ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Secure Data Aggregation Using Fussy Logic in Cluster-Based Wireless Sensor Network

Rachana B.S[*1], Nita Meshram[2]
[*1,2] Lecturer, Department of ISE, APSCE, Bangalore, India
rachanabs9@gmail.com

Abstract

Recent advances in wireless sensor network (WSN) have led to many new promising application including monitoring and target tracking. However data communication between nodes consumes a large portion of energy consumption of wsn.Data aggregation can help to reduce the energy consumption by eliminating redundant data travelling back to base station. In order to provide integrity and to overcome from communication overhead, we propose data aggregation technique using fussy logic. In phase 1 In its first phase, it performs clustering and cluster head selection process. In Phase 2 we do the Distance estimation. In phase 3 fuzzy logic technique was used to select the secure node members for data aggregation.

Keywords: Wireless Sensor Network (WSN), Data aggregation, Fuzzy logic, Cluster head (CH), Dijistraks.

Introduction

A Wireless Sensor Network (WSN) typically consists of a sink node sometimes referred to as a Base Station and a number of small wireless sensor nodes. The base station is assumed to be secure with unlimited available energy while the sensor nodes are assumed to be unsecured with limited available energy. The sensor nodes monitor a geographical area and collect sensory information. Sensory information is communicated to the Base Station through Wireless hop by hop transmissions. To conserve energy this information is aggregated at intermediate sensor nodes by applying a suitable aggregation function on the received data.

Aggregation reduces the amount of network traffic which helps to reduce energy consumption on sensor nodes. Usually in a sensor network thousand of sensor nodes are deployed for area monitoring. Most of them sense the environment and send the data to the base station and at base station and we have to combine all the information for the desired output. If we aggregate the data before reaching the base station we can potentially decrease the number of packets in the network so we will have to send less number of packets to base station and that can save the energy of sensor nodes. These types of data aggregation are called In-Network data aggregation Where packets are combined before reaching the base station. Elena Fosolo al. in [1] defines the in-network aggregation process as follows: "In-network aggregation is the global process of gathering and routing information through a multi-hop network, processing data at intermediate nodes with the objective of reducing resource consumption (in particular energy), thereby increasing network lifetime."

The remainder of this paper is organized as follows: section II describes related work, section III describes problem statement and solution, section IV describes proposed work, section V describes results, section VI describes conclusion.

Related Work

In energy-constrained sensor networks of large size, it is inefficient for sensors to transmit the data directly to the sink. In such scenarios, sensors can transmit data to a local aggregator or cluster head which aggregates data from all the sensors in its cluster and transmits the concise digest to the sink. This results in significant energy savings for the energy constrained sensors. The cluster heads can communicate with the sink directly via long range transmissions or multihoping through other cluster heads. Recently, several cluster based network organization and data aggregation protocols have been proposed. In this section we discuss various clustering protocols.

Leach

LEACH [2] protocol is the first clustering protocol. It provides a conception of round. LEACH protocol runs with many rounds. Each round contains two states: cluster setup state and steady state. In cluster setup state, it forms cluster in self-adaptive mode; in

ISSN: 2277-9655
Impact Factor: 1.852

steady state, it transfers data. The time of second state is usually longer than the time of first state for saving the protocol payload.

E-Leach

Fan el. Al. [2] proposes a new protocol Energy-Leach which improves the CH selection procedure. Like LEACH protocol, E-LEACH protocol also divided into rounds, in the first round, every node has the same probability to turn into CH, that mean nodes are randomly selected as CHs, in the next rounds, the residual energy of each node is different after one round communication and taken into account for the selection of the CHs. That mean nodes have more energy will become a CHs rather than nodes with less energy.

TL-Leach

In the LEACH protocol CH collects the information from cluster member nodes and after aggregation sends the information directly to the base station. CH might be located far away from the base station in that case it would be more energy consuming to send the information directly to the base station and CH will die quickly than other nodes. A new version of LEACH called Two-level Leach has been proposed in [3]. In this protocol; CH collects information from cluster member and in spite of sending it to directly base station it sends it to another CH that lie between the CH and BS as a relay station.

M-Leach

In LEACH CH sends the aggregated information directly to the base station that is more energy consuming. In M-LEACH [4] multi-hop communication is selected among CH. Then, according to the selected optimal path, these CHs transmit data to the corresponding CH which is nearest to BS. Finally, this CH sends data to BS. M-LEACH protocol is almost the same as LEACH protocol, only makes communication mode from single hop to multi-hop between CHs and BS.

Problem Statement and Solution

The following are the problem that we come across from previous work

- High communication overhead
- High complexity
- Consumes more bandwidth
- No proper method for minimizing the energy consumed
- No discussion about collective resolution for integrity and authentication.

In this, we propose to design a secure data aggregation algorithm. This algorithm consists of 3 phases. In phase1, the sensor nodes are grouped into various clusters and each cluster has one elected cluster head. The cluster head initially estimates the distance between each member and itself, by exchanging topology discovery packets. In phase2, the cluster head calculate the distance between each member and also exchanged the topology to discover the packets. Finally the Fuzzy Logic is used to select the best nodes for aggregation. The Parameters like distance from each node through cluster head as taken as input and fuzzy rules are formed. The rules are based on the output will be treated as the best node and worst node. The best nodes are aggregated with the cluster head ID, the data send to the base station. The Cluster Head ID is mentioned like the nodes are the best node in the network. The Remaining Worst nodes are eliminating in the network.

Proposed Work

This Paper detects the shortest path between the neighbor nodes in the network to transmit the energy and improve the network life time of the network using Fuzzy Logic. It includes three phases to improve the network performance.

Phase 1: Cluster head selection process

Each node decided based on a formula whether or not to become a CH for the current round.

$$T(n) = \frac{P}{1 - P \times (r \bmod P^{-1})} \quad \forall n \in G$$

$$T(n) = 0 \quad \forall n \notin G$$

Where n is a random number between 0 and 1
P is the cluster-head probability and
G is the set of nodes that weren't cluster-heads the previous rounds

Where variable p allow us to decide the desired percentage of CH node in the sensor population, r is the current round number and G is the set of nodes that have not been CHs in the last 1/p rounds. Now each node has to choose a random number "T" between 0 and 1. If the random number is less than the calculate threshold, this node will be a good candidate. After this, each node that is elected as a CH will send a broadcast message advertising all nodes

Phase 2. Neighbour Identification and identification of distance between the CH using dijkstra's

Network nodes are represented by the vertices and also direct connectivity between the nodes by the edges. Sensor nodes are maximum flow from one node to

ISSN: 2277-9655
Impact Factor: 1.852

the other node to calculate the distance. The Number of vertices are connected to the source node in a network is called its neighbor node and the number of edges are its size. Two or more edges of a network joining the same pair of vertices are called multiple edges and corresponding network is known as multipath network.

The distance between the CH is calculated using the following algorithm, the code u := vertex in *Q* with smallest dist[], searches for the vertex *u* in the vertex set *Q*that has the least dist[*u*] value. That vertex is removed from the set *Q* and returned to the user. dist_between (*u*, *v*) calculates the length between the two neighbor-nodes *u* and *v*. The variable *alt* is the length of the path from the root node to the neighbor node *v* if it were to go through *u*. If this path is shorter than the current shortest path recorded for *v*, that current path is replaced with this *alt* path. The previous array is populated with a pointer to the "next-hop" node on the source to get the shortest route to the source.

```
1 function Dijkstra(Graph, source):
2     for each vertex v in Graph:    // Initializations
3         dist[v]     := infinity;      // Mark distances from source to v as not yet computed
4         visited[v]   := false;        // Mark all nodes as unvisited
5         previous[v]  := undefined;    // Previous node in optimal path from source
6     end for
8     dist [source]:= 0;          // Distance from source to itself is zero
9     insert source into Q;       // Start off with the source node
10    while Q is not empty:       // the main loop
11        u: = vertex in Q with smallest distance in dist [] and has not been visited;
12        remove u from Q;
13        visited[u]:= true       // mark this node as visited
14        for each neighbor v of u:
15            alt: = dist[u] + dist_between(u, v);      // accumulate shortest dist from source
16            if alt < dist[v]:
17                dist[v]:= alt;      // keep the shortest dist from src to v
18                previous[v]:= u;
19                if! visited[v]:
20                    insert v into Q;    // Add unvisited v into the Q to be processed
21                end if
22            end if
23        end for
24    end while
25    return dist;
26 endfunction
26  endfunction
```

Phase 3. Fuzzy Logic

The degree of the input fundamental steps and condition of fuzzy logic are strong-minded. On the basis of the rule is gritty. The results are acquired every fuzzy rules are multiple together with single overall results. The fuzzy sets of A with a membership function of X rules are determined. Antecedent 1 and 2 are the low the consequent are high.

Distance (D) = { [BN, a], [WN, b] }

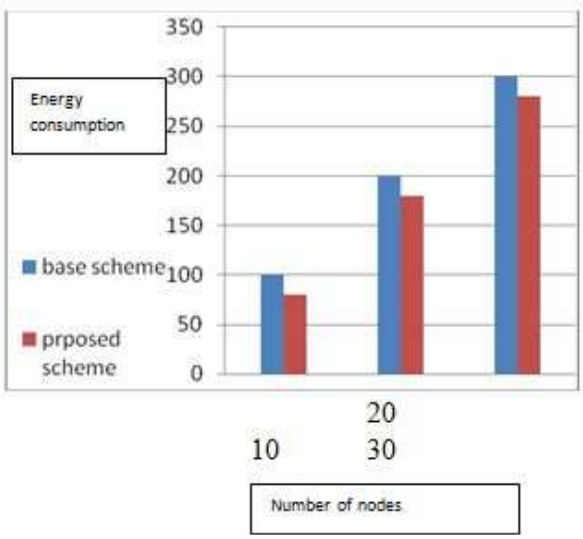
Where,
a-Fuzzy set membership grade Best Node in Cluster ID with distance calculation
b-Fuzzy set membership grade Worst Node in Cluster ID with distance calculation

Power Consumed (P)= { [BN, c], [WN, d] }

Where,
c-Fuzzy set membership grade Best Node in Cluster ID with energy consumption
d-Fuzzy set membership grade Worst Node in Cluster ID with energy consumption

Results

Figure below shows the network throughput in secured data aggregation using Fuzzy Logic *in Cluster-Based wireless sensor Network*



Conclusion

Our technique consists of three phases. In the first phase, the network is divided into clusters. The sensor nodes with the higher signal strength are selected as cluster head. In the second phase, using dijistraks algorithm the distance between the nodes and the cluster

ISSN: 2277-9655
Impact Factor: 1.852

head is calculated. Also the energy consumed by the member nodes in each cluster is determined. These parameters: distance, energy consumed value of the sensor nodes are used to determine if the sensor node can be used for data aggregation. In the third phase, we use fuzzy logic to select the best node. Finally the aggregated data is transferred by each cluster head to the sink. Since the values of malicious and faulty sensors are not aggregated, secure data aggregation is ensured in the wireless sensor network. We conclude that our technique has improved throughput with reduced packet drop and less energy consumption

References

[1] Fasolo E., Rossi M., Widmer J. and Zorzi M. (2007) *IEEE Wireless communication.*

[2] Fan Xiangning, Song Yulin (2007) *International Conference on Sensor Technologies and Applications.*

[3] Loscri V., Morabito G., Marano S. (2005) Vehicular Technology Conference, VTC- 2005, Volume: 3,1809-1813.

[4] Yuhua Liu, Yongfeng Zhao, Jingju Gao, (2009) *International Joint Conference on Artificial Intelligence.*

[5] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan (*2000*) *Energy Efficient Communication Protocol forWireless Microsensor Networks" Proceedings of the 33rd Hawaii International Conference on System Sciences – 2000.*

[6] Lindsey S., Raghavendra C. and Sivalingam K. M. (2002) *IEEE Trans. Parallel and Distributed Systems*, vol. 13, no. 9, 924–35.

[7] Min Ding, Xiuzhen Cheng, Guoliang Xue, (2006) *Proceeding Mobility '06 Proceedings of the 3rd international conference on Mobile technology, applications & systems, ISBN:1-59593-519 3, doi> 10.1145/ 1292331.1292391*

[8] Vaidhyanathan K. et al. (2004) *Technical Report, OSU-CISRC-11/04-TR60, Ohio State University.*