Rule Based Energy Consumption in Cluster-Based Wireless Sensor Networks

Yogavathi G
Department of Computer Science and Engineering,
Jain Global Campus, Jain University,
Jakkasandra Post, Kanakpura Taluk,
Ramanagar District-562112

Manjunath C R
Assistant Professor
Department of Computer Science and Engineering,
Jain Global Campus, Jain University,
Jakkasandra Post, Kanakapura Taluk,
Ramanagara District-562112

Abstract: **A WSN consists of interconnected spatially distributed sensor nodes without the use of wires. Sensor nodes use their communication devices in order to transmit the data being sensed to Base Station over wireless channels to other nodes in network. There is no monitoring of data entering into network during the data transmission, there are chances of over loading the network and due to which energy consumption will be increased. A Rule- based WSN system is proposed. Firstly elect Controller Node (CNode) in order to monitor the packets entering the network. Next application of rules- Interval and Jamming rule. The proposed approach helps in reducing energy consumption and enhancing network lifetime.**

Keywords: WSN, Controller Node, Rules, Interval and Jamming rule.

1. INTRODUCTION

Wireless Sensor Network (WSN) is the group of sensor nodes [1] that are distributed in a wide environment [2] to perform a specific function [1]. Sensor nodes are small devices with sensing capacity [2].An architecture of WSN includes Base Station (BS)/sink and sensor nodes. A typical sensor node consists of memory, power supply, processor, sensing, and transceiver. BS is placed close by to randomly deployed sensor nodes. Wired or wireless network can be used to connect BS to internet. BS gathers sensed data from sensor nodes and also gives instructions to them. Through internet the sensed data is easily accessible after it reaches BS. [1]

Inherent limited energy resource is one of the limitations of wireless sensor nodes [3]. Power consumption can be because of three functional domains: sensing, communication, and data processing. Energy wastage in a sensor node could be due to

- Useful or
- Waste sources

The reasons for energy waste can be either of these: firstly, idle listening; secondly collision – At the same interval if sensor node receives more than one packet that are identified to be collided. Collided packets are discarded and retransmitted which will increase the energy wastage. Third reason is overhearing – a node receives packet which was not for it. The fourth one occurs as a result of control-packet overhead- For data transmission minimum number of control packets to be used. Finally, for energy waste is over-emitting [5].

2. EXISTING SYSTEM

To deal with energy wastage there were many approaches put forth. Forming clusters were the most energy efficient approach followed to date. Grouping of associated objects into one cluster and having a cluster head to aggregate the data and forwarding of data. The cluster forwards the data without having knowledge of data which may lead to attacks and unwanted data transmissions. Though there are many approaches to overcome attacks, the methods concentrate more on attack detection but not on energy consumption and energy going waste. In [6] the author proposes an idea to monitor the data being transmitted but the approach follows data retransmission which again will consume energy.

3. PROPOSED SYSTEM

Sensing, wireless communications and computations are capabilities of wireless sensors that are deployed in an unattended environment. But the limitations of the sensor nodes such as battery, low memory and processing speed play a major role in communication. These limitations are faced because in real time approach sensor nodes are deployed randomly in hostile or impractical environment, and it becomes impossible to recharge the battery. Battery consumption can be encountered due to either normal communication or overloading of data for communication. Due to overloading or flooding of data the energy is wasted. Flooding occurs

when a node sends a packet that it received, to all its neighbors other than the neighbor which sent the packet to it. This leads to unwanted data transmission to the node which was never interested. This has many disadvantages; the most important is it is responsible for large bandwidth consumption and it wastes valuable energy.

Proposed work aims providing a ruled based energy consumption approach in the network. The approach involves two steps: Firstly, Election of Controller node after cluster formation - Monitoring node that monitors for flooding of packets. Secondly, Rule application phase - Rule are incorporated into the controller node to drop data packets which may create flood and lead to energy wastage.

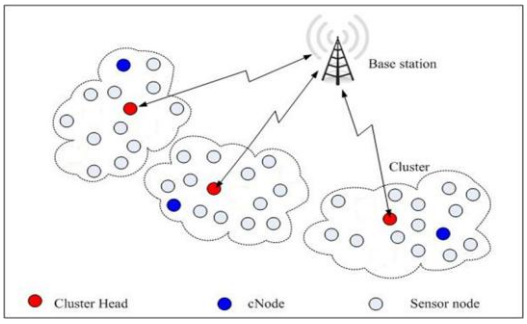

Figure 1: System architecture

Assumptions:

1) All nodes in the network are alive and posses minimum requirement of energy.
2) There is only one Base station.
3) Packets are routed via Controller Node only.

Step 1: Cluster formation

Clustering is the approach of identifying relationship among objects or grouping of similar objects. In each cluster, based on residual energy node is elected as the Controller node (CNode) and other as cluster-head (CH), while the remaining nodes are termed to be member nodes. Member nodes in their respective cluster do sense the data and forwards the same to their corresponding cluster-head or receive data from Cluster head. Cluster-heads handles the responsibilities to collect data/ transmit the data from their member nodes/BS, to aggregate them, and finally to forward the aggregated data either to neighboring cluster or to member nodes or to sink/base station. [9]

Algorithm for electing CNode:

Let RE_i be the measured residual energy of node i at time t, Let max RE be the maximum residual energy. 'M_i' be the monitor node.

1. Nodes calculate RE_i
2. If (RE_i< max RE) then
3. Node 'i' = member node
4. Else if (RE_i> max RE) then
5. Node 'i' is elected as M_i

Step 2: Rule application

There are three main phases involved: Data acquisition phase- Survey the type of data transmission and deciding on type of rules; Rule application phase- in which the pre-defined rules are applied to the data; Flooding detection phase- after rule application[10]

The rules considered for the proposed work are:

Jamming Rule: Jamming can be measured in terms of collision. If collision rate is exceeded then it is said to be creating a jam in network or collision.

Interval Rule: Interval between two consecutive messages should be within the limit. If either low or high packet interval rate then error is raised. Two attacks that can be detected by this rule are the negligence attack and the exhaustion attack. In the negligence attack, malicious node messages are not considered by the intruder. While in the exhaustion attack, the data interval rate is tampered and increments messages sending rate in order to increase the energy consumption.[7]

Algorithm for rules application:

For each data packet apply rule,

if (Message. Interval rate == Threshold. Interval rate || Message. Collision rate ==

Threshold. Collision rate)

then "discard message"

else

Forward the packet to CH

end if

4. ANALYSIS

Proposed work aims to reduce energy consumption compared to existing techniques. It follows rule based approach in order to avoid energy wastage. Election of controller node is done to monitor the data packets. Controller node and Cluster head selection is based on residual energy calculation. The monitoring node is present in proposed work to avoid data flooding. The Controller node will be equipped with the interval rate and collision rate, which are set as thresholds. When threshold is reached, packets are dropped. This is to avoid packets that will create flooding in the network. Flooding or unwanted activity in the network leads to energy wastage. The proposed work is an attempt to avoid unwanted wastage of energy.

5. CONCLUSION

The proposed work main objective is to reduce energy consumption by clustering and rule application. Energy drop may occur due to flooding (unwanted data packet forwarding). The proposed work has two approaches built into one to avoid energy wastage. The clustering is itself followed to save energy. Rule application will avoid unwanted wastage of energy as packets creating energy drop are not entered into the network itself. Since proposed work incorporates these approaches to reduce energy consumption, it must enrich network lifetime.

6. REFERENCES

[1] Babar Nazir, Halabi Hasbullah "Energy Balanced Clustering in Wireless Sensor Network" IEEE 2012.

[2] Advanced Network Technologies Virtual Labs - IIT Kharagpur "Simulating a Wireless Sensor Network" http://virtual-labs.ac.in/cse28/ant/ant/8/theory.

[3] B. P. S. Sahoo, Satyajit Rath and Deepak Puthal "Energy Efficient Protocols for Wireless Sensor Networks: A Survey and Approach" International Journal of Computer Applications (0975 – 8887) Volume- APRIL-2012.

[4] Stefanos A. Nikolidakis , Dionisis Kandris , Dimitrios D. Vergados and Christos Douligeris : "Energy Efficient Routing in Wireless Sensor Networks through Balanced-Clustering" Algorithms 2013, 6, 29-42; doi:10.3390/a6010029.

[5] Zahra Rezaei, Shima Mobininejad "Energy Saving in Wireless Sensor Networks" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.1, February 2012 DOI : 10.5121/ijcses.2012.3103 23

[6] Malek Guechari, Lynda Mokdad, Sovanna Tan "Dynamic Solution for Detecting Denial of Service Attacks in Wireless Sensor Networks" IEEE ICC 2012 - Ad-hoc and Sensor Networking Symposium

[7] Ms. Rachana Deshmukh, Ms. Rashmi Deshmukh, Prof. Manoj Sharma "Rule-Based and Cluster-Based Intrusion Detection Technique for Wireless Sensor Network", IJCSMC, Vol. 2, Issue 6, June 2013, pg.200 – 208

[8] Mamatha G, B G Premasudha "Deployment Techniques of Nodes in WSN for Multi-Domain Applications A Survey on their performance analysis" International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-3 Number-4 Issue-13 December-2013 280

[9] Zhang/RFID and Sensor Networks "Clustering in Wireless Sensor Networks" AU7777_C012 Page Proof Page 323 2009-6-24.

[10] Hosamsoleman, Ali Payandeh, Nasser Mozayyani, "Detection Collision Attacks In Wireless Sensor Network Using rule-Based Packet Flow Rate" SaeedSedighianKashi ISSN: 2248-9622 www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.261-268.