Fast and Energy Efficient Routing Technique for Horizontal Vertical Mapping in Wireless Sensor Network

Sunil Kumar
M.Tech. Student
SEC, Dundlod, Jhunjhunu

Noor Mohammed
Astt. Prof
SEC, Dundlod, Jhunjhunu

Sushma Rani
Astt. Prof
RPSCET,Balana, M/Garh

Abstract— Wireless sensor network consists large amount of sensor nodes. In wireless sensor networks channel and energycapacities are scarce resources.In this paper, we address the problem of energyefficient routing in homogeneous and heterogeneous wireless sensor networks aiming at maximize the network lifetime. Extending system lifetime by effectively managing power on participating nodes is critical in wireless sensor networks. Recent work has shown that, by appropriately powering off nodes, energy may be significantly saved, especially when node density is high.we propose a distributed, randomized improved flooding algorithm like Horizontal –Vertical method for load balancing of the grid network.

Keywords:-Wireless Sensors Network, DC, LML, Leach Replication, ,Clustering.

I. INTRODUCTION

Recent advances in wireless communications and microelectro-mechanical systems have motivated the development of extremely small, low-cost sensors that possesssensing, signal processing and wireless communication capabilities. Wireless sensor network is collection of various sensor nodes that cooperate in wide area network.It consist of one or more base stations and many other neighboring sensor nodes to monitor environmental condition like sound,pressure,tempture etc. through wireless communication.
The key challenge in sensor networks is to maximize the lifetime of sensor nodes due to the fact that it is not feasible to replace the batteries of thousands of sensor nodes. Therefore, computational operations of nodes and communication protocols must be made as energy efficient as possible. Among these protocols data transmission protocols have much more importance in terms of energy, Since the energy required for data transmission takes 70 % of the total energy consumption of a wireless sensor network [1]. Area coverage and data aggregation [2] techniques can greatly help conserve the scarce energy resources by eliminating data redundancy and minimizing the number of data transmissions. Therefore, data aggregation methods in sensor networks are extensively investigated in the literature [2], [3], [4] and [5].

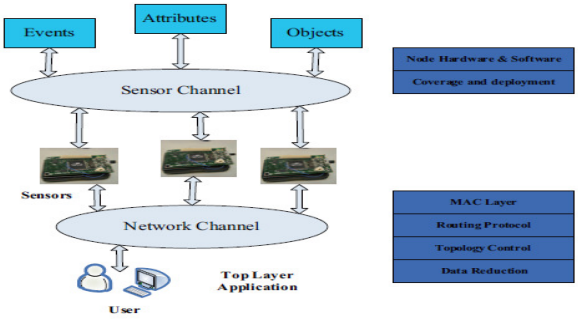

Fig 1.1 WSN Architecture

II. LITERATURE SURVEY

C. Intanagonwiwat et. al.[6] proposed a popular data aggregation paradigm for WSNs, called directed diffusion.Directed diffusion is a data-centric (DC) and application- aware paradigm in the sense that all data generated by sensor nodes is named by attribute-value pairs. The main idea of the DC paradigm is to combine the data coming from different sources enroute (in-network aggregation) by eliminating redundancy, minimizing the number of transmissions; thus saving network energy and prolonging its lifetime.

Rumor routing [7] is a variation of directed diffusion and is mainly intended for applications where geographic routing is not feasible. In general, directed diffusion uses flooding to inject the query to the entire network when there is no geographic criterion to diffuse tasks. However, in some cases there is only a little amount of data requested from the nodes and thus the use of flooding is unnecessary. An alternative approach is to flood the events if the number of events is small and the number of queries is large. The key idea is to route the queries to the nodes that have observed a particular event rather than flooding the entire network to retrieve information about the occurring events.

Heinzelman, et. al. [8] introduced a hierarchical clustering algorithm for sensor networks, called Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH is a cluster-based protocol, which includes distributed cluster formation. LEACH randomly selects a few sensor nodes as clusterheads (CHs) and rotate this role to evenly distribute the energy load among the sensors in the network. In LEACH, the clusterhead (CH) nodes compress data arriving from nodes that belong to the respective cluster, and send an aggregated packet to the base station in order to reduce the amount of information that must be transmitted to the base station. LEACH uses a TDMA/CDMA MAC to reduce inter-cluster and intra-cluster collisions. However, data collection is centralized and is performed periodically. Therefore, this protocol is most appropriate when there is a need for constant monitoring by the sensor network. An enhancement over LEACH protocol was proposed.The protocol, called Power-efficient Gathering in Sensor Information Systems (PEGASIS)[9], is a near optimal chain-based protocol. The basic idea of the protocol is that in order to extend network lifetime, nodes need only communicate with their closest neighbors and they take turns in communicating with the base-station. When the round of all nodes communicating with the base-station ends, a new round will start and so on. This reduces the power required to transmit data per round as the power draining is spread uniformly over all nodes. Hence, PEGASIS has two main objectives. First, increase the lifetime of each node by using collaborative techniques and as a result the network lifetime will be increased. Second, allow only local coordination between nodes that are close together so that the bandwidth consumed in communication is reduced.

Subramanian et al. [9] describes a self-organizing protocol and an application taxonomy that was used to build architecture used to support heterogeneous sensors. The routing architecture is hierarchical where groups of nodes are formed and merge when needed. Local Markov Loops (LML) algorithm, which performs a random walk on spanning trees of a graph, was used to support fault tolerance and as a means of broadcasting. Such approach is similar to the idea of virtual grid used in some other protocols that will be discussed later under location- based routing protocols. In this approach, sensor nodes can be addressed individually in the routing architecture, and hence it is suitable for applications where communication to a particular node is required. communication in EEUC mechanism.

Marti et al. [10] and Buchegger and Boudec [11] consider the problem of minimizing the effect of misbehaving or selfish nodes on routing through punishment, reporting, and holding grudges. These application of these techniques to sensor networks is promising, but these protocols are vulnerable to blackmailers.

Perrig et al. [12] present two building block security protocols optimized for use in sensor networks, SNEP and TESLA. SNEP provides confidentiality, authentication, and freshness between nodes and the sink, and u-TESLA provides authenticated broadcast.

III. PROPOSED WORK

We are representing energy efficient secure routing in case of a Wireless Sensor Network. In it we use Grid network to represent the proposed work.

In our work there are number of possible approaches of routing. One of such approach is Horizontal-Vertical Mapping. In this, first move one step horizontally and the one step node vertically. Because of this approach the load on the centralized node increased.

To resolve this problem there are some existing methods:-

- Shifting the load on neighbor node based on minimum load
- Removing the center node.

There are many more problems which are solved by proposed work.

The major problem is **node replication problem** .In order to solve node replication problem we use an approach to detect the replicated node in wireless sensor networks is centralized scheme. In the Centralized scheme, all nodes in the network transfers data to central node by camparing ID of neighbouring node to which

data to be sent .If any node have same ID that already exists then one node is attacker node then remove that node from the network.Central node contains ID of each node of the network if there is any replicated node then it can be detected on central node & replicated node is removed from the network.

Another problem is related to **secure monitoring** of sensor nodes in WSNs. To solve this problem we can set an alarm watch on the central node.When load of central node increases from threshold value means increases from the value of neighbouring node then central node signals an alarm.After signaling alarm, load of central node distributed to its neighbours.From this we can save energy of sensor nodes which is wasted due to false alarms.

Another problem is related to **data aggregation** on sensor node. Routing protocols providing an optimal data transmission route from sensor nodes to sink to save energy of nodes in the network. Data aggregation plays an important role in energy conservation of sensor network. Data aggregation methods are used not only for finding an optimal path from source to destination but also to eliminate the redundancy of data, since transmitting huge volume of raw data is an energy intensive operation, and thus minimizing the number of data transmission. Also multiple sensors may sense the same phenomenon, although from different view and if this data can be reconciled into a more meaningful form as it passes through the network, it becomes more useful to an application. Moreover when data aggregation is performing data is compress as it is passed through the network, thus occupying less bandwidth. This also reduces the amount of transmission power expended by nodes. Hence secure data aggregation can be considered as a very challenging problem in wireless sensor network.

IV. SIMULATION RESULTS

Fig. 4.1 Packet Lost vs. Packet Received (existing)

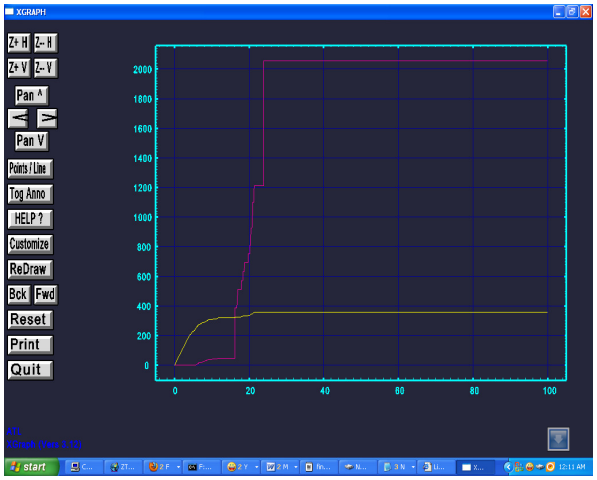

Fig 4.2 Packet Lost Vs. Packet Received (Proposed)

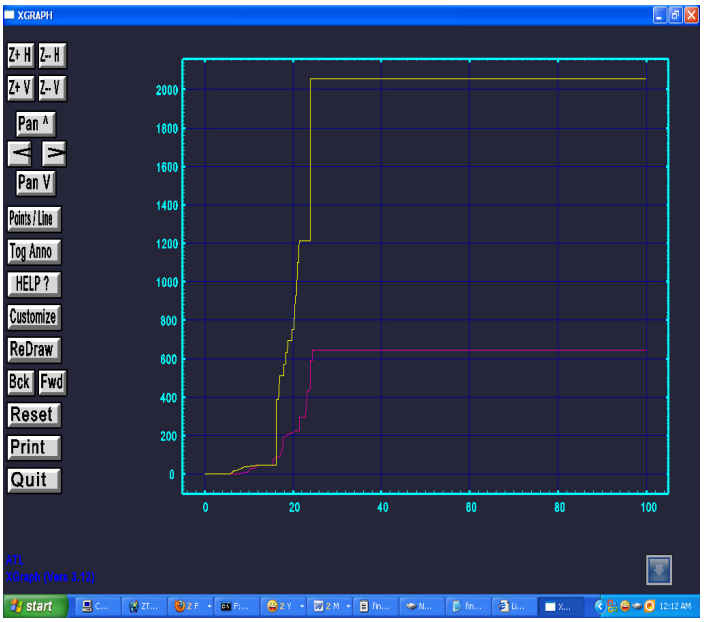

Fig 4.3 Packet Received (Existing Vs. Proposed)

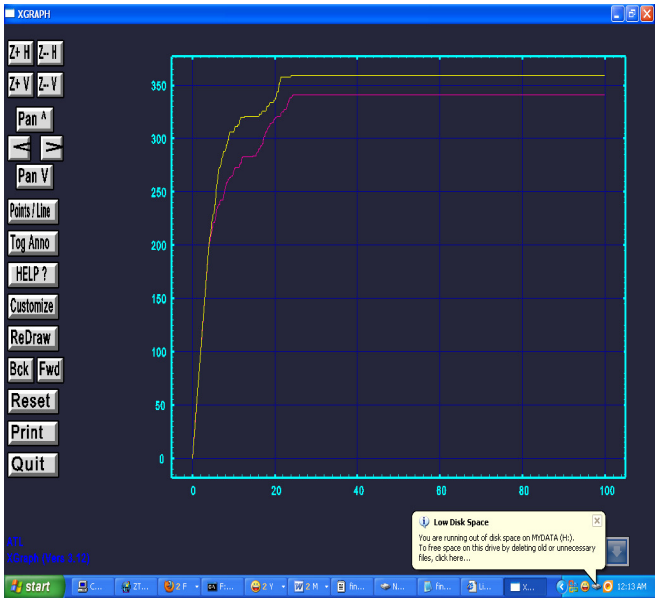

Fig 5.11 Packet Lost (Existing Vs. Proposed)

V. CONCLUSION

We analyzed Horizontal–Vertical method that performs better load balancing of the grid network, all communication mode in a grid network. We will first identify the center node for the exceeding load limit and then release this node from the communication path. Now its load gets distributed on the surrounding other nodes. This distribution will be taken on basis of average distance from the center. After this central node is now not overloaded. Holes would also minimize in this approach. Energy consumption on central node will be

minimum so that the network can be used more efficiently.For security if any node is overloaded then its packets will distributed on neighbouring nodes for avoiding packet loss by overloaded node

REFERENCES

[1] Kumar.S.P. Chee-Yee Chong. Sensor networks: Evolution, opportunities, and challenges. Proc IEEE, August 2003.

[2] Sundeep Karthikeyan Vaidynathan, Sayantan sur and Sinha. Data aggre- gation techniques in sensor networks. Technical Report,OSU-CISRC-11/04-TR60, 2004.

[3] D. Agrawal N. Shrivastava, C. Buragohain and S. Suri. Medians and beyond: new aggregation techniques for sensor networks. Proceedings of the 2nd inter-national conference on Embedded networked sensor systems, pages 239-249, 2004.

[4] Xiuli Ren and Haibin Yu1. Security mechanisms for wireless sensor networks. IJCSNS International Journal of Computer Science and Network Security,VOL.6(No.3):100-107, March 2006.

[5] S. Setia S. Zhu and S. Jajodia. Leap: efficient security mechanisms for large scale distributed sensor networks. IEEEconference on Computer and communications security, pages 62-72.

[6] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks".

[7] D. Braginsky and D. Estrin, Rumor Routing Algorithm for Sensor Networks," First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, October 2002.

[8] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Hawaii International Conference on System Sciences (HICSS '00), January 2000.

[9] S. Lindsey, C. Raghavendra, PEGASIS: Power-Efficient Gathering in Sensor Information Systems", IEEE Aerospace Conference Proceedings, 2002, Vol. 3, 9-16 pp. 1125-1130.

[10] L. Subramanian and R. H. Katz, An Architecture for Building Self Configurable Systems", in the Proceedings of IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing, Boston, MA, August 2000. [18] S. Marti, T. J. Giuli, K. Lai, and M. Baker, “Mitigating routing misbehavior in mobile ad hoc networks,” in Sixth annual ACM/IEEE Internation Conference on Mobile Computing and Networking, 2000, pp. 255–265.

[11] S. Buchegger and J.-Y. L. Boudec, “Nodes bearing grudges: Towards routing security, fairness, and robustness in mobile ad hoc networks,” Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing. Canary Islands, Spain: IEEE Computer Society, January 2002, pp. 403–410.

[12] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, “SPINS: Security protocols for sensor networks,” Mobile Networking and Computing 2001, 2001.