International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 2 | ISSN : 2456-3307

Efficient Data Aggregation for Enhanced Network Lifetime in Wireless Sensor Network

Arjulata Naukarkar[1], Prof. Gurudev Savarkar[2]

[1]M. Tech Student, Department of Computer Science and Engineering, V. M. Institute of Engineering and Technology, Nagpur, Maharashtra, India

[2]Assistant Professor, Department of Computer Science and Engineering, V. M. Institute of Engineering and Technology, Nagpur, Maharashtra, India

ABSTRACT

In wireless sensor networks, data aggregation acknowledge a crucial part in diminishing centrality utilize. Beginning late, explore has concentrated on secure data aggregation because of the open and upsetting condition passed on. The Homomorphic Encryption (HE) think up is by and large used to secure data gathering. Regardless, HE-based data aggregation outlines have the running with injuries: flexibility, unapproved aggregation, and obliged aggregation limits. To manage these issues, we propose a protected data aggregation plot by hardening homomorphic encryption advancement with a check design. To answer this issue we displayed a system tends to a method in that extraordinary cluster head is picked based on the parcel from the base station and remaining noteworthiness. Resulting to picking the cluster head, it impacts utilization of minor measure of centrality of sensor to sort out and what's more enhances the lifetime of the system of sensor orchestrate. Aggregation of the data got from the cluster individuals is duty of cluster head in the cluster. The cluster head going before the data aggregation if data got isn't true blue by then got data is disposed of finishes confirmation of data. Asserted data is taken for aggregation at cluster head. Encryption is finished by making utilization of homomorphic encryption strategy and furthermore encoded data send to the cluster head and data unraveling 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 exhibit the strategy for recuperating the data which is lost in light of the cushion surge. In given system the cluster head to recuperation of data incident give cache memory. Finally test works out as intended demonstrates relying on parameter like time and moreover vitality use on Jung test system that system indicated is mind blowing showed up distinctively in connection to the open system.

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

I. INTRODUCTION

Wireless sensor networks (WSNs) have been by and extensive sent in different applications, for example, organic screens, social security, normal life discernment, and calamity reports [3,4]. WSNs, which are beginning at now thought to be one of the important parts of the Internet of Things [2], include distinctive sensor focus indicates obliged with deference their storage room, battery control, and

computational limit. Along these lines, strategies anticipated that would drag out the lifetime of the system are broadly scanned for.

Data aggregation is known as one of the methods that are useful to oblige the vitality use of sensors [1]. With such system, data distinguished by different part focus focuses are totaled into a particular one by applying some aggregation limits, for example, Sum, Average, and MAX at last transmitted to the base station by strategies for the wireless affiliation. Thusly, data aggregation is profitable to reduce circulate and wealth. For instance, in an old backwoods, sensors are passed on to report their perceived temperature to the base station for flame viewing. For this situation, the base station may require the best estimation of all the recognizing data to trigger alerts. In this way, each cluster head basically needs to pick the most crazy rousing power from among various data respects got from its part focuses and a brief span later send the outcome to the base station.

Surely, the correspondence overhead is decreased in light of the way that select the amassed result is transmitted to the base station. In this manner, data aggregation is useful to drag out the general lifetime of the However, in light of how they are routinely sent in contradicting and unattended conditions, WSNs are acquainted with different strikes, for example, replay assault, blend trap, and cementing assault. The advantage obliged qualities of WSNs make existing inexhaustible security estimations unacceptable for WSNs. Along these lines, guaranteeing security for data aggregation is a test.

Advances in wireless correspondence made it conceivable to make wireless sensor networks (WSN) including little contraptions, which amass data by collaborating with each other. These little distinguishing gadgets are called focus focuses and incorporate CPU (for data dealing with), memory (for data putting away), battery (for hugeness) and handset (for enduring and sending signs or data starting with one focus point then onto the accompanying). The cross of every sensor focus developments with applications. For instance, in some military or observation applications it may be essentially nothing. Its cost relies on its parameters like memory assess, managing rate and battery. WSNs are typically executed regions, for example, open or consistently un-trusted and despite undermining conditions that impel diverse security issues. These join the systems, similar to key affiliation, security, find the opportunity to control, authentication and DoS confirmation and so forth.

There are two or three issues in the sensor compose like changing or empowering the middle batteries in light of thick and exceptionally assigned undertaking in crucial condition and moreover because of in riddle nature of WSNs. There would one say one is fundamental demand builds up that is how to broaden the lifetime of the sensor networks. Regardless of the way that it gets to an incredible degree central like broadening system lifetime by lessening criticalness utilization of focus point in WSNs. Test outcomes exhibits that the exchanging of data is particularly finished the best based on importance utilization (EC) however despite what might be expected side data preparing use low centrality. Additionally, a levelheaded technique expected that would broaden the lifetime of WSN also to control the sensor hugeness utilize while data exchange. There is one more issue of security of data at the time of sending data from source to objective in WSN.

Sensor focuses with obliged assets are at risk to number of strikes; thusly the data encryption is basic in WSNs. In case data is transmitted without encryption then the assailants will disconnect the data and wires false data in the system. In hop-by-hop blended data aggregation (EDAs), which is an inside individual aggregator having keys of all as for sensor focus focuses translates got encoded values,

complete all the unscrambled respects and scrambles the come to fruition for sending to a base station (BS). This system needs that inside individual aggregators store keys for unscrambling in that a got aggregator would reveal these depicted data.

In this paper, on an exceptionally fundamental level spotlight on the three weights which is generally address in the wireless sensor networks. At first enhancing the system lifetime of the sensor system through confining the noteworthiness use in the system. Second is to give the security while the data transmission from sender to beneficiary focus point or from sender to base station. Third is data hardship recuperation, when sending the data to cluster head data is lost by righteousness of most extreme control need of cluster head. For reviving the structure lifetime demonstrated the approach in which cluster head is singled out the introduction of vitality, number of neighbors and division to the base station. By picking the cluster head through picking these three parameters diminishes, the significance regard predicted that would the sensor focus point. Homomorphic encryption is utilized for giving the security to the data. Data is sent in the encoded course to the base station, base station unscramble the data coming to fruition to persevering through the data. In like way the methodology of data aggregation is refined in which cluster head indicate the data which is gathered by the cluster focus focuses. For data occurrence recuperation, we are given cache memory at cluster head. Finally, the outcome is detached for the system lifetime, centrality use and for past and proposed structure.

II. LITERATURE SURVEY

This zone depicts the unmistakable works achieved by the specialists for the data aggregation, improving system lifetime of the sensor focus focuses.

Kyung-Ah Shim [1] proposed a SDA strategy, Sen-SDA, which depends upon the get-together of sensible cryptographic local people in heterogeneous cluster WSNs. To lessen the aggregate length of figure messages and to fulfill end-to-end request, they expect an extra substance HE strategy, so only a BS can unwind encoded data amassed by the CHs got from part focus focuses for each social affair of cluster. To give hop-by-hop insistence, they use a managing free character based stamp (IBS) system, in this manner the BS and the CHs can watch the authenticity of all the transmitted blended data. To upgrade plentifulness of various engravings attestations, they require a stamp method in which specific inscriptions from different endorsers on different messages can be checked quickly.

D. Boneh and M. Franklin [5] propose an absolutely sensible character based encryption approach. This method has figure content security in the subjective prophet show getting an arrangement of the computational Diffie-Hellman issue. This structure relies on bilinear maps between clusters. The Weil relationship on elliptic curve is an event of such an accomplice. They give a correct definition to secure character based encryption masterminds and give a few employments to such structures.

C. Castelluccia, E. Mykletun, and G. Tsudik [6] revolve around beneficial, data transmission going to security in WSNs. More particularly, they join unassuming blended methods with real aggregation systems to perform by and extensive accommodating colossally gainful of encoded data. To audit the sensibility of proposed systems, they review them also, show to a remarkable ensuring works out as intended which unmistakably display quantifiable data transmission oblige affirmation and immaterial overhead start from both blended and aggregation exercises.

C. M. Chen, Y. H. Lin, Y. C. Lin, and H. M. Sun [7] show a thought called as Recoverable Concealed Data Aggregation (RCDA). In RCDA, a base station can recover each seeing data made by all sensors paying little character to the probability that these data have been totaled by cluster heads or

aggregators. With this individual data, two functionalities are given. In any case, the base station can declare the uprightness and authenticity of all seeing data. Next, the base station can play out any aggregation limits on them. By at that point, they propose two RCDA systems named RCDA-HOMO and RCDA-HETE for homogeneous and heterogeneous WSN self-rulingly. They demonstrate that the proposed technique are secure under these strike models in the security examination.

J. Domingo-Ferrer [8] addresses one such PH which can be shown secure against known-clear substance ambushes; the length of the figure content space is liberally higher than the sensible substance space. A couple of employments to undertaking of questionable overseeing and data and to e-betting are immediately tended to.

J. Girao, D. Westhoff, and M. Schneider [9] demonstrate a strategy that 1) covers apparent data end-to-end by 2) starting at beginning late giving gainful and flexible in-compose system data gathering. The social affair mediatory concentration demonstrates are not major work at the obvious plaintext data. They execute a particular class of encoded blended and discuss structures for picking beyond what many would consider possible "run of the mill" and "change divulgence." They demonstrate that the approach is possible for the class of "going down" controlling customs. They consider the hazard of demolished sensor centers by proposing a key pre-scattering tally that restrains an aggressors movement and show up how key pre-arrangement and a key-ID fragile "going down" organizing convention builds up the quality and steadiness nature of the related spine.

E. Mykletun, J. Girao, and D. Westhoff [10] reexamine the congruity of additively homomorphic open key encryption infers certain classes of wireless sensor networks. Finally, they offer recommendation to picking the most sensible open key methods for different topologies and wireless sensor mastermind conditions.

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.

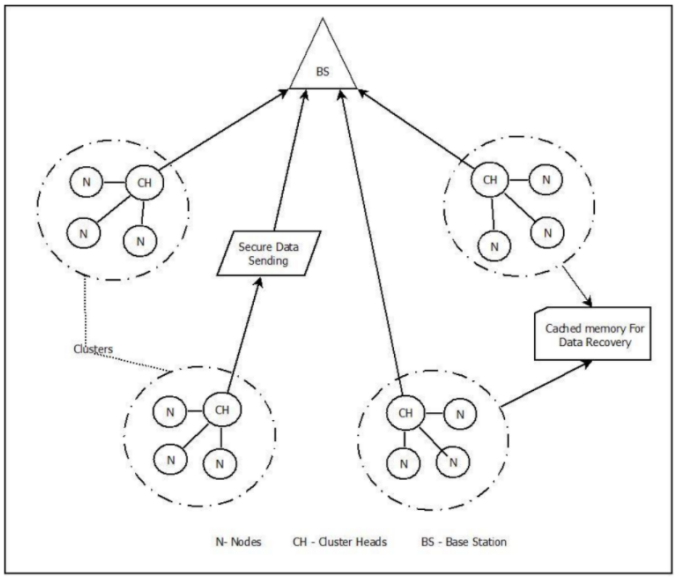

Figure 1. Proposed System Architecture

- 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.

IV. RESULTS AND DISCUSSION

Following are Results generated during the implementation of the system.

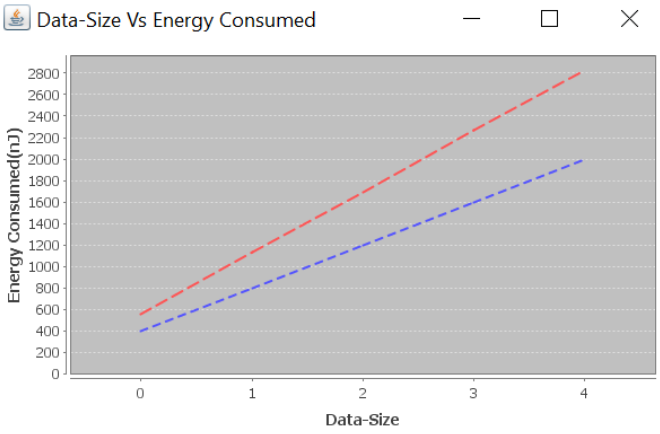

Figure 2. Energy Consumption for Send the Data

The outcomes appeared in Figure 2 and Figure 3 gives the Energy and Time Consumption while sending the information. For better investigation of the outcomes we have demonstrated the consequences of 5 tries. Presently the Energy and Time expended amid the transmission incorporates the assets used in delays. We characterize that handling delay signifies the execution time part nodes require to create their ciphertexts and comparing marks. The aggregation delay is estimated by deciding the time spent checking the marks from part nodes, amassing ciphertexts and marks, and creating the mark of the accumulated outcome. Unscrambling delay shows the time spent on in the end picking up the first information for the BS by confirming the totaled marks and decoding accumulated ciphertexts.

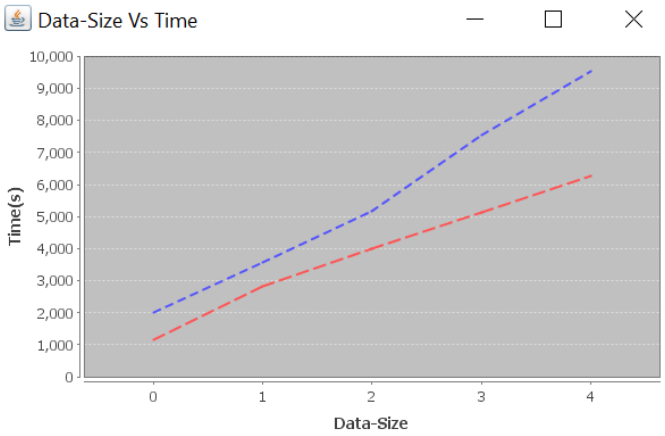

Figure 3. Time Consumption for Send the Data

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 do not 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

By using proposed system we can help the system lifetime of WSN similarly developed the procedure that can pick the cluster head dependent upon three parameters by which system can utilize essentialness adequately and lifetime of the Wireless Sensor Network get pushed ahead. Proposed technique furthermore developed a system for information recovery which is lost while broadcasting the information. At long last the outcome shows that the proposed system will enhance the system lifetime.

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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

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

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

[20] 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 Engg. 25 (7) (2013) 1471–1483.