International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.1., 2016
(Jan-Feb)

RESEARCH ARTICLE

ISSN: 2321-7758

AN EFFICIENT ROUTING PROTOCOL DESIGN USING FAST DATA TRANSFER CHANNEL SELECTION ALGORITHM

GURSHARAN SINGH RAI[1], RAMANJIT SINGH[2]

[1]Student, Electronics And Communication , LCET, Katani Kalan, Ludhiana,

[2]Assistant Professor, Electronics And Communication, LCET, Katani Kalan, Ludhiana

ABSTRACT

Lots of challenges are associated with sensor network. The applications of wireless sensor networks comprise a wide variety of scenarios. In most of them, the nfaetwork is composed of a significant number of nodes deployed in an extensive area in which not all nodes are directly connected. Then, the data exchange is supported by multi-hop communications. Routing protocols are in charge of discovering and maintaining the routes in the network. A new routing algorithm is proposed in which along with the distance, data rates and security is also consider. The route of each message destined to the base station is really crucial in terms network lifetime: e.g., using short routes to the base station.

Keywords: Wireless sensor network, routing protocol, DSR, DSDV, MATLAB

1. INTRODUCTION

Sensor networks are composed of thousands of resource constrained sensor nodes and also some resourced base stations are there. All nodes in a network communicate with each other via wireless communication. Moreover, the energy required to transmit a message is about twice as great as the energy needed to receive the same message. The route of each message destined to the base station is really crucial in terms network lifetime: e.g., using short routes to the base station that contains nodes with depleted batteries may yield decreased network lifetime. On the other hand, using a long route composed of many sensor nodes can significantly increase the network delay. But, some requirements for the routing protocols are conflicting. Always selecting the shortest route towards the base station causes the intermediate nodes to deplete faster. Always choosing the shortest path might result in lowest energy consumption and lowest network delay. The routing objectives are tailored by the application; e.g., real-time applications require minimal network delay. In sensor networks, energy is a critical resource, while applications exhibit a limited set of characteristics. Thus, there is both a need and an opportunity to optimize the network architecture for the applications in order to minimize resource consumed. The requirements and limitations of sensor networks make their architecture and protocols both challenging and divergent from the needs of traditional Internet architecture. A sensor network [1][4] is a network of many tiny disposable low power devices, called nodes, which are spatially distributed in order to perform an application-oriented global task. These nodes form a network by communicating with each other either directly or through other nodes. One or more nodes among

them will serve as sink(s) that are capable of communicating with the user either directly or through the existing wired networks. The primary component of the network is the sensor, essential for monitoring real world physical conditions such as sound, temperature, humidity, intensity, vibration, pressure, motion, pollutants etc. at different locations. Sensor network nodes are limited with respect to energy supply, restricted computational capacity and communication bandwidth. The ideal wireless sensor is networked and scale-able, fault tolerance, consume very little power, smart and software programmable, efficient, capable of fast data acquisition, reliable and accurate over long term, cost little to purchase and required no real maintenance. The basic goals of a WSN are to:

(i) determine the value of physical variables at a given location,
(ii) detect the occurrence of events of interest, and estimate parameters of the detected event or events,
(iii) classify a detected object
(iv) track an object.

Thus, the important requirements of a WSN are: (i) use of a large number of sensors, (ii) attachment of stationary sensors, (iii) low energy consumption, (iv) self organization capability, (v) collaborative signal processing, and (vi) querying ability.

Sensor networks have emerged as a promising tool for monitoring (and possibly actuating) the physical world, utilizing self-organizing networks of battery-powered wireless sensors that can sense, process and communicate.

2. PROBLEM FORMULATION

The attributes of WSNs and the characteristics of the environment within which sensor nodes are typically deployed make the routing problem very challenging. In this,we focused on issues central to routing in WSNs**.** Concerning the routing protocols, the reduced energy resources, the scalability and the resilience arise as the main limitations in wireless sensor networks. Mobile networks have attracted significant interests in recent years because of their improved flexibility and reduced costs. Routing is a fundamental issue for networks. A lot of routing algorithms have been proposed for wired networks and some of them have been widely used. Traditional protocols work on the basis of the distances between the nodes. The protocol that was based on distance approach was not efficient. The security and the data rates are the parameters that need to be consider while routing is done. As security of network will define how much data is transferred safely from one node to other, by in distance approach the security of the network was not consider, in this it was not checked whether the node to which data is send is attacker node or not .Another parameter was data rates, in traditional approach doesn't consider their data rate, i.e. is time in which packet data is send from source to destination. With the help of the data rates, the efficiency of the system is known, as data rate depend on the maximum amount of packet sent in an interval so the data rate of the system should be high .So these parameters should be taken in consideration while the routing is done in the network. So there is need a need to design a new protocol that is efficient than the traditional protocol, and should consider both security and data rates along with some other parameters, so that the routing in the system is much efficient, also the data rates and the security is considered.

3.PROPOSED WORK

Routing is a fundamental issue for networks. Routing mean to find the path between the nodes that are present in the network. Many algorithms have been proposed for the routing. The problem of the traditional approach was that it was entirely dependent upon the distance parameter. It would not consider any other parameter like data rate and security of the network, as these parameters should be consider while designing a network. So by studying previous algorithms, a new routing algorithm is proposed in which along with the distance, data rates and security is also consider. In this the network is created, calculation of the distance, data rate and the security is done. Then the basis of this the node is selected .it will check whether the node receiving data is attacker or not, it will also check the time of sending the data. And will calculate the distance between the node and the minimum distance node is selected. After

checking all these parameters the decision is made of selecting the path. So this approach is consider to be more efficient and secure than the traditional approach , as the parameters that are consider are more and can help in finding the best route .

.4. ROUTING OBJECTIVES

Some sensor network applications only require the successful delivery of messages between a source and a destination. However, there are applications that need even more assurance. These are the real-time requirements of the message delivery, and in parallel, the maximization of network lifetime.

1) ***Non-real time delivery*:** The assurance of message delivery is indispensable for al routing protocols. It means that the protocol should always find the route between the communicating nodes, if it really exists.
2) ***Real-time delivery*:** Some applications require that a message must be delivered within a specified time, otherwise the message becomes useless or its information content is decreasing after the time bound. Therefore, the main objective of these protocols is to completely control the network delay.
3) ***Network lifetime*:** This protocol objective is crucial for those networks, where the application must run on sensor nodes as long as possible. The protocols aiming this concern try to balance the energy consumption equally among nodes considering their residual energy levels. However, the metric used to determine the network lifetime is also application dependent.

5. ROUTING CHALLENGES AND DESIGN ISSUES

Depending on the application, different architectures and design goals/constraints have been considered for sensor networks.

1) ***Node deployment*:** It is application dependent and affects the performance of the routing protocol. The deployment is either deterministic or self-organizing. In deterministic situations, the sensors are manually placed and data is routed through pre-determined paths. Where as in self-organizing systems, the sensor nodes are scattered randomly creating an infrastructure in an ad hoc manner. In later the position of the sink or the cluster-head is also crucial in terms of energy efficiency and performance. When the distribution of nodes is not uniform, optimal clustering becomes a pressing issue to enable energy efficient network operation.

2) ***Power Consumption:*** Since the transmission power of a wireless radio is proportional to distance squared or even higher order in the presence of obstacles, multi-hop routing will consume less energy than direct communication. However, multi-hop routing introduces significant overhead for topology management and medium access control. Direct routing would perform well enough if all the nodes were very close to the sink.

3) ***Data Aggregation/Fusion:*** Since sensor nodes might generate significant redundant data, similar packets from multiple nodes can be aggregated so that the number of transmissions would be reduced. Data aggregation is the combination of data from different sources by using functions such as suppression (eliminating duplicates), min, max and average . As computation would be less energy consuming than communication, substantial energy savings can be obtained through data aggregation.

4) ***Node capabilities*:** Depending on the application a node can be dedicated to a particular special function such as relaying, sensing and aggregation since engaging the three functionalities at the same time on a node might quickly drain the energy of that node.

5) ***Scalability:*** Routing protocols should be able to scale with the network size. Also, sensors may not necessarily have the same capabilities in terms of energy, processing, sensing, and particularly communication.

Hence, communication links between sensors may not be symmetric, that is, a pair of sensors may not be able to have communication in both directions. This should be taken care of in the routing protocols.

SIMULATION RESULTS:

a) Block Diagram:

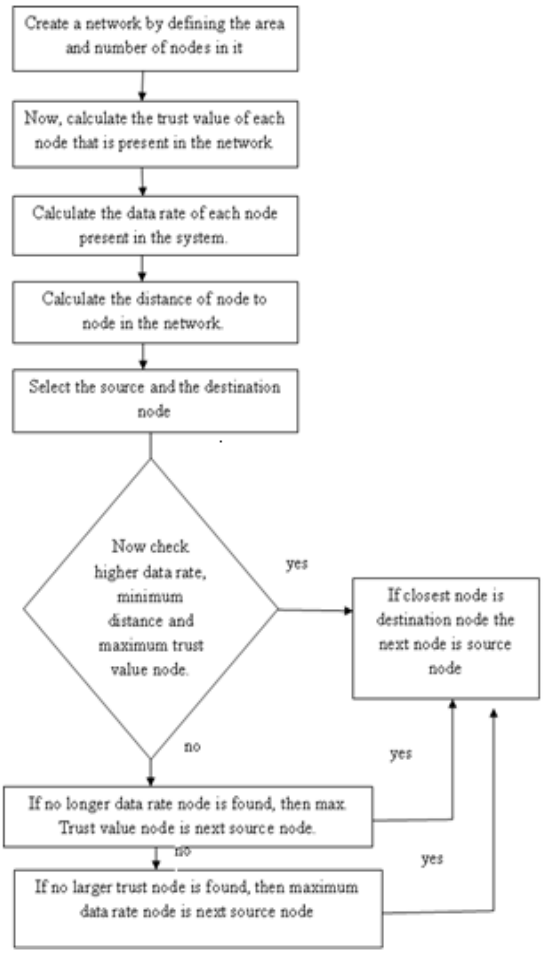

Fig 1:Block diagram of simulation

b) Methodology

In this a new approach is proposed in which along with the distance , data rates and security parameter is also considered for finding the route between the nodes, the proposed approach is considered to be better than the traditional distance approach, following is the methodology of the proposed work :-

1 In wireless communication, a network is created so that the communication is done between the nodes. For creating a network the area and number of nodes are defined, the nodes are placed in the specific area defined.

2 After the network is created by defining nodes and area, next step is to calculate the trust value of the each node that is present in the network area.

3 Now, calculate the data rate of each node, after calculating the trust values of nodes that is present in the network area.

4 After the calculation of the data rates and trust values, next step is calculate the distance between the nodes

5 Now , the selection of the source node and destination node is made , for checking the next source node and destination following conditions is checked

- If the selected node is having the higher data rate, minimum distance and maximum trust value node than that node is considered to be the next source node.

6 If step 5 is not true that means if no longer data rate node is found, then the maximum Trust value node is next source node.

7 If step 6 is not true that means no larger trust node is found, then maximum data rate node is next source node.

8 Finally a route is found on the basis of the step 5, 6 and 7. This is better routing algorithm .

c) Results and discussions

After implementing the above mentioned algorithm the results which are obtained are presented in form of graphs so that can be compared with the traditional approach.

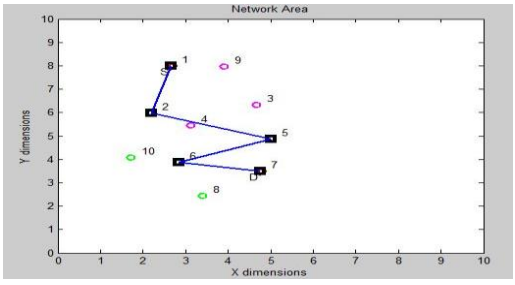

Fig 2: Final route selection after the proposed work

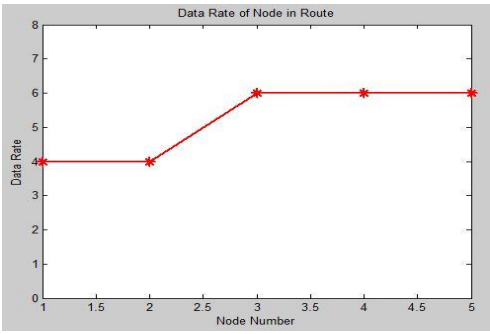

Fig 3: Data Rate Achieved in proposed work

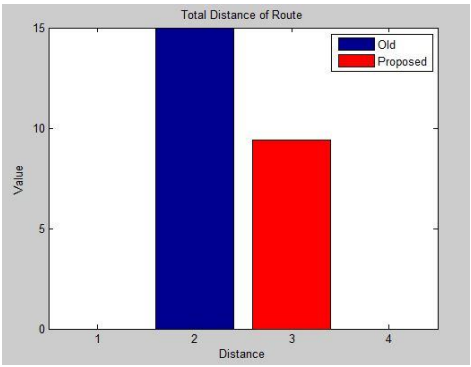

Fig 4: Comparison over Distance of proposed and traditional work

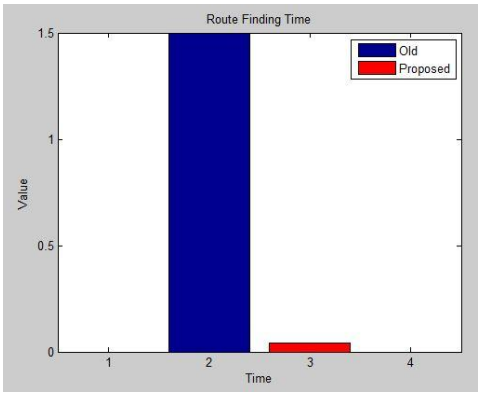

Fig 5: Comparison over time of proposed and traditional work

CONCLUSION

Unlike other networks, WSNs are designed for specific applications. Applications include, but are not limited to, environmental monitoring, industrial machine monitoring, surveillance systems, and military target tracking. Each application differs in features and requirements. To support this diversity of applications, the development of new communication protocols, algorithms, are needed. We have discussed the routing issues like node deployment, power consumption etc. We have read previous algorithms, a new routing algorithm is proposed in which these issues are considered. There are still many issues to be resolved around WSN applications such as communication architectures, security, and management. By solving these issues, we can close the gap between technology and application.

REFFRENCES

[1] C. Y. Chong, S. P. Kumar, ‘‘Sensor Networks: Evolution, Opportunities, and Challenges,’’ Proceedings of the IEEE, Aug. 2003.

[2] D. Estrin, D. Culler, K. Pister, ‘‘Connecting the Physical World with Pervasive Networks,’’ IEEE Pervasive Computing, Vol. 1, No. 1, Jan.–Mar. 2002.

[3] G. J. Pottie, W. J. Kaiser, ‘‘Wireless Integrated Sensor Networks,’’ Communications of the ACM, May 2000. An overview with more of a signal processing viewpoint.

[4] Mainwaring, R. Szewczyk, D. Culler, J. Anderson, ‘‘Wireless Sensor Networks for Habitat Monitoring,’’ Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications (WSNA’02), Atlanta, GA, Sept. 2002.

[5] L. Schwiebert, S. Gupta, J. Weinmann, ‘‘Research Challenges in Wireless Networks of Biomedical Sensors,’’ Proceedings of the 7th ACM International Conference on Mobile Computing and Networking (MobiCom’01), Rome, Italy, July 2001, pp. 151–165

[6] Stephan Olariu, “Information assurance in wireless sensor networks”, Sensor network research group, Old Dominion University.

[7] Holger Karl and Andreas Willig. “Protocols and architectures for Wireless Sensor Networks”, Wiley, 2005, ISBN:0470095105.

[8] Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks”, IEEE Communication Magazine, Aug. 2002.

[9] Akkaya, K.; Younis, M. A Survey on Routing Protocols for Wireless Sensor Networks. Ad Hoc Netw. 2005, 3, 325–349. 6.

[10] Akyildiz, I.; Pompili, D.; Melodia, T. Underwater Acoustic Sensor Networks: Research Challenges. Ad Hoc Netw. 2005, 3, 257–279.

[11] Karl, H.; Willig, A. Protocols and Architectures for Wireless Sensor Networks. John Wiley & Sons: Chichester, West Sussex, UK, 2005.

[12] Jamal Al-Karaki, and Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: Survey", IEEE Communications Magazine, vol 11, no. 6, Dec. 2004, pp. 6-28.

[13] I.F. Akyildiz, W. Su, Y. Sankara subramaniam, and E. Cayirci, "A Survey on Sensor Network", IEEE Communication Magazine, vol. 40, no. 8, Aug. 2002, pp. 102-114.

[14] W.R. Heinzelman, A. Chandrakasan, and H. Bala krishnan, "Energy-efficient Communication Protocol for Wireless Micro sensor Networks", in IEEE Computer Society Proceedings of the Thirty Third Hawaii International Conference on System Sciences (HICSS '00), Washington, DC, USA, Jan. 2000, vol. 8, pp. 8020.

[15] C. Karlof, D. Wagner,\Secure routing in wireless sensor networks: attacks and countermeasures", Ad Hoc Networks, Vol. 1 (2003) pp. 293315.