Improvement in Lifetime of Sensor Devices in IoT

Kiran Thakur[1], Poonam Choudhary[2]
[1]Mtech Scholar, [2]Assistant Professor
[12]SIRDA Institute of Engineering Technology, Sundernagar, Mandi, H.P

Abstract- For sensing the information and forwarding it to the base station, a decentralized type of network called Internet of Things (IoT) is designed. The major concern of this network is the amount of energy being consumed by the sensor nodes since these sensor nodes are very small in size. Energy efficient protocol using which the complete network can be partitioned into clusters of fixed size is called LEACH. 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. When the data is available in the memory it will transmit data to base station. MATLAB simulator is used to perform simulation experiments using proposed approach. With respect to certain performance metrics, the comparisons against proposed and existing approaches are done. Based on the results achieved at the end, it is concluded through this research that the proposed approach outperformed the previously existing approaches.

Keywords- IoT, LEACH, Cache nodes, Energy Consumption

I. INTRODUCTION

The system in which several computing devices are interconnected where unique IDs are provided for each device and the data can be transferred across this network without any human-to-human or human-to-computer interaction is called Internet of Things (IoT). 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 [1]. Internet of Things in the upcoming years will be widely utilized in almost every application. It is defined as the network in which physical objects are connected to each other. Internet is not only the network for the connectivity but also evolve the network of device of all type and sizes. 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. Being the part of small computer is the main criteria for each object or thing [3]. Any kind of forecast present has been outperformed by the microchip to which the connection is made. There has been an increase in the physical scenarios and number of devices with the huge expansion of networks. Thus, in various domains, the services, applications and information communication networks have been modified as per the requirements. It is seen as per the predictive analysis that in near future huge amount of data will be generated from such advanced technologies and applications [4]. Huge amount of data that cannot be processed, stored or analyzed using the existing technologies is called big data. 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 [5]. Various data isolation techniques are provided here which can help in providing encryption measures within the systems. Misdirection attack: It 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. 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 important requirement for IoT framework at its various layers is its security [6]. 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. 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 [7]. The most popular Denial of Service Attack is the Misdirection attack. It changes the path of the packets in order create confusion among nodes. Misdirection attacks are of different types and can be performed in two ways. Packets Transmitted to Largely Distant Node type of misdirection attack is very dangerous as forwarded packets are transferred to a sensor node which is far away and prevents packets to reach the destination timely [8]. It decreases the throughput and increases the delay infinitely. Packets Transmitted to Node Closer to Actual Destination attack is less intense as compared to previous one because it took long route to transfer packets to its destination node. Due to which there is increase in delay and decrease in throughput.

II. LITERATURE REVIEW

Seralathan, et al. (2018) presented all the devices in the internet of things are controlled and connected with the help of internet [9]. In various applications the use of the IOT devices increases as it capture all the present data, in a daily basis using IOT devices. 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. The important of securing IoT and providing important security practices such that the device exploitation can be mitigated is also studied here.

Vorakulpipat, et al. (2018) presented the critical issue currently faced by the devices due large utilization of these devices [10]. The major issue faced currently is the issue of the network security in the devices. It is very necessary to use more services as most of the people are shifted from personal computers to mobile devices that lead to widely utilization of the IOT devices. 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.

Pacheco, et al. (2017) presented a secure architecture for IOT such that they can include the Smart Water Systems securely in them [11]. There are four layers in this used framework. They also presented a methodology for the development of a threat model and this model has been utilized for the identification of the potential attacks against each layer, their effects of the devices and methods such that the affects of these attacks can be recovered. The functionality of this method is based on the concept that it utilizes a profile which is designed appropriately and characterizes the genuine operations of gateway. As per analysis, it is demonstrated that proposed approach of ABAIDS could identify the unknown as well as known attacks. 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.

Oh, et al. (2017) presented a connected, intelligent and context-aware device that works collectively known as internet of things (IOT) [12]. The IOT devices are growing quickly in the recent years as it provides the common functions of IOT devices that are helpful to all. 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. 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.

Mbanaso, et al. (2017) presented a novel configurable policy-based specification and the threats and vulnerabilities faced by an IOT system were analyzed [13]. This specification has been utilized to scale proportionately in solving trust confidentiality and privacy issues in distributed environments. 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.

Zhang et al. (2018) proposed a Recryptor in this paper which is are configurable cryptographic processor which utilizes its computational capabilities in order to enhance the existing memory of a commercial general-purpose processor [14]. A 10-transistorbitcell supports, in-memory bitline computing for the support of different bitwise operations up to 512-bits wide. The high-throughput computing capabilities near memory are provided by the custom-designed shifter, rotator, and S-box modules as they are located near the memory. The programmability of the Recryptor's was demonstrated. 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 decentralized networks that include sensor nodes which sense and pass the information to the base station are known as Internet of Things. Since the sensor nodes deployed here are very small in size, the major concern arising here is the amount of energy being consumed. This research work is focused on the energy consumption of the wireless sensor networks. For increasing the overall lifetime of networks, clustering is an efficient approach that can be applied. The data is partitioned into fixed size clusters through this approach. For every individual cluster, a cluster head is chosen to which all the data collected by each cluster is forwarded. The data is transmitted to the base station through the cluster head. LEACH protocol provides optimization such that the lifetime of networks can be increased. Among the cluster head and base station, the deployment of cache nodes is done within the proposed approach. The data is transmitted to the cache node closest and then forwarded to the base station using cluster heads. From the cluster head closest to it, the data is aggregated by the cache. The distance between the gateway node and cluster head is calculated using Euclidian distance formula.

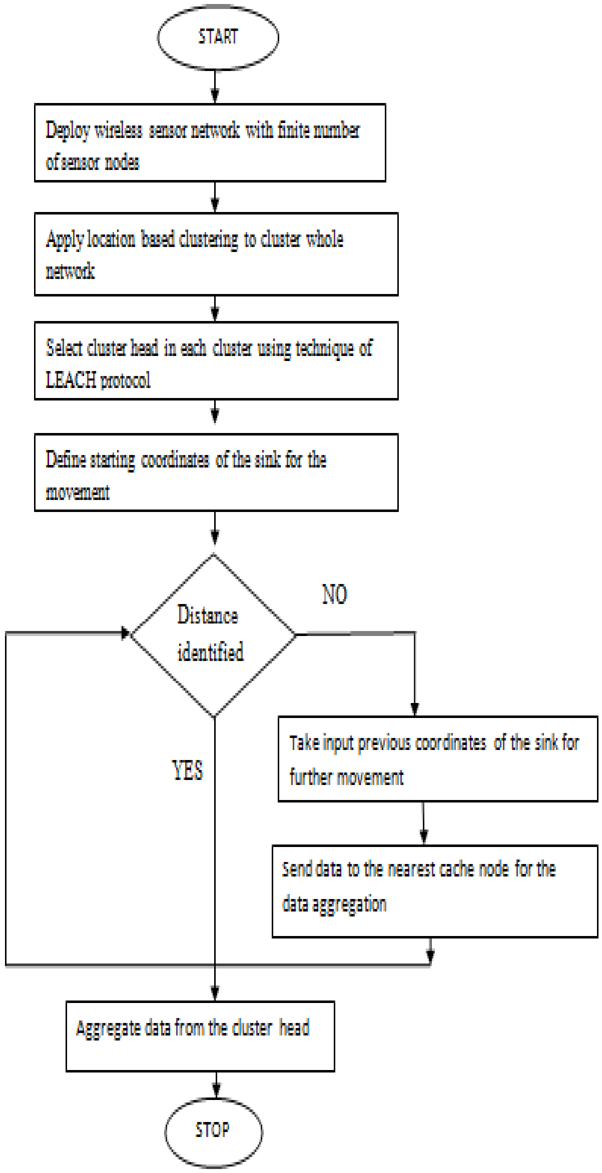
START
Deploy wireless sensor network with finite number of sensor nodes
Apply location based clustering to cluster whole network
Select cluster head in each cluster using technique of LEACH protocol
Define starting coordinates of the sink for the movement
Distance identified
NO
YES
Take input previous coordinates of the sink for further movement
Send data to the nearest cache node for the data aggregation
Aggregate data from the cluster head
STOP

Fig.1: Proposed Flowchart

Description of Flowchart

i. There are finite numbers of sensor nodes deployed in networks and location based clustering is used to deploy the network into clusters of fixed size.

ii. LEACH protocol is applied for choosing the cluster head for every individual cluster. The cluster head is chosen based on the two important factors which are highest energy and least distance of nodes. The data will be aggregated to cluster head by applying other nodes.

iii. The data is aggregated to the cache node closest to the cluster head. Euclidian distance is used to calculate the distances among cluster head and cache node.

iv. This step 3 is repeated until required data get aggregated to base station

IV. EXPERIMENTAL RESULTS

The proposed research is implemented in MATLAB and the results are evaluated by comparing proposed and existing approaches in terms of several performance parameters.

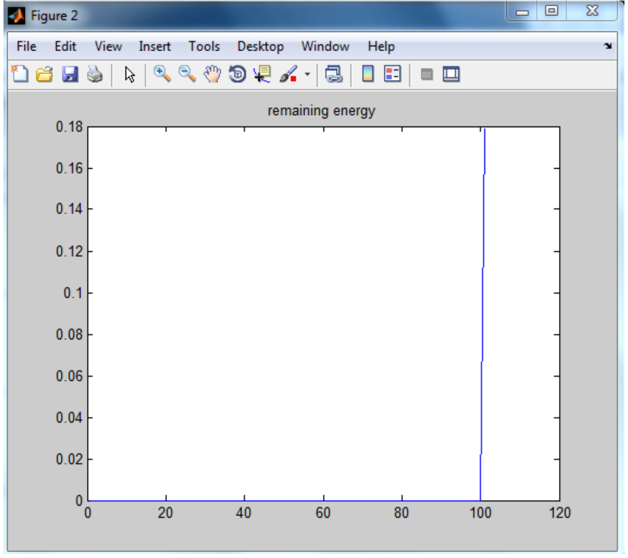

Fig.2: Remaining energy of the proposed scenario

As shown in figure 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.

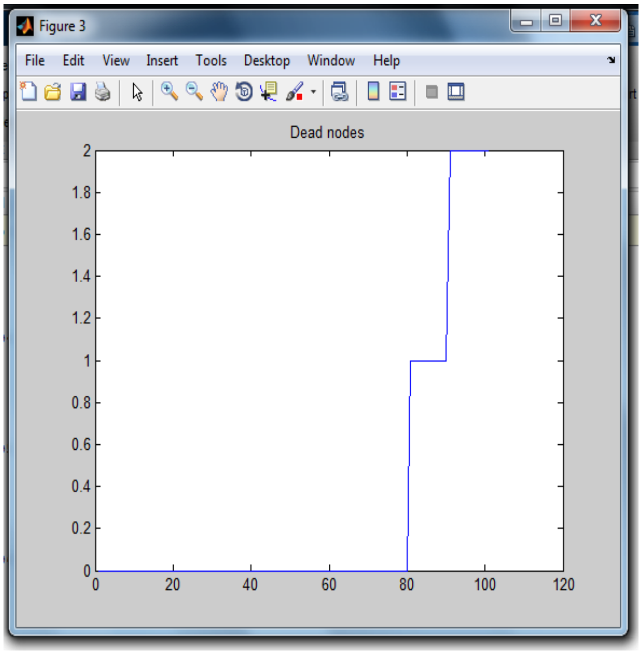

Fig.3: Number of Dead Nodes with Proposed protocol

Figure 3 shows the graph is shown in which number of dead nodes are shown verses number of rounds. The numbers of rounds are depicted on x-axis and the number of dead nodes on y-axis.

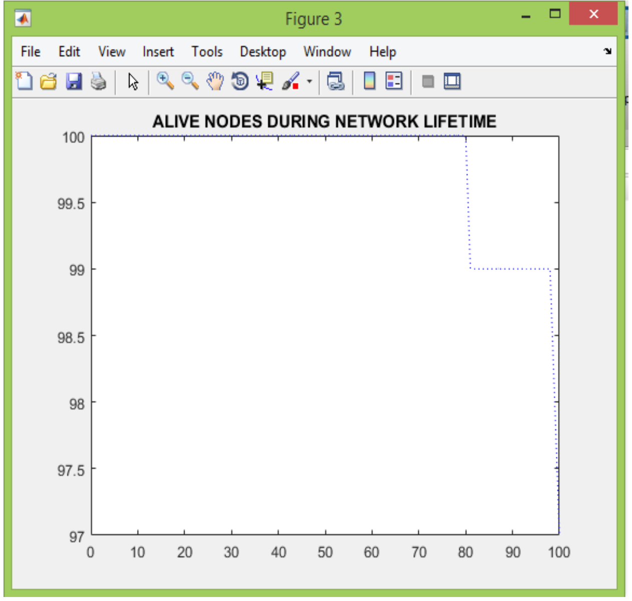

Fig.4: Number of Alive nodes

Figure 4 shows the performance of proposed algorithm is analyzed in terms of number of alive nodes. Only two nodes get dead and all other nodes are alive

V. CONCLUSION

This research concludes that the major concern to be resolved in the IoT networks is the amount of energy being consumed since they are dynamic in nature. The clusters that are of fixed size are generated through clustering and for every individual cluster, a cluster head is selected. Based on the two parameters namely, energy and distance, the cluster heads are chosen. A cluster head is selected by calculating the distances and energy parameters of all the nodes and the node with least energy and highest energy is elected as cluster head. In this research work, a gateway node is used to improve the LEACH protocol. From the cluster head, data will be aggregated by the cache node. The data is transmitted towards the base station statically through the cluster head. MATLAB simulation is used to compare the proposed and existing techniques. It is seen through the evaluations that with respect to number of dead nodes and remaining energy, the proposed technique outperforms other approaches.

VI. REFERENCES

[1]. Rose, K., Eldridge, S., & Chapin, L., “The internet of things: An overview”, 2015, The Internet Society (ISOC), 1-50.

[2]. Patel, K. K., Patel, S. M., & Professor, P. S. A., “Internet of Things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges”, 2016, Int. J. Eng. Sci. Comput, 6(5).

[3]. Nguyen, K. T., Laurent, M., & Oualha, N., “Survey on secure communication protocols for the Internet of Things”, 2015, Ad Hoc Networks, 32, 17-31

[4]. Mitrokotsa, A., & Douligeris, C., “Integrated RFID and sensor networks: architectures and applications. RFID and sensor networks: Architectures, protocols, security and integrations”, 2009, 512, 511-535

[5]. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I., “Internet of things: Vision, applications and research challenges”, 2012, Ad hoc networks, 10(7), 1497-1516.

[6]. K. A. M., & Elmustafa, S. A. A., “Internet of Things applications, challenges and related future technologies”, 2017, World Scientific News, 2(67), 126-148.

[7]. Jo, D., & Kim, G. J., “ARIoT: scalable augmented reality framework for interacting with Internet of Things appliances everywhere”, 2016, IEEE Transactions on Consumer Electronics, 62(3), 334-340

[8]. Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P., “A lightweight IoT security protocol”, In Cyber Security in Networking Conference (CSNet), 2017 1st(pp. 1-8). IEEE.

[9]. Seralathan, Y., Oh, T. T., Jadhav, S., Myers, J., Jeong, J. P., Kim, Y. H., & Kim, J. N., “IoT security vulnerability: A case study of a Web camera”, 2018, In Advanced Communication Technology (ICACT), 2018 20th International Conference on (pp. 172-177). IEEE.

[10]. Vorakulpipat, C., Rattanalerdnusorn, E., Thaenkaew, P., & Hai, H. D., “Recent challenges, trends, and concerns related to IoT security: An evolutionary study”, In Advanced Communication Technology (ICACT), 2018 20th International Conference on (pp. 405-410). IEEE.

[11]. Pacheco, J., Ibarra, D., Vijay, A., & Hariri, S., “IoT Security Framework for Smart Water System”, 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA) (pp. 1285-1292). IEEE.

[12]. Oh, S. R., & Kim, Y. G., “Development of IoT security component for interoperability”, Computer Engineering Conference (ICENCO), 2017 13th International (pp. 41-44). IEEE.

[13]. Mbanaso, U. M., & Chukwudebe, G. A., “Requirement analysis of IoT security in distributed systems”, Electro-Technology for National Development (NIGERCON), 2017 IEEE 3rd International Conference on (pp. 777-781). IEEE

[14]. Zhang, Y., Xu, L., Dong, Q., Wang, J., Blaauw, D., & Sylvester, D., “Recryptor: A Reconfigurable Cryptographic Cortex-M0 Processor With In-Memory and Near-Memory Computing for IoT Security”, 2018, IEEE Journal of Solid-State Circuits