Volume 3, Issue 11, November 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Energy Aware Hybrid Approach for Data Aggregation in Wireless Sensor Networks

Anshul Bansal[1], Dinesh Kumar[2]
Department of Computer Sciences & Engineering,
R.P. Inderaprastha Institute of Technology, Karnal, Haryana, India

Abstract: The emerging field of wireless sensor networks combines sensing, computation, and communication into a single tiny device. Through advanced mesh networking protocols, these devices form a sea of connectivity that extends the reach of cyber space out into the physical world. Unlike traditional wireless devices, wireless sensor nodes do not need to communicate directly with the nearest high power control tower or base station, but only with their local peers. This Paper Presents the power of wireless sensor networks lies in the ability to deploy large numbers of tiny nodes that assemble and configure themselves. Usage scenarios for these devices range from real time tracking, to monitoring of environmental conditions, to ubiquitous computer environment, to in situ monitoring of the health of structures or equipment. While often referred to as wireless sensor networks, they can also control actuators that extend control from cyberspace into the physical world

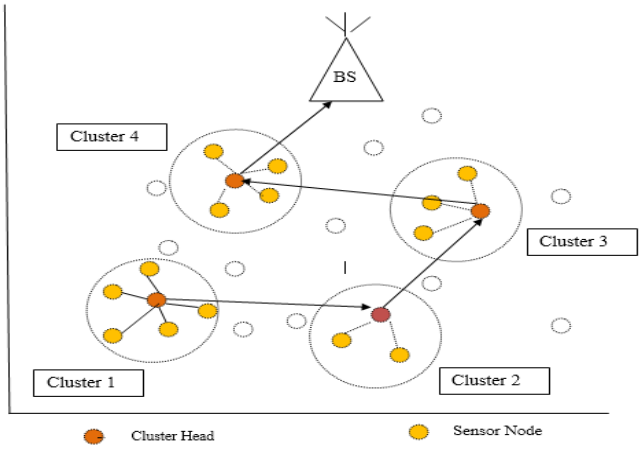
Keywords -wireless sensor networks; Energy; Power; Hybrid.Data Aggergation.

I. INTRODUCTION

Data Aggregation typically involves the mixture of data from multiple sensors at intermediate nodes and transmission of the aggregated data to the base station (sink). Data aggregation efforts to collect the most critical data from the sensors and make it available to the sink in an energy efficient manner with minimum data latency. Data latency is important in many applications such as environment monitoring, where the freshness of data is also an important factor. It is critical to develop energy-efficient data-aggregation algorithms so that network lifetime is enhanced. There are several factors which determine the energy efficiency of a sensor network, such as network architecture, the data-aggregation mechanism, and the underlying routing protocol. Routing protocols can be generally grouped in two broad categories: reactive and proactive protocols. Proactive routing protocols use some kind of periodic beaconing or coordination mechanisms between nodes to pro-actively maintain routing tables at each node. Conversely, reactive protocols don't attempt to maintain routing tables continually; in- stead, they initiate route discovery only when the route is required for a packet transmission. Discovered routes are temporarily cached to be used for subsequent requests addressed to the same node, but will eventually expire after a period of inactivity. The proposed protocol is based on two ways of data aggregation with saving of reliability; the first way is based on distribution of aggregation process by involving additional sensor nodes. The second one is based on complex report interaction between base station and aggregator.

II- METHODOLOGIES

Proposed Model for Data Aggregation



Key issues in architecture:

There are four key issues that must be addressed by the system architecture:

- Firstly, from the basic description of a wireless communication protocol it can be seen that several operations must occur in parallel. The channel must be continually monitored, data must be encoded and bits must be transferred to the radio. The ability to deal with fine grained concurrency is required in order to perform these operations in parallel. Secondly, the system must be flexible to meet the wide range of target application scenarios.

Thirdly, the architecture must provide precise control over radio transmission timing. This requirement is driven by the need for ultra-low power communication in the data collection application scenario.

Finally, the system must be able to decouple the data path, speed and the radio transmission rate.

Factors influencing sensor network design

A sensor network design is influenced by many factors, which include fault tolerance; scalability; production costs; operating environment; sensor network topology; hardware constraints; transmission media; and power consumption. These factors are addressed by many researchers as surveyed in this paper. However, none of these studies has a full integrated view of all factors that are driving the design of sensor networks and sensor nodes. These factors are important because they serve as a guideline to design a protocol or an algorithm for sensor networks. In addition, these influencing factors can be used to compare different schemes.

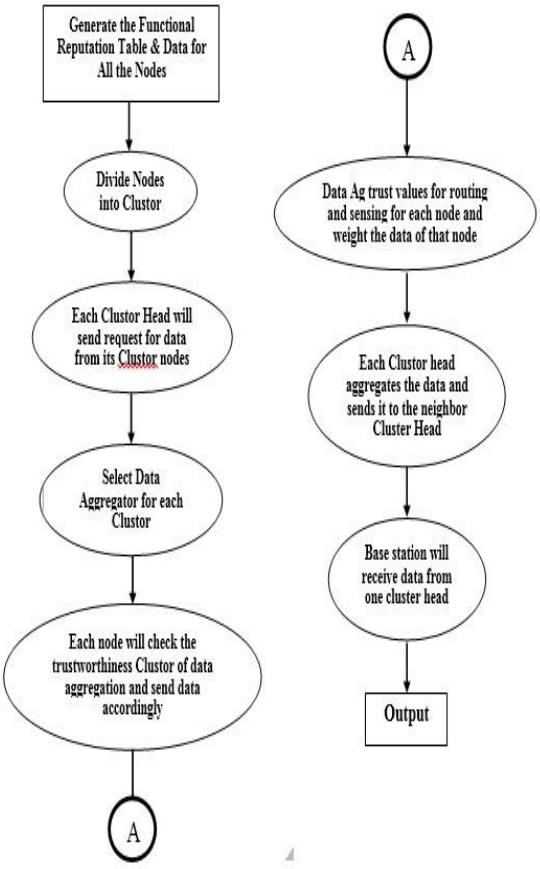
Power consumption

The wireless sensor node, being a micro-electronic device, can only be equipped with a limited power source (<0.5Ah, 1.2V). In some application scenarios, replenishment of power resources might be impossible. Sensor node lifetime, therefore, shows a strong dependence on battery lifetime. In a multi-hop ad hoc sensor network, each node plays the dual role of data originator and data router. The disfunctioning of few nodes can cause significant topological changes and might require re-routing of packets and re-organization of the network. Hence, power conservation and power management take on additional importance. It is for these reasons that researchers are currently focusing on the design of power-aware protocols and algorithms for sensor networks.

The power management plane manages how a sensor node uses its power. For example, the sensor node may turn off its receiver after receiving a message from one of its neighbors. This is to avoid getting duplicated messages. Also, when the power level of the sensor node is low, the sensor node broadcasts to its neighbors that it is low in power and cannot participate in routing messages. The remaining power is reserved for sensing. The mobility management plane detects and registers the movement of sensor nodes, so a route back to the user is always maintained, and the sensor nodes can keep track of who are their neighbor sensor nodes. By knowing who the neighbor sensor nodes are, the sensor nodes can balance their power and task usage.

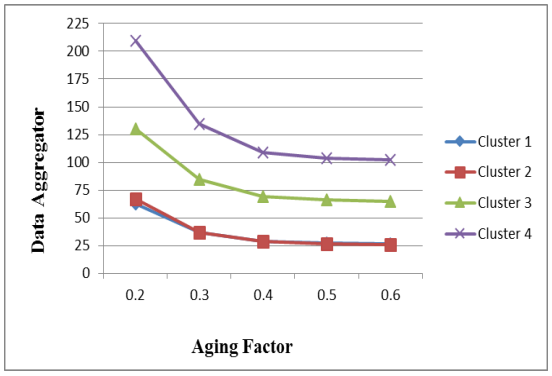
III. RESULTS

A. Figure: - Flow Chart of Proposed Model

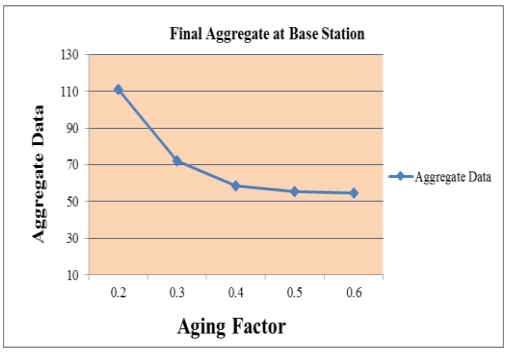


B. Result.

With the simulation result, it can be shown that the protocol implemented in this paper is more energy efficient & secured.



B. Figure: Data Aggregator For All Cluster.



C. Figure: Final Data Aggregater

IV- Conclusion

In wireless sensor networks, compromised sensor nodes can distort the integrity of aggregated data by sending false data reports and injecting false data during data aggregation. Since cryptographic solutions are not sufficient to prevent these attacks, general reputation based trust systems are proposed in the literature. The Proposed Algorithm introduces Cluster based Functional Reputation Data Aggregation concept. In this System total processing is based on cluster and a cluster is a collection of nodes and the aggregator node is selected automatically. Future work includes the simulation of this protocol on any simulation software such as Network Simulator (NS-2) or QUALNET or any other simulation software and get the exact results and compare these results with the implementation results of another reliable data aggregation protocol i.e "Ant Colony data gathering protocol". Carrying out more detailed simulator runs would also allow the protocols to be evaluated in more detail

References

[1] R.Rajagopalan and P.K.Varshney, "Data aggregation techniques in sensor networks: A survey", IEEE Communications Surveys and Tutorials, vol.8, no. 4, 4th Quarter 2006.

[2] I.Khemapech, I.Duncan and A.Miller, "A Survey of Wireless Sensor Networks Technology", School of Computer Science, University of St Andrews, North Haugh, St Andrews, Fife, KY16 9SX.

[3] Tamara Pazynyuk, JiangZhong Li, George S. Oreku, "Reliable Data Aggregation Protocol for Wireless Sensor Networks", IEEE 2008.

[4] Hong Luo, Qi Li, Wei Guo , "RDA: Data Aggregation Protocol for WSNs", Beijing Key Laboratory of Intelligent Telecommunications Software and Multimedia, IEEE2006 (p 1-4).

[5] Yi Yang, Xinran Wang, Sencun Zhu, and Guohong Cao, "SDAP: A Secure Hop by Hop Data Aggregation Protocol for Sensor Networks", Department of Computer Science & engineering, The Pennsylvania State University, ACM 2006 (p 1-12).

[6] A.Srinivasan, J.Teitelbaum, H.Liang, J.Wu, and M.Cardei, "Reputation and Trust-Based Systems for Ad Hoc and Sensor Networks",Algorithms and Protocols for Wireless Ad Hoc and Sensor Networks, Wiley and Sons, 2008.

[7] H.C¸am, S.Ozdemir, P.Nair, and D.Muthuavinashiappan, and H.O.Sanli, "Energy-Efficient and secure pattern based data aggregation for wireless sensor networks", Special Issue of Computer Communications on Sensor Networks, pp. 446-455, Feb. 2006.

