INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) E - ISSN: 2454-4752 P - ISSN : 2454-4744
VOL 2 ISSUE 5 (2016) PAGES 1228 - 1232
RECEIVED : 16/09/2016. PUBLISHED : 21/09/2016

SHORTEST PATH BASED GEOGRAPHIC ROUTING IN CLUSTERED WIRELESS SENSOR NETWORK.

[1]G.Eswari, [2]P.Vinodhini,
[1]M.Phil Scholar, Dept of computer science and Applications, KMG College of Arts & Science, Gudiyatham,
[2]Asst prof, PG and Research Dept of computer science and Applications, KMG College of Arts & Science, Gudiyatham.

Abstract:

In Wireless Sensor Networks (WSNs), it is a very challenging task to transmit data from sensor nodes to a sink in the presence of obstacles. Here, one of the clustering technique called as Energy efficient Homogeneous Clustering (EHC) is used which selects the Cluster Head (CH) among the cluster based on the value of residual energy and utility of sensor to its neighbor. Next, a Route Optimization Technique (ROT) is proposed which is used to select the shortest path among the obstacles using Dijkstra's shortest path algorithm. Using these techniques energy consumption and hop count are reduced and they are also used to improve the network lifetime. The simulation result for various parameters such as average hop count, energy consumption, packet delivery ratio, delay, lifetime and consumed energy per packet are demonstrated.

Key words - Clustering, obstacles, , route optimization, routing.

1. INTRODUCTION

Wireless Sensor Network (WSN) has emerged as one of the most promising technologies of this decade [1]. A WSN is basically composed of a base station and several sensor nodes distributed over a certain geographical area. Sensor nodes monitor the environment in which they are deployed to collect information such as temperature, humidity, pressure, vibration, sound and so on. Each node in a WSN reports the information it gathered to the base station directly or through multi-hop wireless communication link. As soon as people understand the capabilities of a wireless sensor network, hundreds of applications spring to mind. It seems like a straightforward combination of modern technology. However, actually combining sensors, radios, and CPU's into an effective wireless sensor network requires a detailed understanding of the both capabilities and limitations of each of the underlying hardware components, as well as a detailed understanding of modern networking technologies and distributed systems theory. Each individual node must be designed to provide the set of primitives necessary to synthesize the interconnected web that will emerge as they are deployed, while meeting strict requirements of size, cost and power consumption. A core challenge is to map the overall system requirements down to individual device capabilities, requirements and actions. Sensor nodes can be partitioned into a number of small groups, which is known as clusters. These are the organizational unit for wireless sensor networks. Each cluster has the coordinator, called cluster head (CH). In a clustering scheme the sensor nodes in a WSN are divided into different virtual groups, and they are allocated geographically adjacent into the same cluster according to some set of rules. The cluster heads can consolidate the data and send it to the data center as a single packet, thus reducing the overhead. Clustering [2] has advantages for reducing useful energy consumption by improving bandwidth utilization, reducing wasteful energy consumption by reducing overhead. Most of the algorithm aims to extend the network lifetime by balancing energy consumption among nodes and by distributing the load among different nodes from time to time.

2. ROUTING IN A CLUSTERED WSN

In wireless sensor networks, building efficient and scalable protocols is a very challenging task due to the limited resources and the high scale and dynamics. Geographic protocols, that take advantage of the location information of nodes, are very valuable for sensor networks. Geographic routing is a routing principle that relies on geographic position information. It is mainly proposed for wireless networks and based on the idea that the source sends a message to the geographic location of the destination instead of using the network address. Wireless Sensor Network originated as a battlefield surveillance application. Earlier routing protocols did not require point to point communication. Nowadays, the field has been growing with new potential in industrial [3], health and other monitoring applications and so is the need for more efficient routing algorithms [4]-[5]. Wireless sensors have limited memory and they are battery-powered when deployed in the real world. Hence, memory and power consumption are the two typical challenges faced by wireless sensor network programmers. For data-centric point to point wireless sensor network applications efficient routing of data packets is a challenge. Geographic routing algorithms have been proposed for wireless sensors to effectively address this issue. In clustering network the limited battery power will be difficulty in recharging the batteries in a hostile environment require that sensors will be deployed with the high density for a long lifetime of WSNs. Distributed clustering techniques are more useful in sensor network. Low Energy Adaptive Clustering Hierarchy (LEACH) [11] selects Cluster head based on the predetermined probability in orderto rotatethe cluster head rolealong with thesensors to be balance of the residual energy of the sensor network. Following the idea of LEACH protocol, a number of various protocols had presented in this literature. Hybrid Energy-Efficient Distributed (HEED) [13] clustering selects the cluster heads based on the residual energy of the network sensors and a secondary parameter, such as proximity to nearby neighbours. SPAN selects CHs based on that residual energy and more number of neighbours [14]. The cluster head form a network that is used to forward the data to sink.

3. SYSTEM IMPLEMENTATION

A. Network design

To createa network with the number of nodes which is a wireless sensor network and going to creating the network with the WSN specifications i.e., each node can be communicate with any other node directly to which are in coverage area of the node. Then forming one leader node which is known as traffic manger which will controls the traffic of the entire network and remaining are normal nodes. The sensor nodes are usually to be resource constrained with respect to computation capability, bandwidth, memory space, and power supply. The network users use some mobile devices to be disseminating data items into the network. The network owner is responsible for generating keying materials.

B. Monitoring the traffic

To monitor the traffic, it will be handled by the Traffic manager which is to be leader node. It is going to controls the entire network i.e., it will be monitors all the nodes and checks which aregiving goodresponse basedon that itwill be allow other nodes to communicating each other. Networks are assigned aggregation privileges by the trustedauthoritiesin aPKIofthenetworkowner.However, the network is owner may for various reasons; impersonate network users to aggregate data items. The compromised entities are regarded as inside because they are members of the network until they are identified. The adversary controls of these entities to attack the selected network in arbitrary ways. For instance, they could be instructed to aggregate false or harmful data, launch attacks such as DoS attacks or Sybil attacks and be non-cooperative with the other nodes. Data gathered by the individual nodes ultimately routed to the base station. A rate monitoring attack simply makes use of idea that nodes are closest to the base station that tends to forwarded more packets than the farther away from the basestation. An attacker needs to only monitoring which nodes are sending the packets and follow those nodes is sending to the most packets. In time correlation attack of traffic monitoring where an adversary node can simply generates monitors and events to which a node sends its packets.

C. Route discovery process

A node wants to communicate with other node in discovery process whenever it has to find the route for forwarding the data in the network. In this route discovery process if any new node is entered means there is a chance of that a hacking node may be present. So that to avoid that hacking nodes for secure data transmission. For this reason, the nodesare maintaining acorrectlist known as true list, in the nodes are going to be store about their other nodes to finding the secure route. To create trust list nodes are going to create a name list known as true list, in this list they are going to store the node information’s in the network which given proper response to the traffic manager. The utility of a sensor network will relay on its ability to accurately and automatically to locateeach sensor in the network. Asensor network that is designed to locate faults will need to be accurate location information in order to finding of pin point of route and the location of a fault in discovery process. Unfortunately, an attacker can easily manipulate in network that are none secured information present in location by reporting the false signal strengths and replaying the signals. To check trust list whenever a node wants to send the data and it will send route request to all other nodes. Thenode which arereceived bythe route request packet will checks the node in route discovery process whether that nodeis present in true list or not if presented means it will be forward to other nodes and it repeats until it reaches destination. Route trust is computed by the every node for each route in routing table. It measures a reliability with a packet can reach to the destination, if forwarded by the node to particular route in network. The route will be trusts are initially unknown. RREQ's are sent by source node and the routes are established to the destination node as in GPSR.

4. RESULTS AND DISCUSSION

NS2 is one of the most popular open source network simulators. We conduct the following experiments with ns 2.34 simulator. Four obstacles are taken into consideration which is placed at different position. There are 100 static sensors randomly deployed in the communication field.

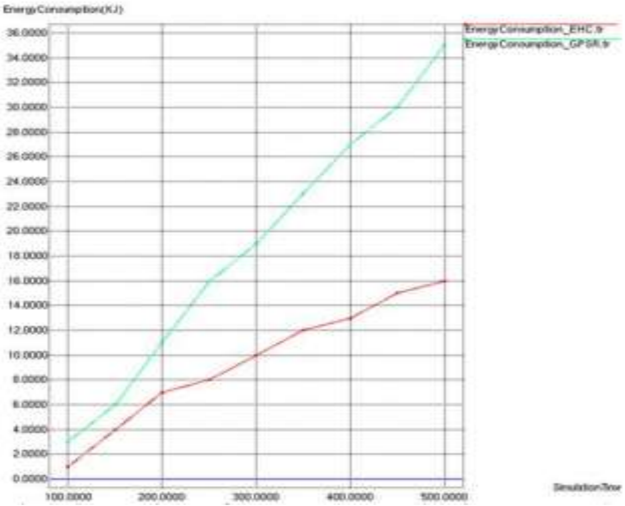

Fig.1. Most of the simulation parameters are similar .

Most of the simulation parameters are similar.The simulation time is 30ms. We have demonstrated various parameters as follows when compared to Greedy Perimeter Stateless Routing (GPSR). The hop count refers to the number of intermediate devices through which data must pass between source and destination. Each time packets are passed to the next device, a hop occurs. Hop count is therefore a basic measurement of distance in a network.

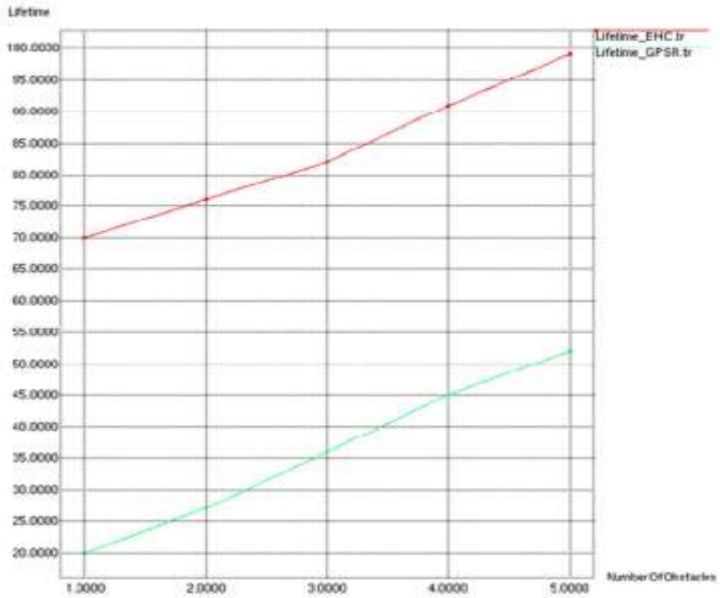

Fig.2. Lifetime of EHC and GPSR

Energy consumption means consumption in energy or power. It can be concluded that when EHC is not used, all the sensors remain active to provide the routing for a short duration. This is because a geographical routing without route optimization technique requires more number of the average hop count for routing the packets. The packet delivery ratio of a flow is the ratio of the number of packets that are received by the sink over packets submitted to the network by the source. In EHC, only CHs remain active to provide the routing and therefore prolongs the lifetime of WSNs. Power consumption should be minimized since it determine the lifetime of network.

CONCLUSION

In this project, we proposed a distributed approach to determine if a sensor is a CH or member of the cluster to meet the desired connectivity requirements. We mainly focused on energy-efficient clustered WSNs to prolong the lifetime of WSNs. We also proposed a technique to optimize the routing path among obstacles in clustered WSNs. We simulated the performance of the proposed EHC and ROT and demonstrated various parameters like average hop count, energy consumption, packet delivery ratio, delay, lifetime and consumed energy per packet. The energy consumption and average hop count in WSNs are reduced due to the clustering of sensors and optimization of routing path, hence the lifetime of WSNs is increased. In future, to reduce the energy consumption for route discovery, we are going to propose a new route discovery method. In this method, the source node calculates a circle around the location of destination node which gives the list of destination's neighbor nodes. The source node defines its forwarding zone (a cone) to be the region enclosed by an angle whose vertex is at source node's location and whose sides are tangent to the circle calculated for destination. Source node sends a RREQ packet for destination to all its neighbors in the forwarding zone.

REFERENCES

[1] Hari Prabhat Gupta, S. V. Rao, Amit Kumar Yadav, and Tanima Dutta, “Geographic Routing in Clustered Wireless Sensor Networks Among Obstacles”, IEEE SENSORS JOURNAL, VOL. 15, NO. 5, MAY 2015.

[2] J.-S. Lee and W.-L. Cheng, “Fuzzy-logic-based clustering approach for wireless sensor networks using energy predication,” IEEE Sensors J., vol. 12, no. 9, pp. 2891–2897, Sep. 2012.

[3] Z. Ha, J. Wu, J. Zhang, L. Liu, and K. Tian, “A general self-organized tree-based energy-balance routing protocol for wireless sensor network,” IEEE Trans. Nucl. Sci., vol. 61, no. 2, pp. 732–740, Apr. 2014.

[4] D. C. Hoang, P. Yadav, R. Kumar, and S. Panda, “Real-time imple- mentation of a harmony search algorithm- based clustering protocol for energy-efficient wireless sensor networks,” IEEE Trans. Ind. Informat., vol. 10, no. 1, pp. 774–783, Feb. 2014.

[5] P. T. A. Quang and D.-S. Kim, “Enhancing real-time delivery of gradient routing for industrial wireless sensor networks,” IEEE Trans. Ind. Informat., vol. 8, no. 1, pp. 61– 68, Feb. 2012.

[6] J. Niu, L. Cheng, Y. Gu, L. Shu, and S. K. Das, “R3E: Reliable reactive routing enhancement for wireless sensor networks,” IEEE Trans. Ind. Informat., vol. 10, no. 1, pp. 784–794, Feb. 2014. [7] R. Xie and X. Jia, “Transmission-efficient clustering method for wireless sensor networks using compressive sensing,” IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 3, pp. 806–815, Mar. 2014.