Data Aggregation Techniques in Wireless Sensor Network: Survey

Ashwini V. Sisal
PG Student, ME(ComputerNetwork)
G.H.R.C.E.M, Wagholi
Savitribai Phule Pune University, India

Simran Khiani
Asst. Professor in I.T Dept.
G.H.R.C.E.M. , Wagholi
Savitribai Phule Pune University, India

ABSTRACT
Data aggregation is very important techniques in wireless sensor network. Data aggregations reduce the energy consumption by eliminating redundancy. In this paper the data aggregation approaches based on the routing protocols and algorithm. Data aggregation is basically used to collect and aggregate data in an energy efficient manner so that network lifetime is improved. Data aggregation protocols aims at eliminating redundant data transmission. The data aggregation is a method used to solve the overlap problems in data centric routing. Data aggregation is the process of collecting and aggregating the useful data. Data aggregation is considered as one of the essential procedures for saving the energy.

General Terms
Your general terms must be any term which can be used for general classification of the submitted material such as Pattern Recognition, Security, Algorithms et. al.

Keywords
Wireless sensor network, Data aggregation, Data aggregation algorithm, Security..

1. INTRODUCTION
The wireless sensor network is ad-hoc network. Sensor nodes consists small light weighted wireless nodes, deployed in physical or environmental condition. Sensor nodes measured physical parameters such as sound, pressure, humidity and temperature. These sensor nodes deployed in huge or thousand numbers also collaborate to form an ad hoc network capable of coverage to data collection sink i.e. base station. Wireless sensor network have different applications like environment monitoring, building monitoring, health monitoring and target tracking. However wireless sensor network is a resource limitation if talk about energy, computation, memory and limited communication capabilities. All sensor nodes in the wireless sensor network are relate with each other or by intermediate sensor nodes.

With advance in technology, sensor networks collected of small and cost effective sensing devices prepared with wireless radio transceiver for environment monitoring have become possible. The key advantage of using these small devices to monitor the environment is that it does not need infrastructure such as electric mains for power supply and wired lines for Internet connections to gather data, no need human interaction while deploying. These sensor nodes can monitor the environment by collecting information from their environment, and work kindly to send the data to a base station, or sink, for analysis.

2. RELATED WORK:
In [2] paper, shown a security vulnerability in the CPDA protocol, in which have recognized how a malicious sensor node in a WSN can exploit the protocol in such a way that it gets access to the private aware values of its adjacent nodes while data aggregation process takes place in an aggregator. Also proposed an appropriate modification of the CPDA protocol to build it robust against this openness and also to make it computationally more efficient.

In [3] paper, introduced a novel collusion attack situation against a number of existing IF algorithms. Moreover, proposed an enhancement for the IF algorithms by providing an initial approximation of the reliability of sensor nodes which makes the algorithms not only collusion strong, but also more accurate as well as faster converging.

In[4] provide a solution for node capture attack. Node capture attacks result from the combination of active, passive and physical attacks by an intelligent adversary. In order to initialize or set up a node capture attack, the adversary will collect information about the WSN by eavesdropping on message exchanges, either local to a single adversarial device or throughout the network with the aid of a number of adversarial devices deployed throughout the network.

In [5]are discussing the security vulnerabilities of data aggregation for systems, and present a survey of robust and secure aggregation protocols that are resilient to false data injection attacks**.** This paper provides a detailed review of secure data aggregation concept in the wireless sensor networks. To give the motivation behind the secure data aggregation, first, the security requirements of wireless sensor networks are presented and the relationships between data aggregation concept and these security requirements are explained.

3. PROPOSED SYSTEM
Data aggregation process is performed by particular routing protocol. To minimize the energy consumption it is the main goal of aggregating the data. So sensor nodes should route packets based on the data packet content also select the next hop in order to support in network aggregation. The process of aggregating the data from many sensors to reduce unnecessary transmission and provide combined information to the base station is called as Data aggregation.

3.1 Data Aggregation: An Outline
Data aggregation is a method of aggregating the sensor data using aggregation approaches. The algorithm uses the sensor data from the sensor node and then aggregates the data by using some aggregation algorithms such as LEACH (low energy adaptive clustering hierarchy), centralized approach, TAG(Tiny Aggregation) etc. This aggregated data is transfer to the sink node by selecting the efficient path.

3.1.1. In-Network Aggregation:
In-network aggregation is the in general process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of

falling resource utilization, thereby increasing network lifetime.

There are two basic approaches for in-network aggregation:

a) With size reduction

b) Without size reduction.

- With size Reduction:

In-network aggregation with size reduction refers to the process of combining as well as compressing the data packets received by a node from its neighbors in order to reduce the packet length to be transmitted or forwarded towards sink.

- Without Size Reduction:

It refers to the process integration data packets received from different neighbors in to a single data packet but without processing the value of data.

3.1.2. Tree Based Approach:

The tree based approach is defining aggregation from constructing an aggregation tree. Tree structure is minimum spanning tree, sink node observe as a root and source node consider as a leaves. Information developed of data start from leaves node up to root means sink node(base station).

Disadvantage of this approach, as known similar to wireless sensor network are not free of charge from crash(failure). In case of data packet failure at any level of tree, the data will be missing not only for single level but also for entire connected sub tree also. This approach is suitable for designing optimal aggregation techniques data centric protocol known as Tiny aggregation (TAG) approach.

The functioning of TAG is depending on two phases:

a) Distributed phase

b) Collection phase

- Distributed Phase:

In distributed phase, in which aggregate or cooperative queries are pushed down into the network.

- Collection Phase:

A collection phase, where the aggregate values are frequently routed up from children to Parents means leaf node to root node.

3.1.3. Cluster-Based Approach:

In energy-constrained sensor networks of huge size, it is inadequate for sensors to transmit the data straightforwardly to the sink. In such scenarios, hierarchical approach called as Cluster based approach. In cluster-based approach, entire network is divided in to a few clusters. Each cluster has a cluster-head which is selected between cluster members. Cluster-heads perform the task of aggregator which aggregate data received from cluster members nearby and then transmit the result to base station (sink).

Now the sensor nodes within a cluster either use direct link or data communicate link to send their data to cluster head which is an energy efficient method. The cluster head aggregates data at forwarding time to another data communicate point or cluster head.

3.1.4. Multi-Path Approach:

The drawback of tree based approach is the limited strength of the system. To overcome this disadvantage, a new approach was proposed by many researchers. In which sending partially aggregated data to single parent node that is Root node in aggregation tree, a node could send data above various paths. In which each and every node can transmitted data packets to its possibly many neighbor's. So data packet flow from source node to the sink node along multiple path, lot of intermediary node between source node to sink node so aggregation done in every intermediate node. Using this approach build the system strong but some further transparency. The illustration of this approach like ring topology, where network is separated in to concentric circle with important rank levels according to hop distance from sink.

The problem with this approach is that it may reason the arising of hot spots and nodes along favored paths will consume their energy resources rapidly, probably causing disconnection in the network.

Protocol/ Algorithm	**Tree**	**Cluster**	**Multipath**	**Hybrid**
TAG	✓			
Directed Diffusion	✓			
DB-MAC	✓			
LEACH		✓		
Diffusion			✓	
Tributaries and Deltas				✓

Table 1- Routing protocol for Tree, cluster, Multipath and Hybrid approach.

4. SECURITY ISSUES IN DATA AGGREGATION

Security in data transmission and aggregation is an important issue to be considered while designing sensor networks. In lots of applications, sensors are deployed in open environments and prone to physical attacks which might compromise the sensor's cryptographic keys. Secure aggregation of information is a challenging task if the data aggregates and sensors are malicious. In this subsection, describe some recent work which solve the secure data aggregation problem and also discuss some of the main issues involved in implementing security in sensor networks.

5. CONCLUSION AND FUTURE WORK:

In this paper studied the most important parts of data aggregation in sensor networks is different from other wireless networks. Wireless sensor networks are power controlled network. The process of data aggregation is most important issue and optimization is needed to energy consumed for sending and receiving. Efficient data aggregations provide energy preservation as well as remove redundancy data. Security is another important issue in data aggregation applications and has been largely unexplored. Integrating security as an essential component of data aggregation protocols is an interesting problem for future research. Data aggregation in dynamic environments presents several challenges and is worth exploring in the future.

6. ACKNOWLEDGMENTS

I would like to sincerely thank Ms. Simran Khiani for her advice and guidance at the start of this paper. Her guidance has also been essential during some steps of this paper and her quick invaluable insights have always been very helpful.

7. REFERENCES

[1] Lu, Student Member, IEEE, Jie Li, Senior Member, IEEE, and Mohsen Huang Guizan," *Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE transactions on parallel and distributed systems*,vol. 25,NO. 3,MARCH 2014.

[2] Jaydip Sen ,"Secure and Energy-Efficient Data Aggregation in Wireless Sensor Networks", Member ACM Kolkata, INDIA

[3] Mohsen Rezvani, Aleksandar Ignjatovic, Elisa Bertino, Fellow, 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) 1545-5971 (c) 2013 .

[4] Shaik Nagul Shareef, Syed Sadat Ali, "Secure and Efficient Hierarchical Data Aggregation in Wireless Sensor Networks", International Journal of Modern Engineering Research (IJMER), Vol. 3, Issue. 4, Jul - Aug. 2013.

[5] Miriyala Markandeyulu and Guttikonda Prashanti, "Secure Reference Based Data Aggregation Protocol for Wireless Sensor Networks ",International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 7, July 2013

[6] Sridhar Sharma , "A Survey of Hierarchical Routing Protocols in Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, Volume 3, Issue 12, December 2013.

[7] Hichem Sedjelmaci and Mohamed Feham "A Novel Hybrid Intrusion Detection System for Clustered Wireless Sensor networks", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011

[8] Laiali Almazaydeh, Eman Abdelfattah, Manal Al- Bzoor, and Amer Al- Rahayfeh"Performance Evaluation of LEACH Protocol in Wireless Network", International Journal of Scientific & Engineering Research, Volume 2, April-2010.

[9] Jun Zheng, Senior Member, Pu Wang, and Cheng Li,"Distributed Data Aggregation Using Slepian–Wolf Coding in Cluster-Based Wireless Sensor Networks", IEEE transactions on vehicular technology, vol. 59, no. 5, June 2010.

[10] Andrea Gabrielli, Luigi V. Mancini, Sanjeev Setia, and Sushil Jajodia, "Securing Topology Maintenance Protocols for Sensor Networks",Universita' degli Studi di Roma "La Sapienza" Dottorato di Ricerca in Informatica XXII Ciclo –2009.