International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-8)

Research Article | **August 2017**

Reliable and Multicast Energy Efficiency Harvesting through IoT

Dr. M.Sughasiny
Assistant professor& Research Supervisor, PG& Research Department of Computer Science, Bharathidasan University, Trichy, Tamil Nadu, India

R. Sakthivel
Research Scholar, PG& Research Department of Computer Science, Bharathidasan University, Trichy, Tamil Nadu, India

Abstract-

A smart city is acondition where a pervasive, multi-service network is occupied to affordpeoplebetter-qualityactive conditions as well as better public safety. Innovative communication technologies are needed to scope this goal. In specific, awell-organized and reliable broadcast network the stage a crucial role in as long as continue, ubiquitous, and reliable interconnections among users, smart devices, and applications. As aimportance, wireless networking appears as the main enabling announcement technology despite the necessity to face severe experimentations to satisfy the wants arising from a smart environment, such as explosive data volume, heterogeneous data traffic, and maintenance of quality of service restraints. Astimulating approach for meeting the developing data demand due to smart city applications is to adopt suitable methodologies to improve the usage of all potential spectrum resources. Towards this goal, a very promising solution is characterized by the Cognitive Radio technology that enables context-aware competence in order to pursue an efficient use of the accessibleannouncement resources according to the neighboring environment conditions. This thesis provides a review of the features, challenges, and solutions of a smart city message architecture, based on the Cognitive Radio technology, by focusing on two new network paradigms—namely, Heterogeneous Network and Machines-to-Machines communications—that are of differentattention to professionallyprovision smart city applications and services.

Keywords- Communication Technology, Data Traffic, Smart City, Energy Efficiency, Cognitive Radio Technology.

I. INTRODUCTION

The worldwide improvement process represents a formidable challenge and attracts respect toward cities. In particular, in the near future, the quality of life of billions of people will depend on capability of cities of saving energy, reducing harmful emissions, improving the quick conditions and cumulative citizen's security. These experimentsessential to be addressed through the application of Information and Communication Technology (ICT) intelligent clarifications in the urban ecosystem. Certainly, the smart city concept is based on functional combination of software systems, network infrastructures, heterogeneous consumer devices, and collaboration technologies. Involved by the fact that a reliable, robust, secure, and scalable communication architecture acting a fundamental role for the effective operation of a smart situation, this project provides ainstantaneous of the communication infrastructure of a smart city and the associatedauthorizing technologies.

A wireless sensor network (WSN) is a network formed by anenormous number of sensor nodes where every node is prepared with a sensor to recognize physical phenomena such as light, heat, pressure, etc. WSNs are observed as a revolutionary information collecting method to build the data and communication system which will significantlyrecover the reliability and efficiency of infrastructure systems. Associated with the wired solution, WSNs feature easier deployment and better flexibility of devices. With the rapid technological development of sensors, WSNs will become the key technology for IoT.

A smart city is asurroundings where a pervasive, multi-service network is employed to provide citizens improved living conditions as well as better community safety and security. Progressive communication technologies are essential to achieve this goalmouth. In specific, an efficient and reliable communication network plays anessential role in if continue, ubiquitous, and reliable interconnections among users, smart devices, and applications. As a consequence, wireless networking appears as the principal enabling communication technology despite the necessity to face severe challenges to fulfill the essentials arising from a smart environment, such as explosive data volume, heterogeneous data traffic, and sustenance of quality of service controls. Astimulatingmethod for meeting the rising data request due to smart city applications is to adopt suitable methodologies to improve the procedure of all potential spectrum possessions.

1.1. Objectives

The communication infrastructure of a smart city essential be appropriatelyconsidered to satisfy the explicitsupplies and requirements of the considered environment. In exact, it has to sustenanceelementary functionalities such as sensing, transmission, and controller. Sensing is approved out by a huge number of sensors and smart devices (even people can be

sensors) that monitor the environment; this data is transferred to a control center that performs data elaboration, thus providing control instructions that are delivered to sensors/actuators. A simplerepresentative of a smart city is that it is self-possessed of numerous heterogeneous devices that are associated regardless of their locations in an independent and scalable way accommodating with the Internet of Things (IoT) paradigm.

II. LITERATURE SURVEY

M2M devices may connect to a core network through two approaches [10]. One method is through an infrastructure-based admittance network, implemented by equipping the M2M devices with cellular connectivity, called Cellular M2M. The other method, called Capillary M2M, is infrastructure-less and is implemented through short-range technologies such as IEEE 802.11, IEEE 802.15.4, Bluetooth and IEEE 802.15.6, which are used to form Wireless Local Area Networks (WLAN), Wireless Sensor Networks (WSN), Wireless Personal Area Networks (WPAN) and Body Area Networks (BAN) respectively. In such case, a gateway assists in communicating the data to the core network. In addition, with the increasing attention paid to carbon reduction, it is expected that the gateways and relays in the communication system will be charged by renewable energy or hybrid energy sources. Energy-harvesting gateways and relays may be widely applied in developing countries where the infrastructure is insufficient. The traffic types of M2M communications are mostly asymmetric uplinks with wide diversity, whereas those of H2H communications are usually downlinks.

In energy-harvesting downlink scenarios, the BS unicasts dedicated data to the corresponding device [6]-[8], or multicasts/broadcasts (re)configuration messages and system information to a group of M2M devices [11]. The Hybrid BSs can be powered by a combination of the power grid and renewable energy with energy-harvesting modules [6][7]. In contrast, BSs that are fully powered by energy-harvesting modules were studied in [8]. The use of a large number of energy-harvesting M2M devices to receive the multicast/broadcast information was studied in [4]. So far, a downlink system where both the transmitters (BSs) and receivers (M2M devices) are all energy-harvesting devices has not yet been addressed. In such a system, traffic delay and synchronization among energy-harvesting transmitters and receivers are issues for further investigation.

Downlink energy-harvesting systems entail several design problems, such as the resource/power allocation of the BSs, the transmission error combined with the properties of energy-harvesting, energy deficiencies, QoS (Quality of Service) guarantee (e.g., outage probability satisfaction), and proportionally fair transmission.

Especially when the M2M devices are equipped with energy-harvesting modules, medium access protocols such as TDMA [8][9], Frame slotted ALOHA [6] [5] and RACH in an LTE-A cellular system [7], can be properly intended according to the energy harvesting characteristics and traffic types. The state-of-the-art research emphases on the uplink transmission of several energy-harvesting transmitters to a central controller powered by nonrenewable energy. M2M uplink transmission to an energy-harvesting/Hybrid BS can still be additional explored

The maximum design problems of the medium access control protocol of energy-harvesting M2M uplink transmission are how to support energy-efficient uplink transmission, congestion control/mitigation caused by the device scalability, well-organized resource allocation rules, long-lasting system lifetime, distinct traffic QoS satisfaction, and the higher data distribution probability.Save-then-Transmit TDMA is introduced in [10] under the assumption of a two-energy-storage-circuit energy perfect and imperfect energy storage efficiency. The optimal value of time fraction $\boldsymbol{\rho}*$ ($\mathbf{0}\leq\boldsymbol{\rho}*\leq\mathbf{1}$) for an energy-harvesting transmitter to concentrate on energy harvesting and 1-$\boldsymbol{\rho}*$ for data transmission in the single-transmitter case is determined to minimize the outage probability, including two mutually exclusive events: a circuit outage and a channel outage. However, in a scenario with multiple energy-harvesting M2M transmitters, the transmitter will deviate from the optimal operating point $\boldsymbol{\rho}*$ if the required energy harvesting time is insufficient.

III. METHODOLOGY

3.1 Ambient Energy Harvesting Technology

Nodes essential an energy source, and ambient energy harvesting from external sources are used to power small isolated sensors such as those based on MEMS technology. These systems are often very small and involve little power; however their applications are incomplete by the reliance on battery power.Ambient energy harvesting cannot only be realized by conventional optical cell power generation, but also through miniature piezoelectric crystals, micro oscillators, thermoelectric power generation elements, or electromagnetic wave reception devices. Certain companies have begun to commercialize sensor network applications using energy acquisition devices. For example, the German company En Ocean has providing light energy harvesting devices, vibration energy harvesting devices and temperature-based energy harvesting devices for smart building lighting and air monitoring presentations.

3.2 Self-Adaptive Flow Control Technology

One of the differences between WSNs and traditional wired networks is the instability of wireless communication. In WSNs, the communication between nodes is disposed to interference and occlusion, subsequent in signal transmission failure. The traditional network is a stable wired network, which data will only be lost due to congestion. The principle of flow control is that the data sender regulates the distribution traffic according to the loss condition of data transmission. When data loss occurs, the sender decreases the transmission rate. And when the data is not lost, the sender increases the transmission rate. Such flow control mechanisms are no longer suitable for WSNs, because the data loss in sensor networks is mostly caused by congestion, intrusion and occlusion. Only decreasing the transmission rate cannot solve the problem, but only lowers the network performance. In order to solve the network performance degradation problem in unstable transmission conditions, adaptive flow control is proposed. Adaptive flow control checks the reason for packet

loss and adjusts the transmission flow. Meanwhile, according to the excellence of the link and the number of transmission errors, the best transmission rate for the data transmission among nodes is prioritized to obtain good network stability while considering the transmission distance and throughput.

3.3 Semantic Representation and Processing

Semantic technology is one of the most significantexploration fields in information technology in recent years, mostly due to enormous expectations and difficulties for knowledge sharing and exchanging through networks. Semantic research on WSN information becomes a hot topic especially with the improvement of WSN and the expansion from the traditional perception of the internet to sensing layer devices. WSN semantic research focuses on the semantic demonstration of the physical world perceived by sensor nodes. In brief WSN semantics refers to the importance or sense of the information perceived by sensor nodes, with which the fundamental data can be put into improvedprocedure.

There are 3parts have been identified as becoming hot research topics for the understanding of sensor semantic issues:

1) Semantic representation technology for terminal devices, directly adds semantic tags to sensor data in terminal device levels to achieve semantic representation,
2) Semantic platform based on querying implements the sensor data query through the semantic interpretation of sensor data, and,
3) Semantic analysis and management of sensor information based on cloud computing technology. It is expected that this could maintenance large-scale sensor nodes, semantic expression, and dispensation based on cloud computing platforms.

3.4 Proposed System

WSN are groups of mobile nodes, enthusiastically forming a temporary network without previous network infrastructure or centralized administration. DSR (Dynamic Source Routing) is on-demand, humble and resourceful routing protocol for multi-hop wireless ad-hoc networks of mobile nodes. DSR uses source routing and protocol composed of two main mechanisms-Route Discovery‟ and Route Maintenance‟, which everythingcomposedcompletely, on demand. The protocol allows multiple routes to destination, loop-free routing, support for unidirectional links, use of only soft state‟ in routing, rapid discovery when routes in the network change, designed for mobile ad hoc networks of up to about two hundred nodes and to work well even with high rates of mobility.

IV. RESULT AND DISCUSSION

4.1 Security and Privacy

Internet of Things is a network of real world systems with real-time interactions done virtually. Unattended operation without human intervention is possible for long periods of time by the wireless area network (WAN) or WLAN. It creates various security threats to IoT. Because of the wireless communication there is a possibility to eavesdropping. IoT components are having low energy and low computation resource so that the complex security support cannot be provided. Authentication and data integrity is also a major problem for security.

Front-end sensors and equipment receives data via sensors. Then they transmit the data using modules or M2M device. An intruder can easily access the nodes which are distributed and damage or imply illegal actions on these nodes. Possible threats are unauthorized access to data, threats to the Internet and denial of service. Since large number of machines sending data to large number of nodes and groups network congestion may occur.

4.2 Privacy

Data collection, mining and provisioning will be different in IoT. For human individuals it will be impossible to personally control the disclosure of their personal information. Once information is collected, that will be retained indefinitely.

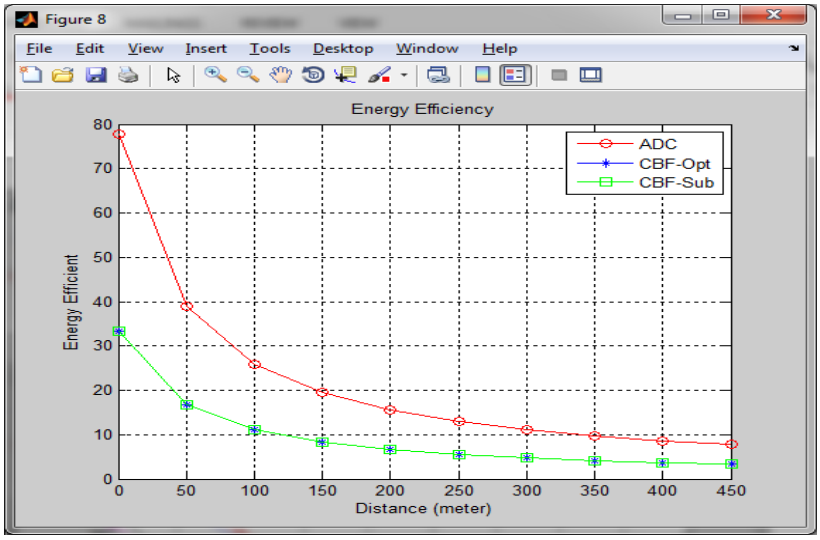

Figure 4.1 Proposed Method Energy Efficiency Analysis

In traditional Internet, privacy problem arises only for the Internet users whereas in IoT the privacy problem arises even for people not using any IoT service. Hence when the data is collected for authorization by the service provider it should be stored only until it is strictly needed. Privacy should be addressed in many perspectives like,

1) **Privacy in Device**: The device may hold sensitive information which may be retrieved by unauthorized persons and reprogrammed. Hence the location of the device should be non-identifiable which means protecting the exact nature of device.
2) **Privacy during Communication**: During data transmission, data confidentiality can be ensured by applying encryption. Encryption on certain occasions adds data to packets which provides a way for tracing, e.g. sequence number, IP sec- Security Parameter Index, etc. These data may be victimized for linking packets. In order to avoid unnecessary collection of location information by the network after a certain period of inactive devices will detach from the network. Secure Communication Protocol could be the suitable approach.
3) **Privacy in Storage**: For protecting privacy of information storage, the least possible amount of information should be stored that is needed. In case of mandatory then only personal information retained. Information is brought out on the basis of "need-to-know". To conceal the real identity tied with the stored data Pseudonymization and Anonymization could be used. Without disclosing any specific record, a database could allow access only to statistical data.
4) **Privacy at Processing**: Firstly, personal data must be treated in a way that it should be simpatico with the intended purpose. Secondly, without explicit recognition and the knowledge of the data owner, their personal data should not be disclosed or retained to third parties. Digital Rights Management (DRM) systems are most suitable which controls the consumption of commercial media and defends against re-distribution illegally. DRM requires trusted devices, secure devices to work efficiently and effectively.

V. CONCLUSION

WSN and even more so, IoT, are not single technologies but instead represent complex systems using numerous technologies from physical communication layers to application program and are used in many application areas and different environments. This diversity has resulted in a complex regularizationlocation. Because more and more nodes are deployed, and performance is usually impacted with the addition of security services in WSNs, particularly in infrastructure, the International Electro-technical Commission (IEC) recommends relative research organizations to association their efforts to develop a common model to ensure security for each layer, and to type the layers work in collaboration with each other.

VI. FUTURE WORK

This explorationworking static task scheduling model to optimize reliability of the Mobile computing. For future studies, energetic task development model can be considered for mobile computing or distributed network. Other future work may include develop some other routing techniques or task assignment model to optimize cost, time and reliability of the distributed computing or mobile computing.

REFERENCES

[1] Q. Han, S. Liang, and H. Zhang, ``Mobile cloud sensing, big data, and 5G networks make an intelligent and smart world," IEEE Netw., vol. 29, no. 2, pp. 4045, Mar./Apr. 2015.

[2] L. Atzori, A. Iera, and G. Morabito, ``The Internet of Things: A survey," Comput. Netw., vol. 54, no. 15, pp. 27872805, Oct. 2010.

[3] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, ``A survey on Internet of Things from industrial market perspective," IEEE Access, vol. 2, pp. 16601679, Jan. 2014.

[4] L. Da Xu, W. He, and S. Li, ``Internet of Things in industries: A survey," IEEE Trans. Ind. Informat., vol. 10, no. 4, pp. 22332243, Nov. 2014.

[5] C. Perera, C. H. Liu, and S. Jayawardena, ``The emerging Internet of Things marketplace from an industrial perspective: A survey," IEEE Trans. Emerg. Topics Comput., to be published.

[6] 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., to be published.

[7] F. K. Shaikh, S. Zeadally, and E. Exposito, ``Enabling technologies for green Internet of Things," IEEE Syst. J., to be published.

[8] V. Namboodiri and L. Gao, ``Energy-aware tag anticollision protocols for RFID systems," IEEE Trans. Mobile Comput., vol. 9, no. 1, pp. 44- 59, Jan. 2010.

[9] Y.-H. Lin, Z.-T. Chou, C.-W. Yu, and R.-H. Jan, ``Optimal and maximized confgurable power saving protocols for corona-based wireless sensor networks," IEEE Trans. Mobile Comput., to be published.

[10] F. Farahnakian et al., ``Using ant colony system to consolidate VMs for green cloud computing," IEEE Trans. Services Comput., vol. 8, no. 2, pp. 187198, Mar./Apr. 2015.

[11] C.-H. Chang, R. Y. Chang, and H.-Y. Hsieh, ``High-delity energy-effcient machine-to-machine communication," in Proc. IEEE 25th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun., Sep. 2014, pp. 91-96.

[12] J. Shuja et al., ``Survey of techniques and architectures for designing energy-effcient data centers," IEEE Syst. J., to be published.
[13] A. Alamri, W. S. Ansari, M. M. Hassan, M. S. Hossain, A. Alelaiwi, and M. A. Hossain, ``A survey on sensor-cloud: Architecture, applications, and approaches,' Int. J. Distrib. Sensor Netw., vol. 2013, Nov. 2013, Art. ID 917923.
[14] S. Misra, S. Chatterjee, and M. S. Obaidat, ``On theoretical modeling of sensor cloud: A paradigm shift from wireless sensor network," IEEE Syst. J., to be published.
[15] P. Sathyamoorthy, E. C.-H. Ngai, X. Hu, and V. C. M. Leung, ``Energy effciency as an orchestration service for mobile Internet of Things," in Proc. 7th IEEE Int. Conf. Cloud Comput. Technol. Sci., Nov./Dec. 2015, pp. 18.

