ISSN 2348 – 9928
IJAICT Volume 1, Issue 11, March 2015 Doi:01.0401/ijaict.2015.11.19 Published on 05 (04) 2015

# CONCEALED DATA AGGREGATION AND EXPONENTIAL PARTICLE SWARM OPTIMIZATION FOR DELAY PERFORMANCE IN WIRELESS SENSOR NETWORKS

***Ms. P. Poornapriya***
***PG Scholar,***

***Ms. M. Ananthi***
***Assistant Professor,***

***Computer Science and Engineering,***
***Info Institute of Engineering College,***
***Coimbatore, Tamilnadu, India***

***Abstract— Wireless sensor networks (WSN) are an exacting category of wireless ad hoc networks with the intention of catch the attention of growing concentration, together in academia and business. Routing in WSN is varied with the purpose of reasonable mobile ad-hoc networks. During this process it needs to support several numbers of transmissions such as single transmission, one to multihop transmission and multihop manner to reach destination. One of the major challenges in routing is security. This security and routing delay problem is solved by using data aggregation schemas in recent years. In this paper focus on routing problem in WSN is solved by using Concealed data aggregation schema. During data aggregation process each sensor nodes in the network generates the information of nodes through sensing its objective location and transmits the information of each nodes to specific node which is called as sink node. During this Concealed data aggregation schema generates the information of nodes through sensing its objective location and the information of each sensor nodes is encrypted using public homorphic system without delay in routing, since the proposed routing is performed based on exponential particle swarm optimization (EPSO) which results high well-organized and flexible Concealed data aggregation. Then routing in WSN is performed based on exponential particle swarm optimization (EPSO) with delay function as fitness function. The experimentation work of the proposed system is implemented in network simulation tool NS2 which is reasonable and normally even more less energy consumption results in well-organized than hop-by-hop encryption.***

***Keywords— Wireless Sensor Networks, Data Encryption, Data Aggregation, Robustness And Reliability, Privacy Homomorphism, Key Predistribution, Delay Performance.***

## I. INTRODUCTION

Wireless sensor networks (WSN) are an exacting category of wireless ad hoc networks with the intention of catch the attention of growing concentration, together in academia and business. In WSN sensor nodes they are if at all possible not expensive and minute consisting of

1. Purpose specific sensors,
2. A wireless transceiver,
3. A straightforward mainframe, and
4. An energy unit with the intention of might be succession or solar-driven.

In exacting, cannot presuppose a sensor node in the direction of exist tamper challenging. This category of sensor nodes determination is present spread out in excess of a geological region to outline a multihop network in a self organizing way. The majority of WSNs are inactive, even though mobile WSNs are moreover feasible. Prospective applications designed for WSNs is military ones which consists the information of military and continuously monitoring information and geolocation area becomes more important through the purpose to recognize difficult and geological extensive interdependencies of natural world. Some of the examples in the wireless sensor nodes are the identification of fire accident through the continuous monitoring of the forest areas, identification of climatic changes in snow wall and snow in alpine wall in vineyards. Some other applications in wireless sensor network focus on the biomedical medical to sense the information of patient in sensor nodes which is moved from one phase to another phase in the wireless sensor network.

One of the most important applications in WSN is the monitoring of the network or geographical location information and their data from one location to another location to focus on central view of the point .During this type of process information from sensor nodes is analyzed and ultimately provide to start a number of specific actions. Examination of this type of information or data plays major important role which reduces the computation of time which in turns to complete the process in less optimum or minimum execution for identification of movement nodes in the wireless sensor

network without loss of information .The computation time of movement process is measured based on central point of view in WSN or network itself. But major issue of this work is the consumption of energy during data transmission phase from one senor nodes to another sensor nodes increases if the amount of information or data is increases which reduces lifetime of the entire wireless sensor network .So the saving energy during this process important which is performed based on efficient transmission of data or information in quick manner, which is solved by using data aggregation schemas in the recent years.

Inside the measured aggregation development designed for stationary WSNs, individual requirements on the way to understandably divide sensor nodes, promote nodes, aggregator nodes, and the base station node, which begin the examining and information accumulate procedure. Among them all of the nodes aggregator nodes, base station node ,and forwarding nodes regarded on the way to the backbone of WSN, whereas sensor nodes persevere in sleep form in anticipation of the base station node start a procedure which necessitate a separation of them to contribute. The base station node might whichever is present the relationship to the predetermined network designed for the information collection procedure. It is assumed to be a large amount more potent than individual's nodes with the intention of sense or collective information.

To conquer all of the above mentioned issues and saving the energy of wireless sensor nodes in the network , in this paper mainly focus how to the delay in the network during Concealed data aggregation schema and data aggregation schema. In a noisy wireless control, preserve the reliability value for entire network and maintaining the computation time during data aggregation becomes more difficult [1]–[3]. Because the data enclosed in a particular packet is extremely exaggerate following more than a few in-network computations, a packet loss can considerably crash the computation effect, and consequently an elevated level of security is necessary intended for every one packet transmission. A packet is able to be confined through error correcting code (EEC) [4] by means of retransmitting the vanished packet. In either case, added interruption is inevitable. In numerous applications, it is significant to calculate the universal purpose in an appropriate and dependable manner, and consequently restrictive the quantity of further delay is imperative.

Some of the methods [4-7] also proposed in recent work to solve delay problem in WSN during data aggregation procedures .The major goal of this methods is to save the energy and reduces the delay in the WSN to attain the safety objective of privacy. If end-to-end encryption is preferred, then pertain the common encryption algorithms entail with the intention of middle nodes cannot capably cumulative information to remain the range of messages promote little. A data aggregation schema belongs to network aggregation schemas have been studied in several numbers of works with various aspect of view [1] some of the aspects are: The maximum attainable computation rate designed for a group of functions have been examined in [8-9]. Energy efficiency of WSN has been studied in [10]. Time and Energy efficiency of WSN have been studied and examined in [11].

## II. BACKGROUND STUDY

Vuran et al[12] developed a novel data aggregation schema based on the spatial and temporal environment in WSN. The most and major important of the key elements are taken during data aggregation schema to make use of the connection in the WSN designed for the expansion of well-organized communication protocols. This schema is applied to unicast transmission communication in WSN and have achieves higher accuracy in the WSN. But the major issue of the work is that it doesn't applied for broadcast communication rather than the single or unicast transmission communication this is solved by using network aggregation schema in the recent years [13]. Opportunistic aggregation system is introduced in [14] for WSN through in the neighborhood of best possible performance under extensively changeable scale of connection. Opportunistic aggregation system, formalize a view of association with the intention of be able to be different according to a constraint k. In [14] also develop a The key contribution in randomized analysis is to bound the average expected collision time based on the random walk theory .

Greedy aggregation scheme is introduced and developed in [15]. This Greedy aggregation scheme with the intention of regulates aggregation position to enlarge the quantity of path division in WSN with decreased energy use. The proposed data aggregation schema is varied from existing methods which is discussed in earlier during path establishment and protection. This proposed Greedy aggregation scheme generates a tree based on the strategy of greedy schema and efficient shortest path is found for sink node to reach destination node in the wireless sensor network (WSN). Redundancy Elimination for Accurate Data Aggregation (READA) is developed and introduced in [16] to solve data aggregation problem. Through make use of the variety of spatial association of information in the network, the proposed schema follows grouping schema

and uses compression mechanism to reduce and remove duplicate information for sensor nodes in base station with less delay and less information loss during data aggregation process.

Secure Hop-by Hop Data Aggregation Protocol (SDAP) [17], is proposed based on the data aggregation schema which follows the procedure of divide and conquer methods through commit and confirm standards. In the initial stage of the work the nodes in the network is separated into several number of sensor nodes in a tree topology and the similar nodes in the network is clustered based on the probabilistic grouping procedure. Secure Data Aggregation and verification Protocol (SDAV) [18] is developed for data aggregation process and it is designed in two stages .

In initial stage of the work key is generated for each sensor nodes in the cluster by the use of Elliptic Curve Cryptography (ECC). After that Data Aggregation and Verification is designed in the secure manner, it is considered as one of the important protocol. This proposed data aggregation and verification protocol detects false collective data through using Merkle Hash Trees, it confirm integrity of information of sensor nodes.

Secure and efficient protocol for Data Aggregation (SEDAN) [19], is introduced and developed in recent years with multihop transmission is performed designed for data integrity. This SEDAN data aggregation scheme does not necessitate base station to authenticate and distinguish inaccuracy in aggregated .During this process every nodes can authenticate reliability of information of multihop absent neighbors. Because of this reason energy of each senor nodes is saved and bogus data is reduced. Secure Data Aggregation protocol [20] is developed and introduced in WSN based on disclosure and explanation double-dealing sensor nodes through their sensed information.

It makes use of outlier discovery algorithm to discover and illuminate absent the outlier sensor nodes. It presents outlier disclosure speed since to the make use of distributed schema. It makes use of MAC designed for verification of information and integrity of information. For provided that secrecy to information, symmetric encryption method is also designed in this work.

## III. PROPOSED CONCEALED DATA AGGREGATION AND PARTICLE SWARM OPTIMIZATION BASED ROUTING METHODOLOGY

Because of the several number of aspects in the wireless sensor network ,the following ways solve the issues , 1) in this work we superficially focus of the Concealed data aggregation schema which is performed based on the public key homorphism encryption schema, then delay value in the WSN between one node to another node is measured based on the routing EPSO schema ; 2) regard as dependability constriction in WSN is also determined and evaluated and 3) examine the result of wireless broadcast communication of both delay and network performance . In the proposed Concealed data aggregation schemas are based on the passive attacker representation propose be appropriate Domingo-Ferrer's schema to hide the procedure of information aggregation in a WSN: Sensors nodes from $S_1$ to $S_n$ in the WSN and their information is encrypted through $s_1' = E_{(r,g')}(S_1)$ and $s_2' = E_{(r,g')}(S_2)$ before performing the communication between one sensor node to another sensor nodes from base station to destination node .After that encryption process then data transmission is performed between nodes ,through the computation of key values $(s_1', \dots, s_n')$. Consequently, the aggregator A communicates $y_0$ to the R which decrypts the $y_0$ and obtain the gather information $y = D(r; g_0)(y_0)$. Regard as $(rg')$ be well-known to $S_1, \dots . S_n$ and at the $R$ .Among them all of the values they $d$ and $g$ are easily identifiable value for aggregator A .The operation of the aggregation is performed based on the multiplicative and addition operation A to $S_1 \dots . S_n$. At $S_i$ with $1 \leq i \leq n$ :Split $s_i \in \mathbb{Z}_{g'}$ into a secret $s_{i,1}, \dots s_{i,d}$ such that $s_i = \sum_{j=1}^{d} s_{ij} \bmod g'$ and $s_{i,j} \in \mathbb{Z}_g$ .Calculate $s_i' = s(i) = (s_{i,1} \bmod g)$ and transmit $s_i'$ to A. Calculate the values of multiplicative and addition operation in homomorphic encryption methods with their aggregation schema $y' = f(s_1', \dots . s_n')$ and send the data to $y'$ to R.

During this data aggregation schema routing plays major important since it reduces the delay in the network ,to solve this routing problem and reduces the delay in the network in this work proposed a swarm intelligence based schema which follows the procedure of particle swarm optimization methods of particle swarm optimization methods which is rely on position and velocity. The particle swarm optimization methods are performed based on towards the direction of less delay function is considered as best investigation space. This is predictable to give the greatest resolution. It can be used to investigate large investigate space. In the proposed work routing is performed based on the Extended Particle Swarm Optimization (EPSO) be able to be common in the middle of the additional intellectual optimization method to propose

many of compound optimization systems. The proposed EPSO routing schema is based on the allocation scheme. The proposed EPSO schema is applied to several number of nodes in the network during data aggregation process to perform efficient routing with less delay in the network is determined based on the fitness function or objective function the number of nodes in the network is selected for data aggregation with encrypted key for information of sensor nodes .To determine the nodes in the network through EPSO algorithm the position of the particles (nodes) and their velocity of the nodes is automatically updated based on the objective function . Routing schema in the WSN the nodes in the network represented as tiered structure each node in $T_i$is a father of node V in $T_{i+1}$if its space is no larger than (n) . Communication are programmed on or after the furthest tier toward the base node through tier one at a time, consequently with the intention of nodes $T_I$ in can broadcast simply following each and every one nodes $T_{i+1}$in complete their transmissions. Noticeably, each and every one nodes$T_i$ in can finish a solitary communication $h_i$in mini-slots. If present is no intrusion among immediate transmissions inside a tier, determination contain a solitary collection through $h_i = 1$ in designed for all tier

$$D_b = \sum_{i=1}^{\frac{1}{\delta t(n)}} h_i\left(1 + r_b(n)\right) \quad (1)$$

In the proposed work routing is performed based on the Extended Particle Swarm Optimization (EPSO) be able to be common in the middle of the additional intellectual optimization method based on the collective behavior of a bird accumulate. Each and every nodes in the network is considered as particles in the wireless sensor network, which is selected based on the objective function where the nodes moves from one particle to another particle if the selected nodes have less delay and higher objective function . Once the nodes in the network is selected position and velocity is updated automatically [21-22]. , $v_i$ is denoted as the velocity of the node which is defined between the interval $v_{min}$ and$v_{max}$ is denoted and updated as ,

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

$$x_{tf}(t+1) = x_{tf}(t) + v_{tf}(t+1) \quad (3)$$

Where w inertia weight for each nodes in the network with intervals [0-1], $c_1 \& c_2$ are the constant values of local and global nodes , correspondingly, $r_{1,tf}(t), r_{2,tf}(t) \sim U(0,1)$ and $k = 1, \ldots, N_d$.

$$y_{tf}(t+1) = \begin{cases} y_{tf}(t) \; if \; f(x_{tf}(t+1)) \geq f(y_{tf}(t)) \\ x_{tf}(t+1) \; if \; f\left(x_{tf}(t+1)\right) < f\left(y_{tf}(t)\right) \end{cases} \quad (4)$$

$$c_2 r_{2,k}(t)\left(\hat{y}_{tf,k}(t) - x_{tf,k}(t)\right) \quad (5)$$

Where $\hat{y}_{tf,k}(t)$ is the selected nodes in the network for routing and data aggregation schema . The PSO is implemented based on the equation (2-3) and is determined based on the fitness function is performed until the iterations which is specified in EPSO ,it the selected nodes in the network not attains delay results until the predefined iteration then the present node is not selected for communication process ,then position and velocity is updated automatically . Once a novel $g_{best}$ is found for routing in data aggregation, it spreads in excess of nodes particles immediately and so all node in the networks are disturbed to this position in the subsequent steps in anticipation of one more nodes in the network is selected .To increase the speed of the algorithm inertia weight w is is newly updated based on the iteration and maximum number of iterations

$$w = (w - 0.4)\left(\frac{MAXITER - ITERTATION}{MAXITER}\right) + 0.4 \quad (6)$$

$$w = (w - 0.4)e^{\left(\frac{MAXITER - ITERTATION}{MAXITER}\right)^{-1}} + 0.4 \quad (7)$$

EPSO algorithm

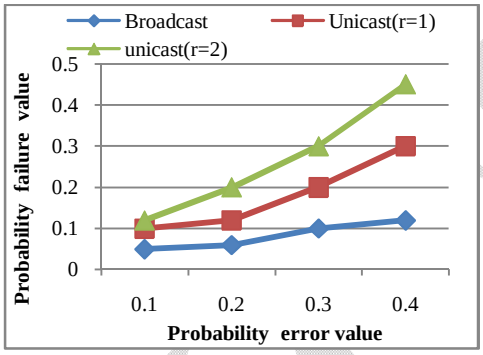
1. Initialize every particle in the node from wireless sensor network
2. for t = 1 to t max do
3. for each particle node randomly do
4. for each data of sensor nodes in the wireless sensor network from data aggregation
5. The similarity of two position vectors in each and every nodes in the wireless sensor networks can be measured by the angle among two senor nodes information by the distance among two particles.
6. Calculate the fitness using equation (1)
7. Update the global best and local best positions
8. Update the sensor node information and perform aggregation using (1) and (2)

## IV. EXPERIMENTATION WORK

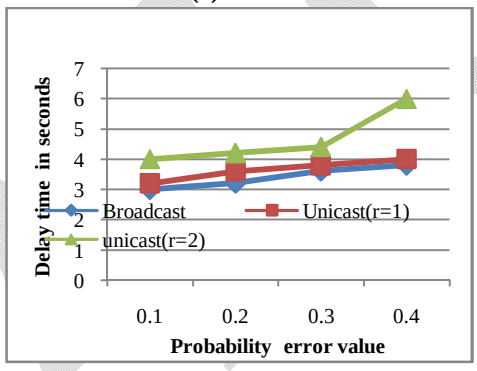
In this section, we measure the performance accuracy of the proposed Concealed data aggregation schema with EPSO and

it is measured based on the network simulation tool NS2 .The proposed Concealed data aggregation schema with EPSO is measured in terms of data dependability with victorious data transmissions in addition to the delay comparison. The proposed Concealed data aggregation schema with EPSO is simulated to Time division multiple access (TDMA) networks not including interfering and continue in the direction of resource-constrained networks through wireless interfering.

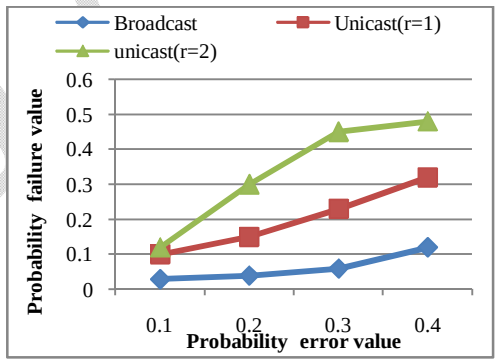
The performance accuracy results of the proposed Concealed data aggregation schema with EPSO based routing is measured in three ways with delay, loss rate and delay and loss rate as shown in Fig.1 demonstrate the failure rate of the significant information assessment and the delay show. Fig. 1(a) illustrates the shows that Concealed data aggregation schema with EPSO for unicast have produces high data loss and produces less data rate when compare to other types of transmission




(a) Loss rate




(b) Delay rate




(c) loss and delay rate

*Fig.1. Loss rate and delay information rate*

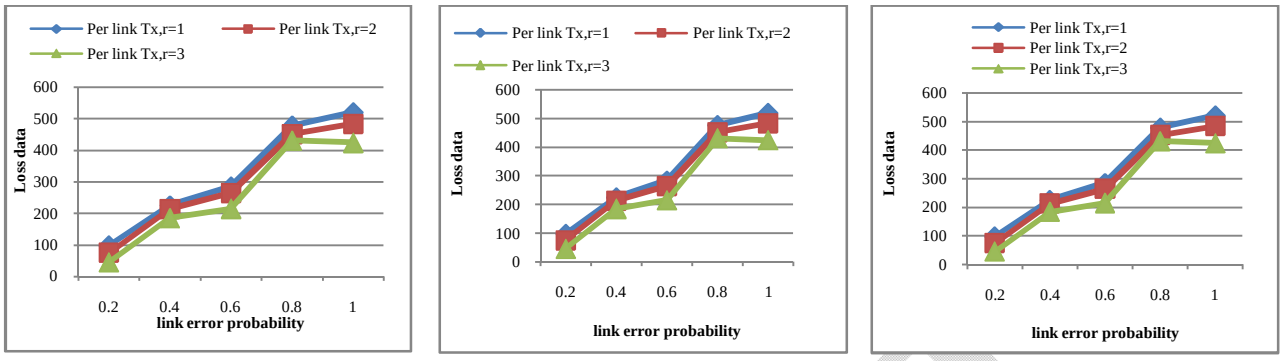



*Fig.2 .Loss information in the presence of inference with k=1,2,3*

such as multicast and broadcast .Conversely, Concealed data aggregation schema with EPSO for unicast delay performance also measured and illustrated in Fig. 1(b). It shows that Concealed data aggregation schema with EPSO for unicast delay performance have less for multicast since it doesn't perform any retransmission similarly for broadcast-based communication. Then combined performance measurement based on the delay and loss rate is measured for unicast ,broadcast and multicast communication then it is experimental in Fig. 1(c) through broadcast attain improved performance.

Fig.2 shows the performance accuracy results of the proposed Concealed data aggregation schema with EPSO routing is measured based on the reliability measurement. This measure the number of loss of information during data aggregation process or schema through diverse connection loss probabilities, several number of retransmissions, and based on the number of forwarders. The proposed Concealed data aggregation schema with EPSO results demonstrate with the intention of a little numeral of forwarders considerably enhanced the consistency, particularly while the connection loss probability is high.

## V. CONCLUSION

Routing in WSN is varied with the purpose of reasonable mobile ad-hoc networks. The major goal of this paper is to solve routing problem in WSN through Concealed data aggregation schema with less delay value is measured based on the exponential particle swarm optimization (EPSO). In addition routing efficiency is also performed based on the exponential particle swarm optimization (EPSO). Conversely, because the thrashing of a collective small package is extreme additional destructive than an unaggregated packet in wireless environments. During this Concealed data aggregation process each sensor nodes in the network generates the information of nodes through sensing its objective location broadcast communication is performed between nodes in the wireless sensor network (WSN) . The experimentation work of the proposed system is implemented in network simulation tool NS2 through hop-by-hop encryption scheme which is reasonable and normally even more less energy consumption results designed for a wide assortment of reasonable WSN. Simulation results of Concealed data aggregation is experimented through broadcast communication which is performs better than existing schemas with unicast traffic, especially in WSN environments.

## VI. FUTURE SCOPES

In future we apply the present schema to combine the procedure of unicast and multicast communication. The future work will be also expanded into the following directions. Concealed data aggregation schema is performed with different types of public key encryption schema in WSN the network. Although delay performance of the proposed schema is applied to other types of optimization and some other constraints also taken during delay calculation which would increases the results with less loss of information and high achievement of results with reduced time complexity.

## References

[1] Giridhar and P. R. Kumar, "Toward a theory of in-network computation in wireless sensor networks," IEEE Commun. Mag., vol. 44, no. 4, pp. 98–107, Apr. 2006.

[2] E. Kushilevitz and Y. Mansour, "Computation in noisy radio networks," SIAM J. Discrete Math., vol. 19, no. 1, pp. 96–108, 2005.

[3] L. Ying, R. Srikant, and G. Dullerud, "Distributed symmetric function computation in noisy wireless sensor networks," IEEE Trans. Inf. Theory, vol. 53, no. 12, pp. 4826–4833, Dec. 2007.

[4] L. L. Peterson and B. S. Davie, Computer Networks: A Systems Approach, 3rd Edition. SanFrancisco, CA, USA: Morgan Kaufmann, 2003.

[5] Weimerskirch and D. Westhoff, "Zero-Common Knowledge Authentication for Pervasive Networks," Proc. 10th Workshop Selected Areas in Cryptography (SAC '03), pp. 73-87, July 2003.

[6] Weimerskirch and D. Westhoff, "Identity Certified Zero-Common Knowledge Authentication," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '03), Oct. 2003.

[7] Weimerskirch, D. Westhoff, S. Lucks, and E. Zenner, "Efficient Pairwise Authentication Protocols for Sensor Networks: Theory and Performance Analysis," Sensor Network Operations, S. Phoha, T.F. La Porta, and C. Griffin, eds. Wiley-IEEE Press, May 2006.

[8] S. Kamath and D. Manjunath, "On distributed function computation in structure-free random networks," in Proc. IEEE ISIT, Jul. 2008, pp. 647–651.

[9] C. Li and H. Dai, "Towards efficient designs for in-network computing with noisy wireless channels," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–8.

[10] J. Zhao, R. Govindan, and D. Estrin, "Computing aggregates for monitoring wireless sensor networks," in Proc. IEEE Int. Workshop Sensor Netw. Protocols Appl., May 2003, pp. 139–148.

[11] N. Khude, A. Kumar, and A. Karnik, "Time and energy complexity of distributed computation in wireless sensor networks," in Proc. IEEE INFOCOM, 2005, vol. 4, pp. 2625–2637

[12] N. Jain, S. Gupta, and P. Sinha, "Clustering Protocols in Wireless Sensor Networks: A Survey," Int. J. Appl. Inf. Syst., vol. 5, no. 2, pp. 41–50, 2013.

[13] N. Jain, S. Gupta, and P. Sinha, "Clustering Protocols in Wireless Sensor Networks: A Survey," Int. J. Appl. Inf. Syst., vol. 5, no. 2, pp. 41–50, 2013.

[14] C. Intanagonwiwat, R. Govindan, D. Estrin, J. S. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking", IEEE/ACM Transactions on Networking, vol. 11, no. 1, p. 2-16, 2003.

[15] M. Enachescu, A. Goel, R. Govindan and R. Motwani, "Scale Free Aggregation in Sensor Networks," Preprint submitted to Elsevier Science 24 January 2006.

[16] K. Khedo, R. Doomun and S. Aucharuz, "READA: Redundancy Elimination for Accurate Data Aggregation in Wireless Sensor Networks," Wireless Sensor Network, Vol. 2, No. 4, 2010, pp. 302- 308.

[17] Y.Yang, X.Wang, S.Zhu and G. Cao "A Secure Hop-by Hop Data Aggregation Protocol for Sensor Networks" in Proc. 7th ACM Int. Symp. Mobile Ad-hoc, 2006

[18] A.Mahimkar, T.S.Rappaport "A Secure Data Aggregation and verification Protocol for Sensor networks", IEEE Communications Society Globecom 2004

[19] M.Bagaa, N.Lasla, A. Ouadjaout, Y.Challal, "Secure and efficient protocol for Data Aggregation in wireless sensor networks", 32nd IEEE Conference on Local Computer Networks, 2007.

[20] M.K.Jha, T.P Shrama, "A New Approach to Secure Data Aggregation protocol for Wireless Sensor Networks", International Journal on Computer Science and Engineering, vol. 2, No. 5, 2010

[21] Cui, X., Potok, T., Palathingal, P., Document Clustering using Particle Swarm Optimization, Swarm Intelligence Symposium, 2005. Proceedings 2005 IEEE, pp. 185- 191.

[22] Li-ping, Z., Huan-jun, Y., Shang-xu, H., Optimal Choice of Parameters for Particle Swarm Optimization, Journal of Zhejiang University Science, Vol. 6(A)6, pp.528-534, 2004.