International Journal of Computer Engineering in Research Trends
Multidisciplinary, Open Access, Peer-Reviewed and fully refereed
Review Paper Volume-8, Issue-12, 2021 Regular Edition E-ISSN: 2349-7084

Review on Data Aggregation Techniques in Internet of Things

Guguloth Ravi[1], M. Swamy Das[2]

[1]*Research Scholar,Department of CSE,University College of Engineerng(UCE),Osmania University(OU),Hyderabad,Telangana,India.*
[2]*Professor, Department of Computer Science and Engineering,Chaitanya Bharathi Iinstitute of Technology, Hyderabad,Telangana,India.*
Email : g.raviraja@gmail.com, msdas_cse@cbit.ac.in

**Corresponding Author: msdas_cse@cbit.ac.in*

Available online at: http://www.ijcert.org

Received: 21/10/2021, Revised: 13/11/2021, Accepted: 24/12/2022, Published: 29/12/2022

Abstract: The "Internet of Things" is a new paradigm that consists of several connected and related instruments with embedded sensing components that communicate with one other and with central nodes across a cordless network and the internet. IoT-enabled health care systems have recently attracted a lot of attention due to the importance of human health. However, because IoT networks are large-scale and battery-powered, it is necessary to set up appropriate energy and resource management systems for them. How to effectively provide information to the right users is a challenging problem for data management. To aid in machine-to-machine communication with linked data, cheap solutions for semantic IoT include dependable circulation distribution systems. In response to specific system queries provided by users, the system compiles integrated information streams produced by multiple collectors and delivers pertinent data to relevant users. To meet the demands of high efficiency data flow propagation in two conditions, such as point-to-point systems and flow breeding in wireless transmission systems, two novel information structures must be developed. Analysis of techniques using real-world datasets reveals that they are much more effective at sending linked information streams than the current technology. In order to maximize the utilization of the network lifetime, this study proposes SUNFLOWER-ALGORITHM based information gathering systems for IoT-enabled in various applications.

Keywords: IOT, WSN, Sunflower algorithm, high security, high accuracy, encrypted data.

---

1. Introduction

The "Web of Points" is a network of interconnected smart gadgets having the capacity to gather and distribute electronic data (IoT). IoT increases process effectiveness, contributes to time and cost savings, and reduces air pollution. It helps the general people comprehend how businesses make their products and provide their services. The Internet of Things (IoT) has the potential to change a number of industries, including healthcare, intelligent transportation, urban planning, intelligent agriculture, and power. For instance, doctors can monitor patients wherever they are with the help of cordless body sensors that can be either implanted or worn by the patient. These sensing devices provide physiological data, which is transmitted to a medical server so that doctors can review it and provide precise as well as superior diagnosis and treatments. Safety and security are crucial considerations in an IoT-enabled WSN environment to ensure information accuracy, discretion, honesty, timeliness, as well as network accessibility in case of assaults [3]. The authentication and accessibility management of big data databases, however, are

extremely demanding and necessitate the availability of data. As a result, unique and application-specific solutions must be taken into account for IoT networks against risks and also susceptibilities to prevent security and privacy breaches. [4] IoT has improved the use of smart devices in healthcare to measure clinical parameters by introducing new alternatives and also creating new research study locations. In order to monitor people, especially the elderly, WSNs are utilized in healthcare. These WSNs pick up devices to measure a variety of parameters, including blood sugar and stress, body temperature, heart rate, fall detection, and tip counting, to mention a few. Generally speaking, biosensors contribute to a wide range of applications, the majority of which are crucial or life-saving [5]. In order for doctors, nurses, and caregivers to find persistent patient conditions, data are acquired in a variety of situations and are continuously refined. We can diagnose many ailments through remote interactions and carry out a portion of the therapeutic procedure in your house using IoT in medical care systems, avoiding the need to refer patients to hospitals. Additionally, improving the accuracy and usability of data registration systems allows for speedier identification, treatment, and tracking of a variety of illnesses. As a result, such a rich, intricate, and nonlinear application area needs specific protocols and solutions.

Information gathering

The Net of Things, when viewed at the system level, is a vastly spread network system made up of numerous intelligent devices that produce and also take in information. In this network, there are several data nodes that are responsible for gathering and storing information from smart objects. These data nodes are typically autonomous and can vary in many ways. Due to this inherent property of circulation, many IoT applications frequently require information that is scattered across numerous information nodes, necessitating the compliance and exchange of the information by these information nodes in order to complete tasks. Aggregating data from dispersed data nodes is the norm in several applications of Industrial Web of Points. To conduct a thorough evaluation of a patient in the healthcare industry, we must combine data from several IoT-based healthcare providers who gather information about that person using various sensing devices. To assess the security of the food supply chain, we need data on how food is produced, handled, stored, distributed, and consumed. All of this data cannot be stored in a single data node. Some key enabling current technologies are based on gathering data from distant data nodes. Numerous applications, including supply chains, monitoring, and security, make use of items' tractability. The targeted item leaves records at each location it visits that are collected by various data nodes.

Utilization of aggregates:

Performance of aggregates is yet another crucial aspect. P2P excels at building large, scalable networks, but aggregation efficiency is a major drawback. The neighborhood information repository of a node is typically insufficient to support the aggregation demands, so the requests must be sent to its surrounding nodes for additional processing. The neighboring nodes then forward the requests to their next-door neighbors in turn, and so on until all pertinent information is gathered. There would be a massive and unpredictably high number of requests forwarded. In contrast, centralized designs do not experience issues with demand forwarding because only one management node has access to the necessary information. Residential property circulation plans might solve this issue and increase the aggregation efficiency. For some dispersed styles, they also need a little amount of forwarding among the administration nodes for various requests.

IoT design offers scalability and independent capability. The four-layer IoT design is described in the sections that follow.

1. Data gathering layer: Data from the surveillance location is gathered by various IoT devices and sensing units in this layer, which then sends the data to the sink. Undoubtedly, a self-organized and multi-hop geography is being created in the monitoring area by the release of millions of IoT tools. In a basic IoT system with sensors, a sink, and management nodes, the sensors collect the data from the tracking location and then send it in a multi-hop fashion to the sink.
2. Networking layer: The networking layer is responsible for providing efficient topologies to transmit data from source devices to destination ones. Although IoT topologies should be able to move large amounts of data quickly between source devices, these systems are sometimes constrained by issues with power consumption, throughput, and even destructive attacks.
3. Cloud computing layer: Advances in cloud computing technology have made it possible to handle huge data more quickly and correctly. The cloud computing layer is responsible for receiving data, processing it, making a decision, and then delivering the results to other layers. While the cloud is the preferred option for storing and processing data on IoT-based devices, some methods favor edge and fog to reduce costs and increase efficiency.
4. Applications layer: This layer includes a number of applications, including wireless sensor networks, mobile communication networks, smart grids, smart homes, and smart cities. Anyone can use innovative tools to communicate with others whenever and wherever they choose. IoT apps are also utilized to monitor ecological conditions and emergency situations. To easily manipulate IoT capabilities in their lives and market, it requires user-friendly interfaces.

2. Survey of Research

[1] The Kirchhoff-Law-Johnson-Noise Secure Trick Exchanger by GERGELY VADAI, ZOLTAN GINGL, and ROBERT MINGESZ, 2016 discusses generalized attack security. Johnson-Law-Kirchhoff Noise Unconditionally secured key exchanger is a promising, surprisingly straightforward, incredibly affordable, and also trustworthy digital alternative to quantum key circulation. In the best situation, a few resistors, switches, and adjacent cords can provide completely safe and secure data transmission by utilizing the thermal noise of the resistors. The main issues with practical understandings are resistance tolerance, restricted cable television resistance, and other less-than-ideal properties that might lead to information loss. In this study, we offer strong protection for the system against cable resistance and resistance mismatch attacks.

[2] Hitch Walker 2.0: An adaptive data collection model for the Internet of Things, Sankar Ramachandran Gowri 2016 explains how current data aggregation techniques confine programmers to certain network architecture or are unable to handle multi-hop data collection. We suggest Drawback Walker 2.0 in this work, an element binding version that helps with multi-hop data aggregation. To find remote component bindings and build a multi-hop overlay network within the free haul space of the current website traffic circulations, Hitch Walker uses part meta-data. In contrast to conventional interactions, Hitch Hiker 2.0 offers end-to-end transmission of low-priority traffic while consuming a negligibly little amount of power. By adding new tools for decentralized route finding and including more application case studies and evaluation, this article builds on our earlier work. For the LooCI component version, we have created a model execution of Hitch Walker. Our analysis reveals that Hitch Walker, when used to provide low-priority website traffic, consumes about 32% less power than Drawback Walker, which consumes very little resources.

Description:

The previously known version of Hitch Walker, known as Hitch Hiker 2.0, has been expanded. The bindings in Drawback Hiker are classified as either high or low top priority bindings. Because of this classification, Drawback Hiker is able to continue information aggregation by incorporating low-priority data into the overlay network that was built using the extra payload space left over from important transmissions. Hitch Walker creates a multi-hop information gathering overlay using the meta data provided by element bindings. Drawback Hiker uses a central meta-manager to conduct course exploration on a multi-hop overlay network in order to maintain end-to-end routing of low-priority traffic. With Ad-hoc Drawback Hiker, a new version of Hitch Walker 2.0's Drawback Walker that doesn't rely on a central meta-manager to reveal the information gathering overlay, it expands upon the original version. Ad-hoc Hitch Walker's method of course exploration is influenced by AODV.

[3] An approach to gathering data from distant data nodes for a business network of points Tao Zhua and Sahraoui Dhelim (2016) highlight how this has made it incredibly simple to get information about a product from a single data node. But in many commercial applications, information about a single product can be scattered across numerous different information nodes, and gathering the information from these nodes has really become a routine task. We present a scattered service-oriented design for this task in this work. In this system, each manufacturer provides service for their particular items, and information nodes store the data they have gathered. Modern semantic technologies are used to handle problems with diversification and serve as the framework for various applications. Finally, as an illustration, we demonstrate how this design might be used to address the issue of product mapping.

Concerning: One of the main drivers of this trend is the similar personalities shared by IoT information and Internet content. To demonstrate the value of semantics in search and the advancement of IoT, Barnaghi et al. studied a few scenarios.
Interoperability: Different stakeholders can access and interpret the data unambiguously by turning expertise into discrete and machine-process able ontologism. - Combination: Semiotics innovations can assist the seamless fusion of data from diverse sources to produce complex abstractions and also settings by enabling interoperability.
Inference: Semantic web contemporary technologies support logical reasoning, which has the capacity to extrapolate new knowledge or skills from established claims and rules.

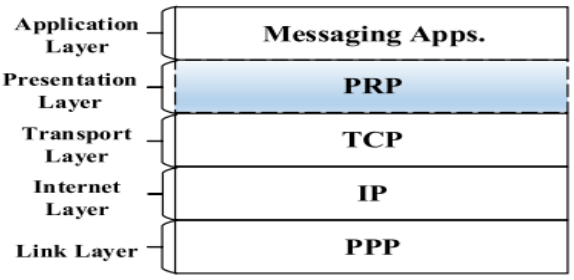
[4] Grey Wolf-based compressive noticing for heterogeneous WSNs based on the Internet of Things, For IoT-based heterogeneous wireless sensing unit networks, Ahmed A. El-Sawy describes and proposes a Reliable Multi-hop Cluster-based Aggregation plan using Hybrid CS (EMCA-CS) in 2017. (WSNs). To increase network longevity and lower repair errors, EMCA-CS efficiently combines CS and routing techniques. These are included in EMCA-CS: a new technique to divide the space into distinct hexagonal cells (collections) and selects a node from each cluster as collection head depending on a number of parameters (CH). Each CH will then use a hybrid CS approach to press its cluster data. Additionally, a new Grey Wolf-based algorithm is introduced, as well as a CSMO-GWO algorithm to improve the process of generating the CS matrix, to provide the optimal path for CHs to transport the compressed data to base stations (BS). In addition, a new Greedy-based Restoration Formula that is based on Grey Wolf is suggested in order to recover the true information.

The suggested approach outperforms the currently accepted standards in terms of lowering power consumption and decreasing reconstruction errors.

The following points provide examples of how the suggested plan contributes:

1. Creates various hexagonal cell divisions throughout the network. The concept of a cluster is applied to each hexagonal cell.
2. Take into account the CH option procedure as a choice issue developed on many needs such node residual power, range from BS, and distance from cluster facility. Provides a solution to this decision-making issue using lexicographical techniques.
3. Provide a fresh Grey Wolf-based formula to select the best course between each CH and the BS.
4. Utilize a hybrid CS approach to reduce the overall data size, achieve load balancing within each cluster, and provide CS matrix optimization using the GWO algorithm.
5. Provide the BS with a novel, very effective reconstruction algorithm that enhances the reconstruction procedure by combining the money-grubbing approach and the swarm algorithm.
6. Provide thorough simulation to show that the suggested strategy outperforms existing techniques in terms of power consumption, network lifetime, and restoration error.

[5] Samet Tonyali, Kemal Akkaya, Nico Saputro, A. Selcuk Uluagac, and Mehrdad Nojoumian (2018) discuss privacy-preserving techniques for trustworthy and secure data collection in IoT-enabled Smart Metering systems. Due to high frequency metering data, secure in-network information aggregation can be used to both safeguard customers' privacy and reduce package website traffic. By collecting data from hidden metering, the privacy can be provided. The techniques that enable performing various operations on hidden information are fully homomorphism encryption (FHE) and secure multiparty calculation (safe MPC). However, in terms of data quantity or message complexity, both safe MPC systems and FHE incur some costs. In IoT-enabled networks like Smart Grid (SG) Advanced Metering Infrastructure, the overhead is increased (AMI). In this paper, we provide fresh strategies for modifying FHE and also secure MPC to be launched in SG AMI networks built with wireless mesh networks. The suggested techniques secure the clever meters' (SMs) reading data (FHE) or compute its shares using an arbitrarily constructed polynomial to hide it (safe MPC).



Algorithm 1 *Receive(segment, from)*

```
buffer ← bufferMap.RetrieveBuffer(from)
if buffer == null then
    header ← segment.GetPRPHeader()
    buffer ← CreateBuffer(header.GetPacketSize())
end if
residualBytes ← buffer.Add(segment)
if buffer.IsFull() then
    appPacket ← CreateAppPacket(buffer)
    ReportUpperLayer(appPacket)
    bufferMap.RemoveBuffer(from)
    if residualBytes.Size() ≠ 0 then
        resSegment ← CreateSegment(residualBytes)
        Receive(resSegment, from)
    end if
end if
```

Threat model and security goals:

We highlight the pertinent security goals as well as the following threats to the security and privacy of SM data collecting in the AMI network.

Risk 1: The UC may misuse fine-grained meter data to analyze consumer behavior or, worse yet, may share the gathered data with a third party for this purpose.

Safety Objective 1: To prevent misuse by the UC or any other third party, combine the obtained fine-grained meter information in-network before transferring it to the UC.

Danger 2: An eavesdropper can monitor the channel of communication to record meter information in communications between a targeted SM and the portal in order to ascertain the behaviors of the SM's individual.

Safety Shield interactions, including SM analyses through data hiding.

Threat 3: An attacker may gain access to an SM and inspect the routines of its child meters.

Use information aggregation techniques that can perform mathematical operations on hidden data to achieve protection goal 3.

Threat 4: To keep the SMs active and to squander the network transmission capacity, an adversary might pose as the portal and send created data collecting requests to them more frequently.

Provide sender verification as part of security goal 4 to confirm the sender and validate the veracity of web information.

Threat number 5: A listener can record and replay data packages to change the state estimate or billing. Identify and eliminate repetitive messages is safety objective number five.

[6] A lightweight data aggregation method that protects privacy and has verifiable security for the internet of things, Sunday IoT terminals are only required to contact the crucial generation centre (KGC) when, according to Oyinlola Ogundoyin 2019. They can then create their pseudonyms independently without interacting with the KGC. In order to punish malicious terminals, an efficient cancellation device is provided. The suggested approach resolves the problem of personal key compromise, is anonymous, and can offer conditional tracking. The efficiency analysis shows that the proposed system is much more efficient than the modern plans and fits the resource-constrained IoT environment. The

official security evidence shows that the plan is secure versus both Kind I and Kind II adversaries in the arbitrary oracle model based upon the intractability of the Discrete Logarithm Issue.

Six algorithms are often included in a certificate much less aggregate signature (CL-AS) system to ensure compliance.

First, the setup The KGC is in charge of this formula. In addition to returning a master secret crucial x, a system public crucial Ppub, and a system parameter pram, it also accepts a security criterion called as input.

Secondly, a partial private key extract The KGC applies this formula on data. It enters the user's IDj, the master secret critical x, and the system criterion pram. Then, it generates a partial copy of the customer's personal security key (PSK) and securely returns it to the customer.

(3) User Key Gen: This formula requires the user to enter their secret value, partial secret key (PSK), and identity (IDj) as inputs. It returns both the comparable public crucial PKj and the secret key SKj.

(4) Indicator: A customer named j is using this algorithm. It requires as inputs the message Mj, the partial secret vital PSKj, the system parameter param, the j's identification IDj, and the j's secret essential SKj and PSKj. Then it gives back a distinctive j on Mj.

(5) Aggregate-Sign: An aggregator executes this formula. It constructs an accumulated signature T on the set of messages as well as the trademarks of n users (1, 2,..., n) on n distinct messages (M1, M2,..., Mn) using the trademarks of n users as input.

(6) Aggregate-Verify: This procedure is carried out by a verifier and requires as inputs the system parameter, the public secrets of n individuals (PK1, PK2,..., PKn), client identifications (ID1, ID2,..., IDn), as well as the total number of signatures (accumulated signature T on the system) (M1, M2, ..., Mn). Then, if the verification is successful, it returns "1," otherwise, it returns "0."

[7] A Special Low-Complexity Compressed Information Aggregation Method for Energy-Constrained IoT Networks, Sumohana S. Channappayya, Amarlingam M, K. V. V. Durga Prasad, P. Rajalakshmi, and C. S. Sastry 2020 describe In this research, we present a unique CS-aided low-complexity compressed data collecting (LCCDA) method that divides the network into constrained overlapped clusters and provides the best possible trade-off between energy consumption, on-node computational complexity, and recovery error. We demonstrate that the restricted isometric residential property (HOLE), which ensures the healing of the aggregated data, is satisfied by the measurement matrix produced by constrained overlapped clustering. We locate the thin representation of the gauged information from randomly distributed networks using the chart Laplacian eigen basis, which is based on the weight adjacency matrix and enables high integrity recovery for aggregated information at the sink node.

In conclusion, the following are the main differences between the suggested approach and the one:

- The method uses non-overlapping clustering with CS to accumulate the information. While the method suggested in this paper accumulates the data using limited overlapped clustering with CS, which may provide excellent recovery fidelity.
- The strategy depends on network release for effective healing. The approach used in this research, however, does not place any such dependence. This greatly reduces the complexity of the method, enabling a wider range of applications.
- This study offers mathematical frameworks for investigating the fundamental connection between information aggregation and CS theory. It also provides academic guarantees for the splitting of aggregated data to repair it.
- The algorithm presented in this research builds Laplacian eigenbasis on the basis of a weight adjacency matrix and offers a thin representation for the data obtained from randomly distributed networks, however no such formula is proposed.
- Additionally, this research provides a method for imagining and evaluating the distinct differences in trade-offs between energy consumption, on-node computational complexity, and recovery error all at once, since no such visualization was previously provided.

[8] F LEACH: a fuzzy-based information aggregation method for IoT systems in the healthcare industry IoT networks are described by Seyedeh Nafseh Sajedi, Mohsen Maadani, and 2021 as being vast and battery-powered, making the development of proper energy and resource management devices for them necessary. Information aggregation is crucial to reduce power consumption and increase network lifespan due to the large amount of data generated in IoT settings, and many academics have really made efforts to enhance its efficiency. However, due to the dynamic, intricate, and nonlinear nature of health care applications, there is no optimum method. Due to its ability to transform qualitative data into quantitative form, perform difficult nonlinear functions, generate approximations of answers in situations where there is no single best solution, and adapt to tiny changes in problems, fuzzy reasoning may be useful in these circumstances.

The following are the paper's main contributions:

1. A fuzzy disturbance system (FIS) has been developed and also optimized for Internet of Things-based healthcare data collection.
2. For IoT-based healthcare, a special data aggregation algorithm has been suggested that extends the network life.

Algorithm:

Given: Initial parameters P_0, standard deviation S, number of iterations K
Returns: The optimized parameters P_K

```
Mi = 0.
for i=0; i≤K;  i = i +1 repeat
    Create a random vector with Normal distribution Ni, mean Mi and standard deviation S
    if E(Pi + Ni) < E(Pi) then
            Pi+1 = Pi + Ni
            Mi+1 = α Mi + β Ni
    else if E(Pi Ni) < E(Pi) then
            Pi+1 = Pi Ni
            Mi+1 = γ Mi Ni
     else
        Pi+1 = Pi
        Mi+1 = δ Mi
     end
end
```

[9] βDSC2 DAM: beta-dominating set centered Cluster-Based Data Aggregation mechanism for the Internet of Things, Ab Rouf Khan, Mohammad Ahsan Chishti 2022 explain Data aggregation has been proven to be an efficient technique to increase efficiency and keep the data fresh in an IoT framework. Aggregating the data efficiently will eventually minimize the latency and increase the throughput of the network as a whole. This paper has proposed a new mechanism for data aggregation, i.e., beta-dominating set centered cluster-based data aggregation mechanism (βDSC2 DAM) for the Internet of Things, which is an improvement of the classical cluster-based data aggregation mechanism. The proposed mechanism is compared with the classical cluster-based data aggregation mechanism and evaluated on the parameters of Data Aggregation Time, Average Latency, Mean End-to-End delay of the arrived packets, and Maximum End-to-End delay of the arrived packets in the IoT network. The algorithms are also compared based on asymptotic time complexity analysis. The results reveal that the βDSC2 DAM performs better in terms of time complexity and the parameters listed than the classical cluster-based aggregation mechanism for the Internet of Things.

Algorithm 1: Beta-Dominating Set Centered Cluster-Based Data Aggregation Mechanism (βDSC^{2}DAM) in IoT

Input: k number of Clusters
Data transmitted by the sensor nodes represented in the form of data points $p = \{p_1, p_2, ..., p_n\}$
Predefined threshold distance value β

1. **procedure:** βDSC^{2}DAM(k,p , β)
2. Select $S_1, S_2, ..., S_k$ as the centroids of the k clusters and place the centroids in a random fashion
3. Repeat until convergence, i.e., till none of the cluster assignments vary
4. for each data point p_i, calculate the distance d between each data point and the centroid c_j as: $d = \sum_{i=1}^{n} (p_i - \bar{p})^2$, where p_i is the i^{th} element of the set $p = \{p_1, p_2, ..., p_n\}$ and $\bar{p}$ is the mean of all the data points in the set $p = \{p_1, p_2, ..., p_n\}$.
5. if $(d_i < \beta)$
   Assign the point to the current cluster
6. for each cluster $j = 1$ *to* k, a new centroid is obtained as - $\forall\{p_i\} \subset \{p_1, p_2, ..., p_n\} \in c_j \vee$ the distance between any points $\in p_i$ in c_j is within a distance $\geq \beta$ to one or more data points in c_j
7. end for
8. end for
9. end procedure

3. Recommended System

For the IoT network, we suggest a trustworthy data aggregation approach. This plan's main goal is to transmit high-quality data while collecting it in an energy-efficient manner. The following is a summary of the contributions of the proposed protocol: We first offer the monarch and sine-cosine (MSC) algorithm to arrange the IoT sensors into clusters, ensuring efficient data distribution. The trustworthiness of each IoT sensor is calculated during the data aggregation phase using a variety of design measures, and the design constraints are optimized using an improved sunflower optimization (ISO) algorithm. The node with the greatest trust level serves as the cluster's cluster head, ensuring data aggregation. Window block updates are presented for the hybrid deep neural network, which uses a trusted network to determine routes between IoT sensors and offers practical routing algorithms. Finally, we test the effectiveness of our suggested routing using various simulation scenarios, and the results are compared to those of the current routing protocols.

Regarding the proposed algorithm: An Improved Sunflower Optimization Algorithm is the name of the new algorithm (ISFO). The Sunflower Optimization Algorithm (SFO) and the Levy Flight Operator are combined in the ISFO. Such invocation can maintain a balance between the proposed algorithm's processes of intensification and diversification and prevent trapping in local minima. Six SI methods are compared to the ISFO algorithm. The suggested algorithm's results demonstrate that it can use less energy than the other algorithms and that there are more active nodes for it than there are for the other algorithms. The ISFO algorithm therefore demonstrated its superiority in lowering the amount of energy spent and lengthening the lifetime of the network.

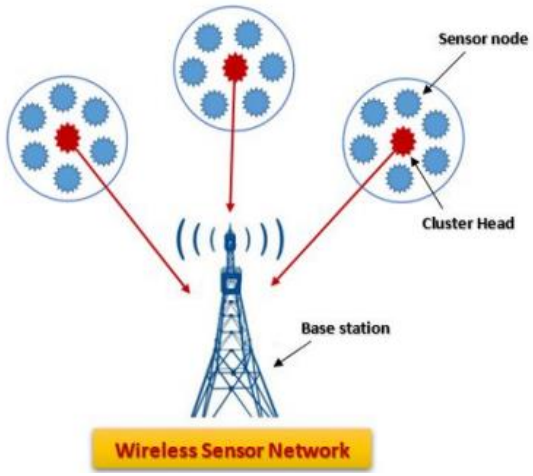


Figure 1. Basic Model of WSN

By combining the sunflower optimization (SFO) method with the Levy trip driver, we proposed an original formula

for the clustering process in Internet of Things networks. The suggested algorithm's characteristic is to identify the best cluster heads, and its name is "an Enhanced Sunflower Optimization Algorithm (ISFO)". As a result, more energy will be conserved and the lifespan of the IoT network will undoubtedly grow. This paper's main contribution can be summed up as follows.

In order to reduce the nodes' energy consumption and increase their lifespan, a new SI formula is proposed. The suggested approach uses the lèvy flight driver to avoid capture in regional minima.

The suggested algorithm is recommended compared to six SI algorithms; its results can use less energy than those of the other algorithms, and its number of active nodes is higher than that of the active nodes for the other formulas.

4. Conclusion

Using IoT The durability of the network is the main issue facing WSN. In order to overcome this challenge, we created a novel technique for selecting the CHs in the NP-hard IoT-WSN. The proposed algorithm is called An Improved Sunflower Optimization Algorithm (ISFO). The Lévy flight operator and the traditional SFO approach are combined to create the ISFO algorithm. With the help of the lèvy flight operator, the ISFO algorithm can diversify its search and assist in escaping local minima. At various BS locations, six SI methods are evaluated against the ISFO. The outcomes of the ISFO algorithm show that, in comparison to other algorithms, it can increase the network lifetime.

References

[1] Generalized Attack Protection in the Kirchhoff-Law-Johnson-Noise Secure Key Exchanger by Authors GERGELY VADAI, ZOLTAN GINGL, AND ROBERT MINGESZ, 2016.

[2] Hitch Hiker 2.0: a binding model with flexible data aggregation for the Internet-of-Things, Gowri Sankar Ramachandran 2016.

[3] An architecture for aggregating information from distributed data nodes for industrial internet of things Tao Zhua , Sahraoui Dhelim, 2016.

[4] Grey Wolf based compressive sensing scheme for data gathering in IoT based heterogeneous WSNs, Ahmed A. El-Sawy year of 2017.

[5] Privacy-preserving protocols for secure and reliable data aggregation in IoT-enabled Smart Metering systems by Samet Tonyali a, Kemal Akkaya a , Nico Saputroa , A. Selcuk Uluagac a , Mehrdad Nojoumian, 2018.

[6] A lightweight privacy-preserving data aggregation scheme with provable security for internet-of-things, Sunday Oyinlola Ogundoyin 2019.

[7] A Novel Low-complexity Compressed Data Aggregation Method for Energy-constrained IoT Networks, Amarlingam M, K. V. V. Durga Prasad, P Rajalakshmi, Sumohana S. Channappayya, and C. S. Sastry 2020.

[8] F-LEACH: a fuzzy-based data aggregation scheme for healthcare IoT systems Seyedeh Nafseh Sajedi, Mohsen Maadani, 2021.

[9] βDSC2 DAM: beta-dominating set centered Cluster-Based Data Aggregation mechanism for the Internet of Things, Ab Rouf Khan, Mohammad Ahsan Chishti 2022.

[10] S. Madden, M. Franklin, J. Hellerstein, W. Hong, TAG: A tiny aggregation service for ad-hoc sensor networks, SIGOPS Operating System Review 36 (2002) 131–146.

[11] C. Alcaraz, P. Najera, J. Lopez, R. Roman, Wireless sensor networks and the internet of things: Do we need a complete integration?, in: 1st International Workshop on the Security of the Internet of Things (SecIoT10), 2010.

[12] S. Tonyali, O. Cakmak, K. Akkaya, M.M. Mahmoud, I. Guvenc, Secure data obfuscation scheme to enable privacy-preserving state estimation in smart grid ami networks, IEEE Internet Things J. 3 (5) (2016) 709–719.

[13] Stop smart meters. URL http://stopsmartmeters.org.

[14] N. Saputro, K. Akkaya, Performance evaluation of smart grid data aggregation via homomorphic encryption, in: Wireless Communications and Networking Conference (WCNC), 2012 IEEE, IEEE, 2012, pp. 2945–2950.

[15] S. Tonyali, N. Saputro, K. Akkaya, Assessing the feasibility of fully homomorphic encryption for smart grid ami networks, in: 2015 Seventh International Conference on Ubiquitous and Future Networks, (ICUFN), IEEE, 2015, pp. 591–596.

[16] S. Tonyali, K. Akkaya, N. Saputro, A.S. Uluagac, A reliable data aggregation mechanism with homomorphic encryption in smart grid ami networks, in: Consumer Communications and Networking Conference (CCNC), 2016 IEEE, IEEE, 2016, pp. 557–562.

[17] C. Rottondi, M. Savi, D. Polenghi, G. Verticale, C. Kraus, Implementation of a protocol for secure distributed aggregation of smart metering data, in: 2012 International Conference on Smart Grid Technology, Economics and Policies, (SG-TEP), IEEE, 2012, pp. 1–4.

[18] C. Rottondi, G. Verticale, C. Krauss, Distributed privacy-preserving aggregation of metering data in smart grids, IEEE J. Sel. Areas Commun. 31 (7) (2013) 1342–1354.

[19] C. Rottondi, G. Verticale, C. Kraus, Secure distributed data aggregation in the automatic metering infrastructure of smart grids, in: 2013 IEEE International Conference on Communications, (ICC), IEEE, 2013, pp. 4466–4471.

[20] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in: International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 1999, pp. 223–238.

