Indian Journal of Advancd Research in Electrical, Electronics and Instumentation Engineering (IJAREEIE)
Vol.2.No.1 2014 pp 23-27.
available at: www.goniv.com
Paper Received :08-03-2014
Paper Accepted:22-03-2013
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

STUDY ON AGGREGATION BASED TRUSTED ROUTING SCHEME FOR WSN

Kalaiarasi.M, Velmurugan.N
Saveetha Engineering College
Chennai, India
arasikalai300@gmail.com velmurugann@yahoo.com

ABSTRACT

Effective utilization of resources is a critical issue in large scale dense Wireless Sensor Networks (WSNs). Due to the high concentration of nodes in these networks, there is more possibility of redundant data. Since energy preservation is a major question in WSNs, data fusion and aggregation should be subjugated in order to save energy. Thus surplus data can be aggregated at in-between nodes, reducing the communication cost and energy consumption by decreasing the number of messages transmitted among sensor nodes. The proposed work uses In-Network data aggregation and energy saving protocol (LEACH) to conserve energy in WSNs. In aggregation process, providing security and integrity of aggregated data while routing is a challenging task. The security can be provided by calculating the trust value among the cluster heads and cluster members based on their node's identities, in order to identify malicious nodes within clusters. The results produced by our proposed work provide an optimal solution for the energy consumption and security problems in WSNs.

Keywords: *LEACH*, In-Network data aggregation, trust value.

1. INTRODUCTION

The wireless sensor network is ad-hoc network. It comprises of undersized, light weighted wireless nodes entitled sensor nodes deployed in substantial or environmental condition. And they can be used to quantify corporal parameters such as sound, force, temperature, and humidity. These sensor nodes deployed in large numbers and collaborate to form an ad hoc network, capable of reporting data to sink (base station). Wireless sensor network have a range of uses like habitat scrutinizing, building screening, human wellbeing monitoring, military survival lance and target tracking. However the nodes in the wireless sensor network are resource restraint, since they are limited by means of energy, computation and memory etc. All sensor nodes in the wireless sensor network can interact with each other directly or by intermediate sensor nodes.

With advance in technology, sensor networks poised of diminutive and cost effective sensing devices equipped with wireless radio transceiver for environment monitoring have become feasible. The key advantage of using these small devices to monitor the environment is that it neither involve infrastructure such as electric mains for power supply and agitated lines for internet links to accumulate data, nor need human interaction while deploying. These sensor nodes can monitor the environment by collecting information from their surroundings, and work cooperatively to send the data to a base station, or sink, for analysis.

2. BACKGROUND

A. Cluster Based Approaches

In energy-restrained sensor networks of huge size, it is incompetent for sensors to transmit the data openly to the sink. In such circumstances, Cluster based approach is one of the best approaches. In cluster-based approach, entire network is divided in to numerous clusters. Each cluster has a cluster-head which is preferred among cluster members. Cluster-heads achieve the task of aggregator which aggregate data received from cluster members locally and then transmit the result to base station (sink). Recently, numerous cluster-based network association and data-aggregation protocols have been anticipated for the wireless sensor network.

B. Data Aggregation: An overview

Data aggregation is a process of aggregating the sensor data by means of aggregation approaches. The wide-ranging data aggregation algorithm works as shown in the below figure.

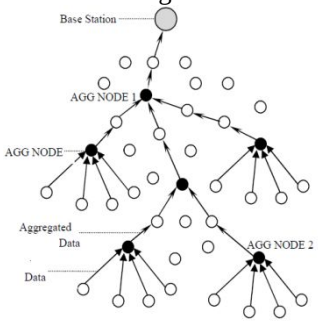

Figure. 1 Data aggregation process in wireless sensor network

The algorithm employs the sensor data from the sensor node and then combines the data by using some aggregation algorithms and shift this aggregated data to the sink node by selecting the proficient path.

In-Network Aggregation: In-network aggregation is the universal practice of gathering and routing information through a multi-hop network, processing data at midway nodes with the objective of reducing resource utilization (in particular energy), thereby increasing network lifetime.

There are two procedures available to achieve in-network aggregation:

1) With size diminution
2) Without size diminution.

With size diminution: In-network aggregation with size diminution refers to the method of merging and squeezing the data packets acknowledged by a node from its neighbours in order to trim down the packet length to be transmitted or forwarded in the direction of sink

Without size diminution: In-network aggregation without size diminution refers to the course of merging data packets expected from diverse neighbours in to a single data packet but without processing the value of data.

3. RELATED WORK

This section discusses about the importance of data aggregation, security and energy saving protocols in wireless sensor networks and also gives a brief description about some of the earlier investigations carried out in the above mentioned topics.

A. Survey of Data Aggregation Based Approaches

Data aggregation practices intends at eliminating unneeded data transmission and thus advance the life span of energy guarded wireless sensor network. In wireless sensor network, data transmission took place in multi-hop style where every node forwards its data to the neighbour node which is closer to sink. Since closely placed nodes may sense same data, the existing approaches cannot be considered as energy efficient. An enhancement over the existing tree based approaches would be clustering where each node sends data to cluster-head (CH) and then cluster-head carry out aggregation on the received raw data and then send it to sink.

More number of data aggregation responsive routing protocols has been proposed for wireless sensor network (WSN) [1], [7], [11] in recent years. All of them are aiming at aggregating quality not on energy conservation and security.

B. Importance of Security in Wireless Sensor Network

Preserving the security, integrity of aggregated data and avoiding the malicious nodes to be selected as forwarding nodes in the routing tree, are the two major challenges in wireless sensor network. If malicious nodes are selected as collaborative nodes then they can modify the data or repair the routing links so that there may be high possibility for insecurity in the network environment. So that security of data and several trust parameters should also be considered while designing the routing protocol for wireless sensor network. The previous work regarding security in WSN was discussed in [3], which provides better security but needs flooding of messages throughout the network which increases the communication among sensor nodes and energy consumption.

C. Energy Saving Protocols in Wireless Sensor Network

Extensive number of energy saving protocols available for wireless sensor networks [2], [9] and [10]. Each of them has its own benefits. For example Directed Diffusion is a data centric routing protocol used in wireless sensor network which can be used to save energy of sensor nodes by tracking the exchanges among the sensor nodes positioned in a particular network locality. But choosing the routing protocol that supports the data aggregation and overcomes security issues is a major challenge.

4. EXISTING WORK

In the existing system [1], it uses the Data Routing for In-Network Aggregation (DRINA) algorithm that decreases the communication cost and the energy consumption. It mainly concentrates on the network lifetime. The routing tree built by DRINA provides the best aggregation quality when compared to existing Information Fusion-based Role Assignment (InFRA) and Shortest Path Tree (SPT) algorithms.It

does not provide Trust management between the cluster members and cluster heads. The cluster head or member may select malicious nodes as collaborative nodes while using the existing algorithm. It provides less security. The communication overhead occurs in the existing system is very high.

5. DATA AGGREGATION AND TRUST

Proposed system implements the routing algorithm which combines the benefits of In-Network data aggregation and energy saving protocol for wireless sensor network called LEACH (Low Energy Adaptive Clustering Hierarchy). The security and integrity of data can be achieved through the trust decision making among both cluster head and cluster members. The proposed system uses In-Network data aggregation protocol to achieve reliable data aggregation and transmission. Additionally it includes trust decision making scheme based on the node's identities in order to provide secure data transfer among sensor nodes. It also ensures efficient and effective data gathering with a minimum use of resources, by eliminating redundancy and decreases the number of transmissions among sensor nodes. It also facilitates large energy saving and extends the network lifetime in wireless sensor networks.

A. System Architecture

The following figure illustrates the system architecture for the proposed system. It includes the clustering and aggregation process of sensor data and explains the efficient ways for transferring the aggregate data to sink node in a secured manner by using the trust value calculation mechanism.

For aggregation purpose it uses three timing strategies namely, periodic simple aggregation, periodic per-hop aggregation, periodic per-hop adjusted aggregation and cluster formation in the proposed system takes place according to LEACH protocol. The security of aggregated data must be ensured in wireless sensor network, since there are more possibilities available for the cluster heads (CH) or cluster members (CM) for choosing malicious nodes as collaborative nodes. In order to overcome this problem an effective trust based routing has been recommended here.

The trust value is calculated based on various trust parameters and trust is provided at both levels namely CH level and CM level.

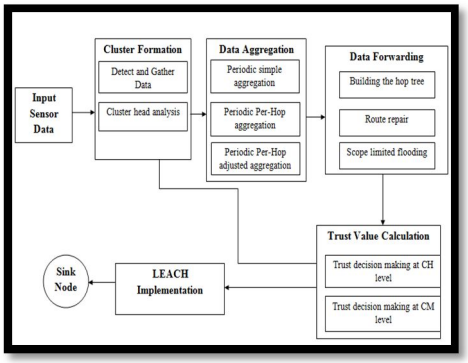

Figure. 2 Proposed System Architechture

In this paper we propose a data aggregation aware routing protocol which uses the obtainable processing capacity afforded by the intermediate sensor nodes beside the routing paths. There are various challenges arise while designing the routing protocol for WSNs. Some of them are guaranteed delivery of the sensed data even in the existence of nodes failures or interruptions in interactions, ensuring the security and integrity of aggregated data, effective route repair mechanism when path failure occurs and providing security to data from malicious nodes. For these purposes the proposed protocol combines the benefits of In-Network Data aggregation aware routing protocol (DRINA) [1] with the concept of LEACH [7] for the purpose of energy saving in WSN. And it also comprises a trust system which offers the security of data in and outside the clusters.

B. ***Sensor Node Configuration***

In this phase the distance from the sink to each node is calculated. Properties of particular sensor node are defined in this module. The properties include node position, transmission range etc. The distance from one node to another node in a particular cluster is also calculated.

C. Cluster Formation and Data Aggregation

A network setup is done by a number of clusters. Grouping of sensor nodes are known as clustering. Each cluster elects a cluster head from its member nodes. The cluster head selection is based on high energy. The data sensed by the member sensor nodes are transmitted to the cluster head where aggregation takes place. Then the data is transmitted to the base station from each cluster head of different clusters. Data sensed by the member nodes are passed to its own cluster head respectively. Data aggregation is the computation of data sensed by the nodes with the corresponding aggregation functions (e.g., max, count, average or median).

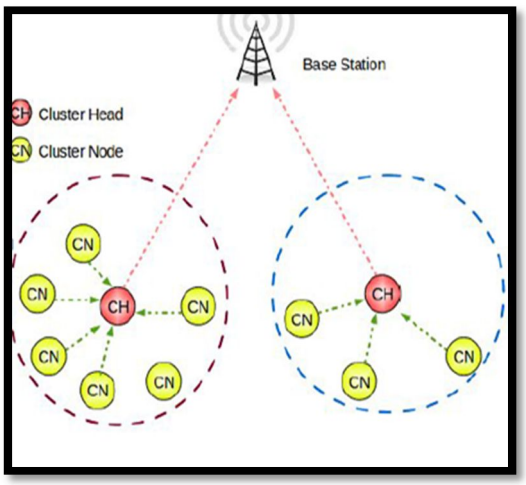

Figure. 3 Simple Cluster formation in wireless sensor networks

Proposed aggregation algorithm eliminates redundant data transmission and flooding of messages to whole network when a new event occurs. It uses 3 main timing strategies for data aggregation, simple aggregation, per-hop aggregation and per-hop adjusted aggregation. Thus by using these schemes the proposed work increases the aggregation points and avoids redundant data communication.

D. Routing Method

The routing tree is built by sending the Hop Configuration Message (HCM) from sink node, which contains ID, HopToTree to all other nodes in the network. After the group leader (cluster head) is elected, it sends a route establishment message to its NextHop node. The retransmission of route establishment message occurs until it reaches the sink node or a node that is part of an already established route. The proposed routing protocol uses a piggybacked, ACK supported route refurbish system which consists of two parts: failure detection at the NextHop node and selection of a new NextHop. Once the routing tree is established the route establishment message transferred during route repair mechanism contains the calculated trust value in order to ensure the security.

E. Trust Value Calculation

The purpose of this phase is to establish a trust-based framework for clustered WSNs. For establishing the trust between Cluster Heads (CH) and Cluster Members (CM), two types of trust are considered. They are direct trust which is based on (DTD- Direct Trust Degree) and feedback trust (ITD-Indirect Trust Degree). The direct trust is evaluated based on the successful/ unsuccessful interactions or message exchanges among the cluster members in wireless sensor network and feedback trust is evaluated based on the value of ITD set by the CH for the specific cluster member. These trust values can be used to provide security at both intra-cluster (CM level) and inter-cluster (CH level). Several trust parameters and metrics can be used to calculate the trust value such as, Transmission range, packet loss, energy consumption, latency, path quality, spot of the nodes, hop count, signal to noise ratio (SNR), bit error rate (BER). Thus the trust value ensures the integrity of aggregated data transferred along sensor nodes.

F. LEACH Implementation

LEACH (Low-Energy Adaptive Clustering Hierarchy) offers localized control and low energy consumption for data transfer in wireless sensor network. It includes cluster-head rotation to evenly distribute the energy load. The Cluster head coordinates transmissions using TDMA (Time Division Multiple Access) schedule. The main benefit of using LEACH algorithm is, it avoids collisions between nodes while data communication since each node (cluster member has a predefined TDMA schedule provided by its appropriate cluster head.

6. CONCLUSION

Thus the proposed routing protocol can achieve a better performance than the existing routing protocols used for wireless sensor networks. Results indicate that the proposed routing protocol provides superior aggregation feature than the previous aggregation aware routing protocols. It increases the network lifetime and ensures the security and integrity of the data transferred along the sensor nodes.

It avoids taking malicious nodes as collaborative nodes by calculating the trust value for each cluster member and cluster head based on various trust parameters. The future work may be based on increasing the aggregation quality of data when there is large number of nodes present in a single cluster and reducing the waiting time needed for aggregation. Also modify the proposed routing algorithm to select nodes that will be part of the communication structure in order to find a balance between overhead and aggregation quality.

ACKNOWLEDGMENT

The authors desire to express their sincere gratitude to all the anonymous assessors for their precious suggestions and comments which encouraged us towards new scope in our research.

REFERENCES

[1] Leandro Aparecido Villas, Azzedine Boukerche, Heitor Soares Ramos, “DRINA: A Lightweight and Reliable Routing Approach for In-Network Aggregation in Wireless Sensor Networks,” IEEE Transactions on computers, vol 62, no 4, 2013.

[2] Ali Norouzi et al., "A Comparative Study based on Power Usage Performance For Routing Protocols in Wireless Sensor Network," IEEE Transactions on Parallel and Distributed Systems, 2013.

[3] Fenye Bao, Ing-Ray Chen, MoonJeong Chang, and Jin-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," IEEE Transactions on Network and Service Management, vol. 9, no. 2, 2012.

[4] Hady S. AbdelSalam and Stephan Olariu, "A Lightweight Skeleton Construction Algorithm for Self-Organizing Sensor Networks," IEEE Transactions on Computers, 2012.

[5] Behrouz Maham, Hjørungnes, Senior Member, and Ravi Narasimhan, "Energy- Efficient Space-Time Coded Cooperation in Outage-Restricted Multihop Wireless Networks," IEEE on communications, vol. 59, no. 11, 2011.

[6] Gao.T, R. Jin, T. Xu, and L. Wang, "Energy-Efficient Hierarchical Routing for Wireless Sensor Networks," Adhoc & Sensor Wireless Networks, vol. 11, pp. 35-72, 2011.

[7] Kiran Maraiya, Kamal Kant, Nitin Gupta, "Wireless Sensor Network: A Review on Data Aggregation," International Journal of Scientific & Engineering Research, vol2, April, 2011.

[8] N.Karthik et al., "Trust calculation in wireless sensor networks," IEEE, 2011.

[9] Halabi Hasbullah, Babar Nazir, "Region-based Energy-aware Cluster (REC) for Efficient Packet Forwarding in WSN," IEEE transaction, 2010.

[10] Anastasi.G et al., "Energy Conservation in Wireless Sensor Networks: A Survey," Ad Hoc Networks, vol. 7, no. 3, pp. 537-568, 2009.

[11] Fan.K, S. Liu, and P. Sinha, "Scalable Data Aggregation for Dynamic Events in Sensor Networks," Proc. ACM Fourth Int'l Conf. Embedded Networked Sensor Systems (SenSys '06), 2006.