Energy Efficient Approach for Data Aggregation in IoT

Er. Baldeep Kaur[1] , Er. Parminder Singh[2]

[1]*Research Scholar, Ramgarhia institute of engineering and technology, Phagwara (RIET)*
[2]*Assistant Professor, Ramgarhia institute of engineering and technology, Phagwara (RIET)*
([1]baldeepkaur2830@gmail.com, [2]hod_cse@riet.ac.in)

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 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 are changes after each round in the network. In this research work, the LEACH protocol is improved to reduce energy consumption of the wireless sensor networks. In the proposed improvement, 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 NS2 and results are compared with the existing approach in terms of certain parameters. It is analyzed that proposed technique performs well as compared to existing technique.

Keywords-IoT, LEACH, NS2

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. 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 [1]. 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. Internet of Things in the upcoming years will be widely utilized in almost every application. The IoT applications provide Internet and various advance software and communication services. Here, the objects can be connected to each other or to the things and can access the media present [2]. The objects and things present worldwide can be interlinked with each other and provide access to communication in order to provide IoT environment [3]. Being the part of small computer is the main criteria for each object or thing. Any kind of forecast present has been outperformed by the microchip to which the connection is made. It involves various technologies such as RFID, sensor and actuator, miniaturization, nanotechnology and smart entities. The integration of wired as well as wireless control, communication and IT technologies together which are responsible for connecting several subsystems and things which operate under a unified platform controlled and managed smartly. Cloud computing is a highly scalable and cost-effective infrastructure for running number of applications such as HPC, enterprise and Web applications [4]. 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. The Big data is a term used where the large volume of data is difficult to process, store and analyze by using traditional existing database technologies. As the nature of big data is indistinct so, there is need to involves considerable processes to identify and translate the data into new insights. Advancement is required in the area of lightweight public key infrastructures (PKI) for the establishment of trust management that will develop trust frameworks in order to address this requirement [5]. In order to enable trust encryption materials, lightweight key management systems have been utilized using minimum communications and processing resources. In the recent year very much importance is given to the Security and privacy as it protects the data from any theft. Protection of data is very much necessary with the increase in the growth of the data nowadays, hence various mechanism are invented to minimize the major limitation of IoT. Security within these systems is always a major concern as there is numerous systems involved during the communication being held. Thus, the data involved within these systems is to be made secure. Various data isolation techniques are provided here which can help in providing encryption measures within the systems [6]. With the application of these systems it can be made sure that the data being transmitted to the destination reaches there without any modifications or stealing of important information by the unauthorized access. One of other major concerns within these systems is the violation of privacy of data present in them. In order to ensure that only the authorized users are given access to the private information, various algorithms are proposed here which can ensure that no unauthorized users have access

to this 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 [7]. 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. In various applications the use of the IoT devices increases as it capture all the present data, in a daily basis using IoT devices. In order to large number of botnets, Malware like Mirai is widely used nowadays [8]. 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 [9]. 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. 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.

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. There are four layers in this used framework such as devices, communication, service, and application layers. 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 [10]. 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 [11]. 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 [12]. 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. 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 issues such as trust, privacy and confidentiality in a unified manner. This method provides a greats success in the IoT environments.

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. In the Internet of Things security is the most important factor that need for the consideration [13]. 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.

III. RESEARCH 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 is the major issues of the sensor network due to far deployment and small size of the sensor nodes. The hierarchal routing protocol is the energy efficient structure free data aggregation protocol which works in the structural manner. The hierarchal routing protocol works in the three phases, in the first phase base station send the hello message

to each node in the network. The node reverts back to base station with their location and other information. In the second phase, whole network is divided into hierarchal structure based on the network density. In the third phase, the next hop node is selected based on the next node buffer size, residual energy and link strength. In this research work, hierarchal routing protocol will be improved to reduce routing overhead in the network. 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 gateway node and then gateway 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.

IV. EXPERIMENTAL RESULTS

The proposed work has been implemented in NS2 and the results have been analyzed against existing technique in terms of packet loss, throughput, and energy consumption.

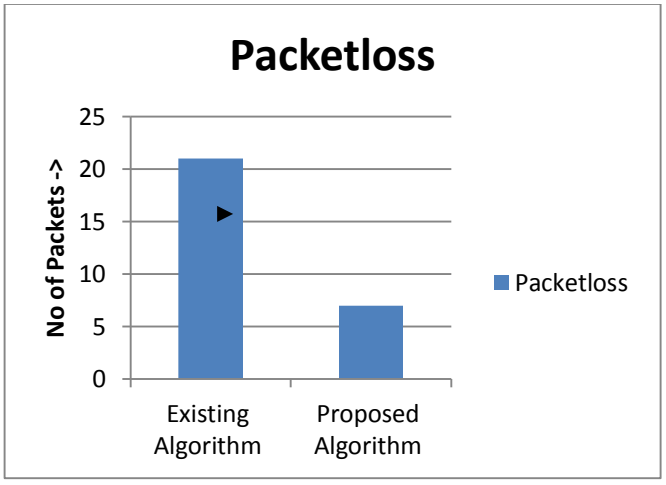

Fig.2: Packet loss Comparison

As shown in figure 2, the packet loss of the proposed and existing algorithm is compared. It is analyzed that packet loss of proposed is less as compared to existing algorithm

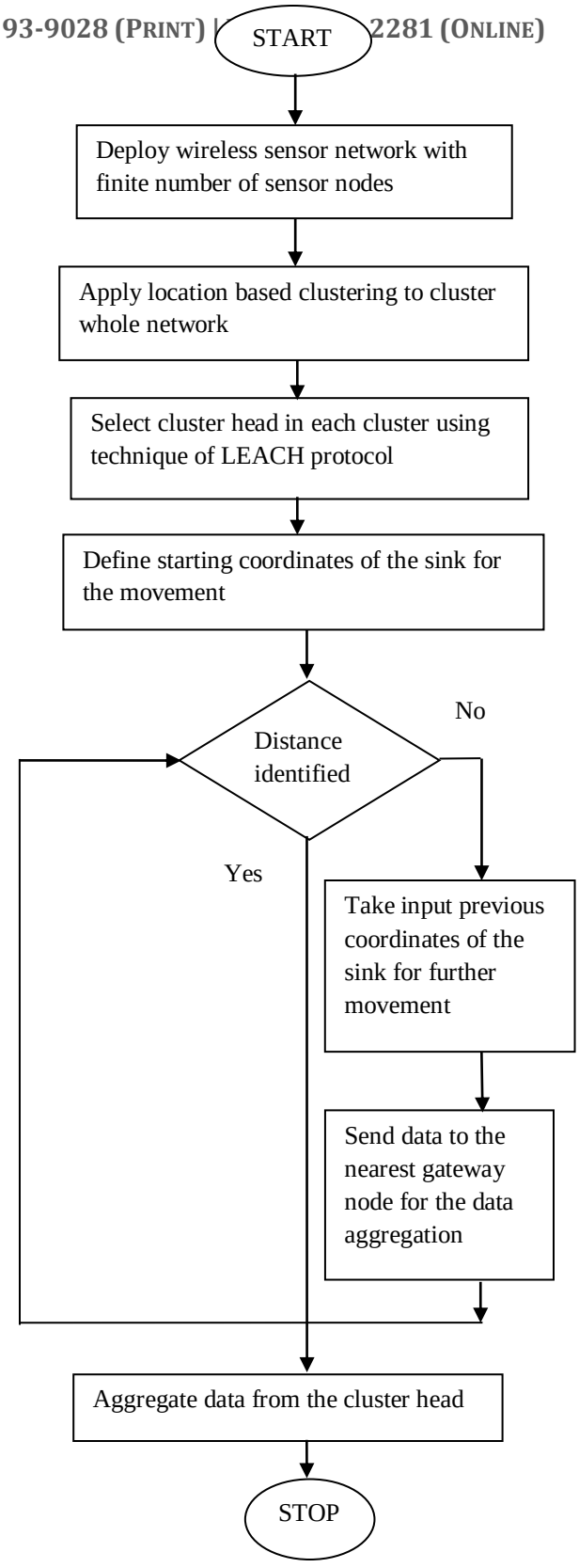

Fig.1:Proposed Flowchart

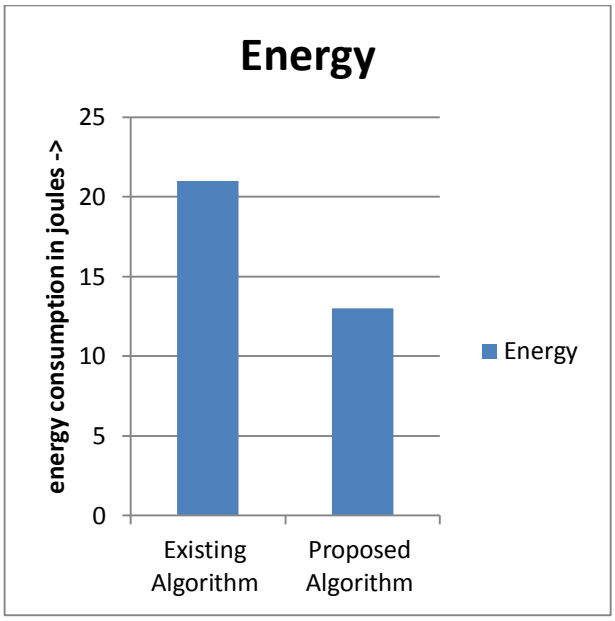

Fig.2: Energy Comparison

As shown in figure 2, the energy consumption of the proposed and existing algorithm is compared for the performance analysis. It is analyzed that energy consumption of the proposed algorithm is less as compared existing algorithm.

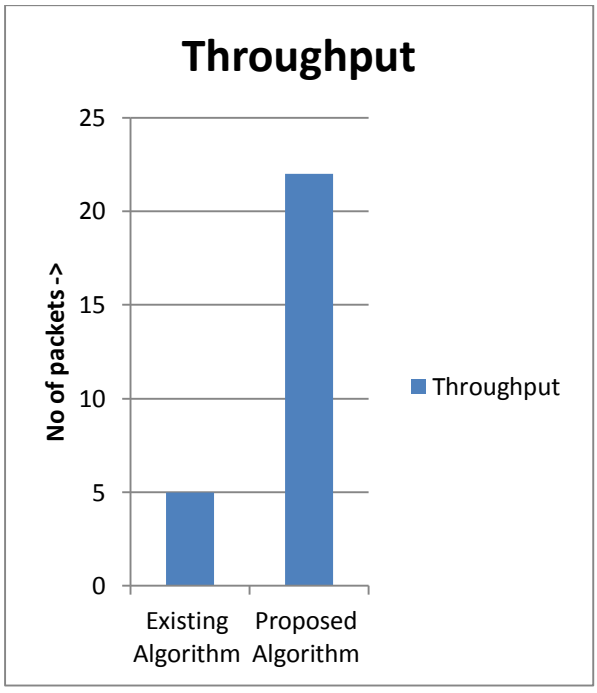

Fig.3:Throughput Comparison

As shown in figure 3, the throughputs of the proposed and existing algorithms are compared. It is analyzed that throughput of proposed algorithm is high as compared to existing algorithm.

V. 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. Protocol or platform interworking must be supported by the IoT gateway. 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 gateway node will aggregate data from the cluster head. The cluster head transmit data to base station which is static in nature. The simulation of the proposed and existing technique is done in NS2 and it is analyzed that proposed technique perform well in terms of throughput, packetloss and delay.

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]. Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad, and Ramjee Prasad, "Proposed security model and threat taxonomy for the Internet of Things (IoT)", In International Conference on Network Security & Applications (CNSA), volume 89, pages 420–429. Springer Berlin Heidelberg, vol. 4, issue 1, pp. 25-30, 2010.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. Se-Ra Oh, Young-Gab Kim, "Development of IoT Security Component for Interoperability", IEEE, vol. 12, issue 4, pp. 67-89, 2017.

[12]. 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.

[13]. 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.