Enhancing Data Aggregation Technique for Wireless Sensor Networks

Gayathri R
Department of Information Technology
KCG College of Technology, Chennai

Kanaka S
Department of Information Technology
KCG College of Technology, Chennai

Abstract

As a sensor network collects the sensed data and transmits to the base station. As a sensor node drives more battery, highly usage of power is essential in order to use networks for long duration. Since to reduced data traffic inside sensor nodes and to reduce the amount of data in base station the data aggregation is performed. The main process of data aggregation is to aggregate the data in energy efficient manner so that network lifetime is increased. However such aggregation is known to be highly dangerous to node concentrated attacks. Iterative filtering algorithm provides solution for such a purpose. Such algorithms simultaneously aggregate data from various sources and provide trustworthiness of these sources, usually in a form of related weight factors assigned to data provided by each source. The angle based routing algorithm is used for shortest path identification and false data injection in nodes. Since secure data aggregation is performed from source to destination.

Keywords: Wireless sensor networks, data aggregation, path identification, false data injection

I. INTRODUCTION

A sensor network typically consists of a sink node and a number of small wireless sensor nodes. The sensor nodes monitor the environment and collect information from their surroundings, and works to send the data to a base station for analysis. The main aim of data aggregation algorithms is to aggregate data so that network lifetime is increased. Wireless sensor networks offer an high method of data gathering in distributed system architectures and dynamic access via wireless connectivity. Sensor networks are increasingly deployed for process such as wildlife habitat analysis, forest fire prevention, and military surveillance etc. In these process the data is collected by sensor nodes from their physical environment needs to be assembled in computer for further analysis. Thus, better algorithms are needed for data aggregation in the future WSN.
In this paper AB-protocol has the following key characteristics:

1) Frequent network topology changes can be handled
2) Dynamic discovery of destination
3) Scalable to size
4) minimizing the memory usage.

The nodes in the networks are usually not aware of their environmental positions. In ABR algorithm, neighbor positions of the nodes with respect to the network topology. In previous paper the data aggregation and trust value calculation has been performed in the basis of IF algorithm..In IF algorithm the false data is identified and since the path of false data injection has not been identified. In proposed system a protocol and related algorithm for finding the path of false data injection in aggregated nodes using (ABR) algorithm.

As discussed in above section, the false data injection, an effect of injected false data into the network to base station or depleting the energy resources of the relaying nodes. Several scholars have given solutions to save from false data injection attacks in sensor networks. The rest of the paper gives detail about the background and related work in the field; in further section we present proposed network and related algorithm for data aggregation and identifying the path of false data injection.
The algorithm finds the following:

- Severe vulnerability of IF algorithms is known.
- Estimation of sensors errors effective in a wide range of sensor error and not capable to the described attack.

The data aggregation algorithm is performed using Iterative Filtering Algorithm and the path of false data injection in aggregator node is done by using Angle Based Routing algorithm.

II. RELATED WORKS

The proposed Iterative Filtering (If) algorithm an attractive option for WSNs because they solve both problems

1) Data aggregation and data trustworthiness assessment
2) Using a single iterative procedure.[1]

A. Iterative filtering

Algorithm 1: Iterative filtering algorithm.
Input: X; n;m.
Output: The reputation vector r
l 0;
w (0) 1;
repeat
Compute r(l+1);
Compute d;
Compute w (l+1);
ll + 1;
Until reputation has converged;
Reciprocal: $g(d) = d^{-k}$;
Exponential: $g(d) = e^{-d}$;
Affine: g(d) = 1 kld, where kl > 0 is chosen so that $g(\max_i fd\{d^{(l)}\}) = 0$.

Algorithm illustrates the iterative computation of the reputation vector based on the above formulas. Such trustworthy calculates data of each sensor is based on the distance of a sensor node is measured by the true values, obtained in the previous round of iteration by some method of aggregation of the readings of all sensors. Such algorithm is assigned less trustable and consequently in the aggregation process in the present round of iteration their readings are given a lower weight .The vulnerability to have collusion attacks comes from the fact that these IF algorithms start the iterates the data, since same trust values are given to sensor nodes. Here we propose a solution for such attack by providing an initial trust values which is based on a robust calculation of errors of individual sensors. Here the false data is injected by a number of compromised nodes and the malicious attack takes place and since there is no solution for identifying the path of false data injection.

III. PROPOSED WORK

Here the process briefly describe the algorithm in the process of data aggregation in network and explain the algorithm for a possible false data injection. In proposed Routing algorithm, when a source node has a packet to send to other destination node and the node initiates destination to find a route; this node is known as initiator of the destination identified, destination of the packet is known as the target. The beginner transmits data Destination Request (DREQ) packet as a local data, denoting the target, unique identifier from the initiator and its position.

IF
The node is never received DREQ before
ELSE IF
The destination in its Neighbors table sends the DREQ to the destination
ELSE IF
The destination does not in the NT Rebroadcast DREQ by calculating the destination using angle (xd, yd, thread).
ELSE IF
Discards the DREQ
ELSE IF

The node is destination forwarding the DREQ and replies SREP to source by measuring the region of source by using angle of source (xs, ys, thetas). And the SREP (source Replay) is now consists both source and destination.

ELSE IF

A node on finding link failure there is no need of passing any error message to the final destination since the intermediate node only acts as a source and sends the packet to destination since false path is identified [2].

In the first stage an initial estimate of two noise parameters for sensor nodes, bias and variance details of the computations for estimating bias and variance of sensors nodes.

Based on such an estimation of the bias and variance of each sensor, the bias value is subtracted from sensors readings and in the next phase of the proposed framework. In the third stage of the proposed framework, the initial reputation vector in the next node is calculated and the trustworthiness.

B. Angle Based Routing

Analytical solutions for the expected path length in wireless sensor networks employing distance-based or angle-based based routing(ABR) algorithm. The underlay many practical routing protocols for wireless sensor networks in which nodes are aware of their environment locations and can use that information to simplify the routing local broadcast, specifying the target, unique identifier from the initiator and its position

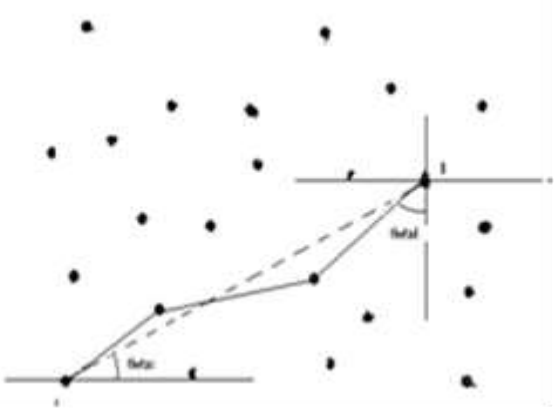

Fig. 31: Angle and direction between source and destination

In fig. 3.1 nodes are created and data is aggregated, reaches destination securely without any injection of false data. Neighbor nodes are discovered using ABR algorithm by specifying the angles [3].

C. Angle Calculation

a = x2 - x1;
b = y2 - y1;
Angle = Atan2 (a,b) * 180 / PI(2);
a=dx, b=dy
Where Atan=Arc tangent.

If the node has angle within 30° in the backward direction, then that node is selected else the node is not selected. Steps involved in optimizing the route to destination:

- Source transmits data in the network, where the neighbor node receives it.
- The intermediate node checks the angle for data transmission range to identify the shortest destination.
- If the node is destination, the data is transmitted, else move on the next hop and find the angle.
- If a single destination is identified the other destinations are found for sending data
- Same process is continued till data is transmitted to all the destinations.

D. Distance Calculation

A=2tan [y1-y2/x1-x2]
x1,x2,y1,y2 are x and y position of the algorithm, when a node has a packet to send to some destination The node initiates Destination Discovery to find a route and the destination of the packet is identified..

IV. IMPLEMENTATION

A. Node Creation

Node creation is the process of creating wireless nodes in the network scenario. The node is created and the node gathers sensor information and communicates with other node in a network.

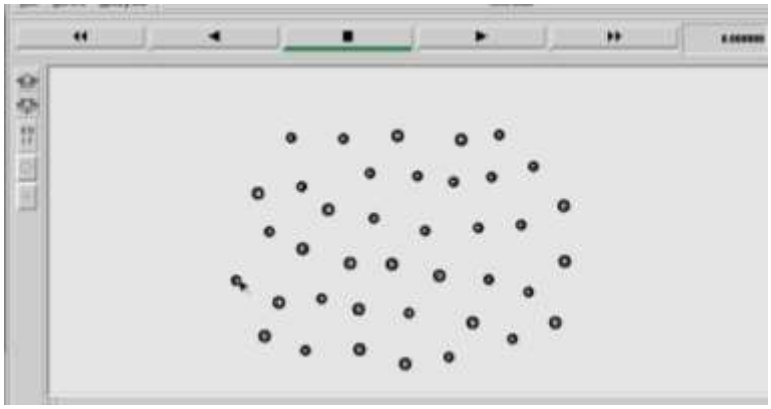

Fig. 4.1: Node Creation

In Fig 4.1 zero to thirty nine nodes are created using ns2 simulation.

B. Neighbor Discovery

Each wireless node finds its neighboring nodes, the ones that are within its transmitting range. Neighbor discovery is the determination of all nodes with which a given node may interact directly. On the other hand, neighbor discovery reveals all possible paths between any two nodes in a network. Neighbor discovery is achieved by the conditions specified in this paper using distance and the number of hops conditions.

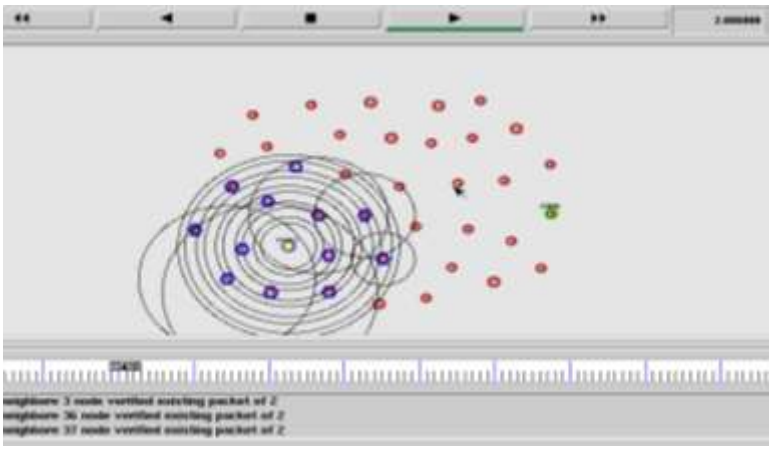

Fig. 4.2: Neighbour discovery

In Fig 4.2 nodes created are formed as a network. Source node will send the data to destination through the neighbour nodes to sender and destination (sink).

C. Data Aggregation

Data aggregation is a process of gathering the sensed data and giving the data as a summary to other node. The aggregated data is transferred within the node by selecting the required path.

V. PERFORMANCE ANALYSIS

The performance of the proposed scheme is analyzed by using the simulator(NS2).The NS2 is an open platform programming language written in c++.NS2 is a discrete event time driven simulator which is used to mainly model the network.

A. Trust Value Calculation

In fig 5.1 trust value is calculated using bias and variance of data aggregation technique in WSNs[1].

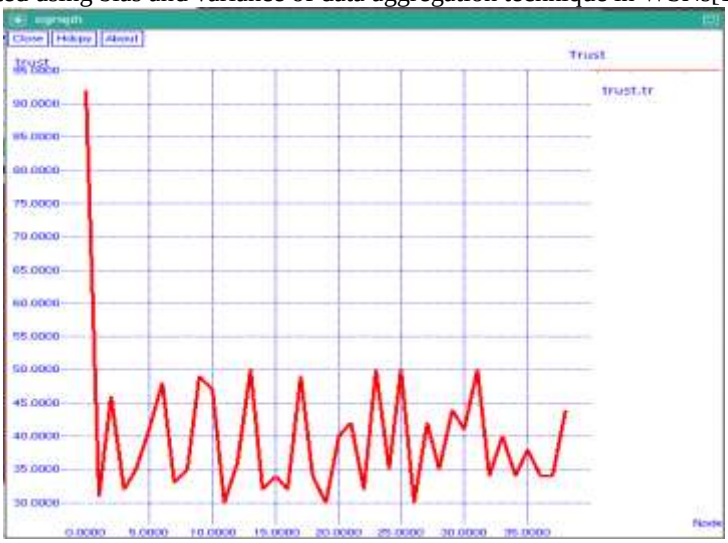

Fig. 5.1: calculating trust value

B. Packet Delivered Rate

Packet Delivered Rate (PDR) is the ratio of number of packets delivered to all receivers to the number of data packets sent by the source node. The packet received rate is calculated by the following graph.

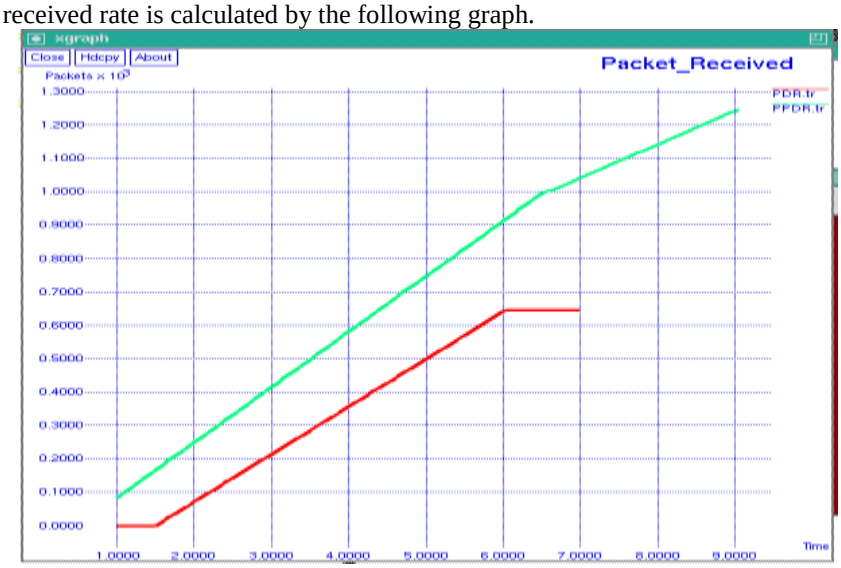

Fig. 5.2: Packet received

In fig 5.2 packets are received from source to destination, red colored line denotes the failure rate of packet received. The green colored line in the graph denotes the successful rate of packet send and received in source and destination using ABR algorithm.

C. Throughput

Throughput is one factor similar to that of the packet delivery rate. Maximum messages is achieved to the destination is measured by throughput. The average throughput is estimated using equation.

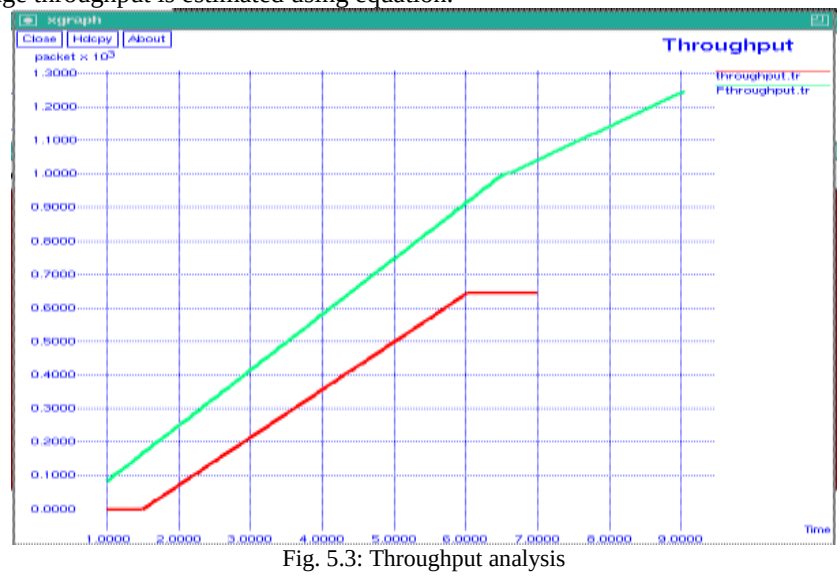

Fig. 5.3: Throughput analysis

In fig 5.3 throughput is calculated using formula mentioned in reference paper [3]

VI. RESULT

In ABR algorithm data aggregation is achieved using without false data injection. Sending data from the source to destination (sink) without data loss and delay.

VII. CONCLUSION

Data aggregation is very essential process. In proposed paper, angle based routing algorithm is used. In this algorithm the angle are provided to find the path of false data injection in a wireless sensor network since the network life time is increased. The benefit

of this method is to identify the path of fault occurred during the communication process between the nodes. Simulation output show that the proposed method has low packet loss ratio, packet delay and better packet delivery ratio and throughput.

VIII. FUTURE WORKS

In future, cryptographic method can be used for data aggregation. By using this method data can be sent more securely from source to destination.

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 transaction on dependable and secure computing(TDSC) ,volume 12,issue 1,2015,98-110.
[2] Suresh P, Maria Navin R, Venkatagiri J, Hemanth Kumar M P,"Angle based routing protocol for MANET", International journal of scientific engineering and research , 4,Volume2 ,issue 2 ,February 2014, 60-63
[3] B.Thendral K. Thiruvananda Sikamani "AMRA: Angle based Multicast Routing Algorithm for Wireless Mesh Networks", Indian Journal of Science and Technology , volume 8,issue 13, July2015, 1-8
[4] Sanjeev SETIA a,Sankardas ROYb and Sushil JAJODI b a Computer Science Department, George Mason University, Fairfax, VA, USAb Center for Secure Information Systems, George Mason University
[5] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru Department of Computer Science and CERIAS, Purdue University 305 N. University St.
[6] Rodrigo Roman, M. Carmen Fernandez-Gago, and Javier Lopez Department of Computer Science, University of Malaga, 29071, Malaga, Spain.