PROPOSED SCHEME FOR RELIABLE DATA TRANSFER IN WIRELESS SENSOR NETWORKS

Pooja Singhal[1], Pankaj Gupta[2],
[1] M.Tech, Scholar, Vaish College of Engineering, M.D.U, Rohtak, India
[2]Professor, Cse Dept.Vaish College of Engineering, Rohtak
poojasinghal273@gmail.com, pankajgupta.vce@gmail.com,

ABSTRACT :- **Wireless sensor networks are a new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. When we work with a large sensor area network with dense sensors , there are some nodes that has to bear the heavy traffic load then over the time such sensor goes weak and they start losing the packet. This packet loss is bearable up to some threshold value, but as the packet loss exceed this level it disturb the whole network and now any kind of data transfer over this node is not reliable. In this paper author will proposed a algorithm that will solve the problem of packets lost and improve the reliability of network. The author will implement this algorithm by help of NS-2 simulator.**

Keywords:-Wireless,Sensors,Data Loss,Aggregation, NS-2S.

I. INTRODUCTION

Wireless Sensor Networks have emerged as an important new area in wireless technology. In the near future, the wireless sensor networks are expected to consists of thousands of inexpensive nodes, each having sensing capability with limited computational and communication power [1] , [2] and [3] which enable us to deploy a large-scale sensor network. Wireless sensor nodes have emerged as a result of recent advances in low-power digital and analog circuitry, low-power RF design and sensor technology. Sensor networks are distinct from traditional computing domains. Their Design assumes being embedded in common environments, instead of dedicated ones. As these devices are deployed in large numbers, they will need the ability to assist each other to communicate data back to a centralized collection point. A critical step towards achieving this goal of cooperative mini device is the design of a software architecture that bridges the gap between raw hardware capabilities and a useful system.

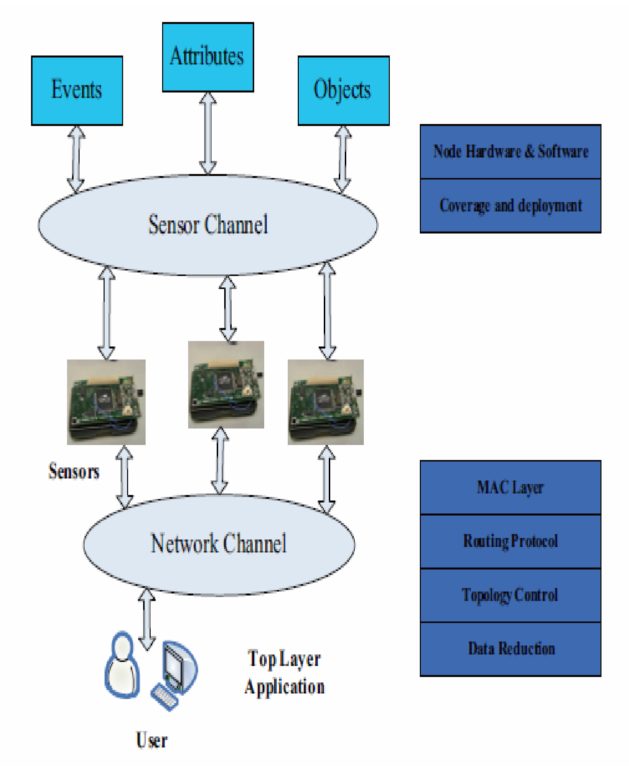

Fig 1 :- Wireless Sensor Network Architecture

1.1 The design of WSN is influenced by many challenging factors. They are following:-

- **Node deployment:** Node deployment in WSN is application dependent and affects the performance of the routing protocol. The deployment can be either deterministic or randomized. In deterministic deployment, the sensors are manually placed and data is routed through pre-determined paths. However, in random node deployment, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner.

- **Energy consumption without losing accuracy:** In a multihop WSN each node plays a dual role as data sender and data router. The malfunctioning of some sensor nodes due to power failure can cause significant topological changes and may need rerouting of packets and reorganization of network.
- **Data Reporting Model:** Data sensing and reporting in WSN is dependent on the application and the time criticality of the data reporting. Data reporting can be categorized as either time-driven (continuous), event-driven, query-driven, The routing protocol is highly influenced by the data reporting model with regard to energy consumption and route stability.
- **Node/Link Heterogeneity:** In many studies, all sensor nodes were assumed to be homogeneous, i.e., having equal capacity in terms of computation, communication, and power. However, depending on the application a sensor node can have different role or capability. The existence of heterogeneous set of sensors raises many technical issues related to data routing.
- **Fault Tolerance:** Nodes may fail due to power failure, physical damage etc. This may require actively adjusting transmit powers and rerouting packets through regions of the network where more energy is available.
- **Network Dynamics:** Routing messages from or to moving nodes is more challenging since route stability becomes an important issue, in addition to energy, bandwidth etc.
- **Transmission Media:** In a multi-hop sensor network, communicating nodes are linked by a wireless medium. The traditional problems associated with a wireless channel (e.g., fading, high error rate) may also affect the operation of the sensor network.
- **Coverage:** In WSN, each sensor node obtains a certain view of the environment. Hence area coverage is also an important design parameter in WSN.
- **Data Aggregation:** Since sensor nodes may generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions is reduced.
- **Data aggregation:** Data aggregation is the combination of data from different sources according to a certain aggregation function. Quality of Service: In some applications, data should be delivered within a certain period of time from the moment it is sensed; otherwise the data will be useless. Therefore bounded latency for data delivery is another condition for time-constrained applications.

II. LITERATURE REVIEW:

In paper [2] we have studied the WSN hardware platforms and secondly about the software platform. Then we study the details information about networking and applications of the Wireless Sensor Networks. At last, idea of the future application of the wireless sensor networks is given.

Paper [35] discuss the introduction of wireless sensor network, how it works, WSN nodes architecture, WSN architecture, power consideration WSN and applications of wireless sensor network.

Paper [10] describes the concept of sensor networks which has been made viable by the convergence of micro electro-mechanical systems technology, wireless communications and digital electronics. The sensing tasks and the potential sensor networks applications are explored, and a review of factors influencing the design of sensor networks is provided. The communication architecture for sensor networks is outlined, and the algorithms and protocols for each layer are explored.

Paper [5] presents a dynamic discover routing method for communication between sensor nodes and a base station in WSN. This method tolerates failures of arbitrary individual nodes in the network (node failure) or a small part of the network (area failure). Each node in the network does only local routing preservation, needs to record only its neighbor nodes' information, and incurs no extra routing overhead during failure free periods.

Paper [3] gives details information about networking and applications of the Wireless Sensor Network and the future application of the wireless sensor networks.

Paper [32] Wireless sensor networks are often deployed in unattended and hostile environments, leaving individual sensors vulnerable to security compromise. We study the novel notion of location-based keys for designing compromise-tolerant security mechanisms for sensor networks.

Paper [30] gives idea of localized sensor localization scheme making full use of controlled mobility of a location-aware actor and the connectivity of the sensor network.

III. PROPOSED WORK:-

We are representing reliable data transfer over the network in case of a Wireless Sensor Network. To solve this problem the proposed system identify the low power nodes, because in sensor area network it is not possible to track all the nodes always

The proposed algorithm we will use for solve the problem of low power nodes in wireless sensor network. In this algorithm we follow the following step:-

Main Algorithm(S,D)

/*S is the source node and D is the destination node, the network defined is dynamic*/

```
{
1.    Find all the nodes that occur in path between
      source and the destination. These nodes are
      representing by NodeList(1 to N ).
2.    for i=1 to N
3.    {
4.    if(PacketLoss(NodeList(i))>
      MAX_THRESHOLD_VALUE)
5.    {
    6.    find the list of compromising nodes for Node NodeList(i). This list is represented by Compromising(1 to K)
    7.    Select any of the compromising node from this list and use it in place of node dropping the data packet
          NodeList(i)=Rand(Compromising,1,k)

    8.    if K= 0  /* if there is no compromising node*/
    9.    {
    10.   NodeList(i)=Include New Node
    11.   }
    12.   }
    13.   }


}
```

IV. FUTURE WORK

This paper shows the Study of wireless sensor network. Based on the study the author identified some problems. So low power nodes (packets lost and unreliable transmission) is one problem among. To solve this problem the author proposed algorithm that will give the best result based on performance and security. The proposed algorithm first detects the weak sensor node over the network and then blocks it or set its load to the minimum. .This algorithm will implement using ns-2 simulator.

REFERENCES:-

[1] W. Su Y. Sankarasubramaniam E. Cayirci Akyildiz, I.F. A survey on sensor- networks. *IEEE Communications Magazine*, pages 102{114, 2002.

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

[3] Ismail H. Kasimoglui Ian .F. Akyildiz. Wireless sensor and actor :research challenges. *(Elsevier) Journal*, 2(38):351{367, 2004.

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

[5] 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. ACM Press.

[6] 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.

[7] S. Setia S. Zhu and S. Jajodia. Leap: e±cient security mechanisms for large scale distributed sensor networks. *Proceedings of the 10th ACM conference on Computer and communications security*, pages 62{72, 2003. ACM Press.

[8] J. Stankovic A. Perrig and D. Wagner. Security in wireless sensor networks.

[9] P.Nair H.Cam, S.Ozdemir and D. Muthuavinashiappan. Espda: Energy-efficient and secure pattern based data aggregation for wireless sensor networks. *Computer Communications IEEE Sensors*, 29:446{455, 2006.

[10] L. Eschenauera nd V. Gligor. A key-managemensct hemef or distributed sensor networks. In *Proceedings of the ACM Conference on Computer and Communication Security (CCS),* Nov. 2002.

[11] H. Chan, A. Perrig, and D. Song. Randomk ey predistribution schemes for sensor networks. In *Proceedings of IEEE Symposium on Security and Privacy,* May 2003.

[12] F. Bouhafs, M. Merabti, and H. Mokhtar, *A Semantic Clustering Routing Protocol for Wireless Sensor Networks*, Proceedings of the 3rd IEEE Consumer Communications and Networking Conference, 2006, pp. 351-355.

[13] I.K. Ibrahim, R. Kronsteiner, and G. Kotsis, *A Semantic Solution for Data Integration in Mixed Sensor Networks*, Computer Communications, 28(13), Elsevier, 2005, pp. 1564-1574.

[14] E. Fasolo, *In-network Aggregation Techniques for Wireless Sensor Networks: A survey*, IEEE Wireless Communications, 14(2), 2007, pp. 70-87.

[15] Krishnamachari, B.; Estrin, D.; Wicker, S. *Modeling Data-Centric Routing in Wireless Sensor Networks*. USC Computer Engineering Technical Report CENG 02-14, 2002.

[16] 6. Yen, H.H.; Lin, F.Y.S.; Lin, S.P. Energy-Efficient Data-Centric Routing in Wireless Sensor Networks. *IEICE Trans. Commun.* **2005**, *E88-B*, 4470-4480.

[17] C. F. Li, M. Ye, G. Chen, and J. Wu, “An Energy-Efficient Unequal Clustering Mechanism for Wireless Sensor Networks,” *IEEE International Conf. Mobile Adhoc and Sensor Systems*, pp. 8, Nov. 2005.

[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.

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

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