

# Chapter 61

## Energy Aware Cluster Head Selection for Maximizing Lifetime Improvement in Internet of Things

**Praveen Kumar Reddy Maddikunta**  
VIT University, India

**Rajasekhara Babu Madda**  
VIT University, India

### ABSTRACT

*Energy efficiency is a major concern in Internet of Things (IoT) networks as the IoT devices are battery operated devices. One of the traditional approaches to improve the energy efficiency is through clustering. The authors propose a hybrid method of Gravitational Search Algorithm (GSA) and Artificial Bee Colony (ABC) algorithm to accomplish the efficient cluster head selection. The performance of the hybrid algorithm is evaluated using energy, delay, load, distance, and temperature of the IoT devices. Performance of the proposed method is analyzed by comparing with the conventional methods like Artificial Bee Colony (ABC), Genetic Algorithm (GA), Particle Swarm Optimization (PSO) and GSO algorithms. The performance of the hybrid algorithm is evaluated using of number of alive nodes, convergence estimation, normalized energy, load and temperature. The proposed algorithm exhibits high energy efficiency that improves the life time of IoT nodes. Analysis of the authors' implementation reveals the superior performance of the proposed method.*

### 1. INTRODUCTION

The development of the sensing devices has expanded with the fast advancement of innovation (Kawamoto et al., 2013; Li et al., 2016). In the field of network technology WSN is considered as the principle importance (Duan et al., 2014). WSN is used to provide quick operation with sufficient self-organization throughout the world at any location. In addition, through the continuous improvement, WSN has been

DOI: 10.4018/978-1-5225-9866-4.ch061

utilizing in vast applications (Dai & Xu, 2010; Agarwal et al., 2015; Wu et al., 2016). The system inter-connected with computing device, digital and mechanical instruments, animals, people or other objects is called IoT (Kougianos et al., 2016; Liu et al., 2016; Park et al., 2016; Misra et al., 2016). These IoT are supplied with unique identifiers. Additionally, in absence of user- to- user or user- to- computer influence, the IoT system has the capability to convey data over the network. Thus, people have close interaction with the physical world based on the real-time activity of the sensor nodes (Ashraf & Habaebi, 2015; Perera & Vasilakos, 2016). Users can observe, sense and regulate the objects placed in the corresponding environment instead of customizing the information (Li et al., 2016; Zhang et al., 2016; Wu et al., 2016).

The resource of the nodes in WSN based IoT have limited capability in terms of processing, bandwidth, volume of storage, power of battery which differentiate WSN from other networks (Wu et al., 2013; Yachir et al., 2016). Basically, the WSN are provided with battery power which is to be recharged Huang et al., 2015. Under such instance, proper scheduling of energy utilization is required especially when the sensors are distantly connected (Abusalah et al., 2008; Zhong et al., 2010). As a distributed wireless network, WSN is vulnerable to many attacks proper security mechanisms must be provided for confidential data (Lin et al., 2015; Dey et al., 2016). Numerous nodes transfer multiple data from node to the base station about the same event, which leads to transfer redundant data (Moosavi et al., 2016; Di Marco et al., 2016). Thus, the consumption of energy associated with the network become high. Since there are three main processes for the nodes such as information sensing, processing and transmitting, complexity of network has increased. Therefore, the transfer of redundant data should be reduced and the large amount of energy should be saved in order to enhance the life expectancy of the network (Cavalcante et al., 2016; Hsu et al., 2016; Raza et al., 2016). With the rapid development of the Internet of Things, the security issues in wireless sensor network WSN, especially traffic anomaly detections, have attracted researchers' attention. As a distributed wireless network, WSN is vulnerable to many attacks, there should be proper end to end trust mechanisms should be provided for sensing data (Lin et al., 2015).

However, some challenges have rose from these developments and triggered the research attention in the up to date years which are unsolved by other researchers. Among the challenges, Energy awareness is considered as the foremost challenges under IoT (Luo & Ren, 2016; Sivieri et al., 2016; Karkouch et al., 2016; Zhu et al., 2016). Energy awareness is used in IoT to provide the energy saving mechanism to the appliances connected to the network. Subsequently, the truthful operating environment is achieved by some primary protocols such as routing protocols and Medium Access Control (MAC). However, these protocols may fail to operate in some cases. Besides, node clustering is an improved method under WSN to improve the network scalability and life time, but unsolved under IoT. Furthermore, hierarchical protocols, location – based protocol, data- centric protocols etc for clustering the nodes in WSN have used to save energy for withstanding the network lifetime using multiple operating conditions.

## **2. LITERATURE REVIEW**

### **2.1. Related Works**

(Huang & Chang, 2015) have proposed Contention-Free Station Communication Matching Algorithm in Multi-Hop Power Management for Wireless Ad-Hoc Networks based on list-based scheduling with Time-Division Multiple Access (TDMA). Contention-Free Station Communication Matching technique schedules the data transmission of nodes and power management. Authors have adopted multiple chan-

19 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/energy-aware-cluster-head-selection-for-maximizing-lifetime-improvement-in-internet-of-things/234996](http://www.igi-global.com/chapter/energy-aware-cluster-head-selection-for-maximizing-lifetime-improvement-in-internet-of-things/234996)

## Related Content

---

### A Compressive Compilation of Cyber Security for Internet of Energy (IoE)

Gustavo Arroyo-Figueroa, Isai Rojas-Gonzalez and José Alberto Hernández-Aguilar (2020). *Cyber Security of Industrial Control Systems in the Future Internet Environment* (pp. 267-294).

[www.irma-international.org/chapter/a-compressive-compilation-of-cyber-security-for-internet-of-energy-ioe/250116](http://www.irma-international.org/chapter/a-compressive-compilation-of-cyber-security-for-internet-of-energy-ioe/250116)

### The Internet of Things and Assistive Technologies for People with Disabilities: Applications, Trends, and Issues

Hwa Lee (2017). *Internet of Things and Advanced Application in Healthcare* (pp. 32-65).

[www.irma-international.org/chapter/the-internet-of-things-and-assistive-technologies-for-people-with-disabilities/170236](http://www.irma-international.org/chapter/the-internet-of-things-and-assistive-technologies-for-people-with-disabilities/170236)

### Sharing Protected Web Resources

Sylvia Encheva and Sharil Tumin (2008). *Encyclopedia of Internet Technologies and Applications* (pp. 539-544).

[www.irma-international.org/chapter/sharing-protected-web-resources/16901](http://www.irma-international.org/chapter/sharing-protected-web-resources/16901)

### Intellectual Property and the Internet

Alexandra George (2008). *Encyclopedia of Internet Technologies and Applications* (pp. 222-227).

[www.irma-international.org/chapter/intellectual-property-internet/16857](http://www.irma-international.org/chapter/intellectual-property-internet/16857)

### Content Delivery Networks: On the Path Towards Secure Cloud-Native Platforms at the Edge

Yannick Le Louédec, Gaëlle Yven, Valéry Bastide, Yiping Chen, Gwenaëlle Delsart, Mateusz Dzida, Frédéric Fieau, Patrick Fleming, Ivan Froger, Lahcene Haddak, Nathalie Labidurie Omnes and Vincent Thiebaut (2021). *Design Innovation and Network Architecture for the Future Internet* (pp. 66-95).

[www.irma-international.org/chapter/content-delivery-networks/276695](http://www.irma-international.org/chapter/content-delivery-networks/276695)