A Trust Framework for Fault-Tolerance Data Aggregation in Wireless Sensor Networks using Routing Protocol

Ms. Priyanka K. Mantur, Mrs. M. S. Kanamadi
Dept of Electronics and Communication Engineering
BLDEA'S CET
Vijaypur, India

***Abstract*— For wireless sensor networks(WSNs) deployed in noisy and unattended environments, It is necessary to establish a comprehensive framework that protects the accuracy of the gathered sensor information .Here considering data aggregation ,information trust and fault tolerance to increase the correctness and trust worthiness of collected information. Based on the multilayer aggregation architecture of WSNs, We developed trust based framework for data aggregation with data aggregation with fault tolerance with a goal to decrease the effect of erroneous data and facilitate measurable trustworthiness for aggregated results .Trust is an important aspect of decision making for the distributed computing applications such as electronic commerce and particularly influences the specification of security policy. There is often a level of trust associated with a relationship and there is a problem concerning representation of ignorance with respect to trust. By extracting statistical characteristics from different sources and extending Josang's trust model. According to trust transfer and trust combination rules designed in our framework, we derive the trust opinion of the sink node on the final aggregated result. Results obtained from both simulation study and experiments on a real WSN test bed demonstrate the validity and efficiency of our framework, which can significantly improve the quality of information as well as more precisely evaluate the trustworthiness of collected information.**

***Keywords*—WSN,framework,clustering,aggregation**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are useful in event detection systems monitoring of the changes of physical phenomena in the surrounding environments . But a common problem in such networks is information error and loss caused by components failure, external interference, wireless transmission error, and security threats such as fake data injection. Due to low reliability and hence accuracy of the data sensed by individual sensor nodes, collaboration among sensors is necessary for reliable event detection and prevention of faulty or fake reports[1]. For event detection with multimode collaboration, the common method is data aggregation , which is leveraged not only to reduce the throughput of transmission, thus saving energy effectively , but also to enhance the accuracy of event detection and avoid interference of the compromised nodes. Users of WSN applications are often concerned whether the aggregated results are trustworthy so as to reflect the real situation of the physical environment. Therefore, for aggregation-based event detection in environment monitoring systems, it is not only important to gather comprehensive data, but also to reduce the impact of faulty and fake data, thus providing trusted and fault tolerant data aggregation[2]. At the same time, the trustworthiness of aggregated results should be reported to the users for decision making. In other words, providing reliable data with measurable trust is the key issue in the design of WSNs in order to improve the quality of information (QoI). In a hierarchical environment monitoring system, sensor nodes collect the environment signals according to a certain sampling mechanism and report them to higher level sensor nodes (called aggregators). An aggregator and its direct children form an aggregation set. The aggregators forward the aggregated results to their higher level aggregators recursively, and eventually to the sink node[3]. Since the nodes participating in the process may be destroyed or the data may be corrupted manipulated, the aggregators and the sink node should have a mechanism to provide trustworthiness of aggregated results to the user.

With the proliferation in automated devices and the development in wireless technologies WSNs have gained worldwide attention in recent years[4]. WSNs as an exciting emerging domain of deeply networked systems of low-power wireless nodes with a tiny amount of CPU and memory for high resolution sensing of the environment.

II.REVIEW OF PREVIOUS WORK

A. *Problem Definition*

When the sensing part of a sensor node fails suddenly, the sampling value collected by the sensor changes accordingly, the node itself can judge the data abnormal immediately based on temporal correlation. In this case, comparing the reports from this sensor with those from its neighbors, the aggregator should determine the trustworthiness of this sensor still low and reduce the weight (contribution) to the aggregation process. This results in fault worthiness. Here we are used AODV routing protocol

Where the nodes can be deployed adhoc manner. Clustering technique also used.

B. *System Models*

- Sensor node: In an aggregation set, each sensor node is associated with a reputation representing the self-trustworthiness of its collected data.
- Aggregator: According to the spatial correlation among sensor nodes in an aggregation set, the aggregator determines the aggregation breadth, which is the number of children taking part in data aggregation.
- Sink node: The sink node receives the aggregated results from the lower level aggregators, fuses them to obtain the final report, and determines the resulting trustworthiness.
- Topology Module: This section contains description of functionality of the scripts used in building topology. This module involves building Wireless Network topology, topology consisting of mobile nodes, each node working with multiple channels.

III. Performance Analysis Module

This module performs processing of output result set to compute the various performance metrics required to analyze the performance of flow slice based routing. This module includes following Units

- AWK scripts to compute various performance metrics.
- Plotting graphs for the performance metric to analyze the performance.

Figure shows the Node Deployment Algorithm. The input to this algorithm contains Number of Nodes and Distance between Nodes. The output contains the map of Node ID and Position of Node.

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.

C. *Source model*

In WSNs, a source provides the original signal of the event. Sensors around it may capture the signal of the source. Usually, in the densely deployed WSNs, the location of the nodes with higher signal intensity can be regarded as the source location. Based on the spatial propagation features of signal, the source can be classified as the source without center or one with a center. The signal strength of the former is almost the same in the event region, such as temperature and humidity in a room.

B. Trust model

According to the self-data trust opinion and peer node trust opinion, the aggregator has to determine the peer data trust opinion on the reports provided by each sensor through transfer. Finally, the aggregator J can derive its self-data trust opinion on the aggregated result through trust combination.

D. *Self-Data Trust Opinion of Sensor Node*

A sensor node calculates its self-data trust opinion by judging whether the collected data conform to its source model. Take audio stream as an example.

E. *Peer Node Trust Opinion*

Sensor nodes in a neighborhood have high spatial correlation in their sensory data. We define aggregation breadth, to describe the spatial correlation. The aggregation breadth is used to illustrate the size of an aggregation set determined by the applications.

F. *Node Deployment Algorithm*

This algorithm is used for placement if the nodes in the network

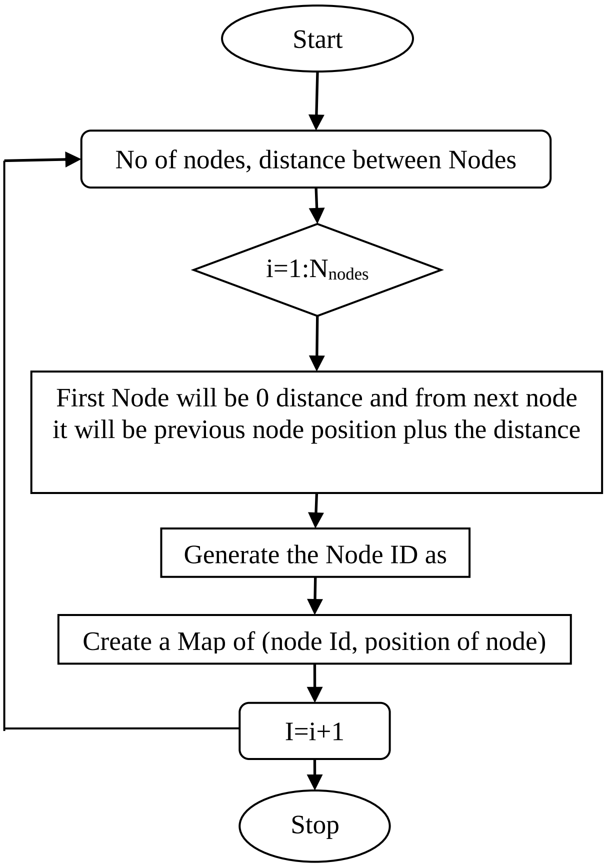
Start
No of nodes, distance between Nodes
i=1:N$_{nodes}$
First Node will be 0 distance and from next node it will be previous node position plus the distance
Generate the Node ID as
Create a Map of (node Id, position of node)
I=i+1
Stop

Fig 1. Node deployment algorithm

G. *Trust Transfer and Peer Data Trust Opinion*

Peer data trust opinion is the aggregator's trust opinion on

the report from a child in an aggregation set. When an aggregator receives a sensor's report, if the sensor believes the report with high confidence and the aggregator trusts this sensor, then the aggregator will also show high confidence in the sensor's report. However, if the aggregator has doubts about the sensor, it discredits the sensor's report regardless of the sensor's opinion.

H. *Trust Combination and Self-Data Trust Opinion of Aggregator*

In Josang's trust model, the trust consensus of two opinions is an opinion that reflects both opinions in a fair and equal way. For example, if two sensors have observed a target over two different time intervals, they might have different opinions about it depending on the behavior of the target in the respective periods.

Cluster architecture guarantees basic performance achievement in a WSN with a large number of sensor nodes. A cluster structure provides some direct benefits like spatial reuse of resources to increase the system capacity, with the nonoverlapping multicluster structure, two clusters may deploy the same frequency or code set if they are not neighboring clusters. Clusters also give performance enhancement in case of routing, because of the set of cluster heads normally form a virtual backbone for inter cluster routing. Clustering in WSNs is very challenging due to the inherent characteristics that distinguish these networks from other wireless networks like mobile ad hoc networks or cellular networks. First, due to the relatively large number of sensor nodes, it is difficult to identify every sensor and the sensed data. Furthermore, sensor nodes that are deployed in an ad hoc manner need to be self-organizing as the ad hoc deployment of these nodes requires the system to form connections between themselves.

I. *Cluster Head Election using Energy Efficiency*

This is used to choose one among a set of nodes in each cluster as a cluster head based on the remaining battery power. If all nodes have the same battery power then the node which is closer to the destination is chosen as the cluster head.

J. *Cluster head design*

Each cluster is controlled by a cluster-head, which is reachable to all nodes in its cluster, either directly or over multi-hop paths. Nodes that have links to peers in other clusters would serve as gateways. The presence of gateways between two clusters implies that the heads of these clusters are reachable to each other over multi-hop path and that these two clusters are considered neighbors..

K. *System Module*

Topology Module

This module involves building Wireless Network topology, topology consisting of mobile nodes, each node working with multiple channels.

Network design

An ad-hoc network is a collection of autonomous nodes that together set up a topology without the support of a physical networking infrastructure. Depending on the applications, an ad-hoc network may include up to a few hundreds or even a thousand nodes. Communications among nodes are via multihop routes using omni directional wireless broadcasts with limited transmission range. It is assumed that clusters are established securely by using pre-distributed public keys, employing a robust trust model, or applying identity based asymmetric key-pair cryptographic methods, and that a proper key management protocol is followed in order to perform reclustering when needed. Clustering is a popular architectural mechanism for enabling scalability of network management functions.

Energy Module

Energy Model, as implemented in, is a node attribute. The energy model represents level of energy in a mobile host. The energy model in a node has a initial value which is the level of energy the node has at the beginning of the simulation. This is known as initialEnergy_. It also has a given energy usage for every packet it transmits and receives. These are called txPower_ and rxPower.

The energy model only maintains the total energy and does not maintain radio states. It is generic enough for future simulations such as the CPU power consumption. Please note that the old energy model indeed maintains some radio states, and have some methods to manipulate them, and they are only used by the adaptive fidelity module. This approach may cause inconsistency with wireless-phy. To keep adaptive fidelity work, we did not remove it from the energy model, but it is obsolete, and should not be used further. Now all access to the energy model should go through wireless-phy.

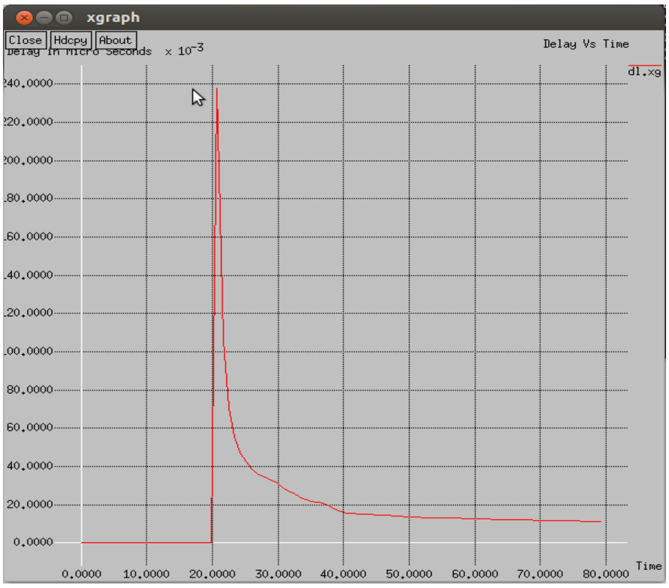

Fig 3 Delay graph

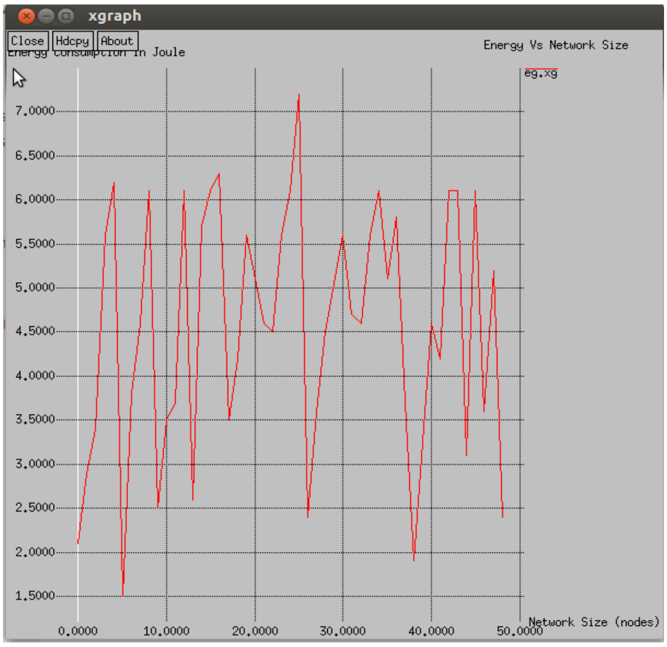

Fig 4.Energy graph

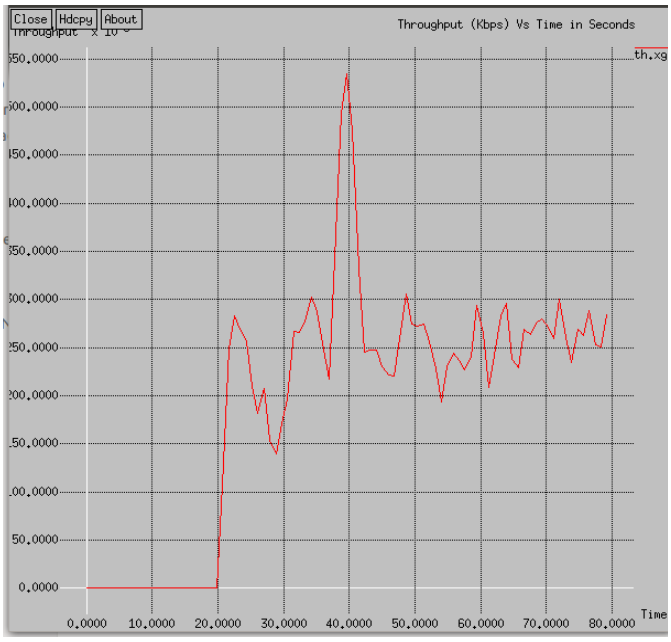

Fig 5.Throughput graph

VI. CONCLUSION

We are used various modules, algorithms and flowchart output result set to compute the various performance metrics required to analyze the performance of trust worthiness of nodes. Here comparing the reports from this sensor with those from its neighbors, the aggregator should determine the trustworthiness of this sensor still low and thus reduce the weight to the aggregation process. This framework can facilitate the functions of trust calculation, data aggregation, and information cleaning with minimal communication overhead and energy consumption. Hence, it is light weight and practical. On the contrary, in the proposed multilayer trustworthy aggregation architecture, we limit the communication only between the nodes in adjacent levels. Therefore, trust is calculated without recommendations from neighboring nodes. Furthermore, the self-data trust opinion can be transmitted along with the reporting data and without additional messages, so the data packet only needs two additional bytes for storing the opinion. The above graphs shows the how efficient is the network.

REFERENCES

[1] Yan Sun, Hong Luo, and Sajal K. Das,” A Trust-Based Framework for Fault-Tolerant Data Aggregation in Wireless Multimedia Sensor Networks,” IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, November/December 2012.

[2] H. Ma and D. Tao, “Multimedia Sensor Network and its Research Progresses,” J. Software, vol. 17, no. 9, pp. 2013-2028, Dec. 2006.

[3] H. Luo, Y. Liu, and S.K. Das, “Distributed Algorithm for Enroute Aggregation Decision in Wireless Sensor Networks,” IEEE Trans. Mobile Computing, vol. 8, no. 1, pp. 1-13, Aug. 2009.

[4] M.P. Michaelides and C.G. Panayiotou, “Snap: Fault Tolerant Event Location Estimation in Sensor Networks Using Binary Data,” IEEE Trans. Computers, vol. 58, no. 9, pp. 1185-1197, Sept. 2009.

[5] J.W. Ho, M. Wright, and S.K. Das, “Zonetrust: Fast Zone-Based Node Compromise Detection and Revocation in Wireless Sensor Networks Using Sequential Hypothesis Testing,” IEEE Trans. Dependable and Secure Computing,, vol. 9, no. 4, pp. 494-511, Dec.2012.