RESEARCHERID
THOMSON REUTERS
[Ramesh, 5(9): September 2018]
ISSN 2348 – 8034
DOI- 10.5281/zenodo.1421054
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

ENHANCING ENERGY EFFICIENCY IN WSN BY INTRODUCING GRID BASED REGION CLUSTERING

V. Sathiyavathi[1], R. Reshma[1], C. Jayakumar[2] & L. Sai Ramesh[*3]
[1]Assistant Professor, JBAS College for Women, Chennai
[2]Professor, DCSE, Sri Venkateswara College of Engineering, Chennai
[*3]Visiting Faculty, Dept. of IST, Anna University, Chennai

ABSTRACT

In general, Wireless Sensor Networks (WSN) are self configured in nature and infrastructure less network. The energy consumption of sensor nodes is the major problem because the nodes are consuming energy even there is no process for particular node. In this paper, a new framework is proposed to avoid the unneeded energy consumption of sensor nodes. This work is mainly concentrates on selecting the cluster head (CH) in each region and try to cluster the nodes with equal number in each region. This grid based approach helps to find the active node and also shortest route node to reach the destination from source by maintain the cluster head table.

Keywords: *Region based clustering, Energy, trust value, sensor.*

I. INTRODUCTION

In recent days, usage of sensor is increased due to the arrival of Internet of Things (IoT) technologies. Sensor based applications are increased due to its availability in emerging internet world. But, still most system based on sensors are suffered a lot by their energy consumption problem. Each node in the sensor network comprises with the information of their neighbor node, radio for transmission with low power, battery for power supply and sometimes with ranging device. Mostly, the energy of the sensor nodes are degraded while searching for their neighbor node or CH. To avoid this energy consumption, a new framework is proposed in this work based on grid based region clustering which also called as geographic based routing mechanism. Most of the previous works are proposed with the energy efficient protocols for routing. But all these mechanisms don't consider reducing the searching strategy of neighbor nodes for each sensor node.

Some of the neighbor nodes are chosen not only based on the distance and also based on their trust value in the particular cluster or region based on their previous packet loss details. While, there is a discussion about trust of sensor nodes, most of the routing mechanisms doesn't need the energy value of the trusted node. In some works, the energy value is calculated for each sensor nodes and doesn't take care about node trust value. In this paper, both the nodes energy value and trust value is consider for enhancing the energy efficiency in sensor networks.

II. LITERATURE SURVEY

There are many works are discussed previously for energy efficient and trust based routing for WSN. In [1], studied the problem of forwarding a packet to nodes in a geographic region of an ad-hoc wireless sensor network. The proposed Geographic and Energy Aware Routing (GEAR) protocol uses energy aware and geographically informed neighbor selection to route a packet towards the target region. This strategy attempts to balance energy consumption and thereby increase network lifetime. Within a region, it uses a recursive geographic forwarding technique to disseminate the packet. The simulation results show that for an uneven traffic distributions,

ISSN 2348 – 8034
DOI- 10.5281/zenodo.1421054
Impact Factor- 5.070

In [2], authors tried to systematically study, under a unified theoretical framework, configurations and routing schemes for the data-centric paradigm in sensor networks. In the first part of the paper, the computed energy requirements for both manual (specific configurations) and random placement of nodes. The second part focused on optimal routing trees for datacentric routing and showed that the minimum spanning tree is energy-optimal. Then, the paper addressed the important problem of constructing MST (or a good approximation of MST) in an energy-efficient and distributed manner

In [3], techniques at various levels of the system hierarchy that take advantage of underlying hardware to produce more energy efficient solutions. In some instances, it shown how to take advantage of hooks and knobs in the physical layer to build more energy-efficient protocols and algorithms. In other instances, demonstration is given to how non-idealities of the hardware can be mitigated by making careful, yet simple protocol design choices. As a whole, the paper investigates a physical layer driven approach to protocol and algorithm design for wireless sensor networks. In order to meet the system lifetime goals of wireless sensor applications, considering the parameters of the underlying hardware are critical. If protocol designers treat the physical layer as a black box, system designers may design protocols that are detrimental to energy consumption.

In [4], authors presented a top-down survey of the trade-offs between application requirements and lifetime extension that arise when designing wireless sensor networks. They first identify the main categories of applications and their specific requirements. Then they presented a new classification of energy-conservation schemes found in the recent literature, followed by a systematic discussion as to how these schemes conflict with the specific requirements. Finally, the survey of techniques applied in WSNs to achieve trade-off between multiple requirements, such as multi-objective optimization.

In [5], they introduced a distributed trust-based framework and a mechanism for the election of trustworthy cluster heads. The proposed mechanism reduces the likelihood of compromised and or malicious nodes from being selected as cluster heads. Their premise is that while individual nodes may still be prone to attack, a significant vulnerability is addressed if the election of compromised cluster heads is prevented. They also performed an evaluation of this approach and the power consumption of the model, by simulations. The results indicate clear advantages of this approach in preventing the election of untrustworthy cluster heads.

In [6], energy efficient routing mechanism using fuzzy ruled based approach is discussed and the results shows that fuzzy approach works better for them specified framework. And in [7], author discussed about trust evaluation method based on fuzzy rules which provides the better detection of malicious nodes.

While, there is a discussion about trust of sensor nodes, most of the routing mechanisms doesn't need the energy value of the trusted node. In some works, the energy value is calculated for each sensor nodes and doesn't take care about node trust value. In this paper, both the nodes energy value and trust value is consider for enhancing the energy efficiency in sensor networks.

III. PROPOSED SYSTEM

In this paper, a new Geographical grid based cluster region (GGCR) algorithm and available watch dog algorithm for detecting trust level of node is used to calculate the trust value and group the nodes geographically. In this approach, packet forwarding process is classified in two different ways.

A. Geographical grid based cluster region (GGCR) algorithm

1. Forwarding the packets from source to destination through intermediate nodes
a. Locate the sensor nodes through the GPS concept
b. Calculate the distance between the nodes within the region

[Ramesh, 5(9): September 2018]
ISSN 2348 – 8034
DOI- 10.5281/zenodo.1421054
Impact Factor- 5.070

c. Choose a cluster head within the region for each which has more energy that calculated using Sensor Energy Aware (SEA) algorithm.
d. Verify that each cluster has not hold than maximum of nodes (maximum have to be fixed based on CH energy level)
e. Check the region of source and destination node before sending the packet.
f. Make sure that the packet should be send through the CH if Source and destination are in different region

The above mentioned GGCR algorithm simply reduces the energy consumption of the intermediate nodes by sending the packet directly to the CH. And also, the nodes have to hold only the CH details and not details of their neighbor nodes. So, the memory consumption of the node has also reduced.

B. Sensor energy aware algorithm

In this section, energy aware algorithm for calculating the energy or energy consumption of the node is calculated. However, under some circumstances, taking the geographically direct path is more energy efficient and consequently prolongs network lifetime. Under the following conditions, the pure geographic mode is used instead of adding the energy aware metric.

1. Geographical routing is used instead of energy aware routing. The motivation behind this is to get to the target directly if the packet has already traveled a long way.
2. After a packet reaches a node whose neighbors are heavily depleted (which indicates a neighborhood where nodes are heavily depleted), the packet will switch to pure geographic mode to avoid taking an alternative longer path, and consequently consuming more energy than the direct path.
3. When nodes are near the target region, pure geographic mode is used. Pure geographic mode is used near the target region to avoid taking a longer path and thereby avoid burning outmore bottleneck nodes more quickly.

C. Trust level of the node

The trust level of the node is calculated for specific region based on the behavior of each node within the region. In this, time is calculated randomly for each node that the time it takes to send to the destination from the specific node.

Node behavior Algorithm:

Input: *{ Packets from source nodes}*
Output: *{Packets reached destination nodes}*

Step 1. Initialize the buffer value for each node

Step 2. Intilize the recovery buffer in the CH

Step 3. Initialize the misbehaving node = 0

Step 4. Calculating the minimum distance though all nodes from the source

Step 5. Calculate the maximum time (node timer) between the nodes to traverse

Step 6. Initialize the watch dog timer to check the node timer is equal to maximum time or greater than that.

Step 6a. If (Watchdog timer > Node timer) **then**
{***Load*** the *packets* to Destination buffer}

[Ramesh, 5(9): September 2018]
ISSN 2348 – 8034
DOI- 10.5281/zenodo.1421054
Impact Factor- 5.070

Step 6b. **Else** {Misbehaving _Nodes = Misbehaving Nodes + 1}

Step 7. Summarize the misbehaving nodes

IV. RESULTS AND PERFORMANCE ANALYSIS

The performance of the proposed work is evaluated by comparing with different strategies. For that, we use the following metrics:
Delivery Rate (r): percentage of packets sent by the source which reached the sink.
Energy Efficiency (Eeff): number of packets delivered to the sink for each unit of energy spent by the network.
Detection accuracy: This represents the detection ratio of malicious node in the available network.

Table 1 shows the detection accuracy of malicious nodes based on node behavior. And the performance compared with watch dog, malicious node detection algorithm. Table 2 shows the delivery rate and energy efficiency of the proposed GGCR algorithm when compared with AODV protocol. The performance is somewhat in increasing manner while going for routing algorithm with trust valuation based on node behavior.

Table 1 Malicious node Detection Accuracy Comparison at 50 packet /sec

No. of Malicious node	Detection Accuracy (%)	
	Watch dog	Proposed System
0	100	100
5	85	89
10	60	85
15	58	82
20	56	78

Table 6.2 Packet Delivery Ratio Analysis

Number of packets per second	No. of Malicious node	Packet delivery Ratio (%)	
		AODV	GGCR
10	0	100	100
	5	95	99
	10	92	98
20	0	100	100
	5	92	98
	10	90	96
30	0	100	100
	5	86	95
	10	78	91
40	0	100	100
	5	80	90
	10	64	87

In Table 2, packet delivery rate is analyzed with the inclusion of malicious nodes to show that the proposed algorithm is providing better delivery rate than AODV when the presence of malicious nodes.

ISSN 2348 – 8034
DOI- 10.5281/zenodo.1421054
Impact Factor- 5.070

Based on the usage of above the trust value and energy level will be calculated for each node and CH. So, finally we got the framework which considers both the energy value of the node and trust value of the node.

V. CONCLUSION

This paper gives an overview about energy efficient routing mechanism for WSN. In this work, both energy value and trust value is calculated for each node. The proposed technique, cluster the nodes based on the geographical regions which help for the nodes to easily select their cluster head within their region. It directly reduces the energy consumption of each node. And also, the neighbor node information doesn't want to stored in each node. This also helps to reduce the energy wastage in nodes. Further, it may implement for real time applications like defense or medical related where the real powers are in very rare condition.

REFERENCES

1. *Yu, Yan, Ramesh Govindan, and Deborah Estrin. "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks." (2001).*
2. *Schurgers, Curt, and Mani B. Srivastava. "Energy efficient routing in wireless sensor networks." Military communications conference, 2001. MILCOM 2001. Communications for network-centric operations: Creating the information force. IEEE. Vol. 1. IEEE, 2001.*
3. *Shih, Eugene, et al. "Physical layer driven protocol and algorithm design for energy-efficient wireless sensor networks." Proceedings of the 7th annual international conference on Mobile computing and networking. ACM, 2001.*
4. *Rault, Tifenn, Abdelmadjid Bouabdallah, and Yacine Challal. "Energy efficiency in wireless sensor networks: A top-down survey." Computer Networks 67 (2014): 104-122.*
5. *Crosby, Garth V., Niki Pissinou, and James Gadze. "A framework for trust-based cluster head election in wireless sensor networks." Dependability and Security in Sensor Networks and Systems, 2006. DSSNS 2006. Second IEEE Workshop on. IEEE, 2006.*
6. *Selvakumar, K., L. Sairamesh, and Arputharaj Kannan. "An intelligent energy aware secured algorithm for routing in wireless sensor networks." Wireless Personal Communications 96, no. 3 (2017): 4781-4798.*
7. *Selvakumar, K., L. Sai Ramesh, and A. Kannan. "Fuzzy Based Node Trust Estimation in Wireless Sensor Networks." Asian Journal of Information Technology 15, no. 5 (2016): 951-954.*