International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Energy Efficient Data Aggregation of Wireless Sensor Network and Attacks using Error Bound

Yogita Hukre [1], S. S. Dongre[2]

[1] M.E. Student, Wireless Communication and Computing, GHRCE, Nagpur, India

[2]Assistant Professor, Department of Computer Science and Engineering GHRCE, Nagpur, India

Abstract: ***A wireless sensor networks (WSNs) consist of as many numbers of nodes which can communicate with each other. The sensor nodes consume energy during sensing, processing and transmission. In Wireless sensor network power and energy resources are limited. The number of sensor nodes is deployed in physical area. If each node sends information to the base station, energy is wasted and therefore the network energy are consume quickly. In this paper for data aggregation the READA technique will be used with some error bound. Redundancy Elimination for accurate data Aggregation (READA) uses a grouping and compression mechanism to get rid of duplicate information within the aggregated set of information to be sent to the base station. In wireless sensor network, security and energy efficiency issues are found. In this paper, different types of attacks associated with WSN and their effects are discussed.***

Keywords: Aggregation techniques, Error Bound, Energy Efficiency, Injection Attack, Sensor Networks, Sybil Attack

1. Introduction

Wireless sensor networks (WSNs) are composed of nodes with the capabilities of sensing, communication and computation. It is necessary to define the capacity of computing and transporting specific functions of sensor measurements to the sink node. In network aggregation plays an important role in prolonging the network life for WSN. To aggregate the sensor data effectively the aggregation technique is to be used. This technique enhances the network lifetime by gathering and aggregating the data in an very efficient manner [1]. To save more energy and improve the fidelity, approximate data aggregation with precision guarantees is performed in many sensor network applications. In precision constraint data aggregation, not all readings have to be reported to the base station. The node sends its reading to the base station only if the difference between its current reading and the last one beyond a threshold. The threshold is called *error bound* in this paper. Using this scheme, suppress the number of transmitting messages in the networks and extend the network lifetime further. Wireless sensor networks square measure at risk of many varieties of security attacks, as well as false information injection, wrong id and position of node. Sensor nodes may be compromised by wrongdoer, and also the compromised nodes will distort information integrity by injecting false information. The transmission of false information depletes the affected battery power and degrades the information measure utilization. False information may be injected by compromised detector nodes in numerous ways in which, as well as information aggregation. As a result of information aggregation is essential to scale back information redundancy and/or to boost information accuracy, false information detection is crucial to the supply of information integrity and economical utilization of battery power and information measure.

In this paper in section 2 various techniques and strategies available for network lifetime maximization is described. In section 3 system model is explained. In section 4 proposed error bound method for enhancing the network lifetime with attacks. Section 5 displays simulation results of the proposed technique. Section 6 is the conclusion thus followed by references.

2. Related Work

The iterative algorithm Iterative filtering algorithm is used to decrease the energy consumption in an efficient manner [1]. It solves the problem of data aggregation. The literature on iterative filtering has been increased day by day. The aggregation algorithm is used to prevent from attacks. Concealed data Aggregation (CDA) places a lot of intensity on passive attacks. Specially, it considers if adversaries will listen in the communications on the air. After CDA, succeeding analysis has been planned to realize higher security levels. If sensors at intervals constant cluster cypher their sensing information with a standard secret key, associate opponent might decode the aggregative cipher text by compromising only one detector. Planned a knowledge aggregation theme supported addition homo-morphic public-key encoding. It's like safer since each detector stores solely public key. It's needed to guard the transmission trend of a node's secret information from neighbors, as a result of the neighbors grasp the aggregative add and therefore the encoding key to realize the privacy. Therefore, protective confidential aggregation may be a difficult task[2]. The ESPDA protocol prevents the replay attack by achieving information freshness throughout aggregation , this will increase the accuracy of the collective result by playacting the aggregation on encrypted information and reduced variety of transmissions. However, This scheme causes further communication overhead as a result of the base station will firmly recover all sensing information instead of collective results[3]. In Candidate based precision allocation system using a multi-hop networks. They extend the adaptive scheme to work in multihop network and topology relation between the sensors nodes. In this technique relationship between the error bound and update rates are not known[14]. For wireless Sensor Networks D-BEDCA technique use for data compression and keep the data distortion in certain range at

the same time. There are two techniques in data compression that is lossy and lossless data compression[16].

3. System Model

Consider a network consisting of n sensor nodes that are randomly deployed in an physical area. The sensor nodes monitor the surrounding environments and send the local measurements such as temperatures to the base station continuously. Assume that all the sensor nodes need to report their readings to the base station. Because of this number of transmission increases which cause more energy wastage.

The network system shown in the figure shows that number of sensor nodes are in cluster. The figure shows that number of sensor nodes are in group. They collect the data from sensor node and aggregated then sends to the base station in secure manner.

For the proposed data aggregation technique, the number of nodes will be arrange in clusters and one of them is work like a cluster head. After that every cluster head is connect to the base station. They will sends the data to the base station. In this paper uses a new data aggregation technique called a "Redundancy Elimination for Accurate Data Aggregation" (READA). All the sensor nodes get connected to the each for communication. Depending on their nearest position they connected to each other. This process done in all cluster is shown below. In the second step nodes are connected to each other. In this process find the sending time, receiving time and pending request. Some nodes are missed due to their long distance. In the third step every sensor nodes are connected to the cluster head. All the data sends to the cluster head. In the fourth step all the cluster head connected to the base station. Every cluster head sends the data to the base station.

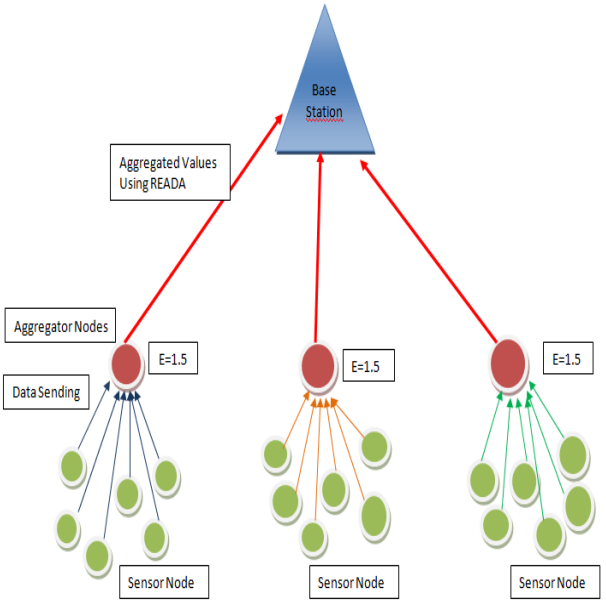


Figure 1: System Architecture

3.1 Aggregation

Aggregation will be performed by two ways that is monitoring system and event detection.

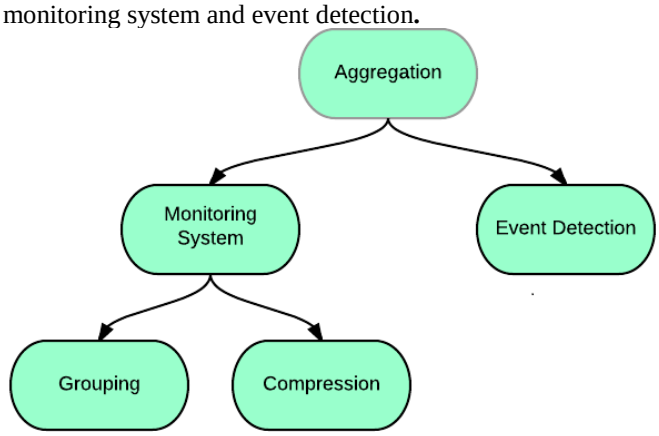
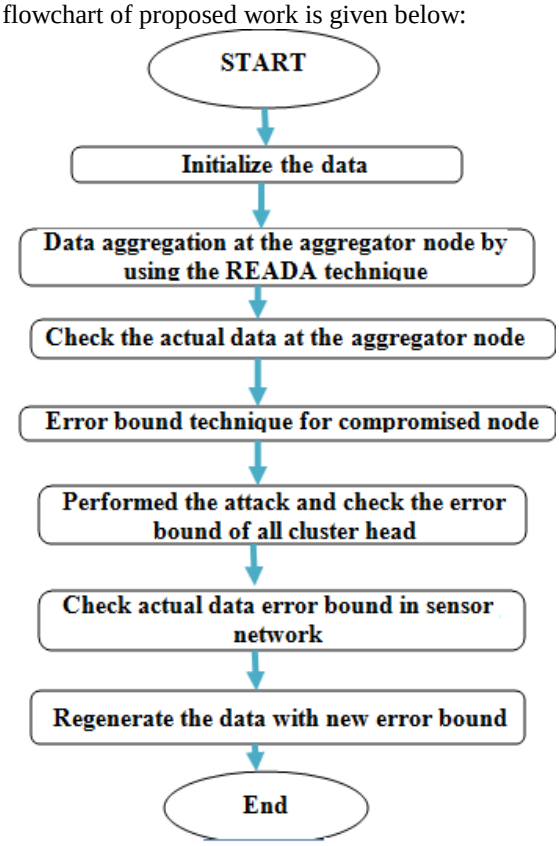


Figure 2: Types of Aggregation

In READA technique aggregation will be perform by two way that is monitoring system and event detection. First of all the monitoring system is used to search the sensor nodes. In this two technique will be used that is Grouping and Compression. For partitioning a data grouping technique is to be used. Instead of sending a single data that sends the group of compressed data. They allocate a id to the every node and same id make a group. This process repeat in all three cluster. By using this process all groups are form with same id's.

3.2 Working of System

The flowchart of proposed work is given below:



In the above flow chart first of all the N number of nodes are connected to the cluster head, collecting the data and

aggregating at cluster head then forward the data to the base station. In second step apply the READA technique provides the trust to the sources. In this process some nodes are compromised by the attackers. To resolve that error bound technique is used to cluster head and find actual error bound and also various attacks.

3.3 Algorithm for READA

Algorithm illustrate the Redundancy Elimination for Accurate Data Aggregation based on above formula.

```
function [ id ] = MainReada( agg_data_node )
data=readData(agg_data_node); %% reading data
v=data(rand); %% choose node to group
%% Rf and p1, p2 for groping data

RF=0.2; %user defined
 id=mod(data(v))
 if is Avalible(id);
 p1=id;
 else
 p2=id;
 end
end
```

4. Attacks and Error Bound

In wireless sensor networks nodes square measure terribly prone to varied security attacks like selective forwarding, wormholes attacks. Additionally, wireless sensor networks additionally suffer from injecting wrong information attack. For Associate in injecting false information attack, Associate in aggressor node initial compromises many device nodes and accesses all keying materials hold on within the compromised nodes then controls these compromised nodes to inject false data and send those information to the sink. Therefore, it is crucial to filter the false information as accurately as attainable in wireless sensor networks which ends up in energy deprivation. To tackle this issue, error bound methodology use to filter false information and additionally secure the id and position of the node. In the Sybil attack, a malicious node behaves as if it were a larger variety of nodes, as an example by impersonating alternative nodes or just by claiming false identities. In the worst case, Associate in injection attacks could generate in injecting false absolute variety of further node identities, exploitation using physical device.

4.1 Bounded Error

In wireless sensor network there are number of attacks are found while aggregating the data. In this case there is possibility to loss the data which is in physical manner. So , to recover that data here using error bound method and that also increasing network lifetime with less energy. First of all allocate the threshold (here error bound) value to the aggregator node. After performing aggregation some nodes are compromised like injecting false data, fake id and position etc.. That's means the total number of data has been increased. Because of this accurate data not to be send to the base station. To provide the security to the aggregator node the error bound is to be used. By using this method the actual data is to be generated. The is less chances to loss maximum amount of data.

4.2 Attacks

In wireless sensor network while aggregating the data the lot many attacks is to be found. In this paper using two attacks that is injecting false data attack and Sybil attack. Injecting false data means while performing aggregation there are lot many extra data is to be added. This aggregation is unsafe to the wireless sensor network. Because of this the more energy is wasted. In Sybil attacks it work on node id and node position. First of all it stole the id and position of the nodes. A Sybil attack is an attack which creates multiple identities from same harmful node. This attack is very crucial to the wireless sensor network. So to protect the sensor network from attacker the current security scheme is a good solution for enhanced the sensor network security.

5. Performance Evaluation

5.1 Simulation Setup

The simulation tool used is Matlab. In this section the performance of the error bound method with READA algorithm and data rate with attack scenario is evaluated by comparing it with previously proposed adaptive filtering. The comparison is done on the basis of designed error bound and network lifetime for physical environment. The experimental result shows that first of all form a clusters. In this there are four clusters are form. Every node senses the sensor field and initialize the location of sensor nodes, locate it. The evaluation metrics in this paper are the data rate and network lifetime. In the below figure show the attack scenario and regenerated data. As discussed earlier that use of error bound with the READA will increase the lifetime of network. The above figure shows that even though the node is compromised the regenerated data is up to 97%. The loss of data is very less. This means the system performance is increased up to 20% than the original system.

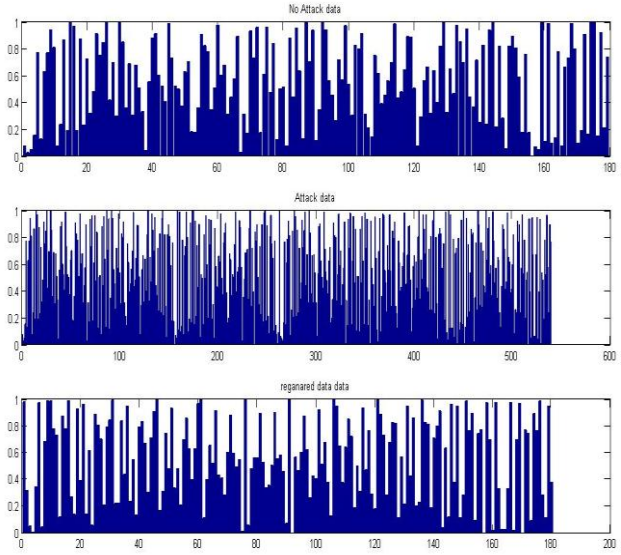


Figure 3: Attack Scenario

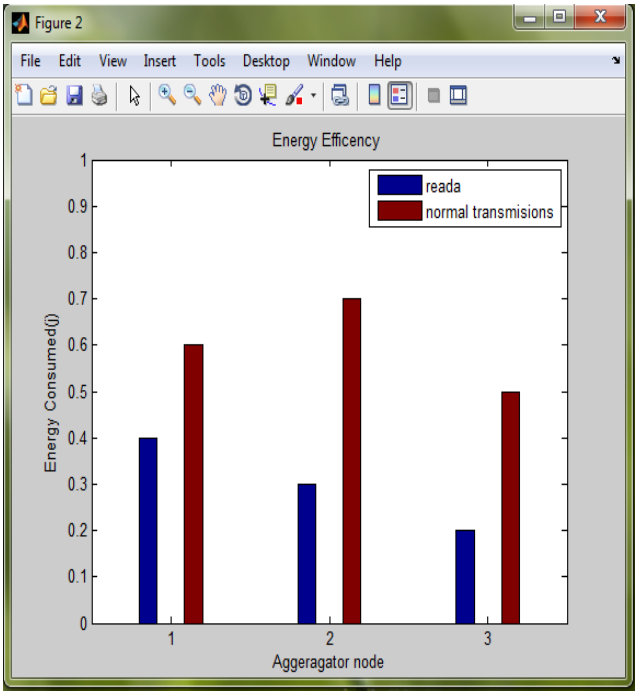


Figure 4: Energy Efficiency

The above graph shows the increase of network lifetime with respect to the designed error bound. This shows that that the use of normal transmission with the READA leads to increase in lifetime of WSN which is the aim of this paper. The increase in network lifetime means the network will be active for longer time as compared to the earlier scenario. The network lifetime is increased up to 30-50% in proposed work. As a result the node failure will not occur soon and the network will work for longer time.

6. Conclusion

In this paper, A READA algorithm using with some error bound and strategies used for lifetime maximization of WSN. Thus considering those factors a new technique READA is to be introduce. READA is used for large and sensor networks lifetime maximization scheme for reducing the power and increasing the lifetime. The proposed work is for enhancing the network lifetime of WSN using READA technique. The technique used for improving the network lifetime. This will reduce the use of energy and the system will be energy efficient, also the power required in the system is reduced as a result increasing the network lifetime of WSN. The energy efficiency of WSN increases from 30-50 % as compared to earlier scenario. The use of error bound helps in increasing the lifetime of the network.

References

[1] Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino and Sanjay Jha, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks", IEEE Transactions On Dependable And Secure Computing (TDSC) 2014.

[2] Junchao Ma, Wei Lou and Xiang-Yang Li, "Contiguous Link Scheduling for Data Aggregation in Wireless Sensor Networks", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 7, July 2014.

[3] Cheng Wang, Chang jun Jiang, Yun hao Liu, Xiang-Yang Li and Shaojie Tang, " Aggregation Capacity of Wireless Sensor Networks: Extended Network Case", IEEE Transactions On Computers, Vol. 63, No. 6, June 2014.

[4] Soonhwa Sung, "Confidential Aggregation for wirelessTransmissions" 2014 IEEE.

[5] Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, and Niraj K. Jha, "A Study of the Energy Consumption Characteristics of Cryptographic Algorithms and Security Protocols"

[6] IEEE Transactions On Mobile Computing, Vol. 5, No. 2, February 2006.

[7] Hani Alzaid Ernest Foo Juan Gonzalez Nieto, "Secure Data Aggregation in Wireless Sensor Network: a survey", 2007

[8] Hemant Sethi, Devendra Prasad, and R. B. Patel "EIRDA: An Energy Efficient Interest based Reliable Data Aggregation Protocol for Wireless Sensor Networks," in proceedings of International of Computer Applications, Volume 22– No.7, May 2011.

[9] Hani Alzaid, Ernest Foo, and Juan Gonzalez Nieto "Secure Data Aggregation in Wireless Sensor Network: A Survey" IEEE on Information Security conference, Wollongong, Australia, January 2008.

[10] Dragos Ioan Sacaleanu, Rodica Stoian, Lucian Perisoara. Vasile Lazarescu, "Increasing the Lifetime of a Wireless Sensor Network through Data Aggregation Techniques" IEEE 2013.

[11] S. 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.

[12] Kavi Khedo, Rubeena Doomun, Sonum Aucharuz." READA : Redundancy Elimination for Accurate Data Aggregation in Wireless Sensor Networks", Wireless Sensor Network, 2010.

[13] R. Rajagopalan and P. K. Varshney, "Data-Aggregation Techniques in Sensor Networks: A Survey," IEEE Communication Surveys and Tutorials, Vol. 8, No. 4, December 2006, pp. 48-63.

[14] X. Li, "A Survey on Data Aggregation in Wireless Sensor Networks," Project Report for CMPT 765, Spring 2006.

[15] Xueyan Tang and Jianliang Xu, "Optimizing Lifetime for Continuous Data Aggregation with Precision Guarantees in Wireless Sensor Networks" IEEE/ACM Transactions On Networking, Vol. X, No. X, Month 200x.

[16] Xiaoyan Wang and Jie Li, "Precision Constraint Data Aggregation for Dynamic Cluster-based Wireless Sensor Networks", 2009 Fifth International Conference on Mobile Ad-hoc and Sensor Networks.

[17] Che-Lung Lin, Jui-Hua Tsai, Yu-Hsien Chu,Ray-I Chang, "Concept of Bounded Error to Improve Wi,reless Sensor Network Data Compression" , ©2014 IEEE

Author Profile

Yogita K. Hukre is pursuing Master of Engineering in Wireless Communication and Computing (WCC), Department of Computer Science and Engineering(CSE) from G.H. Raisoni College of Engineering Nagpur, MS. She received the B.E. degree in Computer Technology Engineering from Manoharbhai Patel Institute of Engineering and Technology in 2012. Her research interests in Wireless Sensor Network, Networking, etc.

Snehlata S. Dongre received B. E. degree in Computer Science and Engineering from Pt. Ravishankar Shukla University, Raipur, India in 2007 and M. Tech. degree in Computer Engineering from University of Pune, Pune, India in 2010. She is currently working as Assistant Professor the Department of Computer Science and Engineering at G. H. Raisoni College of Engineering, Nagpur, India. Number of publications is in reputed International conferences like IEEE and Journals. Her research is on Data Stream Mining, Machine Learning, Decision Support System, ANN and Embedded System. Her book has published on titled Data Streams Mining: Classification and Application, LAP Publication House, Germany, 2010. Ms. Snehlata S. Dongre is a member of IACSIT, IEEE and ISTE organizations.