International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 18 (2018) pp. 13805-13811

Secure Data Aggregation Technique for Wireless Sensor Networks using Iterative Filtering Algorithm

Avinash Rai[1*], Preetu Patel[2]

[1]Assistant Professor, [2]M. E. Scholar,*
[1,2]Department of Electronics and Communication,
Bhopal RGPV, Bhopal, Madhya Pradesh, India.

Abstract

WSN is a thought of detecting and controlling any remote zone or framework utilizing sensor hubs. Sensor networks have been useful in a variety of real time applications like military, indoor and outdoor environmental monitoring and health care systems. Sensor node is small in size, inexpensive and free. Because of constrained computational power and vitality assets, conglomeration of information from different sensor hubs done at the collecting hub is normally expert by straightforward techniques, for example, averaging. Anyway such accumulation is known to be exceedingly powerless against hub trading off assaults. Iterative sifting (IF) calculations hold awesome guarantee for such a reason. Such calculations at the same time total information from various sources and give trust appraisal of these sources, more often than not in a type of comparing weight factors allotted to information given by each source.

Keywords: Wireless Sensor Node (WSN), Data Aggregated Node, IF algorithm, Packet Delivery Ratio, Throughput

INTRODUCTION

Information conglomeration is a successful strategy for preserving vitality in sensor systems. In sensor organizes, the correspondence cost is frequently a few requests of extent higher than the calculation cost. Because of the inborn excess in crude information gathered from sensors, in-organize information total can frequently decrease the correspondence taken a toll by wiping out repetition and sending just the extricated data from the crude information [1]. As decreasing correspondence vitality utilization expands the system lifetime, it is basic for sensor systems to help in-arrange information collection. For data collection applications where sensor nodes send collected readings to the sink periodically, the packet forwarding routes for facilitating data aggregation can be planned in advance for optimality. However, for applications where only a subset of nodes is triggered by an event, designing solutions for efficient aggregation of data originating from these nodes is not trivial.

Information total has been a functioning exploration region in sensor systems for its capacity to diminish vitality utilization. Numerous works have concentrated on various parts of information conglomeration. Some centered on how to total information from various hubs. Some centered on how to build and keep up a structure to encourage information total and further some centered on how to effectively pack and total information by taking the relationship of information into thought. As per the WSN, information total systems can be delegated without structure, structure-based and half and half structure [2]. Figure 1 demonstrates the order of information accumulation instruments. At the point when sensor hubs are haphazardly conveyed in the earth, by nature, they require a sans structure system.

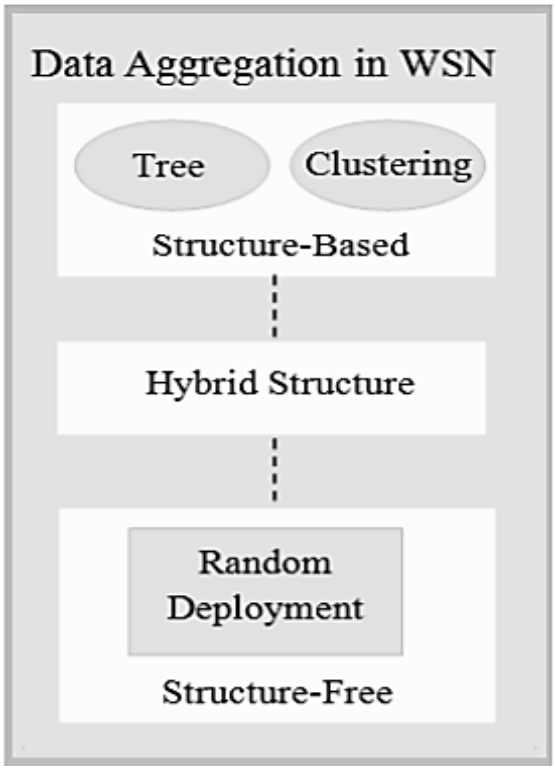

Figure 1: Classification of Data Aggregation Mechanisms

At the point when sensor hubs are conveyed at a huge scale, it winds up troublesome as far as information accumulation and administration of the WSNs, while the structure-based information collections are characterized with an arrangement of calculations, which isolates the system into gatherings or potentially levels. This gathering oversees independently their information total and the diminished perspective of the whole system. Anyway the structure-based systems require an extra overhead to sort out the system and to keep up association amid the system lifetime [3]. Cross breed structure joins attributes of both sans structure and structure-construct contingent on application.

DATA AGGREGATION IN WIRELESS NETWORK

As of late, remote sensor systems (WSN) turns out to be increasingly prominent since it has been conveyed generally in numerous applications [4] e.g. military, medicinal services, and so forth. WSN is made out of a few thousand or hundreds sensor hubs which sense information, for example, temperature, dampness, and splendor et cetera. Sensor hubs have restricted force and calculation capacity; in this way, control sparing is a basic system for WSN. For better power use, a bunch based WSN has been depicted. In such a topology, sensor hubs are partitioned into numerous groups. Every group contains a few sensor hubs and one bunch head. At the point when sensor hubs send their messages to the bunch head, the group head would total numerous messages into one and after that send the collected message to the base station. The reason for the above strategy is sparing vitality by lessening the transmission cost. This system is called information total [5]. When all is said in done, information accumulation can be mathematical operations on numeric information, for example, expansion and increase, or factual operations on numeric information, for example, middle, least, most extreme, and mean of an information set. Nonetheless, sensor hubs are inclined to be caught in a threatening situation. On the off chance that a bunch head was caught, a foe can fake the amassed comes about. It is indistinguishable to bargain the entire group in this way; outlining a safe accumulation plan is important and reasonable [6].

Information total is the procedure of one or a few sensors then gathers the discovery result from other sensor. The gathered information must be handled by sensor to diminish transmission load before they are transmitted to the base station or sink. The remote sensor system comprise of three sorts of hubs: Simple general sensor hubs, aggregator hub and querier. Consistent sensor hubs sense information bundle from the earth and send to the aggregator hubs essentially these aggregator hubs gather information from various sensor hubs of the system, totals the information parcel utilizing a some collection capacity like entirety, normal, tally, max min and after that sends totals result to upper aggregator hub or the querier hub who create the question [7].

Information transmission between sensor hubs, aggregators and the querier expends part of vitality in remote sensor system. Figure 2 contain two models one is information accumulation model and second is non information total model in which sensor hubs 1, 2, 3, 4, 5, 6 are standard hubs that gathering information bundle and reporting them back to the upper hubs where sensor hubs 7,8 are aggregators that perform detecting and amassing in the meantime. In this accumulation model 4 information parcels went inside the system and one and only information bundle is transmitted to the base station (sink). What's more, other non-information collection demonstrate additionally 4 information parcel went inside the system and all information bundles are sent to the base station(sink), implies it can say that with the assistance of information total procedure we diminish the quantity of information weight before they are transmitted to the base station or sink.

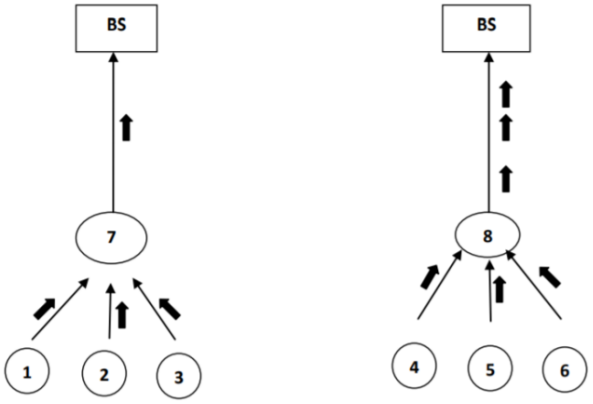

Figure 2: Data Aggregation Model and Non-data Aggregation Model

Figure 3 outlines that information collection is the way toward accumulating the sensor information utilizing conglomeration approaches. At that point the calculation utilizes the sensor information from the sensor hubs and afterward totals the information by utilizing some accumulation calculations, for example, brought together approach, LEACH (Low Energy Adaptive Clustering Hierarchy), TAG (Tiny Aggregation) and so on. This collected information is exchange to the sink hub by selecting the productive way [5].

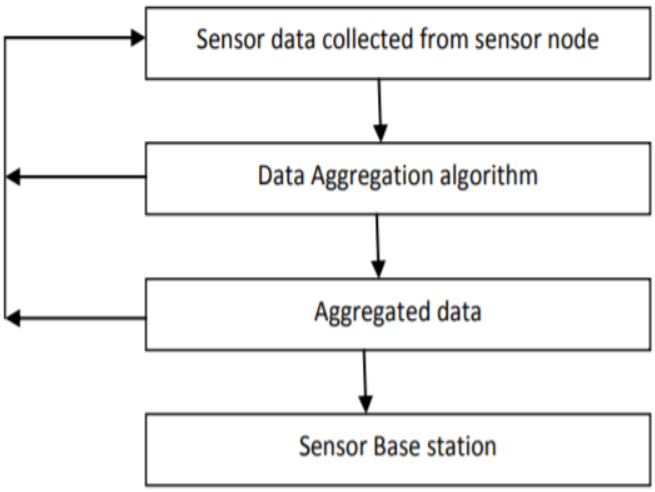

Figure 3: Data Aggregation Flowchart

ITERATIVE FILTERING ALGORITHM

The principle objective of information collection calculation is to assemble and total information in a vitality effective way so arrange life time is upgraded. Remote Sensor Network offers an undeniably, alluring technique for information assembling in disseminated framework models and dynamic access through remote availability. Iterative Filtering strategy gives an answer for a noteworthy issue in regards to with information conglomeration in WSN.IF, all the while total information from numerous sources and give trust evaluation of these sources, as a rule in a type of comparing weight factors relegated to information given by each source. By exhibition it is demonstrated that iterative sifting strategies are

more vigorous against intrigue assaults than the basic averaging techniques, to a novel complex agreement assault. To address this security issue, a change for iterative separating strategies is finished by giving an underlying guess to such system which makes them conspiracy vigorous, as well as more precise and quicker combining.

Focal points

1. If based notoriety framework which uncovers a serious security against any non-stochastic blunders, for example, shortcomings and malevolent assaults.
2. On the off chance that plans ready to secure against advanced arrangement assaults by giving an underlying assessment of dependability of sensors. On the off chance is that enhances exactness and quicker while totaling information.
3. On the off chance that brings execution up within the sight of non-stochastic mistakes, for example, deficiencies and pernicious assaults.

PROPOSED METHODOLOGY

The design outline for the proposed framework is appeared in Fig 4. After enrollment in the system if the client is substantial they can go into the current system topology. The client must enlist their login certifications and to choose the doling out weight factors relying upon the quantity of information must be utilized. By utilizing IF, the sensor mistake is assessed in an extensive variety of sensor flaws and not helpless to the portrayed assault. It uses a gauge of the commotion parameters acquired from sensor hubs. The upgraded IF plans ready to secure against complex intrigue assaults by giving an underlying assessment of dependability of sensor utilizing input. The collected information is playing out a separating activity. On the off chance that any blunder happens on the sifting procedure, first gauge the mistakes and compute the new difference of information utilizing MLE lastly transmit the totaled information in an anchored way.

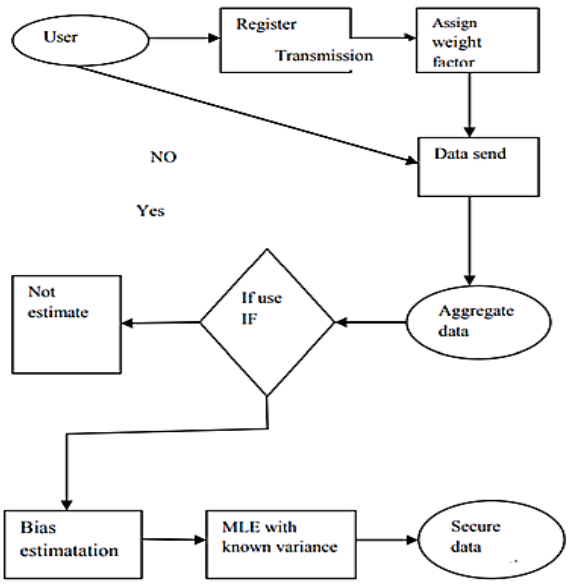

Figure 4: System Architecture

On the off chance is that calculation for figuring notoriety of items and raters in a rating framework. We quickly depict the calculation with regards to information collection in WSN and clarify the defenselessness of the calculation for a conceivable plot assault. We take note of that our change is relevant to other IF calculations also.

We consider a WSN with n sensors Si, I = 1, 2… ….n. We accept that the aggregator takes a shot at one square of readings at any given moment, each square containing reading at m sequential moments. In this manner, a square of readings is spoken to by a network X = [x1, x2… ….xn] where xi = [x1i, x2i … xmi]^T , (1 ≤ I ≤ n) speaks to the ith m-dimensional readings revealed by sensor hub Si. Let r = [r1, r2… … ..rm]^T indicate the total qualities for moments t = 1, 2… ..m, all the while with a succession of weights w = [w1, w2… … .wn]^T mirroring the trust value of sensors.

The iterative system begins with offering validity to all sensors with in introductory esteem

$$w^{(0)} = 1$$

The estimation of the notoriety vector r(l+1) in round of emphasis l + 1 is acquired from the weights of the sensors got in the round of cycle l as

$$r^{(l+1)} = \frac{X.w^{(l)}}{\sum_{i=1}^{n} w_i^{(l)}}$$

Algorithm 1: Iterative filtering algorithm.

Input: X; n; m

Output: The reputation vector r

l ←0;

$w^{(0)}$ ←1;

Repeat

Compute $r^{(l+1)}$;

Compute d;

Compute $w^{(l+1)}$;

l ← l + 1;

until reputation has converged;

d = is the distance b/w the sensor reading and the reputation vector

the weight

$$w_i = \frac{k(v_i)}{\sum_{i=1}^{n} k(v_i)}$$

And

$$k(v_{i)} = \sum_{j=1}^{n} a_{i,j}$$

$a_{i,j}$ the edge that link nodes v_i and v_j the degree $k(v_i)$

Collusion Attack Scenario

The greater part of the IF calculations utilize basic suppositions about the underlying estimations of weights for sensors. If there should arise an occurrence of our enemy demonstrate, an aggressor can delude the total framework through cautious choice of revealed information esteems. We utilize representation procedures from to display our assault situation.

We think about three conceivable situations;

In situation 1, all sensors are dependable and the consequence of the IF calculation is near the real esteem.

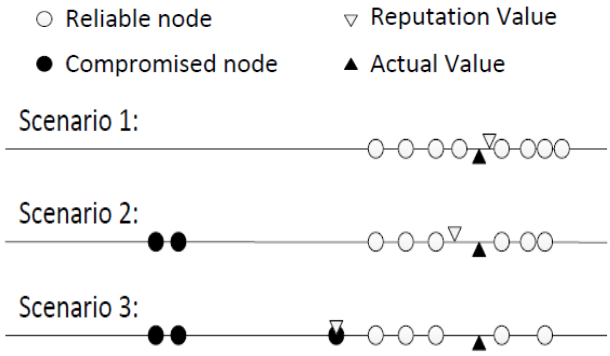

Figure 5: Attack scenario against IF algorithm.

In situation 2, a foe bargains two sensor hubs, and adjusts the readings of these qualities with the end goal that the straightforward normal of all sensor readings is skewed towards a lower esteem. As these two sensor hubs report a lower esteem, IF calculation punishes them and relegates to them bring down weights, in light of the fact that their qualities are a long way from the estimations of different sensors.

In situation 3, an enemy utilizes three traded off hubs keeping in mind the end goal to dispatch an intrigue assault. It tunes in to the reports of sensors in the system and teaches the two traded off sensor hubs to report esteems a long way from the genuine estimation of the deliberate amount. It at that point registers the skewed estimation of the straightforward normal of all sensor readings and orders the third traded off sensor to report such skewed normal as its readings.

PERFORMANCE PARAMETER

Throughput (Kbps) analysis: To gauge the convention execution, throughput fills in as the better parameter. The throughput is characterized as the proportion of number of bundles got to the quantity of parcels transmitted and it is in a roundabout way corresponding to the overhead. The throughput is figured by utilizing the condition 1.

$$Throughput = \frac{x \times 8}{t \times 100} Kbps \qquad (1)$$

Where x is number of bytes received and t is simulation time

Analysis of Packet Delivery Ratio (PDR):- To find the efficiency of the protocols, PDR is one of the important qualitative metrics. It is defined as the ratio of data packets received and packet sent, it is calculate as follows

$$PDR = \frac{x}{y} \times 100 \qquad (2)$$

Where x is the total number of packets received and y is the total number of packets sent at end of the simulation time.

Delay: - The ratio of the total delay of each data packet to total data packet received for wireless sensor network.

$$Delay = \frac{Total\ Delay\ of\ Each\ Data\ Packet}{Total\ Data\ Packet\ \text{Re}ceived} \times 100 \qquad (3)$$

SIMULATION RESULT

In this subsection we evaluate the performance data aggregation system in terms of:

- Packet delivery ratio (PDR): The proportion of successful data packets delivered to the destination compared to the total generated data packets.
- Average end-to-end delay: The mean time required for the surviving data packet to traverse the distance from the source to the destination.
- Normalized throughput: The sum of the transmitting control messages divided by the sum of the delivered data in bytes.

Table 1: IF Algorithm for Packet Delivery Ratio

Number of Node	IF Algorithm
8	98.7%
10	98.3%
12	98.1%
14	98.0%
16	97.9%
18	97.6%
20	97.4%
22	97.2%

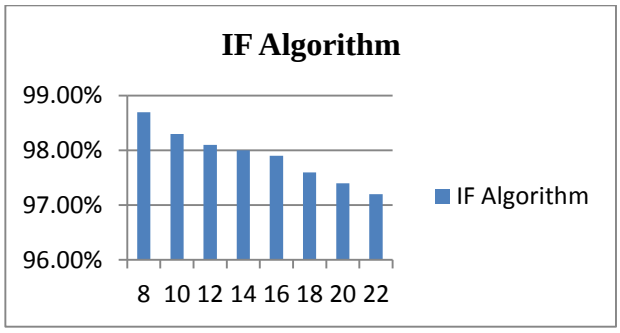

Figure 6: Bar Graph of the Packet Delivery Ratio

Table 2: IF Algorithm for Throughput

Number of Node	IF Algorithm
8	2133.33
10	1882.35
12	1600.00
14	1422.22
16	1280.00
18	1280.00
20	1066.66
22	914.28

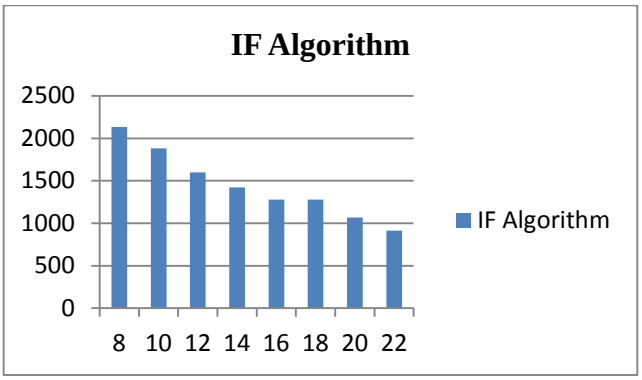

Figure 7: Bar Graph of the Throughput

Table 3: Proposed Algorithm for Delay

Number of Node	Proposed Algorithm
8	0.00045
10	0.00048
12	0.00053
14	0.00062
16	0.00071
18	0.00074
20	0.00082
22	0.00097

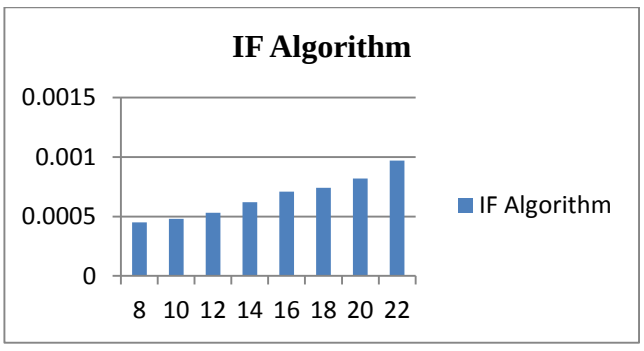

Figure 8: Bar Graph of the Delay

Table 4: Comparison Result of Previous and IF Algorithm for Packet Delivery Ratio

Packet Delivery Ratio (%)			
Number of Node	**Previous Algorithm**	**Proposed Algorithm**	**% Improvement of Previous Algorithm**
8	96.8%	98.7%	1.9%
10	95.9%	98.3%	2.4%
12	96.7%	98.1%	1.4%
14	96.0%	98.0%	2.0%
16	96.0%	97.9%	1.9%
18	95.5%	97.6%	2.1%
20	95.4%	97.4%	2.0%
22	95.1%	97.2%	2.1%

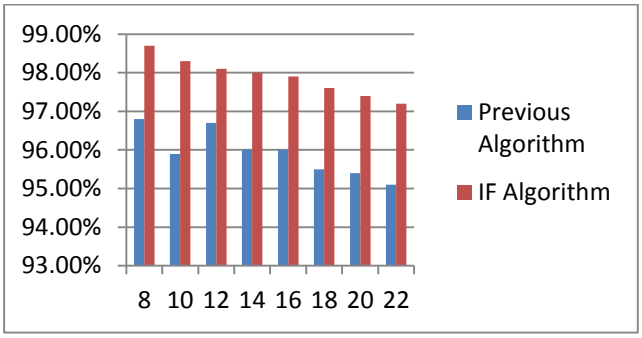

Figure 9: Bar Graph of the Previous and IF Algorithm for Packet Delivery Ratio

Figure 9 shows the graphical illustration of the performance of different wireless sensor network discussed in this research work in term of packet delivery ratio. From the above graphical representation it is inferred that the proposed IF algorithm gives highest packet delivery ratio and percentage improvement 1.9% of eight sensor nodes, 2.4% of ten sensor nodes 1.4% of twelve sensor nodes, 2.0% of fourteen sensor nodes, 1.9% of sixteen sensor nodes, 2.0% of eighteen sensor nodes, 2.1% of twenty sensor nodes and 2.0% of twenty two sensor nodes compared to previous algorithm

As shown in table 5 the delay is obtained from the proposed IF algorithm and multipath ChaMeLeon (CML) routing protocol. CML is a half breed and versatile convention intended for Mobile Ad-Hoc Networks (MANETs), supporting crisis interchanges. M-CML receives the characteristics of the proactive Optimized Link State Protocol (OLSR) and extends it in order to actualize a multipath steering approach in view of the Expected Transmission Count (ETX). The values obtained for various sensor node for proposed and previous algorithm is shown in table 5.

Table 5: Comparison Result of Previous and IF Algorithm for Delay

Delay (Sec)			
Number of Node	**Previous Algorithm**	**Proposed Algorithm**	**% Improvement of Previous Algorithm**
8	0.00050	0.00045	10.00%
10	0.00055	0.00048	12.72%
12	0.00060	0.00053	11.66%
14	0.00070	0.00062	10.78%
16	0.00080	0.00071	11.25%
18	0.00085	0.00074	12.94%
20	0.00095	0.00082	13.68%
22	0.00120	0.00097	19.16%

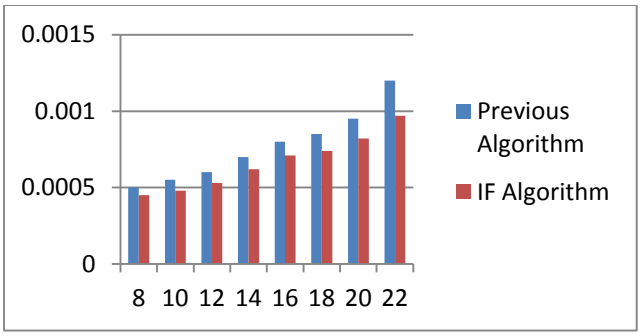

Figure 10: Bar Graph of the Previous and IF Algorithm for Delay

Table 6: Comparison Result of Previous and IF Algorithm for Throughput

Throughput (Kbps)			
Number of Node	**Previous Algorithm**	**Proposed Algorithm**	**% Improvement of Previous Algorithm**
8	1280.00	1548.33	17.33%
10	1163.63	1482.35	21.50%
12	1066.66	1200.00	12.00%
14	0914.28	1022.22	10.56%
16	0800.00	0980.00	18.36%
18	0752.94	0880.00	14.54%
20	0673.68	0766.66	12.14%
22	0533.33	0614.28	13.19%

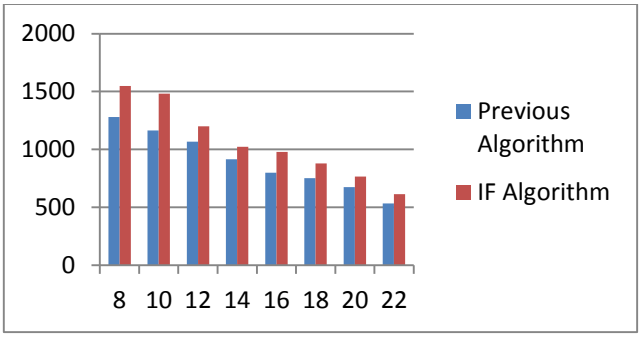

Figure 11: Bar Graph of the Previous and IF Algorithm for Throughput

CONCLUSION

In this paper, secure data aggregation technique with the help of iterative filtering algorithm. In this algorithm good performance compared to previous algorithm.

REFERENCE

[1] M. Bheemalingaiah and M. M. Naidu, "Performance Analysis of Power -aware Node-disjoint Multipath Source Routing in Mobile Ad Hoc Networks", IEEE 7th International Advance Computing Conference, PP. No. 361-371, IEEE 2017.

[2] Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: a comprehensive overview," Comput. Netw., vol. 53, no. 12, pp. 2022– 2037, aug. 2009.

[3] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A survey of attack and defense techniques for reputation systems," ACM Computer Survey, vol. 42, no. 1, pp. 1:1–1:31, Dec. 2009.

[4] Suat Ozdemir and Yang Xiao. Secure data aggregation in wireless sensor networks: A comprehensive overview. Comput. Netw., 53(12):2022–2037, August 2009.

[5] Audun Jøsang and Jennifer Golbeck. Challenges for robust trust and reputation systems. In Proceedings of the 5 th International Workshop on Security and Trust Management, Saint Malo, France, 2009.

[6] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru. A survey of attack and defense techniques for reputation systems. ACM Computer Surv.,42(1):1:1–1:31, December 2009.

[7] Rodrigo Roman, Carmen Fernandez-Gago, Javier Lopez, and Hsiao HwaChen. Trust and reputation systems for wireless sensor networks. In Stefanos Gritzalis, Tom Karygiannis, and Charalabos Skianis, editors, Security and Privacy in Mobile and Wireless Networking, pages 105–128. Troubador Publishing Ltd, 2009.

[8] Hyo-Sang Lim, Yang-Sae Moon, and Elisa Bertino. Provenance-based trustworthiness assessment in sensor networks. In Proceedings of the Seventh International Workshop on Data Management for Sensor Networks, DMSN '10, pages 2–7, 2010.

[9] Hong-Ling Shi, Kun Mean Hou, Haiying Zhou, and Xing Liu. Energy efficient and fault tolerant multicore wireless sensor network: E2MW SN. In Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on, pages 1–4, 2011.

[10] Cristobald de Kerchove and Paul Van Dooren. Iterative filtering in reputation systems. SIAM J. Matrix Anal. Appl., 31(4):1812–1834, March 2010.

[11] Yanbo Zhou, Ting Lei, and Tao Zhou. A robust ranking algorithm to spamming. CoRR, abs/1012.3793, 2010. 31.

[12] P. Laureti, L. Moret, Y.-C. Zhang, and Y.-K. Yu. Information filtering viaIterative Refinement. EPL (Europhysics Letters), 75:1006–1012, September 2006.

[13] Y.-K. Yu, Y.-C. Zhang, P. Laureti, and L. Moret. Decoding information from noisy, redundant, and intentionally distorted sources. Physica A Statistical Mechanics and its Applications, 371:732–744, November 2006.

[14] Rong-Hua Li, Jeffrey Xu Yu, Xin Huang, and Hong Cheng. Robust reputation-based ranking on bipartite rating networks. In SDM'12, pages612–623, 2012.