IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 8, August 2018

# An Improved Energy Efficient Technique for Data Aggregation using Leach protocol in Internet of Things

**Rahul Ralen[1], Baldip Kaur[2]**

Department of Computer Science and Engineering,

Lala Lajpat Rai Institute of Engineering and Technology, Moga, Punjab[1,2]

**Abstract:** The IOT network is the decentralized type of network which can sense the information and pass it to base station. Due to small size of the sensor nodes, the energy consumption is the major issue of the network. The LEACH is the energy efficient protocol which can divide whole network into fixed size clusters. In the proposed work, in each cluster, cluster heads are selected which can transmit data to base station. The LEACH protocol is the dynamic clustering protocol in which cluster heads changes after each round in the network. The cluster heads are selected in network based on the energy of each node and distance from sensor node to base station. The energy of the sensor node is dissipated when each node receive or transmit data to base station. The energy is also consumed when the sensor nodes aggregate data to cluster head. In this work, the LEACH protocol is improved to reduce energy consumption of the wireless sensor networks. In the proposed work, the cache nodes are deployed which can aggregate data from the cluster heads and then pass data to base station. The simulation of the proposed technique is done in MATLAB and results are compared with the existing approach in terms of certain parameters; number of dead nodes, number of live nodes and remaining energy. It is analyzed that proposed technique performs well as compared to existing technique.

**Keywords:** LEACH, IOT, Gateway.

## I. INTRODUCTION

IOT stands for internet of things which is termed by the of the Radio Frequency Identification (RFID) development community in 1999. The application of the IOT is widely used in many applications due to large growth of mobile devices, embedded and omnipresent communication, cloud computing and data analytics [1]. Large numbers of devices are connected over public or private Internet Protocol networks with the help of billions of objects can sense, communicate and share information. The data collected by these interconnected devices continuously, after which it is analyzed to perform action in order to provide a wealth of intelligence for planning, management and decision making. The main objective here is to interconnect all the things present within this self-configuring wireless network which includes numerous sensors. An object that gets involved within a communication chain is also present. The combination of communication capabilities which are given by the data transmission is given by these lines present. RFID is known to be the main object within the IOT. The building of global infrastructure for RFID tags which is known to be a wireless layer present on the top of Internet [2]. The communication is made amongst network of interconnected objects and the interconnected computers. There is a different Internet Protocol (IP) location for the objects at some instants. These objects are embedded within the complex systems. In order to gather the information here, the various sensors are used which gather information related to temperature, and other aspects present in the surroundings. The sensors present near to each other transfer the gathered information in order to provide further processing as per the requirements of the current applications. Cloud computing is a highly scalable and cost-effective infrastructure for running number of applications such as HPC, enterprise and Web applications. However, there is one big critical issue in cloud computing which have been emerging due to its growing demand which have drastically increased the consumption of energy in data centers [3]. The issue of high consumption not only increase the operation cost which reduces the profit of cloud providers but it also affect the environment as the high consumption of energy leads to high emission of carbon. Hence, energy-efficient solutions are required to minimize the impact of Cloud computing on the environment. At the different layers of IOT framework security is the major requirement. The need of the security in IOT framework can be illustrated by identifying the layer wise security requirements. Perception layers, security requirements are data privacy by which only authorized user can read or write data and user is guaranteed about the privacy of their data that no one can utilized their data without proper access permission [4]. For the authentication cryptography hash algorithm has been utilized that provides risk assessment and authentication to the user. With the help of this, device can authenticate and verify that with whom it is interacting is authentic person.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 8, August 2018

Middleware layer is the layer in which it is necessary to access the error free information or data by the authorized person immediately [5]. It is necessary to check the availability of devices I order to know vulnerabilities. Data redundancy monitored every transmission in network and helps in preventing the denial attacks. Application layer, security requirements of the application layer are authentication, risk assessment, data security for the protection of digital content which is very necessary in order to secure environment. It involves the authentications of externals that can permit permission to the data and information. Misdirection attack is the attack in which packets are routed by the attacker to its children to other distant nodes but do not transfer to its legitimate parent [6]. The main purpose of the intruder is to increase the latency by misdirecting the incoming messages due to which few packets are prevented from reaching the base station. The most popular Denial of Service Attack is the Misdirection attack. It changes the path of the packets in order create confusion among nodes.

## II. LITERATURE REVIEW

**Yogeesh Seralathan, et.al (2018)** presented all the devices in the internet of things are controlled and connected with the help of internet [7]. Large number of sensitive data is being processed by the devices due to which the use of IOT devices increases widely. In order to large number of botnets, Malware like Mirai is widely used nowadays. This malware has been utilized in DDoS attacks as well in which every second up to 1.2 Terabytes of networks traffic is generated. They performed various experiments, in order to determine compromise done by an IOT device's in case of threat for the security and privacy of the data and they provide a case study of an IP camera. They also presented the importance of securing IOT and provide essential security practices for mitigating device exploitation.

**Chalee Vorakulpipat, et.al (2018)** presented the critical issue currently faced by the devices due large utilization of these devices. The major issue faced currently is the issue of the network security in the devices. The use of devices nowadays increased drastically in order to access the corporate networks due to which they are prone to the major security risks [8]. Due to these devices it is easy to access more channels for the corporate information. The need of the IOT security changes according to market needs as services of the IOT devices changes from time to time. They presented a concerns related to IOT security, reviews, and challenges faced by the devices as well as discussed the three generations of the IOT security.

**Yiqun Zhang, et.al (2018)** presented it a major challenge for the IOT devices to support different cryptographic algorithms and standards within the physical constraints. Author proposed a Recryptor in this paper which is a reconfigurable cryptographic processor which utilizes its computational capabilities in order to enhance the existing memory of a commercial general-purpose processor [12]. A 10-transistor bitcell supports, in-memory bitline computing for the support of different bitwise operations up to 512-bits wide. The programmability of the Recryptor's was demonstrated by implementing the cryptographic primitives of various public/ secret key cryptographies and hash functions. 6.8% average speedup and 12.8% average energy was achieved by Recryptor running at 28.8 MHz in 0.7 V as compared to software- and hardware.

**Jesus Pacheco, et.al (2017)** presented a framework for the security of IOT for the integration of a Smart Water Systems in the IOT, in a secure way. They also showed the procedure to use the threat model in order to protect or secure gateway which is the necessary part of the communication gateway. The functionality of this method is based on the concept that it utilizes a profile that is developed to accurately and characterizes the normal operations of gateway [9]. As per analysis, it is demonstrated that proposed approach of ABAIDS can detect both known and unknown attacks with high detection rates and low false positive alarms. They also have insignificant overhead in terms of memory and CPU usage. Proposed method protects the normal operation of the gateway in order to provide the availability.

**Se-Ra Oh, et.al (2017)** presented a connected, intelligent and context-aware device that works collectively known as internet of things (IOT). Security is the main consideration in the IOT devices as they are more vulnerable to attacks and directly affect the IOT device in the IOT platform [10]. In the interworking process, they are more prone to critical influence in all connected IOT platforms. The security architecture of the oneM2M was discussed in this paper. Therefore, they developed an OAuth 2.0-based oneM2M security component in order to provide authentication and authorization which is necessary for the security of IOT and for the protection of interworking between IOT platforms.

**U. M. Mbanaso, et.al (2017)** presented a novel configurable policy-based specification and the threats and vulnerabilities faced by an IOT system were analyzed. In order to solve all the issues in multiple domains, these devices work collectively and smart entities have to more trusted, reliable and secure for the security and safety of end-to-end connectivity [11]. A mechanism was proposed by author in this paper by which all the IOT entities can express their capabilities and requirements. For the negotiation of provable attributes and resources they constructed a fine-grained policy mutually. In order to solve the dispute resolution and auditable, they provide a mechanisms which solve the

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 5, Issue 8, August 2018

issues such as trust, privacy and confidentiality in a unified manner. This method provides a greats success in the IOT environments.

## III. PROPOSED METHODOLOGY

The IOT network is the self-configuring network in which sensor nodes sense information and pass it to base station. Due to decentralized nature of the network, energy consumption, data aggregation and security are three major issues of the networks. This research work is focused on the energy consumption of the wireless sensor networks. The energy consumption issues are raised due to small size of the sensor nodes. The clustering is the efficient approach which increase lifetime of the sensor networks. In the clustering approach, the whole network is divided into fixed size clusters. The cluster heads are selected in each cluster and sensor nodes in each cluster will aggregate data to cluster head. The cluster head will transmit data to the base station. To increase lifetime of the sensor network, the optimization is proposed in the LEACH protocol. In the proposed approach, the cache nodes are deployed between the cluster head and base station. The cluster heads will transmit the data to nearest cache node and then cache send data to the base station. The cache aggregate data from the nearest cluster head. The distance between the gateway node and cluster head is calculated using Euclidian distance formula.

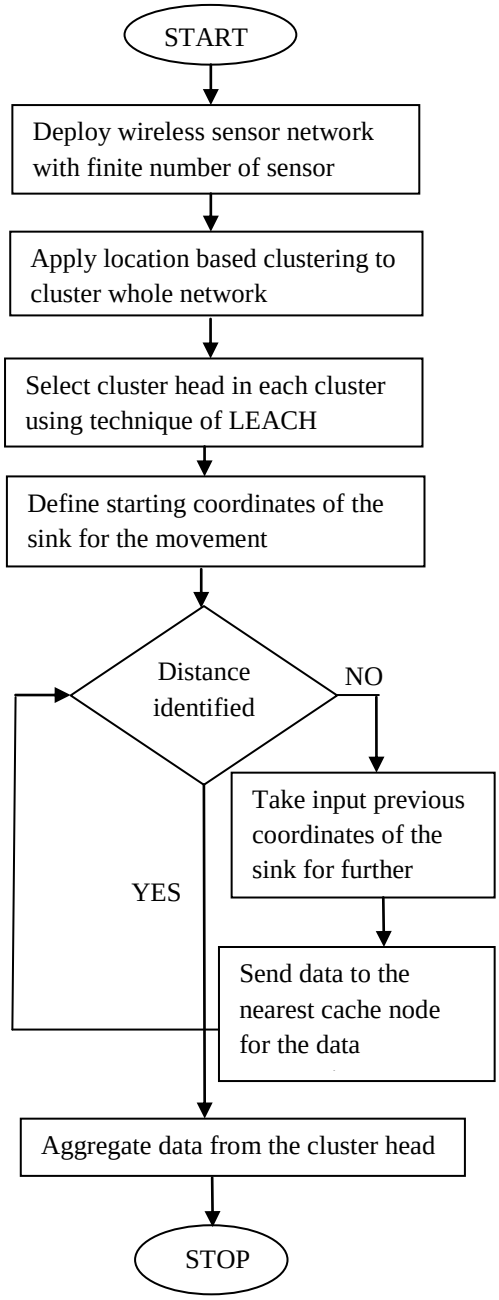


Fig 1: Flowchart of proposed methodology

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 8, August 2018

**Proposed Algorithm**

1. Deploy the network with the finite number of sensor nods
2. Divide the whole network into fixed size using location based clustering
3. For (i=0; i<=n;i++)

    If(energy (i) && distance (i)> energy (i+1) && distance (i+1))

        Cluster head=node(i)

    End
4. Caching of Data ()
5. Apply node localization and gather network information
6. If data aggregated (location (i) > location (i+1))
7. best coordinated =location (i)

Else

Location (i+1)

End

8. Aggregate data and updated cache information

## IV. EXPERIMENTAL RESULTS

This section presents the results of the proposed algorithm implemented in MATLAB.

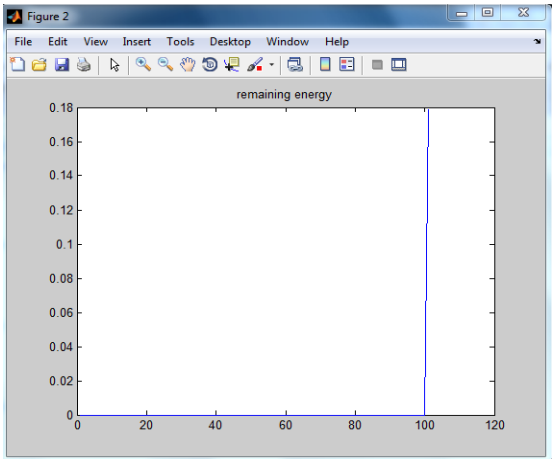


Fig 2: Remaining energy of the proposed scenario

In Fig 2, the remaining energy is shown in which on the x-axis the number of rounds are given and on the y-axis the remaining energy is shown.

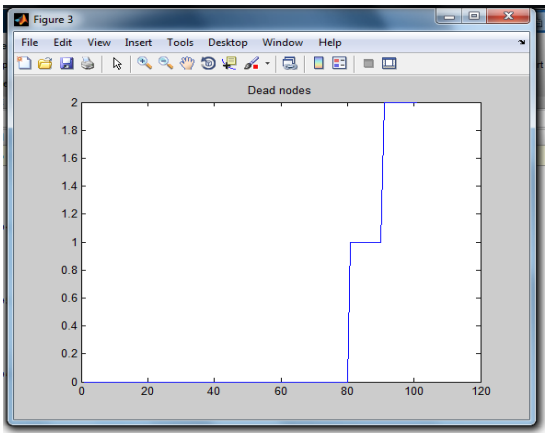


Fig 3: No of Dead Nodes with Proposed protocol

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 8, August 2018

In fig 3, the graph is shown in which number of dead nodes are shown versus number of rounds. On the x-axis the numbers of rounds are shown and on the y-axis the numbers of dead nodes are illustrated.

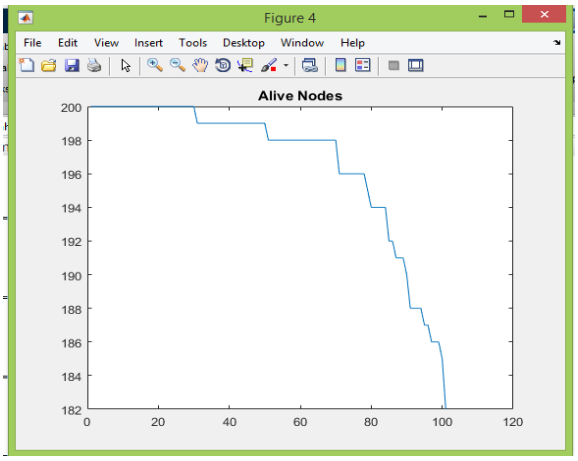


Fig 4: Number of Alive Nodes with LEACH Protocol

In fig 4, the number of alive nodes are analyzed when the data is aggregated with the LEACH Protocol. The total number 192 nodes are alive during the transmission is shown. Further, table 1 shows the comparison of proposed algorithm with the existing algorithm and fig 5 shows the graphical representation of the comparison performed.

Table 1: Table of comparison between proposed and existing algorithm

| Parameter | Proposed Algorithm | Existing Algorithm |
|---|---|---|
| Number of dead Nodes | 2 | 12 |
| Remaining Energy | 0.16 | 0.18 |
| Alive Nodes | 192 | 198 |

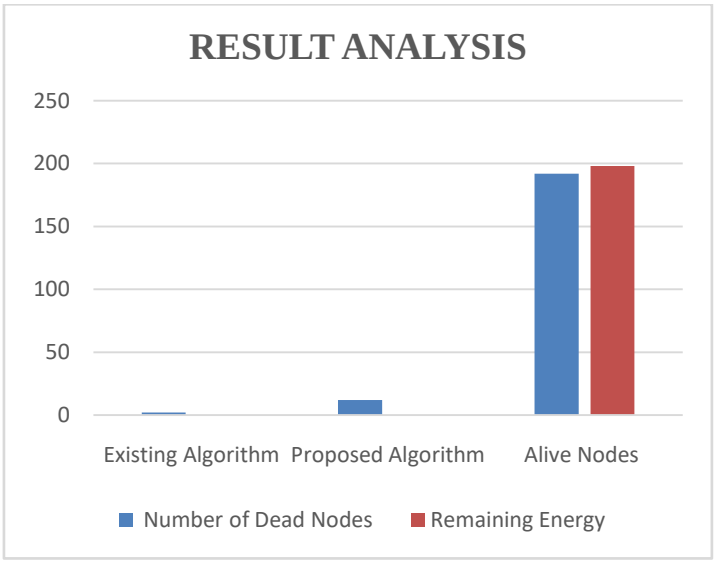


Fig 5: Graphical representation of comparison

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 5, Issue 8, August 2018

## V. CONCLUSIONS AND FUTURE SCOPE

### 5.1 Conclusion

In this research work, it is concluded that due to dynamic nature of the IOT network energy consumption is the major issue which need to resolve. The clustering is the efficient approach which divide whole network into fixed size clusters and cluster heads are selected in each cluster. The cluster heads are selected on the basis of distance and energy. The sensor node which has minimum distance and maximum energy is selected as the cluster head. In this research work, the LEACH protocol is improved with the gateway node. The cache node will aggregate data from the cluster head. The cluster head transmits data to base station which is static in nature. The simulation of the proposed and existing technique is done in MATLAB and it is analyzed that proposed technique perform well in terms of remaining energy and number of dead nodes.

### 5.2 Future Scope Of Work

Following are the various future prospective of this research work:

i. The proposed technique performs well in terms of energy consumption. The reliability of the proposed technique will be tested by comparing with the other energy efficient algorithm.
ii. The proposed technique can be further improved to increase security of the IOT networks.

## REFERENCES

[1] Dongsik Jo and Gerard Jounghyun Kim, "ARIOT: Scalable Augmented Reality Framework for Interacting with Internet of Things Appliances Everywhere", IEEE Transactions on Consumer Electronics, Vol. 62, Issue. 3, pp. 334-340, August 2016.
[2] Xinlie Wang, Jianqing Zhang, Eve. M. Schooler, "Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IOT", Communications (ICC), 2014 IEEE International Conference, vol. 19, issue 3, pp. 56-88, 2014.
[3] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of things (IOT): A vision, architectural elements, and future directions," Elsevier Future Generation Computer System, Vol. 29, issue 4, pp. 23-66, 2013.
[4] Mohamed Abomhara and Geir M. Koien. Security and Privacy in the Internet of Things: Current Status and Open Issues. In Privacy and Security in Mobile Systems (PRISMS), pages 1–8. IEEE, vol. 7, issue 6, pp. 18-3, 2014.
[5] Ahmad W Atamli and Andrew Martin. Threat-Based Security Analysis for the Internet of Things. In Secure Internet of Things (SIOT), vol. 4, issue 1, pages 35–43, 2014.
[6] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The Internet of Things: A survey. Computer Networks, vol. 8, issue 6, pp. 18-30, 2010.
[7] Yogeesh Seralathan, Tae (Tom) Oh , Suyash Jadhav, Jonathan Myers, Jaehoon (Paul) Jeong+, Young Ho Kim, and Jeong Neyo Kim, "IOT Security Vulnerability: A Case Study of a Web Camera", International Conference on Advanced Communications Technology(ICACT), IEEE, vol. 13, issue 9, pp. 16-30, 2018.
[8] Chalee Vorakulpipat, Ekkachan Rattanalerdnusorn, Phithak Thaenkaew, Hoang Dang Hai, "Recent Challenges, Trends, and Concerns Related to IOT Security: An Evolutionary Study", International Conference on Advanced Communications Technology(ICACT), vol. 7, issue 4, pp. 14-33, 2018.
[9] Jesus Pacheco, Daniela Ibarra, Ashamsa Vijay, Salim Hariri, "IOT Security Framework for Smart Water System", 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications, IEEE, vol. 9, issue 3, pp. 11-30, 2017.
[10] Se-Ra Oh, Young-Gab Kim, "Development of IOT Security Component for Interoperability", IEEE, vol. 12, issue 4, pp. 67-89, 2017.
[11] U. M. Mbanaso, G. A. Chukwudebe, "Requirement Analysis of IOT Security in Distributed Systems", 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), IEEE, vol. 5, issue 7, pp. 20-30, 2017.
[12] Yiqun Zhang, Li Xu, Qing Dong, Jingcheng Wang, David Blaauw, and Dennis Sylvester, "Recryptor: A Reconfigurable Cryptographic Cortex-M0 Processor With In-Memory and Near-Memory Computing for IOT Security", IEEE JOURNAL OF SOLID-STATE CIRCUITS, vol. 9, issue 3, pp. 25-56, 2018.