International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 10 (2015) pp. 26761-26768

http://www.ripublication.com

Secured Data Aggregation In Wireless Sensor Network

Shivakumar K.M [1].,Shruthi K[2]., Shruthi V[3].
Dept. of Computer Science, Amrita School of Arts and Sciences,
Amrita Vishwa Vidyapeetham, Mysore Campus,
Mysore, India
shivadrg19@yahoo.com[1],shrujanani.urs@gmail.com[2],
shru.shona123@gmail.com[3]

Abstract

Wireless Sensor Network (WSN) is a network consists of number of nodes with limited sensing computation and communication capabilities. In this type of network we are providing security as well as energy-consuming operation is maintained. Hence to increase the lifetimeof the network it becomes necessary to reduce the number of bits that is been transmitted. One of the widely used methods for reducing the datatransmission is data aggregation (clustering). The security issues such asdata integrity and confidentiality in data aggregationbecome crucial when the WSN is deployed in remote sensing areas. Secure data aggregation in WLN is a method toachieve energy-consumption of battery of a sensor device and data security using homomorphic algorithm. In this paper we propose a protocol called SEEDA (Secured End to End Data Aggregation)-SUM/AVG for secure data aggregationwhich provides end-to-end data security.The protocol SEEDA-SUM/AVG is used to compute the SUM andAVERAGE at aggregator node.

Key words: Support Secure Data Aggregation, end-to-end privacy, homomorphism encryption, Cipher Text, Aggregated data.

Introduction

A Wireless Sensor Network (WSN) is network consists of several sensor nodes which are interconnected with each other.This is used in many applications like tracking, fire detection and disaster prevention. These sensor networks can be described as a collection of sensor nodes that co-ordinates to exchange the data among themselves to perform some calculation which required. The WSN consists of nodes from a few to several hundreds or even thousands of nodes, where each node is connected to one another within a network.Each such node usually consists of a battery, micro controller an electronic circuit. The main challenge for a Wireless Sensor Network is to provide security and to minimum the battery consumption. After sensor nodes are being deployedin theinterested field,these sensor nodes organize themselvesinto a multihop network with the Base Station (BS). Where the base station is central point of controller. The sensor nodes and BS areconnected via wireless network. WSNs are extensively usedin several application fields such as Health Care Monitoring, forestfire detection, Air Pollution Monitoring, tracking and many more. One of the majorapplicationsof WSN is to monitor environmental datasensing and to transmit that sensed data toBS. Then the BS analyzes the received data which is then used to initiatesome specific action. The data analysis carried out by BSin most scenarios is to compute SUM and AVERAGE. These computed values arecalled as aggregates and the computation of aggregates iscalled as data aggregation. Several data aggregation protocol has been processed. Data aggregation is the process of summing up of received data from all the sensor nodes in a cluster. The resultant value will be then sent to the base station where in, BS aggregates resultant value (SUM/ N).The data aggregation can occur either at the BS or at somenode in the network. If aggregation is carried out at BS everysensed data is to be transmitted to BS. Upon receiving the datafrom all the nodes, BS computes the required aggregate. Thisis a straight forward and simple method to aggregate the datawhich is called as All-Node data aggregation scheme. In thisapproach the energy consumption increases linearly with theamount of transmitted data.

Literature Survey

This section gives brief literature review of how Wireless Sensor Network is been implemented using different methodologies by different authors

The data aggregation within thenetwork helps in battery consumption of a sensor node [8], [2]. In dataaggregation, instead of sending each sensor node’s data to the BS,we form a cluster, in which each cluster has a cluster head, which collects all the data from its neighboring nodes which are in the cluster. By summing up the data the cluster head sends the resultant value to the BS. Then BS aggregates the received value from a cluster head.The security issues such as data integrity and confidentiality in data aggregation become crucial when the WSN is deployed in remote sensing areas.Where sensors are prone tonodefailures and compromises.Secure data aggregation protocols are suitable to achieveSecurity in data aggregation. These protocols are extensively studied in [9], [6]. Different data aggregation protocols are discussedin [9] and they are classified into two types. The first type, hop-byhop aggregation protocol. This achieve data aggregation in hopby-hop fashion and they are discussed in [7], [10], [11], [3], [5], [12],[13], [14], [15]. In this type of aggregation an aggregatorhas to decrypt every received message, then aggregate themessages according to its corresponding aggregation function,then finally, encrypt the aggregated result before forwardingit to BS and they require intermediate aggregator to storekeys for decryption and encryption of data. Also hop-by-hop securedata aggregation protocol does not guarantee data confidentialityat data aggregator. To overcome this limitation, a secondtype of aggregation protocol called end-to-end secure data

Aggregation method is proposed in [16], [4], [17], [18],[19], [20]. These protocols perform data aggregation withoutdecryption of the sensor data at aggregator node. In our paperwemainly focus on the data aggregation protocol which provides end-to-end data security using homomorphic encryption. The secure aggregation methods that provide end-to-end data security are discussed in [16], [19], [4], [18]. In [16],in [28] a protocol to find the SUM aggregate is explained. In this method, aggregator node is required to store secret keys of nodes in its cluster head. Also the detailed energy and performance analysis is not discussed. In our paper we propose a protocol for secure data aggregation, Secure End-to-End Data Aggregation (SEEDA) protocol.The SEEDA-SUM/AVG protocol is used to compute SUM at cluster head and AVERAGE at BS. Generally end-to-end aggregation protocols are used to compute the aggregates like SUM and AVERAGE.

Experimental Setup

A cluster based private data aggregation (CPDA) protocol is implemented, where sensor nodes are distributed randomly into cluster based protocol. The cluster leaders are responsible for directly aggregating the data from the cluster members, with the communication secured by a shared key between a pair of communicating nodes.

Two data encryption method has been employed in CPDA:-

End-to-End encrypted data aggregation

In this scheme intermediate nodes can aggregate ciphertext directly without decrypting the messages. Compare to hop-by-hop one, it can guarantee the end-to-end data confidentiality and result in less transmission latency.

Privacy Homomorphism

In this scheme encryption transformation allows the direct computation on encrypted data. The data is encrypted and sent towards the base station, while sensors apply the aggregation function on the encrypted data. The base station receives the encrypted aggregate result and decrypts it.

Algorithm:

Paillier Cryptosystem:

Homomorphic crypt system algorithm:

The Paillier Cryptosystem, named after and invented by Pascal Paillier in 1999, is a probabilistic asymmetric algorithm.

Step1**:** Take p and q were p and q are two large prime numbers where,
gcd (pq,(p-1)(q-1))->1
Step 2: calculate the valuesof n and lambda
Where n->pq, lambda -> (lcm(p-1),(q-1))
Step 3: select random integer g
Where,

g belongs to z*_{n^2}
Step 4: lambda-> LCM (p-1),(q-1))
Step 5: nsquare-> n*n
mu->(L (g^lambda mod nsquare)) ^ -1 mod n
Step 6: where L is L (u)-> u-1/2
Step 7:u->g lambda mod nsquare
Encryption and decryption: is based on modularization arithmetic
Encryption:
Step 8: m is a message to be encrypted
Step 9: select random r
Where
r is an integer
Step 10: Compute cipher text as
C->g^m * r^n mod nsquare

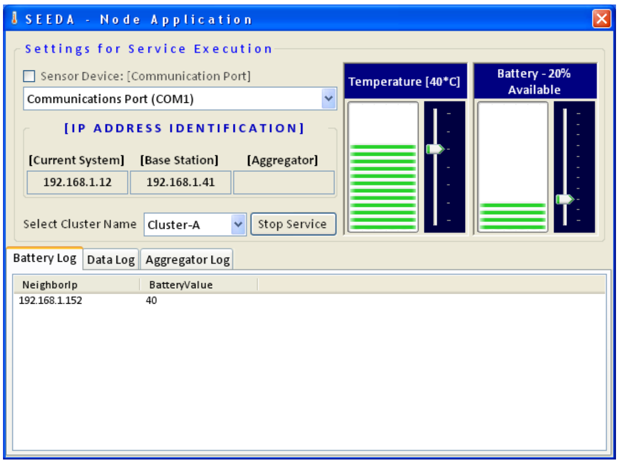
Decryption:
Step 11: let c be the cipher text to be Decryption
Step 12: Compute the plain text message as
m-> L (c^lambda mod nsquare) * mu mod n

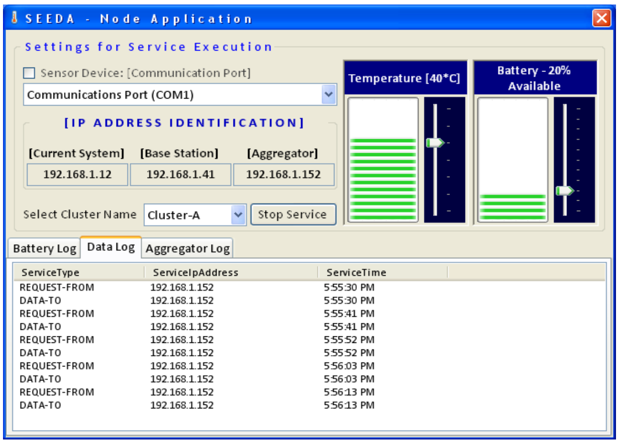
Homomorphic properties:
A notable feature of the Paillier Cryptosystem is its Homomorphic properties. As the Encryption function is additively homomorphic, the following identities can be described.

Homomorphic Addition of plain text:
Step 11: The product of two Cipher texts will Decrypt to the sum of their corresponding plain text,
D(E(m1,r1) * E(m2,r2) mod nsquare) ->m1+m2 mod n
Step 12: The product of a Cipher text with a plain text raising g will Decrypt to the sum of the corresponding plain texts.
D (E (m1, r1) * g ^ m2 mod nsquare) -> m1+m2 mod n

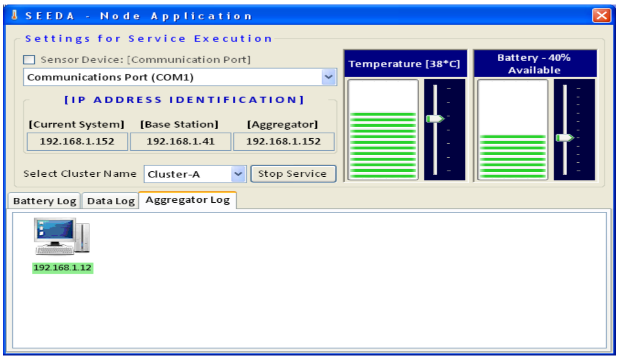
Results

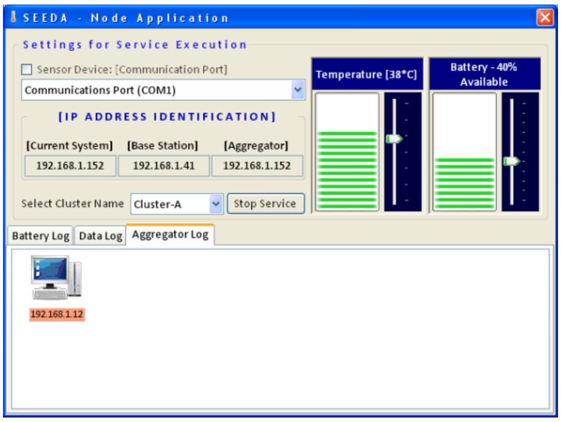
Snap shot 1: Node Application



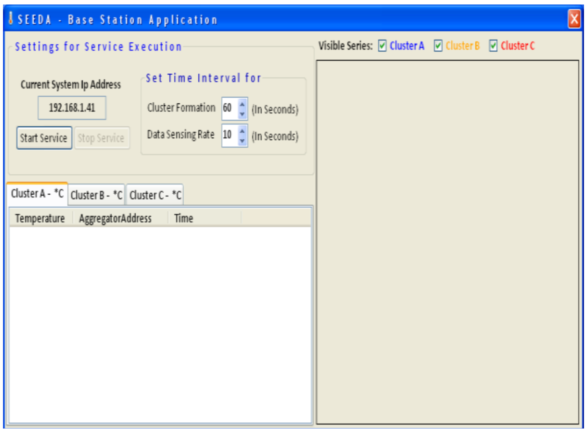


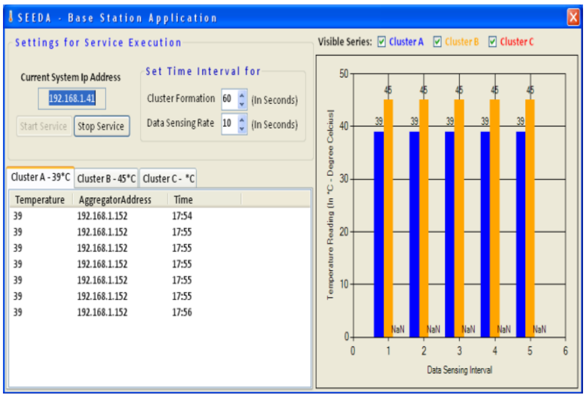
Snap shot 2: Aggregator Formation:





Snap Shot 3: Base station:





Conclusion

By reviewing the existing data aggregation in the WSN, an adversarial model that can be more useful to save the energy of Wireless Sensor Nodes that lead to improve the life time of whole networks. An adversarial model for security on Data Aggregation its help us to give batter performance compare to existing scheme.

References

[1] I.F. Akyildiz, W. Su, Y. Sankara subramaniam, E. Cayirci, " A Survey on Sensor Networks", IIEEE Commun. Mag, Vol.40, No.8, pp.102–114, 2002.

[2] K. Akkaya, M.Demirbas, R.S. Aygun, The Impact of Data Aggregationon the performance of Wireless Sensor Networks, Wiley Wireless Communication Mobile Computing (WCMC), J(8), pp.171–193, 2008.

[3] H. am, S. Ozdemir, P. Nair, D. Muthuavinashiappan, H.O. Sanli, Energyefficient and Secure pattern based Data Aggregation for Wireless Sensor Networks, Comput. Commun., Elsevier, Vol.29, No.4, pp.446-455, 2006.

[4] C. Castelluccia, C-F Chan, E. Mykletun, G. Tsudik, Efficient Provably Secure Aggregation of Encrypted Data in Wireless Sensor Networks, ACM Transactions on Sensor Networks, Vol.5, No.3, May 2009.

[5] W. Du, J. Deng, Y.S. Han, P.K. Varshney, A witness-based approach for Data Fusion Assurance in Wireless Sensor Networks, Proceedingsof the IEEE Global Telecommunications Conference (GLOBECOM 03), pp. 1435-1439, 2003.

[6] Hani Alzaid, Ernest Foo, Juan Gonzalez Nieto, Secure Data Aggregationin Wireless Sensor Network: a survey, sixth Australasian conference onInformation security, Wollongong, NSW, Australia, 2008.

[7] L. Hu, D. Evans, Secure Aggregation for Wireless Networks, Proceedings of the Workshop on Security and Assurance in Ad Hoc Networks, Orlando, FL, 28 January 2003.

[8] J. Yick, B. Mukherjee, D. Ghosal, Wireless Sensor Networks : Survey, Comput. Networks, Vol.52, No.12, pp.2292–2330, 2008.

[9] Suat Ozdemir, Yang Xiao, Secure Data Aggregation in Wireless Sensor Networks : A Comprehensive Overview The International Journal of Computer and Telecommunications Networking, Vol.53, No.12, pp.2022–2037, 2009.

[10] B. Przydatek, D. Song, A. Perrig, SIA : Secure Information Aggregation in Sensor Networks, Proceedings of SenSys03, pp.255-265, 2003.

[11] A. Mahimkar, T.S. Rappaport, Secure DAV: A Secure Data Aggregation and Verification Protocol for Wireless Sensor Networks, Proceedings of the 47th IEEE Global Telecommunications Conference (Globecom), November 29December 3, Dallas, TX, 2004.

[12] K. Wu, D. Dreef, B. Sun, Y. Xiao, Secure Data Aggregation without Persistent Cryptographic operations in Wireless Sensor Networks, Ad Hoc Networks, Vol.5, No.1, pp.100-111, 2007.

[13] H.O. Sanli, S. Ozdemir, H. am, SRDA: Secure Reference-based Data Aggregation Protocol for Wireless Sensor Networks, Proceedings of the IEEE VTC Fall Conference, Los Angeles, CA, pp. 4650-4654, 2004.

[14] Y. Yang, X. Wang, S. Zhu, G. Cao, SDAP: A Secure hop-by-hop Data Aggregation Protocol for Sensor Networks, Proceedings of the ACM MOBIHOC06, 2006.

[15] S. Ozdemir, Secure and Reliable Data Aggregation for Wireless Sensor Networks, H. Ichikawa et al. (Eds.), LNCS 4836, pp.102-109, 2007.

[16] D. Westhoff, J. Girao, M. Acharya, Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption key Distribution and Routing Adaptation, IEEE Trans. Mobile Comput., Vol.5, No.10, pp.1417-1431, 2006.

[17] S. Ozdemir, Secure Data Aggregation in Wireless Sensor Networks via Homomorphic Encryption, Journal of The Faculty of Engineering and Architecture of Gazi University, Vol.23, No.2, pp.365-373, 2008.

[18] I. Rodhea, C. Rohner, n-LDA: n-layers Data Aggregation in Sensor Networks, Proceedings of the 28th International Conference on Distributed Computing Systems Workshops, pp.400-405, 2008.

[19] S. Ozdemir, Concealed Data Aggregation in Heterogeneous Sensor Networks using Privacy Homomorphism, Proceedings of the ICPS07: IEEE International Conference on Pervasive Services, Istanbul, Turkey, pp.165-168, 2007.

[20] W. Zhang, Y. Liu, S.K. Das, P. De, Secure Data Aggregation in Wireless Sensor Networks: a watermark based authentication supportive approach, Elsevier Pervasive Mobile Comput, Vol.4, pp.658-680, 2008.

[21] A. S. Poornima, B. B. Amberker, SEEDA : Secure End-to-End Data Aggregationin Wireless Sensor Networks, In Proceedings of 7th International Conference on Wireless and Optical Communication Networks (WOCN 2010), Srilanka, India, 2010.