**International Journal of Electrical and Computer Engineering (IJECE)**
Vol. 8, No. 6, December 2018, pp. 5162~5168
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i6.pp5162-5168 

# Improving IF Algorithm for Data Aggregation Techniques in Wireless Sensor Networks

**Madhav Ingle, P.V.R.D. Prasada Rao**
Department of CSE, Koneru Lakshmaiah Education Foundation, India

**Article Info**

***Article history:***

Received Dec 28, 2017
Revised May 31, 2018
Accepted Jun 15, 2018

***Keyword:***

Aggregation
Attack
Filtering
Networks
Robust
Sensor
Wireless

**ABSTRACT**

In Wireless Sensor Network (WSN), fact from different sensor nodes is collected at assembling node, which is typically complete via modest procedures such as averaging as inadequate computational power and energy resources. Though such collections is identified to be extremely susceptible to node compromising attacks. These approaches are extremely prone to attacks as WSN are typically lacking interfere resilient hardware. Thus, purpose of veracity of facts and prestige of sensor nodes is critical for wireless sensor networks. Therefore, imminent gatherer nodes will be proficient of accomplishment additional cultivated data aggregation algorithms, so creating WSN little unresisting, as the performance of actual low power processors affectedly increases. Iterative filtering algorithms embrace inordinate capacity for such a resolution. The way of allocated the matching mass elements to information delivered by each source, such iterative algorithms concurrently assemble facts from several roots and deliver entrust valuation of these roots. Though suggestively extra substantial against collusion attacks beside the modest averaging techniques, are quiet vulnerable to a different cultivated attack familiarize. The existing literature is surveyed in this paper to have a study of iterative filtering techniques and a detailed comparison is provided. At the end of this paper new technique of improved iterative filtering is proposed with the help of literature survey and drawbacks found in the literature.



***Corresponding Author:***

Madhav Ingle,
Department of CSE,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Guntur, Andhra Pradesh, India.
Email: ingle.madhav@gmail.com

## 1. INTRODUCTION

Wireless sensor networks (WSN) are usually comprises thousands of low cost, low power sensing devices with limited computational, memory and communication resources. WSN is called as a special class of ad-hoc wireless network. As WSN contains several thousands of sensor nodes distributed in a target detecting environment within its neighborhood collects the data and computes it. Sensor nodes are made up of simple processor, application specific sensors, wireless transceiver and low battery. Data aggregation is used due to limited amount of power in sensor nodes and to reduce transmission overhead. A variety of schemes for data aggregations are provided. Data aggregation is a process wherein data is been merges from numerous sensors at intermediate nodes and transmitting aggregated data to the base station. Data aggregation entangles collection of critical data presented to the base station in energy adequate fashion with nominal latent time.

Two types of protocols categorized in data aggregation based on the topology. The first is tree based and second one is cluster based data aggregation protocol. The groups of nodes form the cluster. The grouping of these nodes into clusters is called clustering. In case of cluster based data aggregation protocols,

cluster head or aggregator performs data aggregation and in case of tree based data aggregation protocol the intermediate parent node near to the sink performs data aggregation. Sensor nodes have limited computation power, battery, less storage capacity; because of all these limitations, there is a need of saving such resources by reducing the amount of data transmission. This can be done by using the efficient technique called data aggregation. Facts from numerous sensors are aggregated toward one node called as aggregator, hence communicates aggregated data with base station.

Iterative filtering (IF) is used for data aggregation and trust assessment. The trustworthiness of each sensor is estimated in accordance with the span of sensor readings from the correct estimate values got in the antecedent turn of iteration as in the alacrity of aggregation of all sensors statistics.

Corresponding data aggregation is habitually a charged average. Sensor statistics are significantly differing from such estimate. So the sensors are considered as less trustworthiness and also in the aggregation process, their statistics are bestowed a minor weight in current turn of iteration.

The sensors knobs are partition into sever clusters, and every cluster possesses a cluster head that comports an aggregator. Sporadically data is amassed and aggregated by the aggregator.

As per as the main motive of security services in WSNs is to precaution in the system and resources from attacks and misbehavior. The security in the form of data confidentiality, data integrity, data authentication, data freshness, robustness, data availability, access control, nonrepudiation, forward secrecy, backward secrecy is important for WSN.

This paper surveys the literature to study various factors of wireless sensor network for iterative filtering. Around twenty three papers are considered for survey. The parameters from each paper are identified and drawback of each author's work is highlighted in the survey. The details of the survey are summarized in a table. With the help of the literature and drawback described from each paper a new approach for trustworthiness of sensors and value of the reputation vector is proposed.

The remaining journal is orchestrated as here. The section II describes the detailed literature survey. Section III tenders gap analysis. Section IV describes proposed work. At last, the journal is concluded in section V.

## 2. RELATED WORK

This section of the paper gives detailed literature survey. The recent papers including the techniques of data aggregation are surveyed and a detailed comparison of surveyed literature is given at the end of this section.

Lathies Bhasker have considered the parameters including Fitness function, Cluster function, distribution item (α), transmission cost item (β) and energy item (γ) [1]. The techniques used are Data Aggregator (DAG), Genetic algorithm. The main problem with the author is improvement required in Estimation of metrics, Energy, transmission and distribution.

Hevin, Rajesh Dhasian, Paramasivan Balasubramanian discussed Energy consumption, Cost reduction, Security, Accuracy, Throughput and other parameters [2]. The algorithms considered are simulated annealing calculus for data aggregation, Multi-path data transmission. The problem with the paper is number of sleep nodes arenot considered so scope for energy improvement.

Parli B. Hari, Dr. Shailendra Narayan Singh discussed Data aggregation, scalability, power uses, overhead, and quality of service [3]. The techniques used are secure routing protocols, data aggregation protocols, intrusion detection, cryptography algorithms. The problem is that the algorithms to provide security are not described in detail.

M. Rezvani, A. Ignjatovic, E. Bertino, S. Jha, author proposed an enhancement for iterative straining methods by furnishing an leading estimation for analogous algorithms that develops themselves not just collusion persistent, but furthermore precise and swifter approaching [4]. The problem with paper is data aggregator node is not compromised.

S. Krithika, D.J. Preshiya discussed on enhanced info aggregation style in WSN toward compromised node [5]. Also discussed challenge to data aggregation is yet to secure aggregative information from conciliation node attacks and revealing all over aggregating technique to acquire precise aggregative consequences. The problem with the paper is the cluster based network, network lifespan is less.

A Secure Data Aggregation scheme recommends by H.S.Annapurna, M.Siddappa which works with Fault Tolerance for Wireless Sensor Networks that offers fault tolerance and mutually end to end privacy throughout info aggregation [6]. In this paper, researcher suggests practice for secure information communication by public cryptography in sensor network. The use of AND & OR operation for sharing secure message & reconstructions is problematic.

V. Vaidehi, R. Kayalvizhi and N. C. Sekar proposes a new pattern to secure the process of data aggregation by as long as a light-weight security system called Combinatorial Key Distribution (CKD)

mechanism that eats a reduced amount of power and its performance is enhanced using hashes of data that is directed through the network [7]. The proposed system reduces the power consumption and maximizes thesecureness of data in the wireless sensor network. The techniques used are location dependent.

P. B.Gaikwad, M. R. Dhage done the survey on data aggregation in secured way for wireless sensor networks. Data aggregation methods can efficiently support to decrease consumption of energy by removing redundant data travelling back to the sink [8]. There are numerous security concerns which contain data integrity, data confidentiality, availability, and freshness in data aggregation that become serious when WSN is installed in an unfriendly environment where sensors drop prone to node failures and compromised by rival. Many algorithmsuse message authentications code & uses symmetric key encryption.

H. Hayouni and M. Hamdi present a survey of Homomorphic encryption properties which used by some secure data aggregation approaches, and then they associated them grounded on certain principles [9]. Lastly, they present and deliberate certain vulnerable topics that want to be observed in upcoming studies indirection to advance the safety of data aggregation in wireless sensor networks. The problem is no ultimate strategy which may encounter the security demands toward data aggregation and settle entire dilemmas evoked by the exceptional properties of WSNs.

A Secure Approximate Data Aggregation (SADA) schemes intends by authros S. Prakash T, Venugopal, G Prathima E, L M Patnaik, K R, S SIyengar, in that outline are made using primitive polynomial and Message Authentication Codes (MACs) are transferred alongside with the outline to guarantee truthfulness [10]. SADA delivers data freshness and truthfulness at a communication cost of O (1).The problemwith the paper is author not worked for aggregator node.

P. R. Vamsi and K. Kant tender a structure for Wireless Sensor Networks (WSNs) using TMS at node point and IDS at Base Station (BS) side for secure data aggregation [11]. Using trust credits each node in the network evaluates the behaviour of its neighbors and enforces the network operation to illustrate cluster head selection, briefing to the BS and data aggregation. Then, BS examines the acknowledged information using IDS and accounts knowledge about mischief you events back to nodes in the network.IDS often produce false report of malicious activity is a problem.

S. k. Md. Rahman, M. A. Hossain, M. Mahmud, M. I. Chaudry, A. Almogren, M. Alnuem, A. Alamri designed resolution grounded on a cryptographic mode [12]. Aggregator can scoop oblivious data at the aggregation level makes key security challenge for data aggregation in WSN. Thus, this level of aggregation is susceptible to attacks by intruders. So, the present proposals do not outfit the security grants which emerge into dynamic node WSN. Hence in this paper authors proposed a system to tackle the security issues in dynamic node of WSN called it lightweight secure data aggregation technique. Security analysis and Energy consumption is not provided is the problem with the paper.

S. S. Ranjani, Dr. S. Radhakrishnan and Dr. C.Thangaraj authors modify their Energy efficient Cluster Based Data Aggregation (ECBDA) system to deliver secure data transmission [13]. Subsequently, sensors nodes are low powered immature; it is not feasible to put on typical cryptography techniques. Cluster head achieves data aggregation and Bayesian fusion algorithm to allow security. Trust is guiding association amongst two sensor nodes. Through inspection there liability of a node, they can allow secure communication. Bayesian fusion algorithm analyzes the trust possibility of a sensor based on the performance of the node.BFA discussed in the paper is Inflexible to sensor changes and the workload is concentrated at a single point. It is not suitable for large-range network.

The trust of the nodes is premeditated by N. S. Renubala and K.S.Dhanalakshmi, they aimed scheme utilizes the Bio-inspired Energy Efficient-Cluster (BEE-C) protocol and fuzzy logic [14]. The black hole and flooding attack discovered by suggested practice and it also banishes this assault. The credit rates are associated along with the limit. The credit rate beyond the limit is deliberated as trusted nodes and data packets are perished over the node. The credit rate inferior than the limit value is labeled as accredited untrusted node which is then eliminated. The projected manner delivers reduced delay pause, expensive overhead, and packet waste with improved packet transfer ratio than the present game theory, Fuzzy with trust (LEACH). Disadvantage of practicing fuzzy logic is rapidly budding extent of the rule-base and mixture.

K. Shim, C. Park, authors propose a real-world SDA, Sen-SDA, founded on preservative Homomorphic encryption scheme, an identity-based signature scheme, and a batch confirmation method with an algorithm for filtering injected false data [15]. Packet drop attacks are not handled in this paper and it is extra overhead.

M. Thangaraj, P. P. Ponmalar proposed Secured Hybrid (GA-ABC) Data Aggregation Tree (SHDT) is being raising the vitality proficiency of a system. The exploitation of former intellectual strategies as an alternative of ABC is trouble [16].

D Manjaiah, M. Bharathi and B.P. Vijaya Kumar precedes a line toward deliberates the handling of multi-dimensional key distribution (MDKD) proposal for safeguarding the connection surrounded by nodes

approachable in the WSN system [17]. The organization is concentrated extra safe through playing node-to-node verification system by altering elliptical curve cryptography as well as Elgamal signature design. Lastly, the advised design is assessed founded on manipulation period in secondhand packet data deliverance ratio to catch the aimed protection system is extremely lucrative in nature. The problem is that ECC algorithm isomer complex as well as more difficult for implement Elgamal Signature algorithm is rarely used in practice.

R. K. Kodali proposes a key management technique, among its reduced resource costs, which is extremely suitable tobe used in hierarchical WSN applications [18]. Together Identity based key management (IBK) and probabilistic key pre-distribution systems are formed employ toward altered hierarchical layers. Designed key management approach is applied adopting IRIS WSN nodes. The main problem is insecurity against Quantum Computer attack.

Karuna Babber and Rajneesh Randhva propose clustering algorithm with energy efficiency and QOS in form of security and reliability [19]. Uniform cluster and centrally located node as a cluster head considered. The author has not considered cluster head failure.

Bharath K. Samanthula considered secure data aggregation mode for MIN and MAX encryption approaches of security aspects [20]. In this paper, reducing size of encoding matrix can be improved.

Ajay. K. Talele author surveyed in this paper about routing protocol and design issues in wireless sensor network [21]. Also overviewed of shortest path tree data aggregation algorithm, DAG based in ss NetworkAlgorithm and ANT Colony Algorithm. DRINA algorithm proposed with delay and latency compare to above in various aspects. Main focus to increase Network Lifetime but due to delay may in increase at the transmission time.

PVRD Prasad Rao, K.Raghava Rao author proposes impending sensor mechanism pleas are explored [22]. Developed RLS Algorithm for localization for WSN in class of security. Main problem is that more focus on localization dependency. Synchronization and still chance of recursive estimation can be improved.

Deepak C. Mehetre, S. Emalda Roslin and Sanjeev J. Wagh author proposes node scheduling control Algorithm in distributed manner; nodes functioned regionally over attentive different surroundings [23]. It consumes less energy consumption and consistency in CA based node scheduling. Authors focused on increasing Network Lifetime, energy consumption but in this case delay gets increased.

In this section a detailed survey is given by the authors. The various parameters including cost reduction, power uses, overhead, fault tolerance, data confidentiality, hierarchical model, attack model, network model, dynamic node topology, key management, trust probability, end to end delay, battery residual capacity, routing tree cost etc.The summary of the surveyed papers is given in the Table 1.

Table 1. Summary of the surveyed papers

| Sr. No. | Author name | Parameters | Techniques/Algorithms | Disadvantages |
|---|---|---|---|---|
| 1 | Lathies Bhasker[1] | Fitness function, Cluster function, distribution item(α), transmission cost item (β), energy item (γ) | Data Aggregator(DAG) Genetic algorithm<br>Estimation of metrics | Energy, transmission and distribution can be improved |
| 2 | Paramasivan Balasubramanian,Hevin RajeshDhasian,[2] | Energy consumption, Security, Accuracy, Cost reduction, Throughput and other parameter | Algorithm of Simulated annealing for data aggregation in WSN<br>Multi-path data transmission | Number of sleep node not considered so scope for energy improvement |
| 3 | Dr. Shailendra Narayan Singh and Parli B. Hari, [3] | Data aggregation, scalability, power uses, overhead, quality of service | Secure protocols of routing division, data aggregation protocols, cryptography algorithms and intrusion detection | The algorithms to provide security are not described in details |
| 4 | Ignjatovic ,M.Rezvani,A., E.Bertino and S.Jha [4] | Network Model, Iterative Filtering in Reputation Systems, Adversary Model, Collusion Attack Scenario | IF algorithm for Data Aggregation. | Assumed data aggregator node is not compromised. |
| 5 | S. Krithika, D.J. Preshiya [5] | Hybrid ,Tree ,Chain ,Grid and Cluster Based | Iterative filtering algorithm approach. | In cluster based network, network lifespan is less. |
| 6 | H.S. Annapurna, M.Siddappa [6] | Fault tolerance, Data confidentiality | Secret sharing algorithm and mask designing technique | Used AND & OR operation for sharing secure message & reconstructions |
| 7 | V. Vaidehi, R. Kayalvizhi and N. C.Sekar [7] | Exclusion Basis System (EBS)<br>The hashing method | Location-aware Combinatorial Key<br>Distribution (CKD)" algorithm | Location dependent |
| 8 | P. B. Gaikwad, M. R.Dhage[8] | Single Aggregator Scheme<br>Multiple Aggregator Scheme | SIA, SDA, TAG, WDA | Many algorithms use message authentication |

Table 1. Summary of the surveyed papers

| Sr. No. | Author name | Parameters | Techniques/Algorithms | Disadvantages |
|---|---|---|---|---|
| | | | | code & uses symmetric key encryption. |
| 9 | H. Hayouni and M. Hamdi [9] | IHCA, EIRDA, RCDA, SA-SPKC, FESA, SDA-HP, SAHE, SKBH | Homomorphic encryption protocols | no exemplary plot which can suitable security warnings as data aggregation and perseverance entire dilemmas generated though the certain peculiarities of WSNs |
| 10 | Venugopal K R and S. Prakash T, [10] | Network Model Attack Model | Secure Approximate Data Aggregation Algorithm, PCSA supported algorithm for procreating summary | Not worked for aggregator node. |
| 11 | P. R.Vamsi and K. Kant [11] | Hierarchical Model, Confidentiality, Integrity, Authentication | Secure DA, using TMS and IDS | IDS often produce false report of malicious activity |
| 12 | S. k. Md. Rahman, M. A. Hossain, M. Mahmud [12] | Dynamic node topology, Key management | Secure DA based on IBE Pairing based cryptography, Chinese Remainder theorem | Security analysis and Energy consumption is not provided |
| 13 | S. S.Ranjani, Dr. S. Radhakrishnan and Dr. C.Thangaraj [13] | Trust Probability, Energy Dissipation, Communication Overhead | Energy efficient, Cluster Based DA (ECBDA), Bayesian fusion algorithm | BFA is Inflexible to sensor changes and the workload is concentrated at a single point. It is not suitable for large-range networks |
| 14 | Consistency, Lasting Energy, Buffer habitation, Packet production Rate, swiftness | Consistency, Lasting Energy, Buffer habitation, Packet production Rate, swiftness | A fuzzy logic legged credit estimation plan Bio-divine Energy competent-Cluster (BEE-C) protocol | Shortcoming of practicing fuzzy logic is the rapidly flourishing volume of rule-basis and combination |
| 15 | K.Shimand, C. Park [15] | Heterogeneous clustering, Confidentiality, Authentication | A realistic protected DA idea. Sen-SDA Additive Homomorphic Encryption design, An identity-based signature idea A batch confirmation | Packet drop attacks are not handled.Generate extra overhead |
| 16 | M.Thangaraj, P.P. Ponmalar [16] | Energy Consumption, End to End Delay, Packet Delivery Rate Battery residual capacity | Geneticalgorithmic program (GA) Secured Hybrid (GA-ABC) Data Aggregation Tree (SHDT) | Exercising other intelligent algorithms instead of ABC |
| 17 | M. A. Bharathi, B.P. Vijaya Kumar and D H Manjaiah [17] | Confidentiality, Packet delivery ratio, Processing Time | Multi-dimensionalkey distribution (MDKD) idea Elliptical curve cryptography , Elgamal signature idea | ECC algorithm is more complex and more difficult to implement Elgamal Signature algorithm is rarely used in practice |
| 18 | R. K.Kodali [18] | Energy Consumption, scalability, Integrity | Identity basedkey management (IBK) Hashing Algorithm Idea of Probabilistic key pre-distribution | Insecure against Quantum Computer attack |
| 19 | KarunaBabber and Rajneesh Randhva[19] | Initial energy of node, Energy Spent on Data Aggregation, Electronics Energy, Packet Size, Number Of Nodes | Energy Efficient Uniform Clustering Algorithm | Sensor Node May reside any location , due to uniformclustering technique, few node may be discarded or cluster head may fail |
| 20 | Bharath K. Samanthula[20] | Encryption Time, Energy Consumption | Encryption scheme, Data Aggregation Algorithm with MIN and MAX | Still Chance of Reduction in Size encoding matrix using appropriate size reduction technique and Heuristics |
| 21 | Ajay. K. Talele[21] | Packet Delivery Rate, Packet Delivery Rate, Efficiency, Routing tree cost, Loss of aggregated datadelay, latency. | Shortest path tree algorithm, Centre at Nearest Source Algorithm, Greedy Incremental Tree Algorithm, DAG based In NetworkAggregation, OPAG, Ant Colony Algorithm | More Focus to increase Network existence but yet affect more transmission delay |

Table 1. Summary of the surveyed papers

| Sr. No. | Author name | Parameters | Techniques/Algorithms | Disadvantages |
|---|---|---|---|---|
| 22 | PVRD Prasad Rae, K.Raghava Rao[22] | WLLS (weighted Linear Least Squares) ,Localization, MSPE and LLS (least mean square), Delay | Algorithm for localization in wireless is RLS ,Recursive Least Squares (RLS) Algorithms | Security for localization dependent |
| 23 | Deepak C. Mehetre, S. EmaldaRoslin and Sanjeev J.Wagh [23] | Network Size ,Number of Nodes ,Data Transfer Rate , Energy consumption and BatteryLifetime | node scheduling controlalgorithm,CA based node scheduling, | Focus on increase Network Lifetime,energy consumption but in this case delay may increasesynchronization and still chance of recursive estimation can be improved |

## 3. GAP ANALYSIS

After reviewing above papers the authors of this paper coming to the conclusion that, the surveyed papers considers the parameters like cost reduction, power uses, overhead, fault tolerance, data confidentiality, hierarchical model, attack model, network model, dynamic node topology, Key management, trust probability, end to end delay, battery residual capacity, routing tree costetching literature none of the paper considers trustworthiness of sensors and value of the reputation vector.

## 4. PROPOSED SYSTEM

In proposed work, an improvement over existing iterative filtering algorithm this can be achieved by furnishing preliminary estimate of the credibility to sensor nodes. This builds the IF algorithm more robust and accurate. Also considered the fact that the adversary could attack on the aggregator node. The approach of iterative filtering for secured data aggregation over compromised aggregator node.

## 5. CONCLUSION

In this survey manuscript we rendered thorough scan of data aggregation algorithms in wireless sensing systems. All of them emphasis on improving significant recital scales in particular energy exhaustion, network existence, data suspension latency and data veracity. Principal components, the gains and losses of individual data aggregation algorithmic rule are depicted. In obligated act trustworthiness of sensors and value of the reputation vector is considered for an improvement.

## REFERENCES

[1] L. Bhasker, "Genetically derived secure cluster-based data aggregation in wireless sensor networks", *IET Inf. Secur.*, 2014, Vol. 8, Iss. 1, pp. 1–7doi: 10.1049/iet-ifs.2013.0133.

[2] H. R. Dhasian, P. Balasubramanian, "Survey of data aggregation techniques using soft computing in wireless sensor networks", *IET Inf. Secur*., 2013, Vol. 7, Iss. 4, pp. 336–342doi: 10.1049/iet-ifs.2012.0292.

[3] P. B. Hari, Dr. S. N.Singh, "Security Issues in Wireless Sensor Networks: Current Research and Challenges", 978-1-5090-0673-1/16/$31.00 ©2016 IEEE.

[4] M. Rezvani, A. Ignjatovic, E. Bertino, and S. Jha "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks*" IEEE Transactions on Dependable and Secure Computing*, VOL. 12, NO. 1, JANUARY/FEBRUARY 2015.

[5] S Krithika, D.J. Preshiya, "Enhanced Data Aggregation Techniques for Compromised Node Attacks in Wireless Sensor Networks", 978-1-4673-9338-6/16/$31.00c 2016 IEEE.

[6] H.S.Annapurna,M.Siddappa, "Secure Data Aggregation with Fault Tolerance for Wireless Sensor Networks", *International Conference on Emerging Research in Electronics, Computer Science and Technology* – 2015, 978-1-4673-9563-2/15/$31.00 ©2015 IEEE.

[7] V. Vaidehi, R. Kayalvizhi and N. Chandra Sekar, "Secure Data Aggregation in Wireless Sensor Networks", 978-9-3805-4416-8/15/$31.00c 2015 IEEE.

[8] P. B.Gaikwad, M. R.Dhage, "Survey on Secure Data Aggregation in Wireless Sensor Networks", 2015 *International Conference on computing communication Control and Automation*,978-1-4799-6892-3/15 $31.00 © 2015 IEEEDOI 10.1109/ICCUBEA.2015.52.

[9] H. Hayouni and M. Hamdi, "Secure Data Aggregation with Homomorphic Primitives in Wireless Sensor Networks: A Critical Survey and Open Research Issues", *Proceedings of 2016 IEEE 13th International Conference on Networking, Sensing, and Control Mexico City*, Mexico, April 28-30, 2016.

[10] G Prathima E, S. Prakash T, K R Venugopal, S SIyengar, L M Patnaik,"SADA: Secure Approximate Data Aggregation in Wireless Sensor Networks", 978-1-5090-1281-7/16/$31.00 2016 IEEE.

[11] P. R. Vamsi and K. Kant," Secure Data Aggregation and Intrusion Detection in Wireless Sensor Networks",978-1-4799-6761-2/15/$31.00 ©2015 IEEE.
[12] SkMdM. Rahman, M. A. Hossain, M. Mahmud, M. I. Chaudry, A. Almogren, M. Alnuem, A. Alamri, "A lightweight Secure Data Aggregation Technique for Wireless Sensor Network", *2014 IEEE International Symposium on Multimedia* 978-0-7695-5437-2/14 $31.00 © 2014 IEEEDOI 10.1109/ISM.2014.84.
[13] S. S. Ranjani, Dr. S. Radhakrishnan and Dr. C.Thangaraj, "Secure Cluster based Data Aggregation in Wireless Sensor Networks", *International Conference on Science, Engineering and Management Research (ICSEMR 2014)* 978-1-4799-7613-3/14/$31.00 ©2014 IEEE.
[14] S.Renubala and K.S.Dhanalakshmi, "Trust based Secure Routing Protocol using Fuzzy Logic in Wireless Sensor Networks", *2014 IEEE International Conference on Computational Intelligence and Computing Research*, 978-1-4799-3975-6/14/$31.00 ©2014 IEEE
[15] K. Shim and C. Park, "A Secure Data Aggregation Scheme based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks", 1045-9219 (c) 2013 IEEE.
[16] M.Thangaraj, P.P. Ponmalar, "Swarm Intelligence based Secured Data Aggregation in Wireless Sensor Networks", *2014 IEEE International Conference on Computational Intelligence and Computing Research*, 978-1-4799-3975-6/14/$31.00 ©2014 IEEE.
[17] M. A Bharathi, B.P. Vijaya Kumar, D H Manjaiah, "Robust and Cost-Effective Security Algorithm for PreStage and Post-Stage of Data Aggregation", *4th ICCCNT* – 2013, July 4-6, 2013, Tiruchengode, India.
[18] R. K. Kodali, "Key Management Technique for WSNs" *2014 IEEE Region 10 Symposium*, 978-1-4799-2027-3/14/$31.00 ©2014 IEEE.
[19] Karuna Babber, Rajneesh Randhva, "Energy Efficient Clustering with Secured Data Transmission Technique for Wireless Sensor Networks", *2016 International Conference on Computing for Sustainable Global Development (INDIACom)*.
[20] Bharath K. Samanthula, Wei Jiang and Sanjay Madria, "A Probabilistic Encryption based MIN/MAXComputationin Wireless Sensor Networks*", 2013 IEEE 14th International Conference on Mobile Data Management*.
*[21]* Ajay. K. Talele, Suraj G. Patil and Nilkanth B. Chopade,"A Survey on Data Routing and AggregationTechniques for Wireless SensorNetworks", *2015 International Conference on Pervasive Computing (ICPC).*
[22] PVRD Prasad Rao, K.Raghava Rao,"Development of RLS Algorithm for localization in wireless sensor networks", *International Conference on Communication, Management and Information Technology*, June 2015.
[23] Deepak C. Mehetre, S. Emalda Roslin, Sanjeev J.Wagh, "Target Coverage and Data Collection for life time maximization in Wireless Sensor Network", *IJCTA*, 10(8), 2017, pp. 201-21.