International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET2183181

An Energy Efficient Clustering Algorithm for Network Lifetime in Wireless Sensor Network

Madhuri N. Khuspare, Dr. Awani S. Khobragade

Department of Electronics Engineering, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

Article Info

Volume 8, Issue 3
Page Number: 426-433

Publication Issue :
May-June-2021

Article History
Accepted : 10 June 2021
Published: 17 June 2021

ABSTRACT

In wireless sensor networks, information aggregation accept a fundamental part in lessening essentialness use. Starting late, investigate has focused on secure information aggregation due to the open and disagreeable condition passed on. The Homomorphic Encryption (HE) contrive is generally used to secure information grouping. In any case, HE-based information aggregation designs have the going with disservices: adaptability, unapproved aggregation, and obliged aggregation limits. To deal with these issues, we propose a safe information aggregation plot by solidifying homomorphic encryption development with a check plan. To answer this issue we exhibited a system addresses a procedure in that intense cluster head is picked based on the partition from the base station and remaining imperativeness. Consequent to picking the cluster head, it impacts use of minor measure of essentialness of sensor to organize and what's more improves the lifetime of the system of sensor arrange. Aggregation of the information got from the cluster people is commitment of cluster head in the cluster. Affirmation of information is done by the cluster head going before the information aggregation if information got isn't honest to goodness by then got information is discarded. Simply affirmed information is taken for aggregation at cluster head. Encryption is done by making use of homomorphic encryption procedure and also encoded information send to the cluster head and information disentangling is performed by base station (BS) for offering end to end security. An ID based stamp system is made for hop by hop authentication. In this paper, we demonstrate the method for recovering the information which is lost in light of the pad surge. In given system cache memory is given by the cluster head to recovery of information mishap. At long last test comes to fruition indicates depending upon parameter like time and furthermore essentialness usage on Jung test system that system showed is incredible appeared differently in relation to the open system.

Keywords : Sensor Nodes, Cluster Head, Base Station, Wireless Sensor Networks, Cache Based System, Hop by hop authentication

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

I. INTRODUCTION

Wireless sensor networks (WSNs) have mostly been used in a variety of applications, including biological screening, social protection, everyday perception, and catastrophe reporting [3,4]. WSNs, which are today believed to be one of the most important components of the Internet of Things [2], include various sensor centre points that are constrained in terms of storage space, battery control, and processing capability. As a result, courses of action that are likely to extend the system's lifespan are widely investigated.

One of the strategies that may be used to limit the imperativeness of sensor use is information aggregation [1]. Information recognised by several portion centre points is summed into a single one by applying some aggregation limitations, such as Sum, Average, and MAX, and then communicated to the base station using wireless association techniques. In this regard, information aggregation is beneficial in reducing distribution and abundance. Sensors are passed on in an abandoned forest, for example, to communicate their recognised temperature to the base station for fire monitoring. In this case, the base station may need to make the best estimate of all the distinguishing information in order to set off alerts. As a consequence, each cluster head just needs to choose the most outrageous driving force from among the many data points received from its portion centres and deliver the result to the base station a short time later.

Without a doubt, the correspondence overhead is reduced due to the manner in which the selected result is conveyed to the base station. As a result, data aggregation is advantageous in extending the overall lifetime of WSNs. However, because they are constantly issued in hostile and unsupervised settings, WSNs are exposed to numerous attacks, such as replay assault, mixing ambush, and solidifying attack. Existing plentiful security estimates are unsuited for WSNs because of their advantage limited qualities. Assuring information aggregation security is a test in this sense.

Wireless sensor networks (WSNs) with small contraptions that collect data by collaborating with each other have become viable because to advancements in wireless communication. The CPU (for information handling), memory (for information storage), battery (for imperativeness), and handset are all examples of modest identifying devices known as centre points (for tolerating and sending signs or information beginning with one centre point then onto the following). With applications, the traverse of each sensor centre moves. In some military or perceptual applications, for example, it might be almost nothing. Its price is determined by factors such as memory evaluation, transaction rate, and battery life. WSNs are typically used in untrustworthy environments, such as open or habitually untrusted regions, and in the face of a variety of security threats. These incorporate approaches such as key association, security, access control, authentication, and DoS protection, among others.

In light of the thick and particularly designated work in basic condition and moreover as a consequence of the in secret nature of WSNs, there are a few challenges in the sensor system, such as adjusting or enabling the centre batteries. One of the most fundamental requests that arises is how to increase the lifetime of sensor networks. Despite the fact that it is vital, such as increasing system lifespan by reducing the imperativeness of using the centre point in WSNs. The results of the tests show that information trading is particularly over the top in terms of imperativeness consumption (EC), whereas information preparation uses little essentiality. In addition, a reasonable method was predicted that would enhance the lifespan of WSN while also limiting sensor imperativeness utilisation throughout data exchange. In the WSN, there is another concern with information security throughout the transmission of data from source to objective.

With limited resources, sensor centres are vulnerable to a variety of attacks; as a result, information encryption is critical in WSNs. In the event that information is transferred without encryption, the attackers will isolate the data and wire bogus data into the system. Hop-by-hop mixed information aggregation (EDAs), which is a central individual aggregator with keys for all sensor centre points interprets encoded values, completes all unscrambled references, and scrambles the data for transmission to a base station, is used (BS). This approach necessitates that separate aggregators in the centre maintain keys for unscrambling in order for a gathered aggregator to uncover the depicted data.

On a very basic level, this study focuses on the three burdens that are most commonly addressed in wireless sensor networks. First, by limiting the usage of imperativeness in the sensor system, the system's lifetime will be improved. The second step is to ensure information security during transmission from the sender to the receiving centre point or from the sender to the base station. The third is information hardship recovery, which occurs when data is sent to the cluster head and is lost due to the cluster head's need for maximum control. The strategy in which the cluster head is singled out the presentation of essentialness, number of neighbours, and division to the base station was shown for renewing the structure lifespan. By selecting the cluster head based on these three characteristics, the noteworthiness of the sensor centre point is reduced. Homomorphic encryption is a type of encryption that ensures the security of data. Information is delivered to the base station in an encoded manner, and the base station decodes the information before storing it. Similarly, the information aggregation mechanism is modified, with cluster heads adding to the information gathered by the cluster centre points. At the cluster head, we are allocated cache memory for information incident recovery. Finally, the outcome is separated for the system's duration, essentiality consumption, and previous and planned structure.

II. LITERATURE SURVEY

This section highlights the researchers' unique contributions to information aggregation and sensor centre point system lifespan enhancement.

Sen-SDA is an SDA process introduced by Kyung-Ah Shim [1], which is based on the social event of sensible cryptographic locals in heterogeneous cluster WSNs. They expect an extra substance HE approach, so that only a BS may unravel encoded information accumulated by the CHs obtained from part centre points for each cluster gathering, in order to lower the overall length of figure messages and to meet end-to-end demand. They use a dealing with free identity based stamp (IBS) mechanism to provide hop-by-hop confirmation, allowing the BS and CHs to monitor the validity of all the mixed data that is delivered. They demand a stamp technique in which specific engravings from distinct endorsers on numerous messages may be evaluated quickly in order to increase the quantity of varied imprinted affirmations. D. Boneh and M. Franklin [5] present a technique of identity-based encryption that is completely reasonable. In the subjective prophet indication, this strategy has figure content security by obtaining an assortment of the computational Diffie-Hellman problem. Bilinear mappings between clusters are necessary for this structure to exist. A good example of such a partner is the Weil association on elliptic twist. They define safe identity-based encryption arrangements correctly and provide two or three alternatives for such structures.

Gainful, information transfer visiting security in WSNs is the focus of C. Castelluccia, E. Mykletun, and G. Tsudik [6]. They use unassuming mixing procedures with enormous aggregation methods to conduct mostly useful gigantically advantageous of encoded information. To assess the appropriateness of suggested systems, they conduct a survey and provide an uncommon guaranteeing outcome that definitely demonstrates measurable information transmission constraint assurance and insignificant overhead resulting from both mixed and aggregate operations.

Recoverable Concealed Data Aggregation is a concept shown by C. M. Chen, Y. H. Lin, Y. C. Lin, and H. M. Sun [7]. (RCDA). In RCDA, a base station can recuperate each sensor's perceiving information, regardless of whether or not that information has been summed by cluster heads or aggregators. Two capabilities are provided with this unique information. To begin with, the base station can vouch for the accuracy and legality of all received data. After that, the base station can apply any aggregate constraints on them. They next suggest two RCDA systems for homogeneous and heterogeneous WSN self-ruling, dubbed RCDA-HOMO and RCDA-HETE, respectively. In the security study, they demonstrate that the suggested approach is secure for certain strike models.

J. Domingo-Ferrer [8] discusses one such PH that has been shown to be secure against known-clear substance ambushes; the figure content space is significantly larger than the sensible substance space. A few applications for questionable management and information, as well as ewagering, are rapidly handled. J. Girao, D. Westhoff, and M. Schneider [9] present an approach that 1) covers perceived information from beginning to finish by 2) starting late and ending early, resulting in lucrative and adaptable in-organize system information collecting. The collecting of mediatory focus reveals that the seeming plaintext information does not need basic labour. They do a special type of encoded mixed and discuss frameworks for selecting "typical" and "improvement disclosure" as much as feasible. They demonstrate that the technique is applicable to the category of guiding traditions that "go down." They consider the danger of wrecked sensor focuses by providing a key pre-dispersing count that limits an aggressor's advancement, and they demonstrate how key preappointment and a key-ID delicate "going down" coordinating tradition improves the associated spine's quality and consistency nature.

E. Mykletun, J. Girao, and D. Westhoff [10] question whether additively homomorphic open key encryption implies certain forms of wireless sensor networks. Finally, they make recommendations for selecting the most appropriate open key strategies for particular topologies and wireless sensor configuration settings.

III. PROPOSED SYSTEM

This section depicts the system survey in which proposed estimation and logical model of the proposed system is in like manner introduce.

A. System Overview

System architecture of the proposed is appeared in figure 1 which shows up in various advances and steps are given underneath.

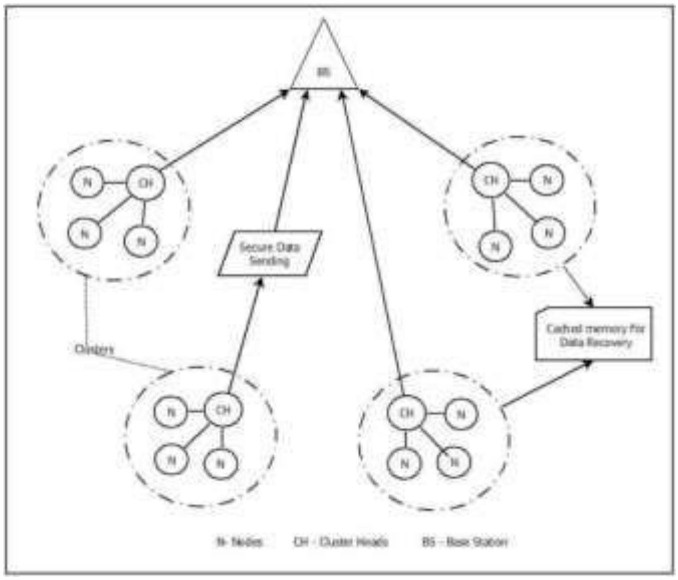

Figure 1. Proposed System Architecture

Network Generation

At begin network is created where vertices/hubs are related with the edges.

Clustering Process

After the network generation, the clustering strategy is executed in that hubs are isolated in various clusters.

Cluster Head Selection

In the wake of making the gathering of clusters, from each gathering of clusters, the cluster head is picked based on vitality and separation from base station and neighbor hubs parameters.

Key generation and distribution

Base station can achieve key generation and dissemination to each hub. Course ages performed from each hub to the base station.

Data Encryption

At every node data is generated and encrypted through the Paillier Encryption.

Hash value evaluation

After the data is encoded, hash esteem is evaluated and recorded the timestamp.

Data Collection

Subsequent to assessing, the hash respect at each middle indicate, each inside advances information its cluster head. Cluster head have some obliged ability to store the information if the cluster head amassing is overpowered then the information is dropped at collect head. The cluster head blends every single one of the information and check the considerable information.

Cached Data

In system, to restrain the loss of data at cluster head because of the impediment of capacity limit we are keeping a cache stockpiling that can store the data dropped during the time spent data sending in cluster individuals and cluster head.

Data verification

By batch verification method, validate the information by making use of hash value and timestamp. In this we are verifying cached data also data which is stored in cluster head storage.

Data aggregation

At last, process of data aggregation is accomplished after verifying the valid data by the cluster head and data forwarded to the base station.

Data Decryption

Base station receives the data from every cluster head and decrypts the data by the appropriate key.

B. Algorithm

Algorithm 1: Proposed Algorithm

Step 1: Generate a network chart as Graph g (v, e) where; V is vertices/hubs and E is edges.

Step 2: Implement clustering calculation over the quantity of hubs and separate the hubs in to number of clusters.

Step 3: based on vitality, number of neighbors and separation to the base station select the Efficient Cluster Head.

Step 4: Perform the key conveyance at each hub by means of Base Station.

Step 5: Perform the course ages from each hub to the base station.

Step 6: Create the data at each hub and scramble the data with general society key of base station.

Step 7: Compute the hash estimation of the scrambled data and Record the timestamp.

Step 8: Send the individual data to the cluster head from each cluster part in every one of the clusters. In the event that capacity limit of cluster head is surpass the farthest point at that point store the data in cache memory.

Step 9: Collect all data at the cluster head. Confirm the data by its hash esteem and acknowledge the checked data or dispose of if hash esteem is invalid.

Step 10: Aggregate every one of the data and send this data to the base station. Base station acknowledges the data from each cluster head.

Step 11: Base station checks the data and unscrambles the data with proper key.

Explanation: Proposed calculation outlines the working stream of the structure. At in the first place, system is made including sensor center points; additionally clustering calculation and number of hubs is isolated in number of clusters. Clusters head is picked in light of parameters; key circulation is executed at every center point by the base station. Course is produced using every center point to the base station. Data encryption is done through the Paillier Encryption with the private key. Hash esteem is surveyed of the scrambled data and timestamp is recorded. Cluster part progresses the data to the cluster head in all clusters and surge data is secured in cache memory. Data check is done on the start of hash esteem; in case it is affirmed then simply recognized for the most part rejects. After that total each data is forward to the base station. Base station decodes the data with the appropriate keys.

Algorithm 2: Paillier Cryptosystem

Step 1: Key Generation:

a) Select two large prime numbers a and b arbitrary and independent of each other such that gcd(n, Φ (n)) = 1, where Φ (n) is Euler Function and n=ab.

b) Calculate RSA modulus n = ab and Carmichael's function is given by λ = LCM (a-1, b-1).

c) Select g called generator where $g \in \mathbb{Z}^{*}_{n2}$ Select α and β randomly from a set $\mathbb{Z}_{n}^{*}$ then calculate g = $(\alpha n + 1)\, \beta^{n} mod\ n^{2}$.

d) Compute the following modular multiplicative inverse μ = (L $(g^{\lambda} mod\ n^{2})^{-1}$ mod n. Where the function L is defined as L(u) = $(u-1)/n$.

The public (encryption) key is (n and g).

The private (decryption) key is (λ and μ).

2) Encryption:

a. Let mess be a message to be encrypted where mess $\in \mathbb{Z}_n$.

b. Select random r where r $\in \mathbb{Z}^*_{n2}$.

c. The cipher text can be calculated as:

Cipher = $g^{mess} \cdot r^n$.mod n^2.

3) Decryption:

a. Cipher text c $\in \mathbb{Z}^*_n{}^2$

Original message: mess = L (cipher$^\lambda$ mod n^2).µ mod n.

C. Experimental Setup

System builds on Java framework (version jdk 8) over Windows platform. For development, the Netbeans (version 8.1) tool is utilized. The network is created utilizing Jung tool with sensor nodes. System doesn't require any particular hardware to run any standard machine is able to run the application.

IV. RESULT AND DISCUSSION

Following are Results generated during the implementation of the system.

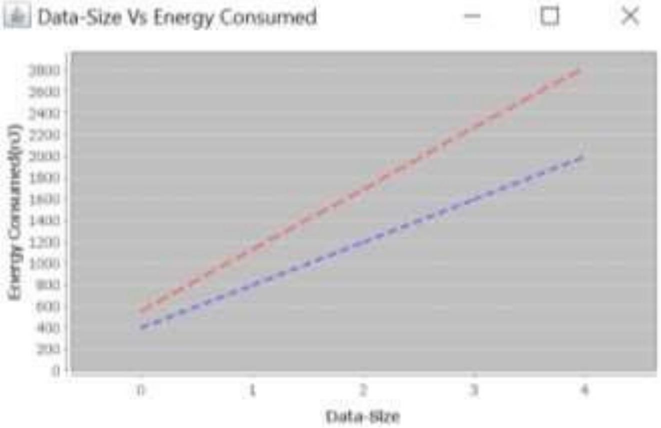

Figure 2 : Energy Consumption for Send the Data

Figure 2 shows the results, and Figure 3 shows the energy and time consumed while transferring the data. We've displayed the effects of 5 trials to help you better understand the results. At this time, the assets utilised in delays are included in the Energy and Time consumed during transmission. We define handling delay as the time it takes part nodes to construct their ciphertexts and compare marks during execution. The time spent validating the marks from component nodes, collecting ciphertexts and marks, and making the mark of the aggregated outcome is used to estimate the aggregation delay. The time spent in the end picking up the initial information for the BS by checking the totalled markings and decoding accumulated ciphertexts is referred to as the unscrambling delay.

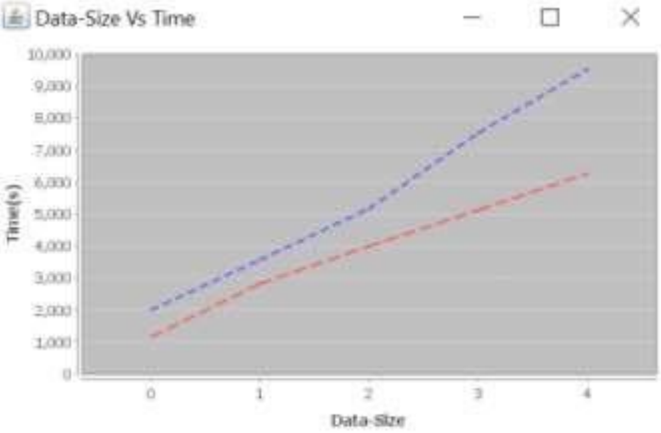

Figure 3 : Time Consumption for Send the Data

To compare the outcomes we have alluded [1] [7] [20]. Our plan has the least handling delay. In regard of the aggregation delay, RCDA-HOMO and CDAMA are relatively like our plan, since they don't give in-organize check and approved aggregation of information which we have. As far as decoding delay, our plan is the better among the greater part of the above information aggregation plans.

V. CONCLUSION

We can aid the system lifetime of WSN by utilising the suggested system. We also designed a technique that can choose the cluster head based on three characteristics, allowing the system to employ essentiality effectively and the Wireless Sensor

Network's lifetime to be pushed forward. In addition, the proposed methodology built a mechanism for recovering information that was lost when broadcasting the information. Finally, the results suggest that the suggested solution will prolong the life of the system.

VI. REFERENCES

[1]. K.A. Shim, C.M. Park, A secure data aggregation scheme based on appropriate cryptographic primitives in heterogeneous wireless sensor networks, IEEE Parallel Distrib. Syst. 26 (8) (2015) 2128–2139.

[2]. O.R.M. Boudia, S.M. Senouci, M. Feham, A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography, Ad Hoc Netw. (2015).

[3]. A. Boukerche, X. Cheng, J. Linus, A performance evaluation of a novel energyaware data-centric routing algorithm in wireless sensor networks, Wirel.Netw. 11 (5) (2005) 619–635.

[4]. X. Fei, A. Boukerche, R. Yu, An efficient markov decision process based mobile data gathering protocol for wireless sensor networks, in: Wireless Communications and Networking Conference (WCNC), IEEE, 2011, pp. 1032–1037.

[5]. D. Boneh and M. Franklin, “Identity-based encryption from the Weil pairing,” SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.

[6]. A. Castelluccia, E. Mykletun, and G. Tsudik, “Efficient aggregation of encrypted data in wireless sensor network, MobiQuitous ’05,” pp. 1–9, 2005.

[7]. C.-M. Chen, Y.-H.Lin, Y.-C.Lin, and H.-M. Sun, “RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 4, pp. 727–734, Apr. 2012.

[8]. J. Domingo-Ferrer, “A provably secure additive and multiplicative privacy homomorphism,” in Proc. 5th Int. Conf. Inf. Security, 2002, pp. 471–483.

[9]. J. Girao, D. Westhoff, and M. Schneider, “CDA: Concealed data aggregation for reverse multicast traffic wireless sensor networks,” in Proc. IEEE Int. Conf. Commun., 2005, pp. 3044– 3049.

[10]. E. Mykletun, J. Girao, and D. Westhoff, “Public key based cryptoschemes for data concealment in wireless sensor networks,” in Proc. IEEE Int. Conf. Commun., 2006, pp. 2288– 2295.

[11]. A. Shamir, “Identity-based cryptosystems and signature schemes,” in Proc. Int. Cryptol. Conf. Adv. Cryptol., 1984, pp. 47–53.

[12]. S. Lindsey and C.S. Raghavendra, “PEGASIS:Power efficient gathering in sensor information system”, in Proc. of IEEE Aerospace conference, vol.3, March 2002, pp.1125-1130. [13] A. Manjeshwar and D.P. Agrawal, “TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks”, Proceedings of the15th International Parallel & Distributed Processing Symposium, IEEE Computer Society, April 2000, pp. 2009-2015.

[13]. A. Manjeshwar and D. P. Agarwal, “APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks,” in Proceedings of the 2nd International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile computing, FL, USA, April 2002, pp.195–202.

[14]. S. Banbyopadhyay and E.J. Coyle, “An energy efficient hierarchical clustering algorithm for wireless sensor networks”, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications IEEE Societies (INFOCOM 2003), vol.3, April 2003, pp.1713-1723.

[15]. O. Younis and S. Fahmy, “HEED: A Hybrid, Energy- Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks”, IEEE Transactions on Mobile Computing, vol.3, no. 4, Oct 2004, pp.366-379.

[16]. S. Soro and W.B. Heinzelman, “Prolonging the lifetime of wireless sensor networks via unequal clustering,” in Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, April 2005.

[17]. A. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” Ad Hoc Networks, vol. 1,pp. 293–315, 2003.

[18]. X. Liu, “Survey on clustering routing protocols in wireless sensor networks,” Sensors, vol. 12, pp. 11113–11153, 2012.

[19]. Y.H. Lin, S.Y. Chang, H.M. Sun, CDAMA: Concealed Data Aggregation Scheme for Multiple Applications in Wireless Sensor Networks, IEEE Trans. Knowledge Data Engrg. 25 (7) (2013) 1471–1483.

Cite this article as :

Madhuri N. Khuspare, Dr. Awani S. Khobragade, "An Energy Efficient Clustering Algorithm for Network Lifetime in Wireless Sensor Network", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 3, pp. 426-434, May-June 2021. Available at doi : https://doi.org/10.32628/IJSRSET2183181
Journal URL : https://ijsrset.com/IJSRSET2183181