Scientific Journal of Impact Factor (SJIF): 5.71

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 5, Issue 02, February -2018

A TECHNICAL REVIEW ON APPLICATIONS AND CHALLENGES WITH PSO IN WIRELESS SENSOR NETWORK

[1]Kuldeep Mathur, [2]Madhukar Dubey

[1]Department of Computer Science, Shriram College of Engineering & Management, Gwalior, India
[2]Department of Computer Science, Shriram College of Engineering & Management, Gwalior, India

Abstract—*Wireless Sensor Network has been generally utilized as a part of a lot of regions exceptionally for surveillance and observing in agriculture and habitat monitoring. WSN comprises of a huge assortment of small nodes with restricted usefulness. Environment monitoring has emerged as a critical subject of control and protection, offering real-time device and manage communication with the physical world. An intelligent and smart WSN system can gather and technique a huge quantity of statistics from the beginning of the monitoring and manage air quality, the conditions of traffic, to climate conditions. Particle swarm optimization (PSO) is an easy, effective, and computationally efficient optimization algorithm. It has been completed to address WSN issues at the side of strength, cost and storage. This paper outlines traumatic situations in WSNs, introduces PSO, and discusses its suitability for WSN packages. In this paper, the targeted survey finished approximately the advantage and drawback of PSO approach.*

Keywords—*Wireless Sensor Node, Sensors, Sink, Particle Swarm Optimization, Particle.*

I. INTRODUCTION

Wireless Sensor Network (WSN) comprises of a gathering of sensor nodes cooperating to detect the earth, impart over a short separation utilizing wireless link and perform simple data preparing. These sensor nodes are ordinarily small in size, battery powered, cost and deployed randomly. WSN has different critical applications in military, environmental observing and target following. The design of a WSN depends fundamentally on the goals of the applications and it must consider factors, for example, the earth, cost, hardware and framework requirements. The quantity of nodes in WSN changes from few to a few hundreds or even thousands, where every node is associated with one sensor. In WSN sensor nodes consistently measures the physical parameters, for example, temperature, humidity, pressure and so on and trade the data with the neighboring nodes so finally it compasses to the sink. Every sensor node in the network has regularly a few sections, for example, radio transceiver with antenna, a microcontroller, interface for associating the sensors and an energy source. Below figure 1 shows the typical WSN.

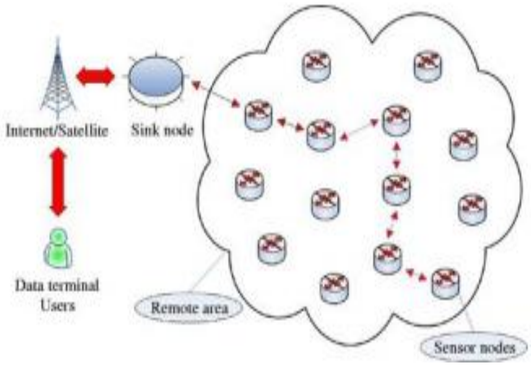

Fig 1.1 WSN

The cost of sensor nodes is variable, running from a couple to several dollars, dependent upon the unpredictability of the individual sensor nodes. Size and cost imperatives on sensor nodes bring about comparing limitations on resources, for example, energy, memory, computational speed and communications. The efficiency of WSN relies upon the energy of the sensor node. In WSNs, the energy is scattered while detecting, preparing, transmitting or receiving data. The detecting subsystem is utilized for data acquisition. Clearly limiting data extricated from transducer will save energy of compelled sensors.

Different experimental results affirm that correspondence subsystem is a prominent source of energy dissipation. Indeed, even in correspondence, large amount of energy is wasted in states, for example, collision, overhearing, control packet overhead, idle listening, impedance and so forth [1].There are five primary classes recognized for energy proficient methods. In[2] probably the most critical ones are discussed they are energy per Packet, network life time, normal energy dispersed, low energy utilization, average packet delay, packet delivery ratio, sit without moving tuning in, packet size and separation between the sender and collector and so forth. The most widely recognized components which influence the outline of routing protocols [3] are node deployment, node /connect heterogeneity, data reporting model, adaptability, adaptation to fault tolerance and so on

II. APPLICATIONS OF WSN

WSNs empower a change in perspective in the art of monitoring, and constitute the foundation of an expansive scope of applications related to security, surveillance, military, medical, and environmental monitoring. They can fundamentally enhance the accuracy and density of scientific estimations of physical phenomena since large numbers of sensors can specifically be conveyed where tests are occurring. In WSN the idea of micro scale detecting and wireless connection of sensor nodes constitute the establishment of a wide scope of use identified with military surveillance security environment monitoring, medical, home and other commercial application areas. They can essentially enhance the accuracy and density of scientific estimations of physical phenomena since huge number of sensor can straightforwardly be conveyed at places where experiments are failing. Some existing real life applications are given below.

1) Military Applications

Sensor networks rely upon the dense deployment of sensor nodes, devastation of a couple of nodes by hostile activities does not impact a military operation. To monitor friendly forces, equipment and ammunition leaders and leaders can always screen the status of well disposed troops, the condition and the accessibility of hardware and ammunition in a war zone by the utilization of sensor systems. In front line observation, basic landscapes approach and ways can be quickly secured with sensor networks and closely watched for the exercises of the opposing forces.

2) Environment Observation

Environment monitoring networks span large geographic areas to monitor and forecast physical processes such as environment pollution. A few kinds of sensors are conveyed for rainfall, water level and weather sensor. The sensors supply data to the brought together database predeterminedly.

3) Precision Agriculture

In agriculture sensor networks are utilized to screen the pesticides level in the drinking water, the level of soil recognition corrosion and the level of air pollution. They are also helping in strategic planning and counter measures to increase the yield of the crop.

4) Medical Applications

In medical, sensor networks are used for tracking and monitoring doctors and patients inside a hospital. Doctor may in like manner convey a sensor node which empowers distinctive doctors to discover them inside a hospital. Sensors are to a great degree helpful in expire determination and observing. Biosensors are inserted in the human body to screen the patient's physiological parameters, for instance, heart beat or circulatory strain. The data so gathered is sent routinely to alert the concerned doctor on identification of an anomaly. Such an arrangement provides patients a greater freedom of movement instead of being constantly confined to the hospital bed. Rapid advancements in MEMS technology has made bio-sensors so sophisticated as to empower rectify identification of sensitivities and related diagnosis.

5) Habitat Monitoring

Researchers in the life sciences are winding up progressively worried about activities of birds, small animals and insects. WSNs therefore can be used to gather information on the habitat of animals without disturbing them.

6) Home Automation

As technology progresses, smart sensor nodes and actuators are utilized as a part of uses, for example, vacuum cleaners, microwave oven and refrigerator. They allow end users to manage home devices locally and remotely more easily.

7) Other Commercial Applications

Sensors can be used in building for detecting and controlling of fire and smoke. In case of a fire in building, the deployed sensor network can track and scan the direction in which fire is expanding. Likewise sensors can be utilized to monitor the vibration in the building that can damage the structure.

1) Disaster Management

The early warning framework in view of WSN can be dependably conveyed in regions with high risk of disasters. The utilization of WSN promises to give continuous data of the disaster area to protect groups making coordination and arranging more powerful. Location data of victims, rescuers and objects in the disaster is indispensable for the safeguard operations. It has been understood that, for an operationally compelling disaster management detecting, monitoring and basic leadership should be incorporated seamlessly. Timely and updated disaster data is critical for efficient response and viable activities, it will help disaster managers with making better choices and take actions in time. Fig. 2 demonstrates the utilization of WSN [4].

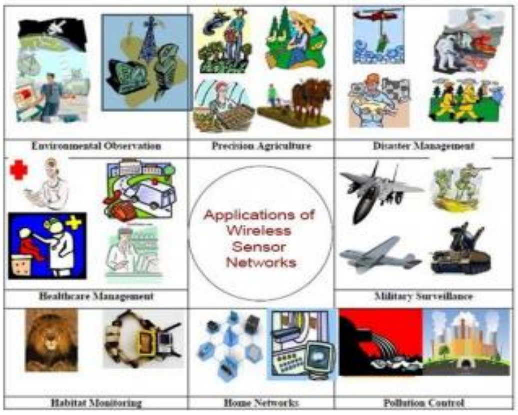

Fig 1.2 Applications of WSNs

III. CHALLENGES OF WSN

With the proceeded with headway in micro electro mechanical frameworks the miniaturization and expanded correspondence capacities of sensors has empowered their omnipresent and undetectable sending anyplace whenever. A sensor network is a framework included detecting (estimating), processing and correspondence components that enable a user to watch instrument and respond to events and phenomena in a specified environment. To design and develop protocols or algorithms some challenges are needed to be understood [4]. These major challenges are summarized below:

a) Limited Functional Capabilities

A sensor node has low end processor, small memory and small amount of stored energy. This limits many of the functional capabilities in terms of processing and communication. A good algorithm should make utilization of shared resources inside a hierarchical structure, while considering the restriction on singular node abilities.

a) Limited Energy

Much of the time, renewing energy isn't plausible or even impossible. Sensors are typically unattended in the field. The limited energy in sensor nodes must be considered as proper consumption or utilization that can reduce the overall energy uses in a network.

b) Network Lifespan

Limited resources and energy in sensor nodes results in limited lifespan in a network. Ideally, a network should become ineffective only when all nodes become exhausted. In all reality, the lifespan of a sensor network is the base time upto which the network is practically compelling. A network is practically successful, on the off chance that it can monitor the whole sensor field and gather the detected data with a predefined quality of service (QOS). Proper techniques should attempt to reduce the energy usage and thereby increase network lifetime. The topology of network and quickly change in channel situation due to high mobility. Since we cannot set up and handle the configuration as rapidly as the topology change. It also makes complicated to expect the node's location [5].

c) Scalability

Sensor nodes deployed in a sensing area should be optimal. To oblige some more nodes later on, network scalability is one of major deterrents to achieve this goal. Scalability in the sensor network demonstrates the capacity to deal with developing measures of work in a powerful way and be readily.

d) Redundancy

Lack of global distinguishing proof Due to extensive number of sensor nodes in a sensor organize the global identification (GID) is for the most part impractical. In spite of the way that once in a while, the Global Positioning System (GPS) [6] gives situating data to sensor nodes. However it requires viewable pathway to a few satellites, which is for the most part not accessible within working, underneath dense foliage, underwater, when stuck by an adversary or amid MARS exploration and so on.

e) Storage, Search and Retrieval

The sensor network can produce a large volume of raw data such as continuous time-series of observations over all points in space covered by the network. Since the data source is continuous traditional database are not suitable for WSNs.

f) Production Cost

The cost of a single node is essential to legitimize general cost of the network; since the sensor networks comprise of a substantial number of sensor nodes in this manner cost of every sensor node must be kept low.

g) In- network Processing

As a rule transport protocols utilized as a part of wired and wireless networks [7] have accepted end-to-end approach ensuring that data from the senders have not been changed by intermediate nodes until the point when it achieves a recipient.

Nevertheless, in WSNs information can be changed or accumulated by intermediate nodes in order to expel excess of data. The previous solutions did not suit idea of in network processing, called data aggregation or dispersion in WSNs.

h) Latency

Latency alludes to delay from when a sender sends a packet until the point that the packet is effectively gotten by the receiver. The sensor data has a worldly time interim in which it is legitimate, since the idea of the earth changes continually; it is along these lines essential to get the data in a favorable way.

i) Fault tolerance

Sensor nodes are sensitive and they may fall flat as a result of weariness of batteries or decimation by an external event. Understanding a fault tolerant operation is basic, for effective working of the WSN, since defective segments in a network prompts lessened throughput, along these lines decreasing efficiency and execution of the network.

IV. PSO

Molecule remains for the potential arrangement in D-dimensional space. The particles change its condition according to the following three concepts:

- To keeps its inertia
- To change the consistent with the swarm's most optimist position.

The position of each particle within the swarm is affected both by essentially the most optimist position for the period of its motion (individual experience) and the Operate of essentially the most optimist particle in its surrounding (near expertise) When the entire particle swarm is surrounding the particle, probably the most optimist position of the encompassing is the same as the presumably the most whole most optimist particle; this algorithm is alluded to as the entire PSO. If the slender surrounding is used within the algorithm, this algorithm is referred to as the partial PSO.

Each particle can be proven with the aid of its present speed and position, essentially the most optimist position of each and every person and probably the most Optimist position of the encompassing. In the incomplete PSO, the speed and position of every particle change agreeing the accompanying equality (Shi Y,Eberhart R C,1998) [8]:

$$v_{id}^{k+1} = v_{id}^{k} + c_1 r_1^{k} \left(pbest_{id}^{k} - x_{id}^{k}\right) + c_2 r_2^{k} \left(gbest_{d}^{k} - x_{id}^{k}\right) \qquad (1)$$

$$x_{id}^{k+1} = x_{id}^{k} + v_{id}^{k+1}$$

In this equality, k id v and k id x remain for exclusively the speed of the particle "I" at its "k" times and the d-dimension variety of its position; k id pbest represents the d-measurement amount of the individual "I" at its most confident person position at its "k" times. K d gbest is the d- dimension number of the swarm at its most optimist position. In order to avoid particle being far away from the searching space, the speed of the particle created at its each direction is confined between -vdmax, and vdmax. If the number of vdmax is simply too big, the answer is a ways from the pleasant, if the number of vdmax is simply too small, the solution would be the nearby optimism; c1 and c2 describe the speeding decide, directing the length when traveling to the most molecule of the whole swarm and to probably the most optimist individual particle.

If the determine is simply too small, the particle is on the whole some distance away from the target field, if the figure is too massive, the particle will maybe fly to the target area instantly or fly beyond the target discipline. For the most part, c1 is equivalent to c2 and they are equivalent to 2; r1 and r2 represent random fiction, and 0-1 is a random number. In local PSO, rather of inducing the confident person molecule of the swarm, every molecule will intrigue the hopeful person molecule in its enveloping to control its speed and position.

Formally, the equation for the speed and the position of the molecule is totally indistinguishable to the one in the entire PSO.

V. ADVANTAGES AND DISADVANTAGES OF THE BASIC PARTICLE SWARM OPTIMIZATION ALGORITHM

Focal points of the fundamental PSO algorithm:

- PSO is set up on the insight. It can be used into each logical research and designing use.
- PSO haven't any overlapping and mutation calculation. The hunt may also be implemented with the aid of the speed of the particle. For the duration of the development of a few generations, simplest mainly probably the most optimist particle can transmit information onto the inverse particles, and the speed of the researching is fast.
- The computation in PSO is exceptionally straightforward contrasted and the other developing figurings, it involves the greater optimization capacity and it can be finished effectively.
- PSO adopts the true number code, and it is resolved right away through the arrangement. The quantity of the measurement is equivalent to the consistent of the solution.

Disadvantages of the fundamental PSO algorithm:

- The system effectively suffers from the partial optimism, which motives the much less specific at the legislation of its speed and the path [9].
- The strategy cannot work out the issues of non-arrange framework, for example, the answer for the energy field and the moving tenets of the particles in the energy field.

PSO is without doubt one of the SI paradigms which have obtained well known attention in research at the moment. It is a novel populace headquartered stochastic search algorithm that provides a solution to complex non-linear optimization problem. It's an evolutionary computation procedure which simulates the action and flocking of birds that performs a world search in the resolution space. PSO produces higher results in tricky and multi-top problems with few parameters to adjust giving speedy as good as accurate computation outcome which makes. Hence, PSO will probably be a exceptional option for locating method to probably the most challenging issues in clustering.

VI. LITERATURE SURVEY

Shreshtha Misra et al. [10] In this paper, our have presented various clustering approaches used in WSN. Firstly, we have arranged the protocol utilized as a part of Wireless Sensor Network as Protocol Operation (PO), Network Structure (NS) and Path Establishment (PE). Besides, we have given an expansive outline of the cluster based routing protocol utilized as a part of WSN as square cluster, chain cluster and grid cluster. We have likewise thought about different clustering routing protocols in view of various qualities and furthermore talked about the different issues in these routing protocols.

Sekhar et al. [11], in this paper, a protocol in view of open key cryptography for external agent confirmation and session key foundation has been proposed. An external agent imparts through an public key encryption system with a base station, which speaks with sensor nodes through sharing of a private key. The procedure for this protocol is separated into three stages: registration, confirmation and session key foundation.

Praveena et al. [12], In this approach, a summed up and changed Vernam cipher strategy is utilized with various block sizes and keys for each block. As an additional security criterion for this algorithm, feedback is also added to this method. After the direct stage encryption is finished, the whole document is separated into two exchanged parts and the modified Vernam cipher technique with feedback and another key will be repeated. Repeating this whole operation various circumstances brings about a framework that is highly secure. The main level will be begun with an interleaving strategy. Second, the estimation of a pseudo-random number generator is seeded. Third, a number bank is dispersed at first. The last level is begun by applying operations to the number bank.

Celestine et al. [14], in this paper, a flooding method routing method is presented that relies upon dummy data sources. The fundamental thought behind this method is that every node can be considered as a dummy data source that sends real data in the wake of detecting an occasion to the destination node; the majority of this present node's neighbor nodes will get dummy data. In spite of the fact that this approach has the upside of making it troublesome for an enemy to recognize the real packet and dummy ones. The dummy packets will vary in estimate from the real packets, in this way saving energy; notwithstanding, a foe will even now think that it's hard to recognize the real packet from the dummy ones.

Markert et al. [15], in this paper, the use of a honey pot framework for WSNs is shown to provide the ability to explore for security weaknesses, vulnerabilities and breaches. This proposed approach, however, remains a prototype that needs further testing to assess its effectiveness as a complete system for detecting real network attacks and other attacks. Another side effect of this technique is related to the power consumption of the honey pot sensor nodes. This technique does not apply to other security concerns so should be integrated with other solutions.

VII. CONCLUSION

WSN is a network, which can self- organize them with countless sensors. These sensor nodes can play out the packet transmission among themselves inside their radio range and furthermore they are composed in an approach to detect, observe, and perceive the physical element of this real world condition. WSN comprises of an unlimited number of sensor nodes that can detect their region and convey either among themselves or to outside base transceiver station. PSO is a populace based optimization plot. The random solutions of the framework are introduced with a populace and inquiry ideal arrangements in every generation. The potential solutions in each generation are called particles. Every molecule in PSO keeps the put away record for every one of its directions which are identified with acquiring the better arrangement by following the current best particles.

References

[1] P. Minet, "Energy efficient routing", in Ad Hoc and Sensor Wireless Networks: Architectures: Algorithms and Protocols.Bentham Science, 2009.

[2] L. Alazzawi, A. Elkateeb, "Performance Evaluation of the WSN Rout-ing Protocols Scalability," Journal of Computer Systems, Networks, and Communications, 2008, Vol. 14, Issue 2, pp. 1-9.

[3] L. Junhai, X. Liu, Y. Danxia, "Research on Multicast Routing Protocols for Mobile ad-hoc Networks," Computer Networks, 2008, Vol. 52, Issue 5, pp. 988-997.

[4] Sanjeev Kumar Gupta, Poonam Sinha, "Overview of Wireless Sensor Network: A Survey" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 1, January 2014.

[5] Agarwal, Pallavi and Bhardwaj, Neha, A Review on Trust Model in Vehicular Ad Hoc Network, International Journal of Grid and Distributed Computing, Vol. 9, No. 4, pages 325–334, 2016.

[6] C.C. Shen, C. Srisathapornphat, C. Jaikaeo, "Sensor Information Networking Architecture and Applications", IEEE Personal Communications, August 2001, pp. 52-59.

[7] P. Bonnet, J. Gehrke, and P. Seshadri, "Towards Sensor Database Systems," in proceedings of 2nd Int'l Conf. on Mobile Data Management (MDM'01), 2001, pp. 314–810.

[8] Jayshree Ghorpade-Aher and Vishakha Arun Metre," PSO based Multidimensional Data Clustering: A Survey", International Journal of Computer Applications (0975 – 8887) Volume 87 – No.16, February 2014.

[9] Qinghai Bai," Analysis of Particle Swarm Optimization Algorithm", Computer and Information Science, 2010.

[10] Shreshtha Misra, Rakesh Kumar "A Literature Survey on Various Clustering Approaches in Wireless Sensor Network" A Literature Survey on Various Clustering Approaches in Wireless Sensor Network" 978-1-5090-3210-5/16/$31.00 © 2016 IEEE.

[11] Sekhar, V.C. and M. Sarvabhatla. Security in wireless sensor networks with public key techniques. in Computer Communication and Informatics (ICCCI), 2012 International Conference on. 2012. IEEE.

[12] Praveena, A. and S. Smys. Efficient cryptographic approach for data security in wireless sensor networks using MES VU. in Intelligent Systems and Control (ISCO), 2016 10th International Conference on. 2016. IEEE

[13] Navin, A.H., et al. Encrypted Tag by Using Data-Oriented Random Number Generator to Increase Security in Wireless Sensor Network. in Computational Intelligence and Communication Networks (CICN), 2010 International Conference on. 2010. IEEE.

[14] Celestine, J., et al. An energy efficient flooding protocol for enhanced security in Wireless Sensor Networks. in Systems, Applications and Technology Conference (LISAT), 2015 IEEE Long Island. 2015. IEEE.

[15] Markert, J. and M. Massoth. Honeypot framework for wireless sensor networks. in Proceedings of International Conference on Advances in Mobile Computing & Multimedia. 2013. ACM.