Received: March 19, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Evolutionary Secure Energy Efficient Routing Protocol in Internet of Things

Praveen Kumar Reddy[1]* **Rajasekhara Babu [1]**

[1]*Vellore Institute of Technology University, Vellore, Tamil Nadu, India*
* Corresponding author's Email: praveenkumarreddy@vit.ac.in

Abstract: Recently, Internet of Things (IoT) devices are highly utilized in diverse fields such as environmental monitoring, industries, smart home etc. Under such instance, a cluster head is selected among the diverse IoT devices of wireless Sensor Network (WSN) based IoT network to maintain the reliable network with efficient data transmission. To accomplish the efficient cluster head selection, we have used Fuzzy C-Means (FCM) clustering algorithm. Therefore, it is necessary to implement secure energy aware routing protocol in IoT. This paper proposed a novel method with the combination of Optimal Secured Energy Aware Protocol (OSEAP) and Improved Bacterial Foraging Optimization (IBFO) algorithm. The aforesaid challenges against the secure energy awareness objective under IoT are not yet dealt by any researchers. Furthermore, the Optimal Secured Energy Aware Protocol (OSEAP) and Improved Bacterial Foraging Optimization (IBFO) algorithm is one of the best methods to save more energy with security among the nodes. The performance analysis in terms of delay, throughput, and energy determined by comparing the proposed method with the existing method Secure Energy aware routing protocol (SEAP). Thus, the analysis of our implementation reveals the superior performance of the proposed method.

Keywords: Internet of things, Optimal secured energy aware protocol, Improved bacterial foraging optimization, Group key distribution.

1. Introduction

With the rapid development of technology, the growth of the sensing devices has increased [1-2]. Generally, WSN is considered as the principle importance in the field of network technology [3]. 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 utilizing in vast applications [4-5]. The system interconnected with computing device, digital and mechanical instruments, animals, people or other objects is called IoT [6-9]. 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 [10-11]. Rather than customize data from the surrounding environment, the users can observe, sense and regulate the objects placed in the corresponding environment [12-13]. 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 another network [14-15]. Basically, the WSN are provided with battery power which is to be recharged. Under such instance, proper scheduling of energy utilization is required especially when the sensors are distantly connected [16-17]. Numerous nodes transfer multiple data from node to the base station about the same event, which leads to transfer redundant data [18-19]. 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 [20]. 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 [21]. In order to decrease the energy consumption in IoT, our projected technique uses OSEAP. The virtual topology on the basis of network topology is industrialized that encompasses a set of sensor nodes. The sensor nodes are clustered with the help of fuzzy c means (FCM) algorithm. After clustering the sensor node, the cluster head is nominated. Successively to decrease energy consumption preliminary from a group of sensors that are concerned with a precise event, we endorse an Optimal Secured Energy Aware Protocol (OSEAP) that facilitate every sensor in the way to continue dynamic or to upsurge the duty cycles as well as every remaining neighbouring to be in their sleeping state thereby successively permitting steady. Information routing with no sustaining wastage of power. In order to confident energy-aware protocol the recommended method uses the group key distribution procedure based on minimum energy consumption. The key will be arbitrarily changed in order to eliminate the attacks. At this time, the optimal Key will be designated with the help of Improved Bacterial Foraging Optimization (IBFO) algorithm.

The rest of the paper is organized as follows. Section 2 describes about the related work regarding the recent trends in the field of energy aware in IoT. Section 3 explains about the problem definition of proposed work. Section 4 frames the problem formulation for cluster head selection and group key distribution. Section 5 discuss about the simulation environment and the results evaluation. Finally, Section 6 concludes the overall contribution of the research work.

2. Related work

In [22], the authors presented propose online heuristics for public data delivery in smart city settings and also introduce a pricing utility function for data acquisition. There pricing function considers resource limitations in terms of delay, capacity and lifetime on the data provider's side, as well as user's quality and trust requirements from the requesters' side. The simulations associated with delay, lifetime of a node were performed. In this method authors failed in showing the stability and convergence of network.

In 2016, ZhangBing et al. [23] have embraced the Enhanced - Channel-Aware Routing Protocol (E-CARP) to make the organization of Internet of Underwater Things. The standard goal considered in this experimentation was the accomplishment of modest information sending and less vitality utilization framework. Moreover, the proposed strategy has tended to the fundamental issues from the traditional Carp technique that does not take after the reusability property and PING-PONG strategy that chooses the hand-off hub when the system is in relentless state. The simulation results were taken which have given the system minimum correspondence cost and high ability. The main drawback of this method is authors failed to provide security among the nodes.

Shelby et al. [24] have offered a routing protocol for IoT systems that explains how to route the data via Internet among non-internet sensors or devices. The efficacy of the trust assessment procedure was mainly directed using dependence source, as that controls the burden in the procedure as well as the function of WSNs was predominantly responsive for burden because of the minimized energy.

In 2016, Tie Qiua et al. [25] have carried a Greedy Model with Small World (GMSW) in order to maintain the robustness of the IoT structure with expanded execution. At to start with, the nearby significance of the hubs was dictated by the voracious criteria. Here, they considered that the attainability of the streamlining calculation was gotten by the little world model. The speed of the GMSW calculation to get to the system with modest number of alternate ways can be accomplished through the execution assessment of the proposed with the current techniques. The method is applicable for smaller networks which is the main drawback.

In [26], the authors have proposed a directing convention for Emergency Response IoT based on Global Information Decision (ERGID) to enhance the exhibitions of solid information transmission and productive crisis reaction in IoT. In particular, authors have plan and understand an instrument called Delay Iterative Method (DIM), which depends on postpone estimation, to take care of the issue of overlooking legitimate ways. In addition, a sending technique called Residual Energy Probability Choice (REPC) is proposed to adjust the heap of system by concentrating on the remaining vitality of hub. Recreation results and investigation demonstrate that ERGID beats EA-SPEED and SPEED as far as end to end (E2E) delay, energy consumption, packet loss. Authors have not addressed the reliable end to end trust mechanism which is the main drawback of this method. In order to circumvent false carrier sensing and saturation of amplifiers, Lee and Kim [27] have offered a Wi-Fi design that integrates multi-level and multi-channel carrier sense and gain control system

and it was an interference-aware self-optimizing (IASO).

Secure end-to-end communication, a smart gateway with the help of robust mobility models and fortified authorization and integrity between IoT devices that are projected by Moosavi et al. [28]. In their method, without necessitating any reconfiguration at the device layer, the fog layer succor's ubiquitous mobility. The core idea of Wireless networking was totally exaggerated by the development of IoT. Numerous devices in MAC and other protocols are industrialized to ensure the function of WN. Marco et al. [29] has defined MAC as well as forwarding rules to IoT that was given using the objective on the IEEE 802.15.4 MAC as well as IETF RPL procedures. The routing parameters and MAC parameters are permitted in the projected system to upsurge the performance. IoT is an emergent concept in wireless communication in which Wu et al. [30] has defined an inspiring design on the basis of IEEE 802.11 MAC. In their mechanism, they are with the help of RTS, CTS and ACK for handshaking. They are eliminating the unseen terminal issue in multicast routing.

3. Problem definition

To decrease the failure, proportion and to diminish energy occupancy, consecutively to incredulous these apprehensions, we hope to plan appropriate mechanisms. Increased vitality as well as safeguard ratio was chosen for retreating the loss ratio, and nodes [31]. By ease minimum duty cycle process and signal analysing, we are using minimum energy utilization in sensing links for permitting longer effective network duration. A power control protocol proficient is envisioned to expand the duration of the network. To trace the appropriate preliminary transmission power preliminary phase is engaged for every neighbouring node as quickly as probable. With the ecological change, the preserving phase is employed to energetically solve and alter the appropriate broadcast power level.

By operating an adaptive power control instrument energy utilization of inactive nodes could be focussed. To weaken vitality rate of sensing nodes and energy talented MAC is thus obligatory. To doze just to enhance the endless information routing devoid of obtaining vitality desecrate of unlinked nodes we necessitate a MAC which could notify every node via the way for continuing dynamic as well as enhance the duty cycles as well as every remaining neighbourhood node [32]. The broadcast power may be accustomed, derived from the things presented by the sensors. To the captivated things to be issued the communication stems the opportunity of registering dependent sensors. Starting from the dependent sensors the virtual topology is derived from the notification [33].

IoT is one among the promising topics in the field of wireless communication and there are no precise protocols for IoT. The protocols, namely AODV, DSR, OLSR, IPv6 and IEEE 805.15.4 that are utilized with respect to ad-hoc network are further extended as well as their function in IoT circumstances are further scrutinized for future IoT protocols. Energy-aware systems in IoT devices will diminish the power consumptions of all nodes in the multicast group. Because the nodes having constrained power and energy only.

4. Proposed methodology

General diagram of the projected technique is as follows. In the projected IoT scheme has a network topology comprising a number of sensor node. Then the numbers of sensor nodes are clustered by FCM algorithm. From the clusters, a cluster head is nominated with maximum communication and minimum energy consumption. In our recommended method, the power usage needed for nodes is abridged by Optimal Secured Energy Aware Protocol (OSEAP). In order to secure energy-aware protocol, the recommended method utilizes the group key distribution. The group key distribution procedure is utilized for conveying a message from source to destination node thru the selected path. This key gets changed at the time of packet drop and attack. Henceforth, the keys are optimally designated with the help of Improved Bacterial Foraging Optimization (IBFO) algorithm. Brief elucidation of the general procedure is exposed in the additional segment.

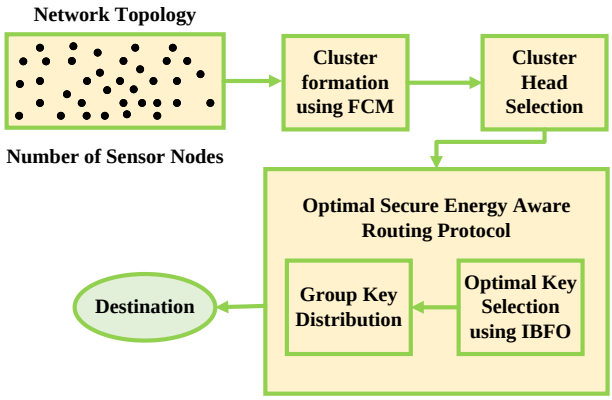

Figure.1 Overall Semantic Diagram

4.1 Cluster formation

Firstly, the virtual topology on the basis of network topology is developed that comprises a group of sensor nodes. The nodes are gathered with the help of FCM algorithm. The cluster is well-defined as a set of analogous nodes positioned or occurring closely together. Cluster formation aids to progress data transmission which decreases energy consumption. The comprehensive description of the FCM algorithm is as follows.

4.1.1. Fuzzy C-means clustering algorithm (FCM)

Fuzzy c-means (FCM) is the method of grouping that allows a piece of information to be in more or less than two groups. It provides the best result for overlapped information set and moderately better thank-means algorithm. At this time, information regards were allocated partisanship for all groups as a solution of that information regards might come under the category greater than a cluster centre. The objective performance of projected fuzzy c means algorithm is efficiently elucidated as follows.

$$O_{f=\sum_{i=1}^{n}\sum_{k=1}^{c}M_{ik}^{m}d_{ik}^{2}} \quad (1)$$

Where d_{ik} is the distance between cluster and data

$$d_{ik} = \|N_i - C_k\| \quad (2)$$

Here,

m → Real number more than unity

M_{ik} → The level of membership of i belonging to the group k

N_i → i_{th} of d-dimensional calculated information of node

C_k → Cluster centre of the d-dimension

Algorithm 1: Fuzzy c-means (FCM)

Step 1: FCM algorithm and its objective function are revealed in Eq. (1).

Step 2: Compute the fuzzy centers C_k

$$C_K = \frac{\sum_{i=1}^{n}M_{ik}^{m}N_i}{\sum_{i=1}^{n}M_{ik}} \quad (3)$$

Step 3: Compute the fuzzy membership function M_{ik} using

$$M_{ik} = \frac{1}{\sum_{j=1}^{c}\left(\frac{\|N_i-C_k\|}{\|N_i-C_j\|}\right)^{2/m-1}} \quad (4)$$

Step 4: Repetition of task 2 as well as 3 unless the greater O_f measure obtained.

Thus, clusters are formed with the help of FCM algorithm. Once the clusters are formed it is vital to designate the cluster heads to enable easy transmission of messages. Transmitting messages from source to sink without cluster head is a tedious procedure. Henceforth to evade this cluster head selection procedure is favoured.

4.2 Cluster head selection

After cluster development cluster heads are designated in each cluster. The CH gathers as well as collects and receives information from nodes belonging to the same cluster and then transfers on information to reach the destination. By rotation of the cluster-head arbitrarily, energy consumption is anticipated to be uniformly dispersed. Normally CHs are designated from the organized nodes on the basis of the criteria like residual energy, and connectivity. CH selection may be indeterministic or probabilistic manner. The following steps are related to cluster head selection. The predicted system marks a sensor as a cluster head if it has minimum energy consumption. The node containing maximum level of communication with other cluster nodes is designated as a head of the cluster. Cluster head election will further add additional levels contingent on the topology of the network. Customarily, a node will be designated as CH based on above-mentioned criteria. The CH in each cluster keeps fluctuating based on its energy consumption. If the node designated as CH moves to sleep state in the course of transmission of messages, then the node remaining active with low energy consumption and maximum communication will be nominated as CH in the cluster. For diminishing the energy consumption of the cluster head, Optimal Secured Energy Aware Protocol (OSEAP) is utilized in our projected technique.

4.3 Optimal secured energy aware protocol

If all the nodes remain active for the period of data transmission, then there is a possibility for depletion of energy. Henceforth in order to save the energy delivered to the undesired nodes the nodes that are not convoluted in data transmission is set to sleep state and henceforth the energy is delivered only to the nodes lingering inactive state. EARP protocol unswervingly controls the energy consumption. In specific, it attains balanced energy consumption amongst all contributing mobile nodes. In EARP, the receiver nodes need not to be paused for getting most energy effectual routing path to forward the information. Depending on the battery level, the nodes have the choice to regulate whether or not to accept and forward the route request

message to their neighbour nodes. Meanwhile, the energy is not wasted this protocol aids the best in energy consumption. After conserving energy consumption using Optimal Secured Energy Aware Protocol (OSEAP) group key distribution procedure is utilized for transmitting messages from source node to destination node.

4.3.1. Group key distribution

It indicates a security key which is provided within consumer groups. Primarily, group key will be delivered to set of nodes utilized for transmitting messages to the sink node. The designated nodes have minimum energy consumption. If there is any packet drop or attack in the node convoluted in the transmission of messages, then another path will be designated for message transmission. Henceforth the group key will be transformed for the path designated. The main usage of this key scheme is that it allows permitting the set of consumers to decode a transmitted information which was envisioned to the whole consumer groups as well as none others. The key will be arbitrarily changed in order to eliminate the attacks. At this time, the optimal Key will be designated with the help of the Improved Bacterial Foraging Optimization (IBFO) algorithm.

4.3.2. Improved bacterial foraging optimization (IBFO) algorithm

Bacterial Foraging Optimization (BFO) algorithm is an innovative evolving calculation algorithm projected on the basis of the food searching characteristics of Escherichia coli (E. coli) organism existing in the intestines of people. Food searching characteristics of bacteria is the way of increasing the vitality attained for single duration. Bacteria likewise interconnect to all others via transmitting replies. Bacteria consider scavenging choice only then bearing in mind dual prior facts. The procedure, using what a bacteria steps using few stages when probing to food searches, is known as chemotaxis. The chief notion with respect to BFO is imitation of the chemotactic motion of actual bacterium with respect to the issue based foraging areas. After investigation of optimization mechanism, sequences of values were considered for improving the traditional BFO as well as ti is known as enhanced bacterial foraging optimization (IBFO) algorithm. The step by step process of BFO algorithm is illustrated in below.

Algorithm 2: Improved Bacterial Foraging Optimization (IBFO)

Table 1. Definition of terms

Symbol	Explanation
P	Measurements of the parameters
S	Amount of bacterium group
R	Foraging radius
C	Stage represented using the fall over
V	Speed of bacterium in chemotaxis
N_c	Amount of chemotaxis tasks
N_s	Stages of swimming action
N_r	Amount of reproducing
N_{ED}	Amount of elimination-dispersal action
P_{ED}	Likelihood of elimination- dispersal action
$\emptyset$	Unity vector in arbitrary
Δ	Random Vector
ω^a	Original location of a^{th} bacteria
J_{gbest}	Finest fitness of bacteria
ω_{gbest}	Respective location of the J_{gbest}
ω_{min} ω_{max}	Foraging capacity of bacterium swarm
a	Numerical value of bacterium directory, a =1, 2, …S
b	Directory of chemo taxis task, b=1, 2, …, N_c
c	Directory of the reproduction, c =1, 2, …, N_r
d	Directory of the elimination-dispersal action, d =1, 2, …, N_{ED}
e	Directory of the action of swimming, e =1, 2, …, N_s

Step 1: Initialization of the original values.

Step 2: Computation of the consistent charge rate of bacteria $J(a,b,c,d)$ and memorize the J_{gbest} and ω_{gbest}.

Step 3: Dynamic search is achieved with the help of the following equations.

$$\omega_{max}(j) = \omega_{gbest} + \left({}^{R}/_{2^b}\right) \quad (5)$$

$$\omega_{min}(j) = \omega_{gbest} - \left({}^{R}/_{2^b}\right) \quad (6)$$

Step 4: Update location of bacteria with the help of the below equation. Once the criteria are good, the action of swimming design might occur accompanied with track as well as measurement of task remains unmodified just to obtain the predefined numerical.

$$\omega^a(b+1,c,d) = \omega^a(b,c,d) + C(a)\emptyset(a) \quad (7)$$

$$\emptyset(a) = \Delta(a)/\sqrt{\Delta^T(a)\Delta(a)} \quad (8)$$

$$C(a) = C_{max}(a) - C_{max}(a) - C_{min}(a)/N_c \,.\, b \quad (9)$$

Step 5: The location of bacteria next to each motion swimming is reorganized using the subsequent equations

$$V_a^b = \left(1 + \emptyset_1\emptyset_2\sqrt{(\emptyset_1 + \emptyset_2)(2 + \emptyset_1 + \emptyset_2)}\right).V_a^b + \emptyset_1(\omega_{gbest} - \omega^a(b)) \quad (10)$$

Step 6: Bacterium goes to the reproductive stage while that influences the predefined amount of the chemotactic stages. Compute the food criteria of bacterium, and then wrap bacterium of maximum J_{health} with using the other bacterium.

Step 7: Eliminate and disperse bacteria during the optimization section using the likelihood of P_{ED}.

Step 8: The algorithm would terminate on the criteria of attaining the stopping condition, then produce the fittest parameter ω_{gbest}, or else return to step 2.

On the basis of the above procedure, the recommended method picks the optimal group key. In order to save the transmission of messages, the optimal group keys are desirable. So, that the security level of the recommended method is enhanced with minimum energy consumption. Hence it is appropriate for better data transmission in IoT with minimum energy. The performance of the suggested technique is described in section.5.

5. Results and Discussion

The simulation of the proposed work for IoT devices under the WSN based IoT network was implemented in MATLAB R2015a. The real-time data acquisition is done by Xively IOT platform from which the data are read through Xively IOT API (downloaded from http://in.mathworks.com/matlabcentral/fileexchange/46986-xivelyread). The experimentation was performed by considering the delay, packet delivery ratio, throughput, packet drop and energy of the IoT devices. The simulation procedure was accomplished based on the fixed values of the following parameters. At the beginning of the experimentation, the base station of the IoT network was localized in the centre followed by localizing the IoT devices in the area of 100m × 100m.

5.1 Evaluation metrics

With the help of the assessment metrics end to end delay, Packet delivery ratio, throughput as well and energy consumption the function of the recommended system is assessed.

5.1.1. End to end delay

End-to-end delay or else one-way delay (OWD) indicates the total duration needed for a data to get transferred from starting to the end node.

$$d_{end-end} = n\left[d_{trans} + d_{prop} + d_{proc} + d_{queue}\right] \quad (11)$$

Where,

$d_{end-end}$ → Delay with respect to end to end transmission

d_{trans} → Delay involved during transmission of data

d_{prop} → Interruption during propagation

d_{proc} → Interruption while analysing

d_{queue} → Queuing delay

End to end delay of the WSN based IoT network is graphically represented in Figs. 2 and 3. Figure 2 compares the delay comparison by varying number of nodes with conventional methods like SEAP. Here, in the proposed method for 20 nodes, the delay is 0.06593 and 1.150234 of delay is obtained using the existing method. On other hand, for 100 nodes, the delay obtained using the proposed method is 0.794335 and 0.867135 of delay is obtained using the existing method. Figure 3 shows the graphical representation of the delay comparison results by varying the number of rate value. For 50 rates the delay using OSEAP is 0.356015 and the delay using SEAP is 0.581344. 2.422758 of delay is obtained using the proposed method for 250 rates and 7.594994 of delay is obtained using the existing method. This achievement of the proposed method is definitely better than the conventional methods.

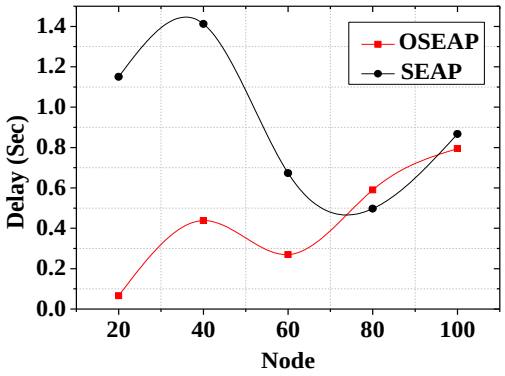

Figure.2 Delay comparison by varying number of nodes

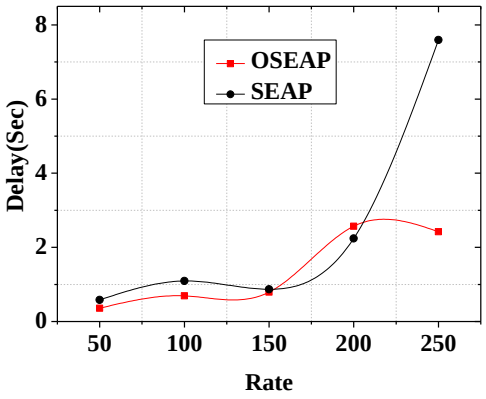

Figure.3 Delay comparison by varying number of rate

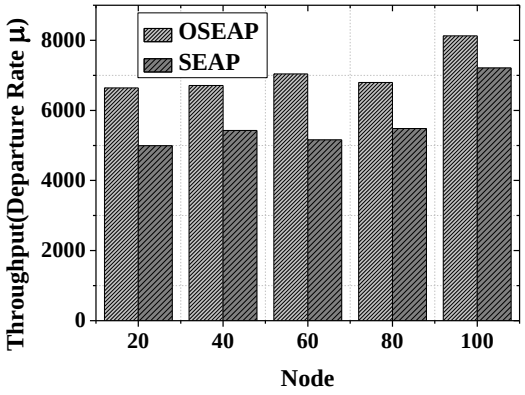

Figure.4 Throughput comparison by varying number of nodes

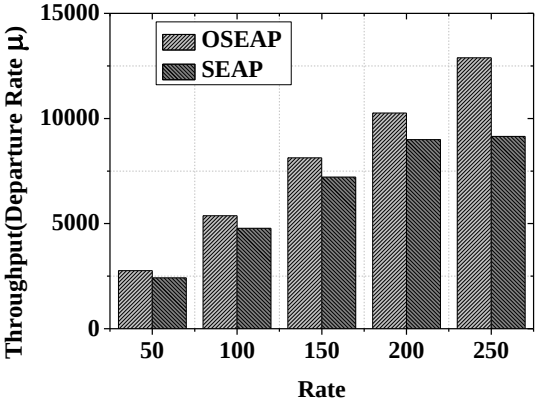

Figure.5 Throughput comparison by varying number of rate

5.1.2. Throughput

It indicates the total information which was transferred from the sender to the receiver.

$$Throughput = \frac{File\ Size}{Transmission\ Time} \quad (12)$$

The analysis of the proposed with the conventional methods in terms of throughput for the IoT devices is shown Figs. 4 and 5. Basically, the stability of the network maintains if the throughput of IoT devices perform better. Throughput comparison results for proposed and existing methods are plotted in Fig. 4. Initially, throughput is less for 20 nodes and after then throughput is increased for 100 nodes. On comparing the proposed and the existing methods, throughput of the proposed method is better than the existing method. Figure 5 represents the pictorial representation of the throughput comparison results by varying the number of rate value. Collectively, at different rates, throughput of the proposed method is better than the conventional methods, which therefore maintains the consistency of IoT based WSN network.

5.1.3. Energy Consumption

Energy consumption is well-defined as the communication overhead of the nodes where a firm number of false data are injected into a network.

$$Energy = Power \times Time \quad (13)$$

The performance analysis of Energy Consumption in IoT devices is shown in Fig. 6 and 7. Figure 6 shows the graphical representation of the energy comparison results for proposed and existing method. The energy of the proposed method is 13.21J at the beginning and 13.21J at 100 nodes. The energy consumption of the proposed method is better than the conventional methods till 100 nodes which thus provide superiority to the proposed algorithm. Figure 7 represents the graphical representation of the energy comparison results by varying the number of rate value. Here, 14.324J of energy is spent using OSEAP for 50 rates and 17.628J of energy is spent for SEAP. For 250 rates 12.591J of energy is needed for the proposed method and 14.567 of energy is needed using the existing method.

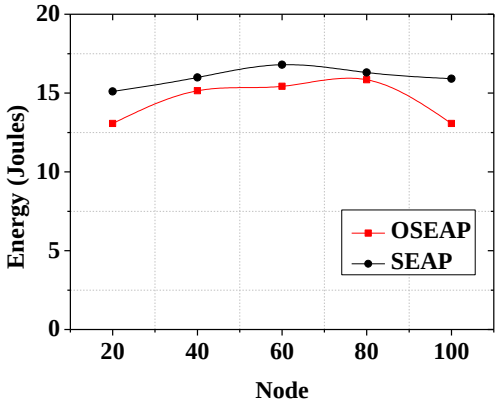

Figure.6 Energy comparison by varying number of nodes

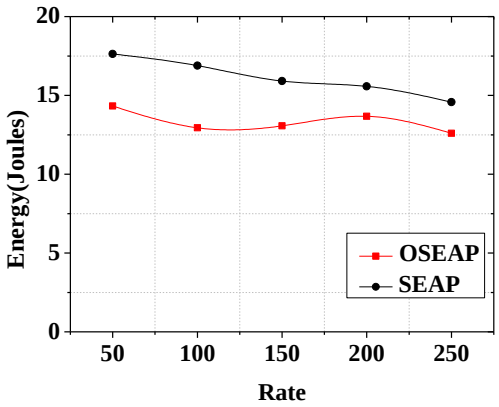

Figure.7 Energy comparison by varying number of rate

6. Conclusion

Optimal Secured Energy Aware Protocol (OSEAP) with the assistance of Improved Bacterial Foraging Optimization (IBFO) algorithm is projected in this paper. Primarily, the virtual topology on the basis of network topology is industrialized. All the sensor nodes in the network topology are clustered with the help of Fuzzy C-Means (FCM) clustering algorithm. In order to facilitate the protected transfer of messages from the source node to destination node group key distribution procedure is engaged in OSEAP. The key selection is performed by IBFO algorithm. The performance of the projected system is assessed by means of delay, throughput and energy. The experimental results display that our proposed method serves better performance with minimum energy consumption, delay and better throughput than the existing method Secured Energy Aware Protocol (SEAP). Hence the proposed scheme achieves 11% of overall reduction in consumed energy rate when compared to existing protocol which provides 15% of energy consumption rate. In future, some other advanced cluster head section techniques using meta heuristic algorithms could be utilized for increasing the life time of a node.

References

[1] Y. Kawamoto, H. Nishiyama, M. Fadlullah and N. Kato, "Effective Data Collection Via Satellite-Routed Sensor System (SRSS) to Realize Global-Scaled Internet of Things", *IEEE Sensors Journal*, Vol.13, No.10, pp.3645-3654, 2013.

[2] L. Fagen, H. Yanan and J. Chunhua, "Practical access control for sensor networks in the context of the Internet of Things", *Computer Communications*, Vol.89, No.1, pp.154-164, 2016.

[3] J. Duan, D. Gao, D. Yang, C. Foh and H. Chen, "An Energy-Aware Trust Derivation Scheme with Game Theoretic Approach in Wireless Sensor Networks for IoT Applications", *IEEE Internet of Things Journal*, Vol.1, No.1, pp.58-69, 2014.

[4] H. Dai and H. Xu, "Key Predistribution Approach in Wireless Sensor Networks Using LU Matrix", *IEEE Sensors Journal*, Vol.10, No.8, pp.1399-1409, 2010.

[5] A. Agarwal, G. Misra and K. Agarwal, "The 5th Generation Mobile Wireless Networks- Key Concepts, Network Architecture and Challenges", *American Journal of Electrical and Electronic Engineering*, Vol.3, No.2, pp.22-28, 2015.

[6] E. Kougianos, S. Mohanty, G. Coelho, U. Albalawi and P. Sundaravadivel, "Design of a High-Performance System for Secure Image Communication in the Internet of Things", *IEEE Access*, Vol.4, No.1, pp.1222-1242, 2016.

[7] Y. Liu, W. Han, Y. Zhang, L. Lulu, J. Wang and L. Zheng, "An Internet-of-Things solution for food safety and quality control: A pilot project in China", *Journal of Industrial Information Integration*, Vol.3, No.1, pp.1-7, 2016.

[8] P. Hyuncheol, K. Hoichang, J. Hotaek and S. Jaeseung, "Recent advancements in the Internet-of-Things related standards: A one M2M perspective", *ICT Express*, Vol.2, No.3, pp.20-26 2016.

[9] Sivieri, L. Mottolaa and G. Cugola, "Building Internet of Things software with ELIoT", *Computer Communications*, Vol.89 No.1, pp.141-153, 2016.

[10] Q. Ashraf and M. Habaebi, "Autonomic schemes for threat mitigation in Internet of Things", *Journal of Network and Computer Applications*, Vol.49, No.1, pp.112-127, 2015.

[11] C. Perera and V. Vasilakos, "A knowledge-based resource discovery for Internet of Things", *Knowledge-Based Systems*, Vol.109, No.1, pp.122-136, 2016.

[12] Lawanyashri, S. Subha, and Balamurugan. "Energy-Aware Fruitfly Optimisation Algorithm for Load balancing in Cloud Computing Environments", *International Journal of Intelligent Engineering and Systems*, Vol.10, No.1, pp.75-85, 2017.

[13] Shakkeera and L. Tamilselvan, "Towards Maximum Resource Utilization and Optimal Task Execution for Gaming IoT Workflow in Mobile Cloud", *International Journal of Intelligent Engineering and Systems*, Vol.10, No.1, pp.134-143, 2017.

[14] D. Wu, L. Bao and C. Liu, "Scalable Channel Allocation and Access Scheduling for Wireless Internet-of-Things", *IEEE Sensors Journal*, Vol.13, No.10, pp.3596-3604, 2013.

[15] A. Yachir, Y. Amirat, A. Chibani and N. Badache, "Event-Aware Framework for Dynamic Services Discovery and Selection in the Context of Ambient Intelligence and Internet of Things", *IEEE Transactions on Automation Science and Engineering*, Vol.13, No.1, pp.85-102, 2016.

[16] L. Abusalah, A. Khokhar and M. Guizani, "A survey of secure mobile Ad Hoc routing protocols", *IEEE Communications Surveys & Tutorials*, Vol.10, No.4, pp.78-93, 2008.

[17] S. Zhong and F. Wu, "A Collusion-Resistant Routing Scheme for Noncooperative Wireless Ad Hoc Networks", *IEEE Transactions on Networking*, Vol.18, No.2, pp.582-595, 2010.

[18] S. Moosavi, T. Gia, and E. Nigussie, "End-to-end security scheme for mobility enabled healthcare Internet of Things", *Future Generation Computer Systems*, Vol.64, No.1, pp.108–124, 2016.

[19] P. Marco, G. Athanasiou, P. Mekikis and C. Fischione, "MAC-aware routing metrics for the internet of things", *Computer Communications*, Vol.74, No.15, pp.77- 86, 2016.

[20] V. Cavalcante, J. Pereira, M. Pitanga, R. Moura, T. Batista, C. Flavia and F. Paulo, "On the interplay of Internet of Things and Cloud Computing: A systematic mapping study", *Computer Communications*, Vol.89, No.1, pp.17-33, 2016.

[21] S. Luo and B. Ren, "The monitoring and managing application of cloud computing based on Internet of Things", *Computer Methods and Programs in Biomedicine*, Vol.130, No.1, pp.154-161, 2016.

[22] A. Fagih, M. Fadi, M. Waleed, Alsalih, and S. Hossam,"A Priced Public Sensing Framework for Heterogeneous IoT Architectures", *IEEE Transactions on Emerging Topics in Computing*, Vol.1, No.1, pp.133-147, 2013.

[23] Z. Zhou, B. Yao, R. Xing, L. Shu and S. Bu, "E-CARP: An Energy Efficient Routing Protocol for UWSNs in the Internet of Underwater Things," *IEEE Sensors Journal*, Vol.16, No.11, pp.4072-4082, 2016.

[24] Shelby, Zach, and C. Bormann, *6LoWPAN: The Wireless Embedded Internet*, Vol. 43, John Wiley & Sons, Chichester, 2009.

[25] T. Qiu, D. Luo, F. Xia, N. Deonauth, "A greedy model with small world for improving the robustness of heterogeneous Internet of Things", *Computer Networks*, Vol.101, No.1, pp.127-143, 2016.

[26] Q. Tie, L. Yuan, F. Xia, N. Chen, J. Wan, and A. Tolba. "ERGID: An efficient routing protocol for emergency response Internet of Things," *Journal of Network and Computer Applications*, Vol.72, No.1, pp.104-112, 2016.

[27] I. Lee, and M. Kim, "Interference-aware self-optimizing Wi-Fi for high efficiency internet of things in dense networks," *Computer Communications*, Vol.89, No.1, pp.60-74, 2016.

[28] R. Moosavi, T. Gia, E. Nigussie, M. Rahmani, "End-to-end security scheme for mobility enabled healthcare Internet of Things", *Future Generation Computer Systems*, Vol.64, No.1, pp.108-124, 2016.

[29] P. Marco, G. Athanasiou, P. Mekikis and C. Fischione, "MAC-aware routing metrics for the internet of things", *Computer Communications*, Vol.74, No.15, pp.77-86, 2016.

[30] D. Wu, L. Bao and C. Liu, "Scalable Channel Allocation and Access Scheduling for Wireless Internet-of-Things," *IEEE Sensors Journal*, Vol.13, No.10, pp.3596-3604, 2013.

[31] B. Alcaraz, A. Cristina, and J. Lopez. "A security analysis for wireless sensor mesh networks in highly critical systems", *IEEE Transactions on Systems, Man, and Cybernetics*, Vol.40, No.4, pp.419-428, 2010.

[32] A. Cristina, B. Alcaraz, R. Roman, P. Najera and J. Lopez, "Security of industrial sensor network-based remote substations in the context of the Internet of Things", *Ad Hoc Networks*, Vol.11, No.3, pp.1091-1104, 2013.

[33] C. Atzori, B. Luigi, A. Iera, and G. Morabito. "The internet of things: A survey", *Computer networks*, Vol.54, No.15, pp.2787-2805, 2010.