International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.2, Issue No.8, pp : 797-802 1 Aug. 2013

"Designing a Multi Hop Secured Reactive Routing Protocol for Heterogeneous Wireless Sensor Network using Clustering"

Sapan Kumar Jain[1], Vivek Badhe[2]

[1] Student of M. Tech Computer technology and application (CSE deptt.), Gyan Ganga College of Technology Jabalpur (R.G.P.V University BHOPAL), India
sapan.jin@gmail.com
[2]Faculty member in Gyan Ganga college of Technology, Jabalpur, India
Vivekbadhe@yahoo.com

Abstract: In the wireless sensor network we used hundreds of sensor node. If energy, range and hardware capabilities are different in various nodes in the network than these types of network are mainly known as heterogeneous network. It is noted that, to maintain a reliable information delivery, data aggregation and information security that is necessary for efficient and effective communication between these sensor nodes. Only concise information should be delivered to the sink nodes to reduce communications energy which help to increase the effective network lifetime with optimal data delivery to base station and end user. An inefficient use of the available energy of nodes leads to unreliable performance and short life cycle of the sensor network. Energy in the sensors is a scarce resource and must be managed in an efficient manner to expand the life of network. We want to design a secure multi-hop reactive protocol for heterogeneous wireless sensor network with clustering.

1. Introduction: We study the Impact of heterogeneity of nodes, in terms of their hardware, range and energy, in wireless sensor networks that are hierarchically clustered. In heterogeneous network some high-energy nodes are elected as "cluster heads" to aggregate the data of their cluster members and transmit it to the chosen "Base station (sink node)" which are also high energy node [1]. It requires the minimum communication energy to reduce the energy consumption of cluster head and maximize the energy utilization of all nodes and properly balance energy dissipation.

In this work, a heterogeneous sensor deployment and topology control method is presented. It aims to deal with the deployment problem of heterogeneous sensor nodes with different communication and sensing range. In addition, an irregular sensor model is proposed to approximate the behavior of sensor nodes. According to experiment results, the proposed method can achieve longer life rate under the same deployable sensor nodes in different network. Besides, the deployment cost is much lower with different configurations of sensor nodes. The fundamental aim of any routing protocol is to furnish the network useful and efficient. A routing protocol organizes the activities of individual nodes in the network to achieve global goals and do so in a proficient manner. In the following subsection existing routing models are discussed.

There are mainly three type of network based on data information. The nodes in proactive type of network periodically switch on their sensors and transmitters. It senses the environment and transmits the data of interest. They provide a snapshot of the relevant parameters at regular intervals [2]. It is not continuously transfer the data over the network .They are well suited for applications requiring periodic data monitoring For example protocol such as leach and pegasis protocol [3]. In the reactive networks, nodes sense the value or react immediately as soon as changes occur in networks. It's not work from time to time but when sudden and drastic changes in the value of a sensed attribute is measured it reported to the base station at any time. Reactive protocol is well suited for those applications where time is critical factor like military field applications [4]. It is a combination of proactive and reactive network.

The nodes in such a network not only react to time-critical situations, but also work at periodic intervals in a very energy efficient manner for entire network [5]. Hybrid network enables the user to request past data, present data and future data from the available network in the form of historical queries, one-time queries and persistent query respectively. In our heterogeneous network, we considered this hybrid form of deployment and functioning.

Routing protocols are also classified based on sensor network architecture [6]. Various WSNs consist of homogenous nodes, while some WSNs consist of heterogeneous nodes. On the basis of different nodes **(homogeneous and heterogeneous)** we can check for which topology routing protocol will work whether they are operating on a flat topology or on a hierarchical topology. In Flat routing protocols all node in the network are having equal properties (like range, energy etc.). When node needs to send data, it may find a route consisting of other hops towards the sink. Hierarchical routing protocol is an approach used for heterogeneous networks where some of the nodes are more powerful than the other nodes in network. The hierarchy does not always depend on the power of nodes. In Hierarchical (Clustering) protocols different nodes are grouped to form clusters and data from nodes belonging to a single cluster can be grouped in single node (aggregated) [7].The hierarchical protocols have several advantages like scalability, energy efficient in Finding routing routes and easy to manage the path[8, 9, 10].

Wireless Sensor Network is performs not only civilian tasks but military tasks also. Traditional computer security techniques are not applicable as WSN also brings some resource constraints such as power and data storage with itself. The most important constraint in wireless sensor capabilities is Energy. In this work we will not only increase the life of the node and but also increase the lifetime of the entire network. On adding a cryptographic code in the network protocol energy impact on the node due to Encryption energy, Decryption energy, cryptographic storages etc are so considered [11]. In our routing protocol security constraints would be equally important as energy constraints and with security feature it is more efficient and reliable. Here are the security requirements for routing protocols are Data Confidentiality, Data Integrity, Data Freshness, Self-Organization and Time Synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to- end delay of a packet as it travels between two pair-wise sensors. A more collaborative sensor network may need group synchronization for tracking applications etc.

2. Proposed Protocol: Our main aim is to design a secure energy efficient reactive routing protocols for heterogeneous wireless sensor network using clustering. Regarding the designing aspects we have made certain assumptions:

2.1 First Order Radio Energy Model: The use of clusters for transmitting data to the base station leverages the advantages of small transmit distances for most nodes, it require only few nodes to transmit information from far distance node to the base station. In First order model [**12**], there is a great deal of research in the area of low-energy radios. Different assumptions about the radio characteristics, including energy dissipation in the transmission and receive nodes, will change the advantages of different protocols **[12]**. In our work, we assume a simple model where the radio dissipates 50nJ/bit to run the transmitter or receiver circuitry and 100pJ/bit/m2 for the transmit amplifier to achieve an acceptable Eb/No. These parameters are slightly better than the current state-of-the-art in radio design.

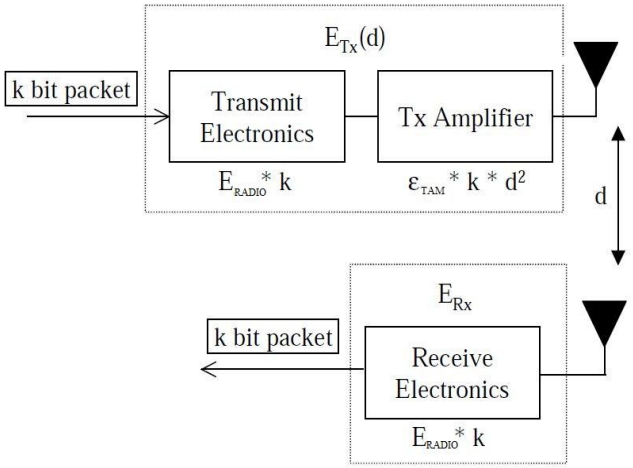


Figure 4.2: First order radio energy model [13]

Transmitting a k-bit message a distance d radio expends:

$E_{TX}(k, d) = E_{TX-elec}(k)$

$E_{TX}(k, d) = E_{TX-elec}(k) + E_{TX-amp}(k, d) + E_{ecc} + E_{sensing} + E_{switching} + E_{da} + E_{encrp}$

Where, k=number of bits, d= distance between two nodes. In table 2 we show the various parameters which are used to energy calculation of node. For these parameter values, receiving a message is not a low cost operation. Therefore the protocols should try to minimize transmit distances as well as number of transmit and receive operations for each message.

2.2 Algorithm for Network Deployment and Energy Computation

Setup phase and Deployment

In this phase we randomly deploy the sensor nodes and make the connection between sink node to the cluster heads and also the connection

Symbol	Description	Value (approx.)
E_{elec}	Energy consumed in the electronics circuitry to transmit or receive signal.	50nJ/bit
E_{TX-amp}	Energy consumed by the amplifier to transmit at a larger distance.	0.0013 pJ/bit/m^2
E_{ecc}	Energy consumed for error correction coding.	50 pJ/bit/m
$E_{sensing}$	Energy consumed for sensing and recording sound as in our military case.	100 pJ/bit/signal
$E_{switching}$	Energy consumed for switching between transmission ranges.	10 pJ
E_{da}	Energy consumed for data aggregation	5 nJ/bit/signal
E_{encrp}	Energy used for encrypting the data before transmission.	20 pJ/bit
$E_{processing}$	Energy used for processing the data received.	20 pJ/bit
E_{decyp}	Energy consumed for decrypting the data at the receiver end. [14]	20 pJ/bit

Table 2 Energy considerations in our routing protocol

$= E_{elec} * k + \varepsilon * k * d^2 + E_{ecc} + E_{sensing} + E_{switching} + E_{da} + E_{encrp}$

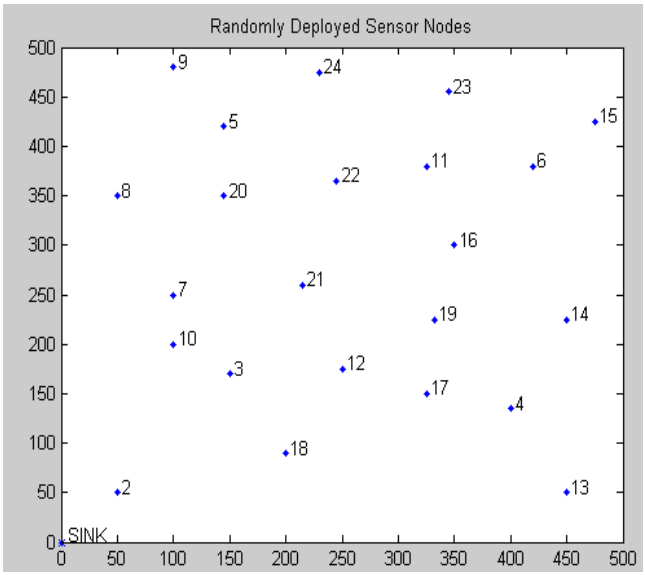
Receiving this message, radio expends:

$E_{RX}(k) = E_{RX-elec}(k) + E_{processing} + E_{decyp}$

$= E_{elec} * k + E_{processing} + E_{decyp}$

between cluster heads and their connected nodes. In Figure 5.1, Sensors are randomly deployed in the region (500m x500m). Total number of nodes in the region is 24, including the sink (base station) and heterogeneous node which will be the cluster heads. After deployment sensor node becomes stationary. In the simulation our aim is to calculate the total no. of round in a reactive network.

In Figure 5.2 , the node_id 1 represents the sink node and node_id 2,3,4,5 and 6 represent the cluster head with red circle. Remaining others are normal sensor nodes with less energy as compared to sink and cluster heads.



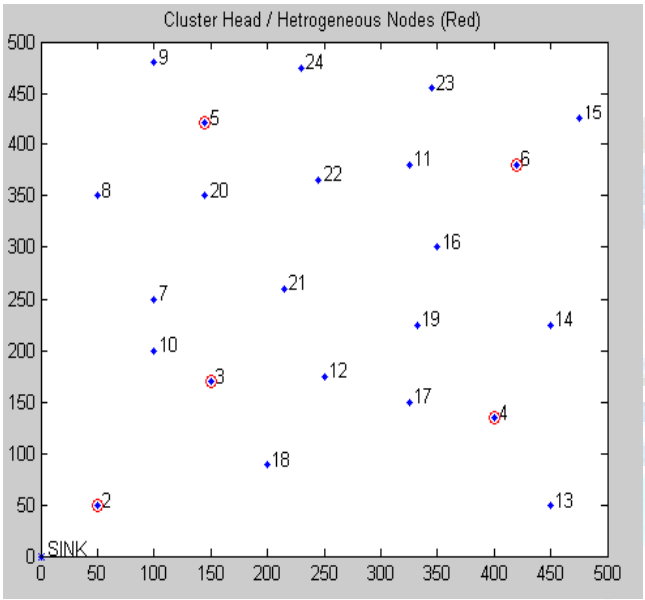


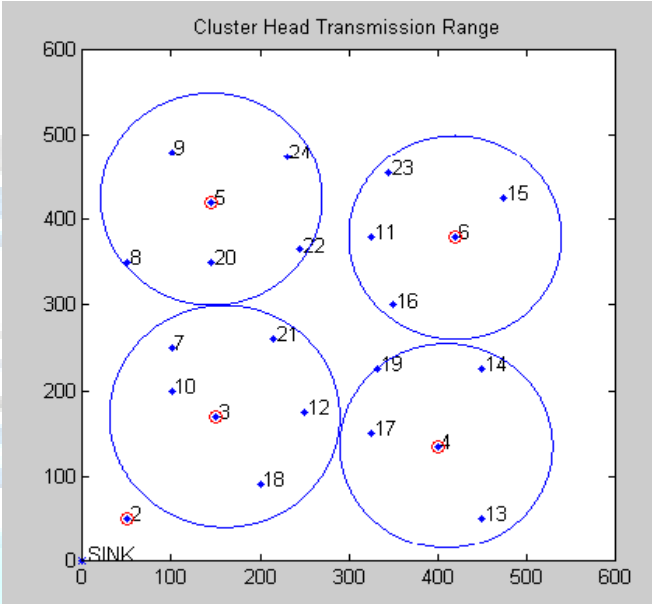
Figure 5.1 Randomly deployed sensor node

*Figure 5.2 cluster head selection*The initial energy of sink node is 5 joule, the cluster head energy is 2 joule and node energy of the remaining nodes is 1 joule (assumed). Sink node is defined at position (0,0) assumed that it is outside the selected region. In the Figure 5.3 we show the cluster head and its selected regionion. The cluster head represent its transmission range inside which various normal node can communicate with cluster head.

In fig 5.4 we show the connection link between the cluster region node with cluster head. In fig 5.5 we show the connection between the base (SINK node) station and cluster head.

After the above steps during the setup phase, the routing table is constructed. For example, node_id 8 path is {8, 5, 3, 1}.

2.3 Data delivery phase: After the routing table, the data delivery phase is started. Based on the distances between the sensors, the sensing energy, processing energy and communication energy are calculated and correspondingly the total energy is calculated. The processing energy of the node depends upon the data aggregation techniques and encryption-decryption techniques applied. The proposed protocol is for a secured application, so encryption-decryption energy is required to be calculated.



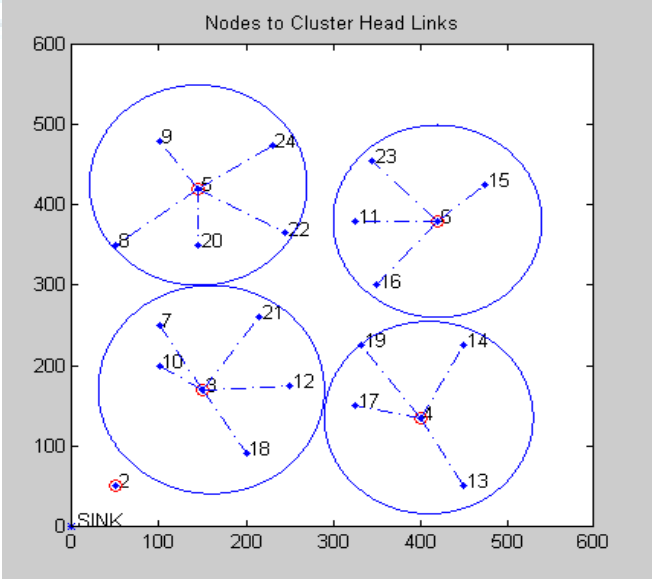


Figure 5.3 cluster head transmission range *Figure 5.4 nodes to cluster head links*

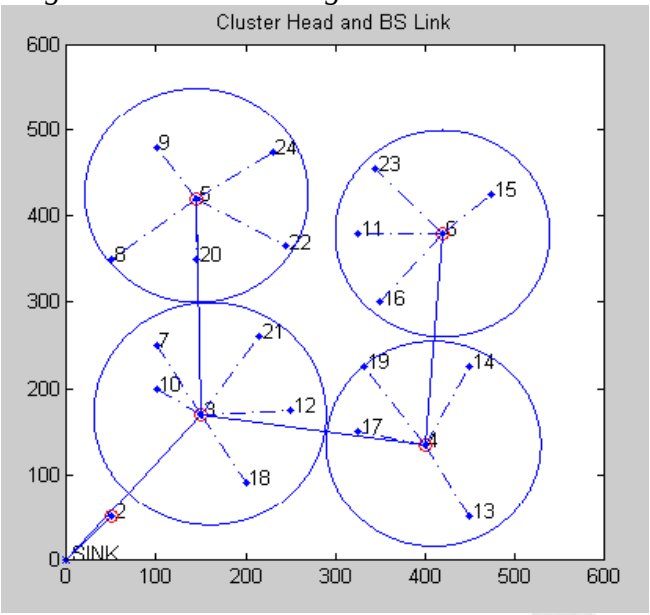
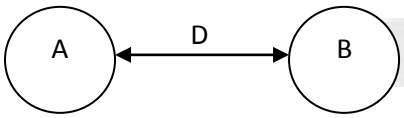


Figure 5.5 cluster Head and Sink link

Table 3 hop routing table for sink nodes

node_id	Routing Path
2	{2,1}
3	{3,1}
4	{4,3,1}
5	{5,4,3,1}
and so on…	…
22	{22,8,3,1)
23	{23,6,4,3,1}
24	{24,6,8,3,1}



In the above Figure, transmit the data from node A to node B. Suppose node A is sense the data and node B receive data after the following steps

3. Results: After the simulation we got the total number of rounds 66000 approximately in the case of reactive network and in the case of proactive network the number of rounds is approximately 10000. One Round means data transmit form any one node to base station. In this paper, we propose a heterogeneous WSN with random node deployment method which works as reactive protocol. It aims to deal with the deployment problem of heterogeneous sensor nodes with different communication and sensing range. In addition, with multi-hop model is proposed to utilize the energy of nodes and examine the energy calculation of sensor nodes. The deployment process is starting from sink node which is outside the selected region, and other nodes are deployed to the region centered with it.

According to simulation results, the suggested protocol achieve good coverage rate under as well as the deployment cost is much lower as compare with different configurations of sensor nodes. In the future work, a sensor node model considering environmental factors and individual behavior is needed. In addition, considering the interactions between different types of sensors is important. At least, the proposed method will be extended as the topology control protocol for heterogeneous WSN.

4. Reference

i. Chun-Hsien Wu1 and Yeh-Ching Chung1,Heterogeneous Wireless Sensor Network Deployment and Topology Control Based on Irregular Sensor Model, Second International Conference, GPC 2007, Paris, France,pp 78-88,May 2-4, 2007.

ii. Carlos Agreda Ninot DIRECTOR: Prof. Dr.-Ing. Ulrich Heinkel,Initialization algorithms for wireless ad-hoc networks,M.S in Telecommunication Engineering & Management,CHEMNITZ UNIVERSITY OF TECHNOLOGY,26 april 2010.

iii. Sunita Rani, Er.Tarun Gulati,AN IMPROVED PEGASIS PROTOCOL TO ENHANCE ENERGY UTILIZATION IN WSN,IJCCR,VOLUME 2 ISSUE 3 May 2012.

iv. Vidyasagar Potdar, Atif Sharif, Elizabeth Chang,Wireless Sensor Networks: A Survey,2009 International Conference on Advanced Information Networking and Applications Workshops,IEEE 2009,pp-636-641

v. N.Pushpalatha,B.Anuradha,A Comparative Analysis of WSN Sensor Positioning Method using Iterative Routing Algorithm with Conventional Methods,International Journal of Computer Applications (0975 – 8887)Volume 53– No.7, September 2012.

vi. *Jamal Al-Karaki, and Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A*

vii. *Survey", IEEE Communications Magazine, vol 11, no. 6, Dec. 2004, pp. 6-28.*

viii. *Shalini, Sangeeta Vhatkar,A Survey: Analysis of Characteristics and Challenges in Wireless Sensor Network Routing Protocols,IJAEEE,V2N1:119-125*

ix. *Dr. Praveena Chaturvedi,"Introduction to Wireless Sensor Networks ",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, pp 33-36, October 2012*

x. *Dilip Kumar and R. B. Patel,"Multi-Hop Data Communication Algorithm for Clustered Wireless Sensor Networks", International Journal of Distributed Sensor Networks,Volume 2011, Article ID 984795, 10 pages,25 February 2011*

xi. *Shio Kumar Singh, M. P. Singh, D. K. Singh," Applications, Classifications, and Selections of Energy-Efficient Routing Protocols for Wireless Sensor Networks",(IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES,Vol No. 1, Issue No. 2, pp-085 – 095*

xii. *Wireless Sensor Network Security: A Survey by John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary, Department of Computer Science Wayne State University,2006.*

xiii. *Energy-Efficient Communication Protocol for Wireless Microsensor Networks Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan Massachusetts Institute of Technology Cambridge.*

xiv. *Jun Zheng and Abbas Jamalipour, "Wireless Sensor Networks: A Networking Perspective", a book published by A John & Sons, Inc, and IEEEE, 2009.*

xv. *Shipra Khurana,Ashish Gupta,DESIGN AND ANALYSIS OF SECURITY ALGORITHMS FOR ROUTING IN WSN,IJREAS,Volume 2,Issue 2,pp-1066-1075,February 2012.*