International Journal of Applied Engineering & Technology

AN EFFECTIVE PSO CLUSTERING BASED SECURE DATA AGGREGATION PROTOCOL FOR WIRELESS SENSOR NETWORK

[1]Ms. U. Suriya, [2]Mr. P. D. Sajin and [3]Ms. M. Sandhiya.
[1]Assistant Professor, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore
[2,3]PG Student, II MCA, Department of Computer Applications, Dr. SNS Rajalakshmi College of Arts & Science, Coimbatore

ABSTRACT
Data aggregation in Wireless sensor Network (WSN) is typically done by some easy technique like averaging. These ways are liable to sure attacks. Refined data aggregation formula would create the sensor nodes less vulnerable thereby achieving the trust of knowledge and name. Secure information aggregation protocol holds nice promise for this purpose. To beat the safety problems in WSN, Particle Swarm improvement bunch (PSOC) based mostly secure data aggregation protocol is planned. This method makes them not solely collusion sturdy however, a lot of correct and conjointly achieves quicker convergence. Then the optimized cluster head is chosen for data aggregation by PSO. The cluster formation is reduced the ability consumption and bandwidth allocation. Trust and name have a big role in supporting the operations of a large vary of distributed systems, from wireless detector network to social network. Assume that the random elements of detector errors are independent random variables with a Gaussian distribution. If error distribution of sensors is either familiar or calculable, planned algorithms may be custom-made to alternative distributions to realize associate best performance. A sensor node solely accepts data things aggregate by licensed users. So as to make sure security, every step of the prevailing data aggregation protocol runs ought to be known then protected. The first challenge of providing security functions in wsns is that the restricted capabilities of sensor nodes in terms of computation, energy and storage.

Keywords: Wireless Sensor Network, Aggregation, PSO, clustering, Certificate Authority, Threshold Value, Security.

1. INTRODUCTION
The wireless sensor network is outlined because the extremely distributed networks of tiny, light-weight wireless node deployed in massive numbers to trust the environment or system by the measure of physical parameters like temperature, pressure or ratio. In the WSN, the data from the sensor nodes are collected by suggests that of knowledge aggregation. Sensory data is collected by the nodes. WSN consists of a base station and also the range of nodes. The aggregator node is employed to combination the data from multiple sensor nodes then the data is forwarded to the bottom station.

There is many security challenges may be faced throughout the aggregation of data [1]. Because of this wireless aggregation, eavesdropping and packet injection are occurred. Providing security within the sensor network is tougher than the mobile adhoc network. To realize the safety in WSN, they perform varied cryptographic operations like encryption, decryption and authentication then on. For any cryptographic operation they need to use any of the key like rhombohedral key or uneven key. If symmetric key is used then it is terribly tough to style for security purpose. If uneven key is used then it is too expensive. For applying any of the cryptography theme then it has further bits, memory needed, delay occurred then on.

In the existing system, varied algorithms are accustomed succeed the safety throughout data aggregation. Several algorithms focus solely on the specific attacks or issues. The iterative filtering formula [2, 3] is merely focus on collusion attack [4]. The secure data aggregation protocol is wide accustomed overcome the faults that chiefly occurred on the prevailing system. Within the existing system, the information is transferred to the bottom station. So a lot of quantity of energy is employed. To produce the energy strained mechanism, then the transfer of the unwanted information should be prevented. This can be achieved by Secure Data Aggregation Protocol (SDAP).

Here the nodes are classified as clusters and cluster head is chosen supported PSO. All the mandatory process is finished inside the cluster. Now, all the teams transfer the processed data to the base station. From the received data, the teams with malicious nodes are known. The safety to the info is provided exploitation the cryptographic keys. The aggregation is performed through hop-by-hop. This performs efficiency at every node to observe the malicious node. The problem arises by using per-hop aggregation, since it does not verify the correctness of the data.

2. RELATED WORKS

Sharmin, S., Ahmedy, I., & Md Noor, R. (2023) address the issue of energy efficiency [5]. The authors proposed a solution where hybrid particle swarm optimization (HPSO) is paired with improved low-energy adaptive clustering hierarchy (HPSO-ILEACH) for CH selection in cases of data aggregation in order to increase energy efficiency and maximize the network stability of the WSN. In this approach, HPSO determines the CH, the distance between the cluster's member nodes, and the residual energy of the nodes. Then, ILEACH is used to minimize energy expenditure during the clustering process by adjusting the CH. Finally, the HPSO-ILEACH algorithm was successfully implemented for aggregating data and saving energy and its performance was compared with three other algorithms: low energy-adaptive clustering hierarchy (LEACH), improved low energy adaptive clustering hierarchy (ILEACH), and enhanced PSO-LEACH (ESO-LEACH).

Pavani, M., & Trinatha Rao, P. (2019) proposed SCBRP is based on the hexagonal sensor network architecture, and it is designed by three processes to include energy-efficient clustering, secure routing, and security verification. And also propose a secure cluster-based routing protocol (SCBRP) that uses adaptive particle swarm optimisation (PSO) with optimised firefly algorithms during data transmission in a wireless sensor network [6]. The objective of this study is to minimise energy consumption over an individual node to improve the whole network lifetime. The performance of the proposed SCBRP is evaluated using NS-3, and it is estimated by different metrics such as encryption time, decryption time, energy consumption, packet drop rate, and network lifetime. The simulation results are compared with the previous approaches and finally, the authors' proposed SCBRP is proved that it obtained better performance than previous approaches.

Sharifi, S. S., & Barati, H. (2021) provides one of the major challenges facing WSNs is their limited energy resources, which affects network lifetime directly [7]. The proposed work provides a method of hierarchical routing and data aggregating for WSNs. In the proposed method, the network is clustered, and some nodes are selected as cluster heads. On constructing a rendezvous region and selecting backbone nodes, a tree is formed within backbone-tree nodes. The aggregated data are sent to the sink through backbone-tree nodes and cluster heads. Here, there are two modes of data transmission. The proposed method is simulated by Network Simulator (NS-2) software and compared with based data aggregation and rendezvous-based routing protocol. The results of simulation reveal that our method causes a decrease in end-to-end delay and energy consumption as well as an increase in the number of alive nodes and packet delivery rate..

Lipare, A., Edla, D. R., & Dharavath, R. (2021) provides the solution to improving energy efficiency in wireless sensor networks. In most of the existing fuzzy approaches, the CHs are selected first, and then clusters are generated, but this may lead to uneven distribution of the sensor nodes in the clusters [8]. In the proposed work the clusters are generated using the famous Fuzzy C-means (FCM) algorithm and the Cluster Head (CH) from each cluster is selected using the Sugeno fuzzy system. FCM generates load-balanced clusters and the proposed approach named SF-MPSO selects the suitable CH from each cluster. The local information of the sensor node such as residual energy, its distance from cluster centroid and the distance from the BS is provided to SF-MPSO. A novel fitness function is designed to identify the effectiveness of the generated solution. The simulations are performed under three scenarios where SF-MPSO outperforms existing EAUCF, DUCF, FGWO and ARSH-FATI-CHS when evaluated under the parameters such as energy consumption and network lifetime.

The system performs knowledge aggregation with security and attack handling mechanism. Repetitive filtering techniques with initial approximation model square measure accustomed secure knowledge aggregation method.

Owing to restricted procedure power and energy resources, aggregation of data's from multiple device nodes done at the aggregating node [9]. Such aggregation is understood to be extremely liable to node compromising attacks. Repetitive filtering algorithms hold nice promise for such a purpose. Such algorithms at the same time mixture knowledge from multiple sources and supply trust assessment of those sources, typically in an exceedingly sort of corresponding weight factors allotted to knowledge provided by every supply. The present paper demonstrate that many existing repetitive filtering algorithms, whereas considerably a lot of sturdy against collusion attacks than the easy averaging strategies, are even so susceptive to a unique subtle collusion attack. To handle this security issue, this work proposes Associate in Nursing improvement for repetitive filtering techniques by providing an initial approximation for such algorithms that makes them not solely collusion sturdy, however additionally a lot of correct and quicker convergence. This algorithm doesn't handle packet drop attack and not economical for centralized approach.

3. DATA AGGREGATION PROCESS

To overcome the matter occurred within the iterative filtering algorithm new technique referred to as Certificate Authority (CA) is introduced in every cluster. Knowledge Aggregation is employed to mixture data's by the cluster head finally transmit it to the base station [10]. The base station collects all the data's from cluster head and mixture for secure data transmission. To perform the aggregation safer the CA is employed to ascertain every node condition whether or not a node is trust node or malicious node. By exploitation the CA the node method are monitored.

The data's should be transmitted from member node to cluster head and from cluster head to either cluster head or base station inside a given time. If a time exceeds or any modifications wiped out the information then the certificate authority checks the threshold value of that node. If the threshold value is in vary then the node it trustworthy node and data aggregation is finished through this node. If the threshold value is in out of vary then the node is marked as malicious node. once marking the malicious node the information is not transferred at the actual node. so the information is transmitted solely the trustworthy node and it is collective additional securely and with efficiency. Provides safer for all the nodes due to exploitation the certificate authority. It will increase the packet delivery ratio and additionally improves the performance of non-stochastic elements errors like node fault etc.

3.1. Cluster Head Choice and Cluster Formation

The cluster head choice is predicated on the space, residual energy, position, velocity parameters. The optimized cluster head selected by exploitation PSO algorithm. Particle swarm optimization (PSO) could be a population-based random search method, shapely once the social behavior of a bird flock [11, 12]. The algorithmic rule maintains a population of particles, where every particle represents a possible answer to an optimisation drawback. Within the context of PSO, a swarm refers to variety of potential solutions to the optimisation problem, wherever every potential answer is cited as a particle. The aim of the PSO is to find the particle position that ends up in the simplest analysis of a given fitness (cluster head) operate.

Each particle represents an edge in N dimensional area, and is "flown" through this multi-dimensional search area, adjusting its position toward each the particle's best position found so far, and the best position within the neighborhood of that particle.

Each particle i maintains the following information:

x_i The *current position* of the particle

v_i : The *current velocity* of the particle

y_i: The *personal best position* of the particle. Using the above notation, a particle's position is adjusted according to

$$v_{i,k}(t+1) = wv_{i,k}(t) + c_1 r_{1,k}(t)(y_{i,k}(t) - x_{i,k}(t) + c_2 r_{2,k}(t)(\hat{y}_k(t)) - x_{i,k}(t)) \quad (1)$$

$$x_i(t+1) = x_i(t) + v_i(t+1) \quad (2)$$

where w is the inertia weight, $c_1$and $c_2$are the acceleration constants, $r_{1,j}(t), r_{2,j}(t) \sim U(0,1)$, and $k = 1, \dots, N$.The velocity is thus calculated based on three contributions:(1) a fraction of the previous velocity, (2) the cognitive component which is a function of the distance of the particle from its personal best position, and (3) the social component which is a function of the distance of the particle from the best particle found thus far (i.e. the best of the personal bests).The personal best position of particle is calculated as

$$v_{i,k}(t+1) = \begin{cases} y_i(t) & if\ f(x_i(t+1) \geq f(y_i(t)) \\ x_i(t+1) & if\ f(x_i(t+1) < f(y_i(t)) \end{cases} \quad (3)$$

Two basic approaches to PSO exist based on the interpretation of the neighborhood of particles. Equation (3) reflectsthe *gbest* version of PSO where, for each particle, the neighborhood is simply the entire swarm. The social component then causes particles to be drawn toward the best particle in the swarm. In the *lbest* PSO model, the swarm is divided into overlapping neighborhoods and the best particle of each neighborhood is determined. For the *lbest* PSO model, the social component of equation (3) changes to

$$c_2 r_{2,k}(t)(\hat{y}_{j,k} - x_{i,k}(t)) \quad (4)$$

where $\hat{y}_j$is the best particle in the neighborhood of the i-thparticle.

Cluster Formation

In the context of clustering, a single particle represents the$N_c$cluster centroid vectors. That is, each particle$x_i$is constructed as follows:

$$x_i = (m_{i1}, \dots, m_{ij}, \dots, m_{iN_c}) \quad (5)$$

Wherem_{ij}refers to the j-th cluster centroid vector of the i-th particle in cluster C_{ij}. Therefore, a swarm represents a number of candidate clusterings for the current data vectors. The fitness of particles is easily measured as the quantization error,

$$j_c = \frac{\sum_{j=1}^{N_c} [\sum_{\forall z_p \in C_{ij}} d(z_p, m_j)/|C_{ij}|]}{N_c} \quad (6)$$

Where d is defined as $d(z_p, m_j) = \sqrt{\sum_{k=1}^{N_d} (z_{pk} - m_{jk})^2}$, and C_{ij} is the number of data vectors belonging to cluster C_{ij}, i.e. the frequency of that cluster.

This section first presents a standard *gbest* PSO for clustering data into a given number of clusters is given below.

Gbset PSO cluster algorithm

Using the standard *gbest* PSO, data vectors can be clustered as follows:

1. Initialize each particle to contain randomly selected cluster centroids.

2. For t=1 to do
3. For each particle I do
4. For each data vector
5. Calculate the Euclidean distance to all cluster centroids
6. Assign to cluster such that $d(z_p, m_{ij}) = \forall_{c=1,\ldots,N_c}\{d(z_p, m_{ic})$
7. Calculate the fitness using equation (6)
8. Update the global best and local best positions
9. Update the cluster centroids using equ (1) and (2)

Where t_{max} is the maximum number of iterations.

The clustering can be reduced the energy and bandwidth allocation. And the overall process of proposed system is explained in fig 1.

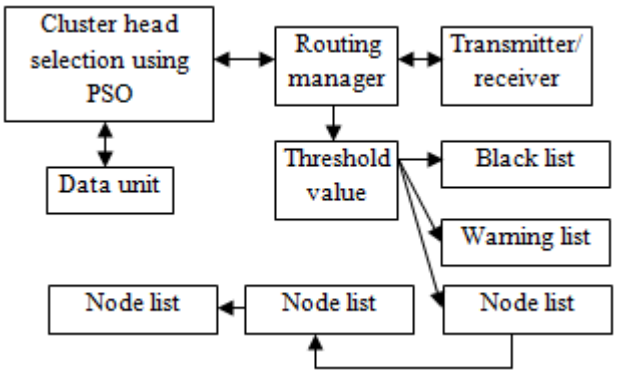

Fig 1: System Architecture

In Fig 1 describes that for each information transmission starts, the routing manager assures that the node could be a trustworthy node or not. Supported the threshold value the node trust is set. Each node features a specific threshold value. The threshold value is calculated supported the nodes gift within the network. If the threshold value is in vary then the node is captive to the Node list. If the threshold value is in out of vary then the node is captive to the black list. If the threshold value of the node is not even then it's captive to the warning list.

The trust node is gift solely within the node list. When the trust nodes are known then the nodes are monitored by network monitor and raise the member list. The member list nodes are solely allowed for information aggregation. The collection of information's are named as data units. The data's are collected from the cluster to the cluster head. This method is additionally monitored by routing manager. When complete this method the information aggregation starts firmly and with efficiency.

Initially, all the nodes are aggregated from the base station. The protection of the information throughout aggregation isn't ensured. By archiving this security, the certificate authority is provided by every cluster. The certificate authority checks whether or not the node is a certified node or malicious node. The certificate is simply provided to the licensed node. In fig 1, shows that there are many clusters. Every cluster features a specific set of nodes, cluster head and therefore the certificate authority. The cluster head collects the information from the whole licensed node and it send to the bottom station. If the cluster head is way aloof from the base station then it transfers the close cluster head and once more aggregated to the base station. Generally there's a malicious node

within the cluster head. There's no communication within the malicious node. The malicious node is simply known by mistreatment the certificate authority.

A. Network design

To produce a network with variety of nodes that could be a wireless sensor network and conjointly create the network with the WSN specifications i.e., every node will communicate with the other node directly that square measure in coverage space of the node. During this network, a group of nodes forming clusters. Every cluster has one leader node that is thought as cluster head which could be able to controls the whole traffic gift within the cluster of the network and that is a traditional node.

The other sort of node could be a certificate authority that monitors the whole traffic and finds the trustworthy node. The detector nodes are sometimes resource forced with relevancy memory house, computation capability, bandwidth and power offer. The network users use some mobile devices to aggregate data things into the network. The network owner is liable for generating keying materials. It will be offline and so the node is assumed to be uncompromisable.

B. Certificate Authority

This is a node that goes to require care of all different nodes by managing the traffic. It's getting to check whether or not the reply's sending by the nodes are applicable or not in regular intervals, whenever any new node enter in to the network it'll check whether or not the node is hacking node or not by the reply it sending and inform to all or any different nodes regarding the new node for the secure information transmission.

If any node is not responding properly then the certificate authority checks the threshold value for that node. If the threshold value is in out of vary then it mark the node is malicious node. The data transmission isn't done through this node. If the threshold value is in vary then the node could be a trust node. The data transmission is completed through this node. If the threshold value isn't even then the node is captive in to the warning list till the threshold value is even. The certificate authority work properly and secure with efficiency.

C. Watching the Traffic

Certificate Authority is employed to handle the protection method that is vital node within the network. It's getting to pay attention of the whole network i.e., it monitors all the nodes and checks that are giving sensible response supported that it'll enable different nodes to speak with one another. Networks users are appointed aggregation privileges by the trustworthy authority in a very public key infrastructure on behalf of the network owner. However, the network owner could, for numerous reasons, impersonate network users to combination information things. The compromised entities are considered insiders as a result of they are members of the network till they are known. The someone controls these entities to attack the network in arbitrary ways that. For example, they may be taught to combination false [13] or harmful information, launch attacks like Sybil attacks or Denial of Service attacks and be non-cooperative with different nodes. Information gathered by the individual nodes ultimately routed to the base station. A rate monitoring attack merely makes use of the thought that nodes nighest to the base station tend to forward additional packets than those farther aloof from the bottom station. AN attacker want solely monitor that nodes are causation packets and follow those nodes that are causation the foremost packets. Therefore the node nearer to the bottom station is monitored endlessly and transmits the information when finding that the node could be a trust node.

D. Route Discovery Method

Whenever a node need to speak with different node it got to realize the route for forwarding the information. During this route if any new node is entered suggests that there's an opportunity of which will be a hacking node. So, avoid that hacking nodes for secure information transmission. For this nodes are maintaining an inventory called true list, during this nodes are getting to store regarding the opposite nodes for locating the secure route. In external attacks, someone has no management of any sensor node within the network. The channel may additionally be jammed by someone, however this could solely last for an explicit amount of your time when that

someone are detected and removed. Route discovery should be initiated once a supply node desires to search out a route to a brand new destination or once the time period of an existing route to a destination has invalid.

- **Create trust list**

Nodes are getting to produce an inventory called true list. During this they are getting to store regarding the node information's that given correct response to the certificate authority. The utility of a sensor network can trust its ability to accurately and automatically find every sensor within the network. A sensor network designed to find faults can want correct location data so as to pin purpose the situation of a fault. Unfortunately, an attacker will simply manipulate non secured location data by coverage false signal strengths and replaying signals.

- **Check trust list**

Whenever a node needs to send the information it will send route request to different nodes. The node that received the route request packet can checks whether or not that node is present within the true list or not if conferred suggests that it will forward to different nodes and it will repeats till it reaches destination. Route trust is computed by each node for every route in its routing table. It is a live of the responsibleness with that a packet will reach the destination, if forwarded by the node on it specific route. For each transmission starts before it check the route whether or not it's a trust list or hacking list. If it is a trust list then the data aggregation is completed firmly certificate authority. The secure node is known solely by the certificate authority. The certificate authority checks whether or not the node is that the trust node or not and at last the information aggregation is performed.

4. RESULTS AND DISCUSSION

In this section, simulation experiments are presented to demonstrate the effectiveness and superiority of the proposed PSOC based secure data aggregation protocol algorithm in comparison with the existing algorithms such as improved iterative filtering protocol [14]. The performance is measured by network parameters such as energy consumption, throughput, message delivery ratio, network lifetime, delay.

1. Energy consumption

The average energy consumed by each node during the given simulation time and expressed in Joules (J).

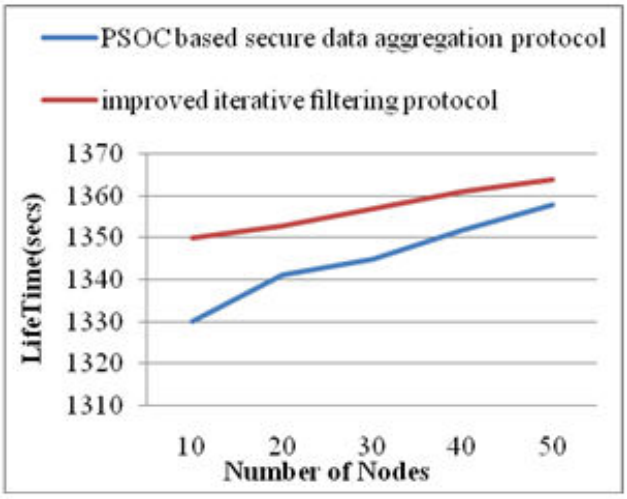

Fig 2: Comparison of Energy consumption vs. Number of Nodes

Fig. 2 shows that the graphical representation of energy consumption for different number of nodes in WSN. The PSOC based secure data aggregation protocol algorithm has low energy consumption when compared with the existing system improved iterative filtering protocol. The energy for each and every node is calculated and cluster formation is done based on the energy values.

2. LIFETIME EVALUATION

Fig. 3 shows the lifetime of the WSN network in PSOC based secure data aggregation protocol, improved iterative filtering protocol with different data effective time. In this figure, the lifetime of both two schemes decreases as the node number increases in the most cases. As the number of nodes in the ad hoc network increases, the load of the storage node in iterative filtering protocol and that of the nodes energy consumption high. It is noted that the lifetime of the ad hoc network in PSOC based secure data aggregation protocol does not change as the node number increases. The reason is that, when the data effective time is small enough, almost all the queries meet the desired event data in existing protocol. The PSOC based secure data aggregation protocol algorithm has high network lifetime when compared with the existing system.

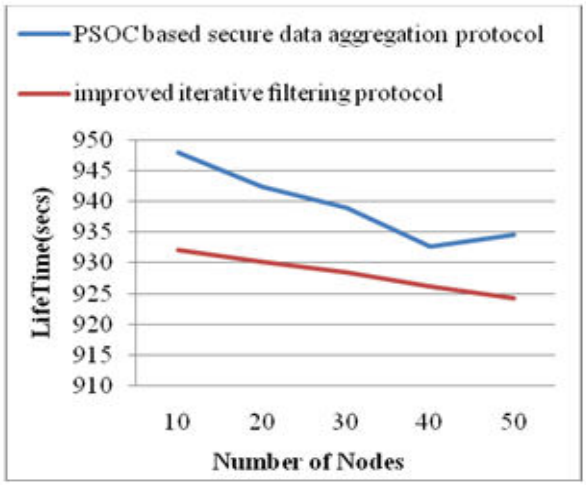

Fig. 3: Comparison of Network lifetime vs. Number of Nodes

3. Delay Evaluation

Fig. 4 shows the average delay of data storage in PSOC based secure data aggregation protocol, improved iterative filtering protocol. It is obvious that the average delay of PSOC based secure data aggregation protocol is much less than that in improved iterative filtering protocol. In proposed protocol, the event data routing is much easier than routing the event data to the storage node using existing routing protocol. Besides, there are many nodes located in the proposed protocol, and they just need to store the data generated by themselves locally, which can greatly decrease the average delay of data storage and retrieval.

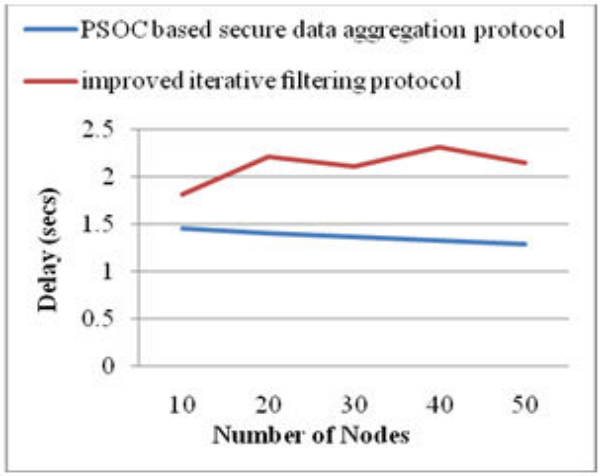

Fig. 4: Comparison of Delay vs. Number of Nodes

4. THROUGHPUT EVALUATION

Fig. 5 shows the throughput comparison of the proposed PSOC based secure data aggregation protocol approach and the existing improved iterative filtering protocol. It is noted that the proposed protocol attains higher throughput when compared with the existing algorithm. The reason is that, the probability to meet the desired event data in a short hop count is very high in such a way.

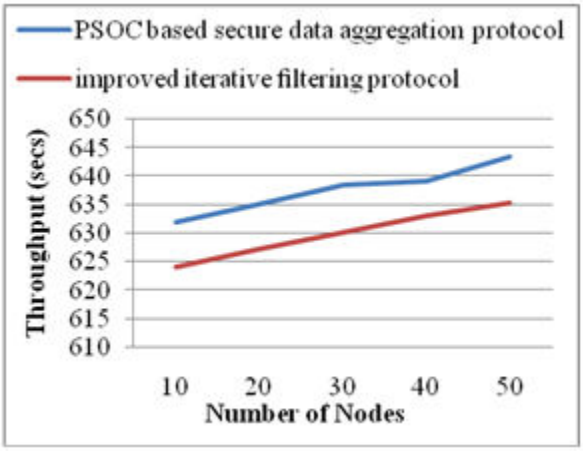

Fig 5: Comparison of throughput vs. Number of Nodes

5. MESSAGE DELIVERY RATIO (PDR) EVALUATION

Fig. 6 shows the comparison PDR of the proposed protocol approach and the existing improved iterative filtering protocol. Message delivery Ratio (PDR) is defined as the ratio of total messages transmitted to total messages received at the destination. In existing protocol some of the messages may drop due to congestion and buffer overflow at the cluster heads, this results in the drop of PDF whereas proposed protocol performed load balancing and this improves PDR.

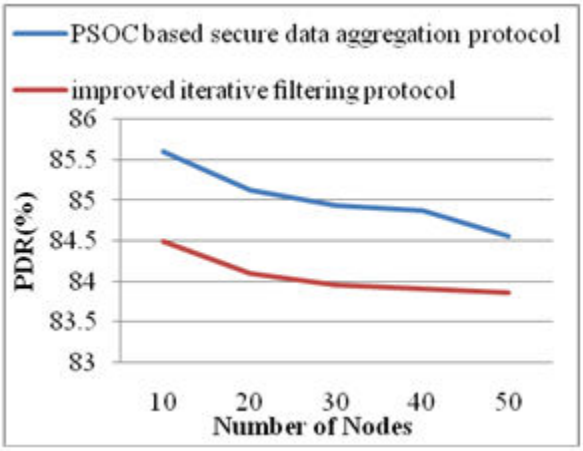

Fig 6: Comparison of PDR vs. Number of Nodes

5. CONCLUSION AND FUTURE WORK

The planned cluster based trust management theme that enhances the protection of WSN. By using the planned methodology Secure routing path may be established in malicious environments. The results of WSN routing situation absolutely support the effectiveness and performance of the theme, which improves throughput and packet delivery ratio significantly, with slightly weakened average delay and overhead of messages. The protection needs of wireless sensor networks needed to strengthen attack-resistant information aggregation

protocols. The certificate authority computes verity mixture by filtering out the contributions of compromised nodes within the aggregation hierarchy. The nodes are secured by the planned methodology. In future work, the opinion request is send to the neighbour's node as a result of the supply node finds the malicious node. Within the presence of malicious nodes, the need might cause serious security drawback such nodes might disrupt the routing method. A malicious node will attract all packets by using forged Route Reply packet. The supply node broadcasts a Route Request packet to any or all the nodes gift within the network. Once destination receives the Request, it will recognize every intermediate node's address among the route.

REFERENCES

[1] Soltani, K., Farzinvash, L., & Balafar, M. A. (2023). Trust-aware and energy-efficient data gathering in wireless sensor networks using PSO. Soft Computing, 27(16), 11731-11754.

[2] Sreedevi, P., & Venkateswarlu, S. (2022). An Efficient Intra-Cluster Data Aggregation and finding the Best Sink location in WSN using EEC-MA-PSOGA approach. International Journal of Communication Systems, 35(8), e5110.

[3] Sahoo, B. M., Amgoth, T., & Pandey, H. M. (2020). Particle swarm optimization based energy efficient clustering and sink mobility in heterogeneous wireless sensor network. Ad Hoc Networks, 106, 102237.

[4] Jubair, A. M., Hassan, R., Aman, A. H. M., Sallehudin, H., Al-Mekhlafi, Z. G., Mohammed, B. A., & Alsaffar, M. S. (2021). Optimization of clustering in wireless sensor networks: techniques and protocols. Applied Sciences, 11(23), 11448.

[5] Sharmin, S., Ahmedy, I., & Md Noor, R. (2023). An energy-efficient data aggregation clustering algorithm for wireless sensor Networks using hybrid PSO. Energies, 16(5), 2487.

[6] Pavani, M., & Trinatha Rao, P. (2019). Adaptive PSO with optimised firefly algorithms for secure cluster-based routing in wireless sensor networks. IET Wireless Sensor Systems, 9(5), 274-283.

[7] Sharifi, S. S., & Barati, H. (2021). A method for routing and data aggregating in cluster-based wireless sensor networks. International Journal of Communication Systems, 34(7), e4754.

[8] Lipare, A., Edla, D. R., & Dharavath, R. (2021). Fuzzy rule generation using modified PSO for clustering in wireless sensor networks. IEEE Transactions on Green Communications and Networking, 5(2), 846-857.

[9] Rawat, P., & Chauhan, S. (2022). Particle swarm optimization based sleep scheduling and clustering protocol in wireless sensor network. Peer-to-Peer Networking and Applications, 15(3), 1417-1436.

[10] Roy, S., Mazumdar, N., & Pamula, R. (2021). An energy optimized and QoS concerned data gathering protocol for wireless sensor network using variable dimensional PSO. Ad Hoc Networks, 123, 102669.

[11] Han, Y., Li, G., Xu, R., Su, J., Li, J., & Wen, G. (2020). Clustering the wireless sensor networks: a meta-heuristic approach. IEEE Access, 8, 214551-214564.

[12] Yousefpoor, E., Barati, H., & Barati, A. (2021). A hierarchical secure data aggregation method using the dragonfly algorithm in wireless sensor networks. Peer-to-Peer Networking and Applications, 14(4), 1917-1942.

[13] Huangshui, H., Xinji, F., Chuhang, W., Ke, L., & Yuxin, G. (2023). A Novel Particle Swarm Optimization-Based Clustering and Routing Protocol for Wireless Sensor Networks. Wireless Personal Communications, 133(4), 2175-2202.

[14] Wohwe Sambo, D., Yenke, B. O., Förster, A., & Dayang, P. (2019). Optimized clustering algorithms for large wireless sensor networks: A review. Sensors, 19(2), 322.