms where the interface is described by Web Services Description Language (WSDL), and messages

are exchanged through the Simple Object Access Protocol(SOAP),² which is based on the HTTP protocol and XMLdata format. However, the standard Web service can be usedonly from the browser's plug-ins, and not from the standardHTML-JavaScript based platform.

*Remote Object Method Call*_this method is available invarious Web frameworks Application Programming Interfaces(API), and is based on the standard HTTP request.The idea is to provide a proxy object with certain methodson the client side, which represents the remote object.Invocation of a method of a proxy object is propagated tothe remote object. The common approach is that the clientprovides a callback object/function that is called when theoperation is completed.

Protocol	Description
ZCL	“ZigBee Cluster Library”. A set of application layer protocols for how devices like lights, sensors, and switches can communicate with each other.
ZigBee Pro	Mesh networking specification that specifies security, routing, and provisioning. The name comes from “Zig Zag Bumble Bee” due to the fact that the path of a bee and the path of a message in a mesh network can be similar.
ZigBee 3	Upcoming update to the ZigBee Pro specification.
802.15.4	Physical layer protocol designed for use by resource constrained devices. Focus is on allowing battery powered devices to have a long battery life by making the most common action take less energy. The name comes from an IEEE working group.
HTTP	“Hyper Text Transfer Language”. The (application layer) language of the World Wide Web. This enables quick and easy data transfer using URLs to specify locations of resources.
IP	“Internet Protocol”. Routing layer for the World Wide Web and most in-home computer networks.
WiFi AKA 802.11	Physical layer standard that allows devices to exchange data over wireless links. The “802.11” name comes from an IEEE working group.
Ethernet AKA 802.3	Physical layer standard that allows devices to exchange data over wired Ethernet connections.
dotdot	This is the ZCL application layer protocol modified to run over IP networks.
Thread 1.1	Mesh networking specification that specifies security, routing, and provisioning. Thread gives a method for mapping the protocols of low-power-devices to IP networks.
Thread 2.0	Upcoming update to the Thread 1.1 specification. This is targeted at commercial applications, and adds other new features.
GAP	Bluetooth Generic Access Profile. This describes how two Bluetooth devices can find and communicate with each other.
GATT	Application profile for Bluetooth devices. This specifies how specific information is exchanged.
Bluetooth Mesh Stack	In-development mesh networking specification that specifies security, routing, and provisioning for mesh on Bluetooth networks.
Bluetooth PHY	The physical layer that supports the Bluetooth stack and profiles.

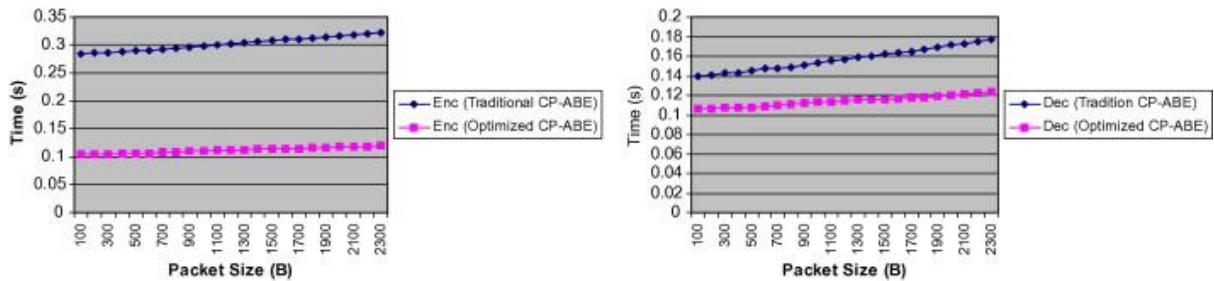
V. V. Simulation

We conducted simulations using WSN_{et}, an opensource event-based simulator for WSNs. WSN_{et} was developed by the Center of Innovation in Telecommunication CITI Laboratory associated with INSA Lyon France. WSN_{et} uses object-oriented C++ language, Linux operating system, and provides a platform where new modules can be developed. In addition, it provides support for energy model and event modeling, features which are important in WSNs.

A. Simulation environment

The WSN is deployed into a square area A, where the square length A.L takes values between 440m and 1100 m. The values have been selected such that the area can be divided into a grid, with cell size of 44 m. In this way, any sensors in horizontally or vertically adjacent cells can communicate directly. This feature is useful for our grid-based algorithms.

The number of attributes used in the experiments is from 5 to 50, and the experimental result is the average number of 10 runs. We consider this range to be representative enough for a wide range of real world IoT applications. First, we analyze the time cost of the data encryption and decryption by comparing our scheme with Zuo et al. and Zhang et al. In data encryption phase, a data owner encrypts with an access policy and an update policy, and posts the encrypted to the public cloud through fog nodes. We can see the encryption time of our scheme and Zhang et al. is constant since most of the laborious decryption operations are delegated to the fog nodes, while it versus the number of attributes in access policy in Zuo et al. The decryption time on users versus the number of users' attributes. Specifically, in Zuo et al., Zhang et al. and our scheme, the heavy computation operations of decryption are outsourced to external server, such as cloud servers and fog nodes, thus the computation operations for users to decrypt in these schemes are irrelevant to the number of attributes in the access policy. The time complexity on users of cipher text update which mainly refers to signing algorithms in both our scheme and Su et al.



(a) Encryption Time comparison between Traditional and Optimized CP-ABE for Subgroup Communication.

(b) Decryption Time comparison between Traditional and Optimized CP-ABE for Subgroup Communication.

Concerning on the local computation performed by the signer, our scheme achieves much nearly constant performance compared with the linear increasing efficiency of the scheme of Su et al. by outsourcing many computations to fog nodes. This advantage allows our scheme to be applied for the resource-constrained IoT devices to complete the signing task. Moreover, we consider that the IoT device has limited storage ability. Since the outsourcing key can be firstly generated by attribute authority and then sent to the fog nodes. Therefore, the user only needs to store a small-sized component D locally but still maintaining encryption, decryption and signing capability. We argue that such amount is acceptable for IoT devices such as Samsung phone used in our experiments. In summary, the experimental results show that our scheme incurs less computational cost on the encryption of data owner, the decryption and signing of user, which ensures both grain data access control and efficient cipher text update in fog computing. Hence, our scheme could be applied to smart healthcare, vehicular cloud computing, and etc.

VI. Conclusion

In this paper, we propose a secure data access control scheme in fog computing for IoT based on CP-ABE and ABS. These sensitive data of users are first encrypted with both access policy and update policy, and then outsourced to cloud server through fog nodes. Thus, the users whose attributes satisfy the access policy can decrypt the ciphertext. In order to address the issue of data modification, the CSP will check the signature, to ensure that only the users whose attributes satisfy the update policy can renew the ciphertext. Hence, our scheme achieves both fine-grained data access control and secure ciphertext update. Moreover, our scheme presents an outsourced encryption, decryption and signing construction by delegating most of the operations to fog nodes. The extensive performance analysis and experiments are conducted, and the results indicate our scheme can well tolerate the increasing number of attributes, which is suitable for the resource-constrained IoT devices in fog computing.

References

- [1] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787-2805, Oct. 2010.
- [2] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497-1516, Sep. 2012.
- [3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347-2376, 4th Quart., 2015.
- [4] Z. Babovic and V. Milutinovic, "Novel system architectures for semantic based integration of sensor networks," *Adv. Comput.*, vol. 90, pp. 91-183, Dec. 2013.
- [5] J. Åkerberg, M. M. Gidlund, and M. Björkman, "Future research challenges in wireless sensor and actuator networks targeting industrial automation," in *Proc. 9th IEEE Int. Conf. Ind. Inform. (INDIN)*, Jul. 2011, pp. 410-415.
- [6] R. van der Meulen. (Nov. 2015). *Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015*, accessed on Jul. 20, 2016.
- [7] (Nov. 2015). *Ericsson Mobility Report*, accessed on Jul. 20, 2016. [Online]. Available: <http://www.ericsson.com/res/docs/2015/mobilityreport/ericsson-mobility-report-nov-2015.pdf>

- [8] M. Asay. (Jun. 2014). *The Internet of Things Will Need Millions of Developers By 2020*, accessed on Jul. 20, 2016. [Online]. Available: <http://readwrite.com/2014/06/27/internet-of-things-developers-jobsopportunity>
- [9] COMET, accessed on Jul. 20, 2016. [Online]. Available: <http://infrequently.org/2006/03/comet-low-latency-data-for-the-browser>
- [10] I. Fette and A. Melnikov, "TheWebSocket protocol," IETF Internet Draft, Work in Progress, Dec. 2011.
- [11] (Jul. 20, 2016). *HTML Canvas 2D Context*. [Online]. Available: <http://www.w3.org/TR/2dcontext/>
- [12] Z. Shelby, K. Hartke, and C. Bormann, *The Constrained Application Protocol (CoAP)*, document RFC 7252, Jun. 2014, accessed on Jul. 20, 2016. [Online]. Available: <https://tools.ietf.org/html/rfc7252> [13] C. Gutwin, M. Lippold, and T. C. N. Graham, "Real-time groupware in the browser: Testing the performance of Web-based networking," in *Proc. ACM Conf. Comput. Supported Cooperat. Work*, 2011, pp. 167_176.
- [13] K. Poulsen. (2003). *Slammer Worm Crashed Ohio Nuke Plant Network*. [Online] Available: <http://www.securityfocus.com/news/6767/>
- [14] B. Miller and D. Rowe, "A survey SCADA criticalinfrastructure incidents," in *Proc. Annu. Conf. Res. Inf. Tech.*, Oct. 2012, pp. 51_56.
- [15] J. M. McCune et al., "TrustVisor: Efficient TCB reduction and attestation," in *Proc. IEEE Symp. Security Privacy (SP)*, May 2010, vol. 41, no. 3, pp. 143_158.
- [16] F. McKeen et al., "Innovative instructions and software model for isolated execution," in *Proc. Hardw. Archit. Support Secur. Privacy (HASP)*, Jun. 2013, Art. no. 10.
- [17] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294_1312, 1st Quart., 2015.
- [18] T. R. Gruber, "A translational approach to portable ontologies," *Knowl. Acquisition*, vol. 5, no. 2, pp. 199_220, Jun. 1993.
- [19] W. N. Borst, "Construction of engineering ontologies for knowledge sharing and reuse," *Univ. Twente.*, vol. 18, no. 1, pp. 44_57, Jan. 1997.
- [20] R. Studer, V. R. Benjamins, and D. Fensel, "Knowledge engineering: Principles and methods," *Data Knowl. Eng.*, vol. 25, nos. 1_2, pp. 161_197, 1998.
- [21] E. D. Simmonet et al., "A vision of cyber-physical cloud computing for smart networked systems," Nat. Inst. Standards Technol. (NIST), Tech. Rep. 7951, 2013.
- [22] I. Butun, M. Erol-Kantarci, B. Kantarci, and H. Song, "Cloud-centric multi-level authentication as a service for secure public safety device networks," *IEEE Commun. Mag.*, vol. 54, no. 4, Apr. 2016.
- [23] H. Song, G. Fink, S. Jeschke, and G. Rosner, *Security and Privacy in Cyber-Physical Systems: Foundations and Applications*. Chichester, U.K.: Wiley, 2016. G. A. Shah, V. C. Gungor, and O. B. Akan, "A cross-layer QoS-aware communication framework in cognitive radio sensor networks for smart grid applications," *IEEE Trans. Ind. Informat.*, vol. 9, no. 3, pp. 1477_1485, Aug. 2013.
- [25] J. Ren, Y. Zhang, Q. Ye, K. Yang, K. Zhang, and X. S. Shen, "Exploiting secure and energy-efficient collaborative spectrum sensing for cognitive radio sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6813_6827, Oct. 2016.
- [26] M. Monemian and M. Mahdavi, "Analysis of a new energy-based sensor selection method for cooperative spectrum sensing in cognitive radio networks," *IEEE Sensors J.*, vol. 14, no. 9, pp. 3021_3032, Sep. 2014.
- [27] M. Najimi, A. Ebrahimzadeh, S. M. H. Andargoli, and A. Fallahi, "Energy-efficient sensor selection for cooperative spectrum sensing in the lack or partial information," *IEEE Sensors J.*, vol. 15, no. 7, pp. 3807_3818, Jul. 2015.
- [28] M. Najimi, A. Ebrahimzadeh, S. M. H. Andargoli, and A. Fallahi, "A novel sensing nodes and decision node selection method for energy efficiency of cooperative spectrum sensing in cognitive sensor networks," *IEEE Sensors J.*, vol. 13, no. 5, pp. 1610_1621, May 2013.
- [29] S. Maleki, A. Pandharipande, and G. Leus, "Energy-efficient distributed spectrum sensing for cognitive sensor networks," *IEEE Sensors J.*, vol. 11, no. 3, pp. 565_573, Mar. 2011.
- [30] J. Ren, Y. Zhang, R. Deng, N. Zhang, D. Zhang, and X. Shen, "Joint channel access and sampling rate control in energy harvesting cognitive radio sensor networks," *IEEE Trans. Emerg. Topics Comput.*, to be published.
- [31] M. Ozger, E. Fadel, and O. B. Akan, "Event-to-sink spectrum-aware clustering in mobile cognitive radio sensor networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 9, pp. 2221_2233, Sep. 2016.