INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

To propose and implement cluster based technique to data aggregation for wireless sensor network

Shammi Kumar
shammi20940@gmail.com
L.R. Institute of Engineering and Technology, Solan, Himachal Pradesh

ABSTRACT

Wireless Sensor Network (WSN) are widely distributed sensors (nodes) to measure the change in physical and environmental conditions by sensing variations in temperature sound pressure etc., to achieve this purpose sensor nodes work together in a predetermined fashion to transfer the data to the main location (generally referred to as sink node). Modern networks are bi-directional making it easy for controlling the sensor activity. These nodes have computational and communication capabilities making them a good choice over conventional cables for operating in varied locations and harsh environments. So the aim of any data forwarding protocol is to conserve energy to maximize the network lifetime. Sensor nodes are capable of performing in-network aggregation of data coming from more than one source. In this paper, we have concentrated on energy consumption issue. Thus protocol using a cluster-based wireless sensor network is more relevant. Each cluster is executed independently and thus we obtain an energy efficient data, which finally is aggregated in a cluster by this the lifetime of the cluster is also increased.

Keywords: *WSN, Cluster node, Caching node*

1. INTRODUCTION

Wireless Sensor Networks (WSN) are widely distributed sensors (nodes) to measure the change in physical and environmental conditions by sensing variations in temperature sound pressure etc., to achieve this purpose sensor nodes work together in a predetermined fashion to transfer the data to the main location (generally referred to as sink node). Modern networks are bidirectionally making it easy for controlling the sensor activity. These nodes have computational and communication capabilities making them a good choice over conventional cables for operating in varied locations and harsh environments. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet.

Wireless networks can be classified into two types. These are defined as follows:

Infrastructure fewer Networks: The infrastructure less network does not need any infrastructure to work. In this network, each node can communicate directly with other nodes. So in this network, no access point is required for controlling medium access. Infrastructure fewer networks do not have fixed routers. In this network, all the nodes need to act as routers and all nodes are capable of movement and can be connected dynamically in an arbitrary manner. The outermost nodes are not within transmitter range of each other. However, the middle node can be used to forward packets between the outer most nodes. The middle node is acting as a router and the three nodes have formed an ad-hoc network.

Infrastructure Networks: Infrastructure based network, communication is taking place only between the wireless nodes and the access points. The communication is not directly taking place between the wireless nodes. Here the access point is used to control the medium access as well as it acts as the bridge to the wireless and wired networks. In this network base stations are fixed as the node goes out of the range of the base station, it gets into the range of another base station. The example of an infrastructure based network is cellular networks.

2. REVIEW OF LITERATURE

In this paper, the problem of decentralized detection in the presence of one or more classes of misbehaving nodes can be considered [1]. The fusion center first estimates the nodes operating points) on the ROC curve and then uses this estimation to classify the nodes and to detect the state of nature. Numerical results have presented that show the proposed algorithm significantly outperforms the reputation-based methods in classification of the nodes as well as the detection of the hypotheses. The estimated operating points are compared to the Cramer- Rao lower bound which shows the efficacy of the proposed method. [2].In this paper, by exploiting the approximately linear relationship between the

scheme parameters and the network size, a simplified q-out-of-m fusion approach for final decision making in the SENMA architecture can be considered. The performance of the proposed scheme is investigated under Byzantine attacks. It was shown that at a fixed percentage of malicious nodes, the false alarm rate of the simplified q-out-of m scheme decrease exponentially as the network size increase. The detection accuracy of the proposed scheme is further investigated under static and dynamic attacking strategies.

In this paper data confidentiality in a distributed detection scenario with the TBMA protocol in which the wireless channels between the sensors and the ally FC are vulnerable to eavesdropping by an unauthorized enemy, FC can be focused.[3]. To secure the wireless channels a novel TBMA protocol called secure TBMA which provides data confidentiality by taking advantage of randomness and independence of the main and eavesdropping channels. Instead of securing the individual wireless channels based on cryptographic algorithms, the key idea behind secure TBMA is to have the activated sensors secure their transmissions from possible eavesdropping in a cooperative manner in which the sensors follow different reporting rules depending on the magnitudes of their main channel [4]. Wireless Sensor Networks often operate in a resource-constrained environment. Optimal resource utilization is the main objective of WSN. But Wireless Sensor Networks are equally vulnerable to security attacks. Ensuring security in a hostile operational environment of WSN is a hurricane task. The idea of this paper is to provide comprehensive information on types of attacks WSN is exposed to and possible methods of countering such attacks effectively. The motto here is to help novice researchers with the objective to work on security challenges in Wireless Sensor Network environment. When wireless sensor networks are deployed in an open or hostile environment security becomes extremely important, as they are prone to different types of malicious attacks. [5].Based on the canonical parallel fusion structure that incorporates the fading channel, an LR-based fusion rule has been derived. For robust performance in the absence of prior knowledge regarding the local sensors and/or fading channels, several alternatives were proposed. The two-stage implementation using the fusion rule provides high SNR approximation to the LR-based fusion rule, whereas the statistic in the form of an MRC statistic gives a low SNR approximation. Performance evaluation is conducted using both the ROC curve as well as the deflection measure. Fusion of binary decisions transmitted over fading channels has particularly important applications in low-cost low-power wireless sensor networks

3. APPROACHES USED

A. Overview

Data aggregation is a process of aggregating the sensor data using aggregation approaches. The general data aggregation algorithm works as shown in the below figure. The algorithm uses the sensor data from the sensor node and then aggregates the data by using some aggregation algorithms such as centralized approach, LEACH, TAG etc.

B. Cluster-Based Approach

In energy-constrained sensor networks of large size, it is inefficient for sensors to transmit the data directly to the sink in such scenarios, Cluster based approach is the hierarchical approach. In cluster-based approach, the whole network is divided into several clusters. Each cluster has a cluster-head which is selected among cluster members. Cluster-heads do the role of an aggregator which aggregate data received from cluster members locally and then transmit the result to the base station (sink). Recently, several cluster-based network organization and data-aggregation protocols have been proposed for the wireless sensor network.

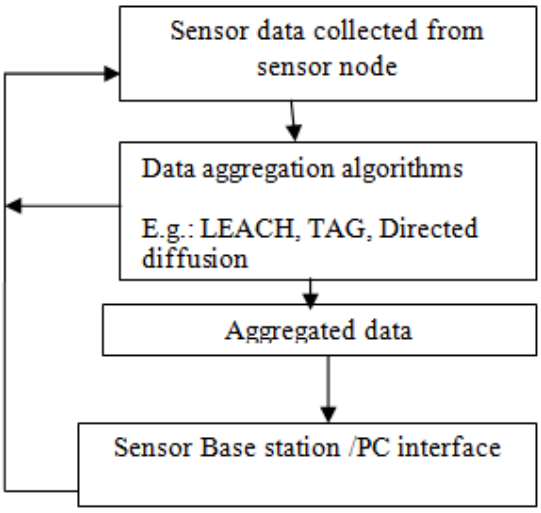


Fig. 1: Architecture of the data aggregation Algorithm

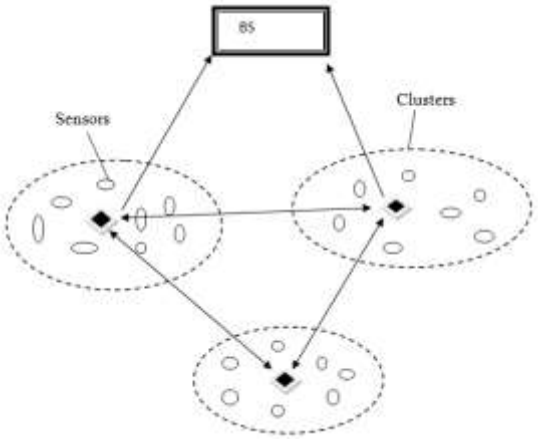


Fig. 2: Cluster-Based sensor networks

The cluster heads can communicate with the sink directly via long-range transmissions or multi hopping through other cluster heads.

4. PROPOSED METHODOLOGY

Wireless Sensor Network is the application based network. The sensor is divided into different parts. Sink nodes send query messages based upon temperature suppose. If the temperature does not arise then no reply is given by the nodes to the sink. But battery degrades due to processing. In cache cooperative networks is deployed in same manners as sensor networks. Nodes are selected on the basis of some assumptions. Sensor nodes are store data on the cache. Sink nodes do not flood messages. It sends to message only to a selected node of each part. Then these nodes give data called cooperative cache.

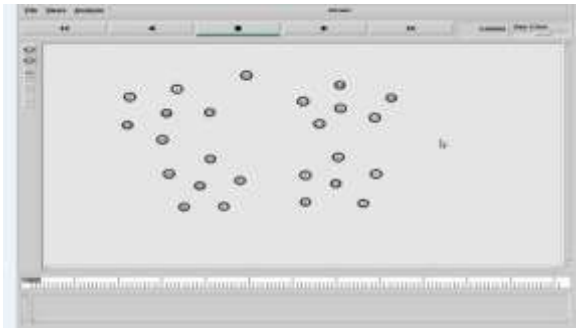
Suppose we have selected four nodes in a network. Sink send a query to the first node to get the data from that node. But node 1 has outdated data latest data is available at node 4. So inconsistency problem occurs here. To improve the inconsistency problem caching nodes has no inconsistency during replication. Consistency should be there during replication so that any node can give data during the query.

Because all nodes have the same and latest data. The network is divided into four parts. Each part has selected nodes which give information about data. Sink node sends a query to node 1 to get the latest information but node 1 has outdated data because latest data is available at node 4. So there is no consistency between two selected nodes. To overcome consistency problem we have to apply consistency algorithm so that all the replica has the same data and latest data.

5. RESULTS

A. Problem Implementation:

First of all, deployment of the network with finite numbers of nodes.

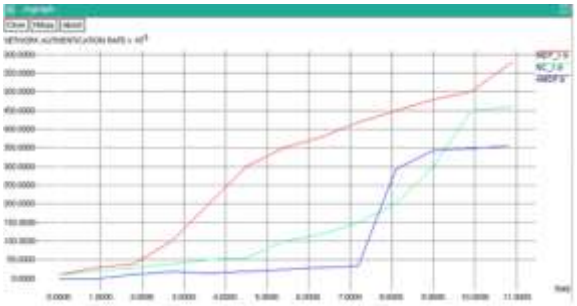


B. A solution of Implementation:

Formation of cluster heads according to the node which has higher energy level. After the deployment of network and formation of cluster head, then cluster head sends data to caching nodes. Now sink sends a query message to caching node for data availability. The node having data reply back to sink. When sink sends a query message to one of node than node reply with outdate data where inconsistency occurs. The requesting cache node does not have data that is required by the sink. Then cache node asks another cache node for required data. If data available than it reply to sink otherwise cache miss occur. If new requesting cache node also does not have required data then this further send it to another cache node also.

Now again cache miss occur than first cache node asks another cache node for data availability and that node has data available. Now the cache node which has data available send update data to sink.

According to pushing technique now update all the cache node according to update data and maintain consistency.



6. CONCLUSION

The main objective of this research paper is to discuss various challenges and technique of WSN. We also focused on cache cooperative technique and its procedure. We believe that proposed algorithms discussed in this paper will give benefit for various research scholars. Its experimental results show that proposed technique gives a better result which has better throughput and energy as compared to existing techniques.

7. REFERENCES

[1] "Decentralized Hypothesis Testing in Wireless Sensor Networks in the Presence of Misbehaving Nodes", Erfan Soltanmohammadi, Mahdi Orooji, and Mort Naraghi-pour, IEEE Transactions on Information Forensics and Security Volume 8 Issue 1 March 2011.

[2] "Reliable Data Fusion in Wireless Sensor Networks under Byzantine Attacks", Mai Abdelhakim Leonard ,E. Lightfoot Tongtong Li, The 2011 military communications conference on Network Protocols And Performance Track January 2011.

[3] "Secure Type-Based Multiple Access", Jeongseok Ha, Hyuckjae Lee, Daesung Hwang, IEEE Transactions on Information Forensics and Security September 2011.

[4] "Security Vulnerability Issues In Wireless Sensor Networks: A Short Survey", C K Marigowda, Manjunath Shingadi, and July 2013.

[5] "Channel Aware Decision Fusion In Wireless Sensor Networks", Biao Chen, Ruixiang Jiang, Teerasit Kasetkasem, Pramod K. Varshney , IEEE Transactions On Signal Processing December 2004.

