© 2019 IJSRSET | Volume 6 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology
DOI : 10.32628/IJSRSET196190

Data Aggregation Scheme for Energy Efficiency in Wireless Sensor Network

Bhagyashri Julme[1], Prof. Pragati Patil[2]

[1] PG Scholar, Department of Computer Science & Engineering, Abha-Gaikwad Patil College of Engineering, Nagpur, Maharashtra, India

[2]Assistant Professor, Department of Computer Science & Engineering, Abha-Gaikwad Patil College of Engineering, Nagpur, Maharashtra, India

ABSTRACT

In wireless sensor networks, data aggregation assumes an essential part in diminishing vitality utilization. As of late, explore has concentrated on secure data aggregation because of the open and unfriendly condition conveyed. The Homomorphic Encryption (HE) conspire is widely used to secure data classification. Be that as it may, HE-based data aggregation plans have the accompanying disadvantages: flexibility, unapproved aggregation, and constrained aggregation capacities. To take care of these issues, we propose a secure data aggregation plot by consolidating homomorphic encryption innovation with a mark conspire. To answer this issue we presented a system speaks to a strategy in that powerful cluster head is picked based on the separation from the base station and remaining vitality. Subsequent to choosing the cluster head, it influences utilization of minor measure of vitality of sensor to network and in addition enhances the lifetime of the network of sensor network. Aggregation of the data got from the cluster individuals is obligation of cluster head in the cluster. Confirmation of data is finished by the cluster head preceding the data aggregation if data got isn't legitimate at that point got data is disposed of. Just confirmed data is taken for aggregation at cluster head. Encryption is finished by making utilization of homomorphic encryption technique and additionally encoded data send to the cluster head and data decoding is performed by base station (BS) for offering end to end security. An ID based mark system is created for hop by hop authentication. In this paper, we show the technique for recuperating the data which is lost because of the cushion flood. In given system cache memory is given by the cluster head to recuperation of data misfortune. Finally test comes about shows relying upon parameter like time and additionally vitality utilization on Jung test system that system exhibited is great contrasted with the accessible 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 generally sent in numerous applications, for example, ecological screens, social insurance, natural life observation, and mishap reports [3,4]. WSNs, which are as of now thought to be one of the fundamental parts of the Internet of Things comprise of various sensor hubs obliged regarding their storage room, battery control, and computational ability[2]. Along these lines, arrangements intended to drag out the lifetime of the network are broadly looked for.

Data aggregation is known as one of the strategies that are useful to limit the vitality utilization of sensors [1]. With such system, data detected by

different part hubs are totaled into a solitary one by applying some aggregation capacities, for example, Sum, Average, and MAX lastly transmitted to the base station by means of the wireless connection. Subsequently, data aggregation is useful to decrease parcel transmissions and excess. For instance, in an antiquated woodland, sensors are conveyed to report their detected temperature to the base station for flame observing. For this situation, the base station may require the greatest estimation of all the detecting data to trigger alerts. Thusly, each cluster head just needs to choose the most extreme incentive from among various data esteems got from its part hubs and afterward send the outcome to the base station.

Plainly, the correspondence overhead is reduced in light of the fact that exclusive the accumulated outcome is transmitted to the base station. Along these lines, data aggregation is advantageous to drag out the general lifetime of the However, in light of the fact that they are regularly sent in antagonistic and unattended situations, WSNs are presented to different assaults, for example, replay assault, infusion assault, and hardening assault. The asset compelled qualities of WSNs make existing copious security calculations unsatisfactory for WSNs. In this manner, guaranteeing security for data aggregation is a test.

Advances in wireless correspondence made it conceivable to create wireless sensor networks (WSN) comprising of little gadgets, which gather data by collaborating with each other. These little detecting gadgets are called hubs and comprise of CPU (for data handling), memory (for data stockpiling), battery (for vitality) and handset (for accepting and sending signs or data starting with one hub then onto the next). The span of every sensor hub shifts with applications. For instance, in some military or observation applications it may be minutely little. Its cost relies upon its parameters like memory estimate, handling rate and battery. WSNs are customarily executed regions, for example, open or normally un-trusted and even threatening situations that provoke diverse security issues. These join the strategies, similar to key organization, security, get to control, authentication and DoS protection and so forth.

There are a few issues in the sensor network like altering or empowering the hub batteries in light of thick and specially appointed operation in basic condition and also because of in secret nature of WSNs. There would one say one is imperative inquiry emerges that is how to expand the lifetime of the sensor networks? Despite the fact that it gets extremely basic like expanding network lifetime by lessening vitality utilization of hub in WSNs. Test outcomes shows that the exchange of data is particularly exorbitant based on vitality utilization (EC) however on the opposite side data preparing use low vitality. Moreover, a down to earth strategy expected to expand the lifetime of WSN additionally to limit the sensor vitality usage while data exchange. There is one more issue of security of data at the season of sending data from source to goal in WSN.

Sensor hubs with compelled assets are subject to number of assaults; in this way the data encryption is indispensable in WSNs. If data is transmitted without encryption then the assailants will separate the data and fuses false data in the system. In hop-by-hop scrambled data aggregation (EDAs), which is a middle person aggregator having keys of all as for sensor hubs decodes got encoded values, complete all the unscrambled esteems and scrambles the result for sending to a base station (BS). This method needs that middle person aggregators store keys for unscrambling in that a got aggregator would reveal these characterized data.

In this paper, fundamentally concentrate on the three inconveniences which is generally address in the wireless sensor networks. At first enhancing the system lifetime of the sensor system through limiting the vitality use in the system. Second is to give the security while the data transmission from sender to

beneficiary hub or from sender to base station. Third is data misfortune recuperation, when sending the data to cluster head data is lost on account of limit restrain requirement of cluster head. For updating the structure lifetime displayed the methodology 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 choosing these three parameters diminishes the imperativeness regard anticipated that would the sensor hub. Homomorphic encryption is utilized for giving the security to the data. Data is sent in the encoded route to the base station, base station unscramble the data resulting to tolerating the data. In like way the strategy of data aggregation is refined in which cluster head total the data which is gathered by the cluster hubs. For data misfortune recuperation we are give cache memory at cluster head. Finally, the outcome is separated for the system lifetime, vitality utilization and for past and proposed structure.

II. LITERATURE SURVEY

This section depicts the different works achieved by the scientists for the data aggregation, improving network lifetime of the sensor hubs.

MEDDAH Meriem, HADDAD Rim, EZZEDINE Tahar,"An Energy Efficient and Density control Clustering Algorithm for Wireless Sensor Network", 13th International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE June 2017.

In this paper, author introduce an energy efficient and density control clustering algorithm (EEDCA) which chooses the best nodes in the network to become cluster heads then divides the network into clusters. On this proposed approach, the selection of the cluster head depends on residual energy, density and distance. Each node compares its residual energy with nodes placed on its range. The EEDCA algorithm extends the lifetime of the wireless sensor network, and to prove its efficiency our simulation results show that the proposed solution aims to prolong the lifetime of the wireless sensor network more efficiently.

Kyung-Ah Shim, “A Secure Data Aggregation Scheme Based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks”, in IEEE Transactions on Parallel and Distributed Systems, August 2015.

Sensor Networks Energy cost of transmitting a single bit of information is approximately the same as that needed for processing a thousand operations in a typical sensor node. Thus, a practical way to prolong a wireless sensor network lifetime is to reduce the sensor energy consumption in data transmissions. Data aggregation is an efficient way to minimize energy consumption on sensors. The System proposes a practical SDA scheme, Sen-SDA, based on the combination of the HE scheme, ECElGamal+ and the pairing-free IBS scheme, mID-Sch and the batch verification with BQS for finding invalid signatures in heterogeneous clustered WSNs.

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

The system is based on bilinear maps between groups. The Weil pairing on elliptic curves is an example of such a map. We give precise definitions for secure identity based encryption schemes and give several applications for such systems. Here, Author proposes a fully functional identity-based encryption scheme (IBE). The scheme has chosen ciphertext security in the random oracle model assuming a variant of the computational Diffie- Hellman problem.

Sushmita Ruj, Amiya Nayak, Ivan Stojmenovic,”Pairwise And Triple Key Distribution In Wireless Sensor Networks with Applications”, IEEE Transactions on Computers, November 2013.

Here author addresses pairwise and triples key establishment problems in wireless sensor networks (WSN). Several types of combinatorial designs have already been applied in key establishment. We introduce a novel concept of triple key distribution, in which three nodes share common keys, and discuss its application in secure forwarding, detecting malicious nodes and key management in clustered sensor networks. The Proposed presents a polynomial-based and a combinatorial approach (using trades) for triple key distribution. We also extend our construction to simultaneously provide pairwise and triple key distribution scheme, and apply it to secure data aggregation.

Jyoti Rajput, Naveen Garg," A Survey on Secure Data Aggregation in Wireless Sensor Network ", International Journal of Advanced Research in Computer Science and Software Engineering, May 2014.

Wireless sensor network is a collection of large number of low cost resource constraint sensor nodes that are communicating using wireless medium. Sensor nodes are resource constrained in memory, sensing, communication capability, computational capability, battery power. Communication requires more power in sensor networks. One of the solutions to reduce number of bits transmitted is data aggregation. Data Aggregation is a process of aggregating data coming from different source using aggregation function to reduce redundancy in the Transmitted data.

The aggregated results have great impact in accuracy and robustness of the final result get from the base station. Security is an important criterion to be considered because; wireless sensor nodes are deployed in a remote or hostile environment area that is prone to attacks easily. So data aggregation and security are essential for WSN. Many secure aggregations are proposed in wireless sensor network. But due to resource constrained nature, secure data aggregation also need new approaches. This survey gives the comparative analysis of existing secure data aggregation protocol and their limitations and advantages.

Bo Sun, Xuemei Shan, Kui Wu, Yang Xiao, "Anomaly Detection Based Secure In-Network Aggregation for Wireless Sensor Networks", IEEE Systems Journal, Vol. 7, No. 1, March 2013

Secure in-network aggregation in wireless sensor networks (WSNs) is a necessary and challenging task. In this paper, we first propose integration of system monitoring modules and intrusion detection modules in the context of WSNs. We propose an extended Kalman filter (EKF) based mechanism to detect false injected data. Specifically, by monitoring behaviors of its neighbors and using EKF to predict their future states (actual in-network aggregated values), each node aims at setting up a normal range of the neighbors' future transmitted aggregated values. This task is challenging because of potential high packet loss rate, harsh environment, and sensing uncertainty. This paper illustrates how to use EKF to address this challenge to create effective local detection mechanisms. Using different aggregation functions (average, sum, max, and min), we present how to obtain a theoretical threshold. Author further apply an algorithm of combining cumulative summation and generalized likelihood ratio to increase detection sensitivity.

Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, Sanjay Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks", IEEE Transactions On Dependable And Secure Computing, February 2015.

Author proposed a framework, called RFSN, in which each sensor node maintains the reputation for each other node in a network, based on which the trustworthiness is calculated. The framework also considers the limitations of the sensor nodes. Within

RSFN, a beta reputation system is established which uses Bayesian formulation to estimate the trustworthiness of sensor nodes. BRSN i.e Beta Reputation System for sensor Networks is used for reputation representation, updates, integration and trust evolution. RFSN gives the approach to detect all misdeed resulted from malicious and faulty sensors in a network. It also integrates various solutions of security.

III. EXISTING SYSTEM

This segment portrays the past system used for secure sending the data.

Working of the past system is as per the following:

1. Network chart created as Graph G (V, E) where; V is vertices/hubs and E is edges.
2. Clustering is done on the quantity of the hubs and delegated number of clusters and pick the cluster head haphazardly.
3. Play out the key dispersion and course ages at every hub through Base Station.
4. Make the data and Encrypt with people in general key of base station at every hub.
5. Process the hash estimation of the scrambled data and Record the timestamp.
6. Forward the individual data to the cluster head from each cluster part in every one of the clusters.
7. Get all data at the cluster head and check the data by its hash esteem and acknowledge the confirmed data or dispose of if not confirmed.
8. Solidify every one of the data and forward the same to the base station.
9. Base station gets the data from each cluster head.
10. Base station confirms the data and unscrambles the data with legitimate key.

IV. PROPOSED SYSTEM

This section portrays the system review in which proposed calculation and scientific model of the proposed system is likewise present.

System Overview

System architecture of the proposed is shown in figure 1 which appears in different advances and steps are provided beneath.

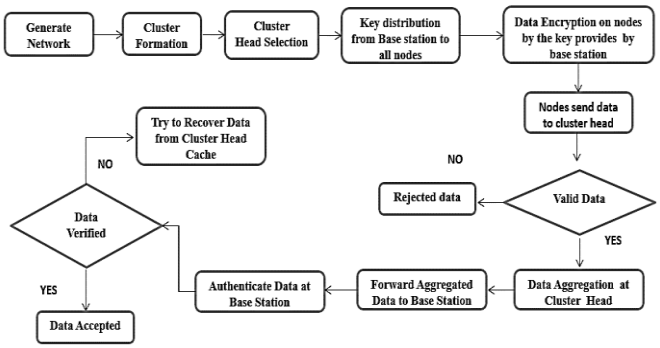

Fig. 1. Proposed System Architecture

1.Network Generation

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

2.Clustering Process

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

3.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.

4.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.

5.Data Encryption

At every node data is generated and encryptedthrough the Paillier Encryption.

6. Hash value evaluation

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

7. Data Collection

Consequent to evaluating, the hash regard at every center point, every center advances data to its cluster head. Cluster head have some constrained capacity to store the data if the cluster head stockpiling is overwhelmed then the data is dropped at assemble head. The cluster head merges each one of the data and check the substantial data.

8. 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.

9. Data verification

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

10. Data aggregation

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

11. Data Decryption

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

V. CONCLUSION

By utilizing proposed system we can boost the network lifetime of WSN likewise built up the strategy that can choose the cluster head contingent upon three parameters by which network can use vitality effectively and lifetime of the Wireless Sensor Network get moved forward. Proposed strategy additionally built up a system for data recuperation which is lost while broadcasting the data. Finally the result demonstrates that the proposed system will amplify the network 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] 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.

Cite this article as :

Bhagyashri Julme, Prof. Pragati Patil, "Data Aggregation Scheme for Energy Efficiency in Wireless Sensor Network", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 6 Issue 2, pp. 504-510, March-April 2019.

Journal URL : http://ijsrset.com/IJSRSET196190