ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 4, April 2016

Reliable Geographic Routing for Cluster Based Wireless Sensor Networks

M.Balapriya, T.V.P.Sundararajan, P.Savitha

Abstract— **Wireless Sensor Networks (WSNs) mostly used in industries and civil organizations where monitoring and recognition of physical environment are a priority. Their possible applications are expected to be intensely applied in different types of domains such health, agriculture, habitat monitoring, routing traffic, security and military. WSN represent a reliable technology that attracts more and more considerable research attention in recent years. Wireless Sensor Networks (WSNs) consist of a large number of devices called sensor nodes scattered among a geographical area called sensor fields. These nodes are attempted to collect information or data which is forwarded through gateways called base stations. In this paper the selected cluster heads have equal number of neighbors and residual energy. By using geographic routing protocol the routing path will be secured and malicious node will be identified. By using this protocol the packet delivery ratio and throughput will be increased.**

***Index Terms*—Clustering, Energy-Efficient, Malicious node, Geographic routing**

I. INTRODUCTION

Wireless sensor network (WSN) consists of several tiny and low-power sensors which is used as radio frequencies to perform distributed sensing tasks. WSNs find their applications in many areas that will be including such as fire detection, battlefield surveillance, plant monitoring, leakage of toxic chemicals, gas detection and radiations [1]–[5]. In such WSNs, a large number of sensors are deployed in a field of interest (FoI) in stochastic manner of sensor network. In stochastic field of deployment, sensors are usually dropped randomly in large numbers to guarantee reliability [1], [4], [6], [7]. By minimizing the energy consumption while ensuring the connectivity of a network is an most important issue to be addressed in sensor network because the batteries powering the sensors may not be often for accessible for recharging in sensor network. Cluster-based routing in WSNs has been investigated by researchers to achieve the network management and scalability, which maximizes the lifetime of the network by using local collaboration among the sensors field [2]–[5], [8]–[14]. In a clustered network, every cluster has a cluster head (CH). CHs periodically select and collect the data, aggregate, and forward data to the sink.

Manuscript received April 11, 2016.

***M.Balapriya,** PG Student, ECE Department, Bannari Amman Institute of Technology, Sathyamangalam, India.*

***T.V.P.Sundararajan,** Professor, ECE Department, Bannari Amman Institute of Technology, Sathyamangalam, India.*

***P.Savitha,** PG Student, ECE Department, Bannari Amman Institute of Technology, Sathyamangalam, India.*

Security is one of the crucial requirements for these wireless network services. And to implement the security is therefore of prime importance in some networks. Provisioning protected the communications between mobile nodes in hostile environment, in which malicious attacker can launch the various attacks to disrupt the network security.

The limited battery power and the difficulty in recharging the batteries in a hostile environment to require the sensors to be deployed with a highest density for a long lifetime of network. Distributed clustering techniques to be more useful in the WSNs. Low Energy Adaptive Clustering Hierarchy (LEACH) [11] selects CHs based on a predetermined probability of order to rotate the cluster head role among the various sensors to balance the residual energy of the sensor network. Following the idea of LEACH protocol, a number of various protocols have been presented among in the literature [9], [10], and [25].

In absence of infrastructure, sensor nodes in a WSN have to implement the aspects of network functionality themselves; and they act as both end users and routers, which relay packets for other nodes. So the conventional network, to another feature of WSNs is the open network environment conditions where the nodes can leave and join the network freely. Therefore, then the wireless and dynamic nature of WSNs to expose them more vulnerable and to different types of security attacks various than the wired networks. Wireless sensor networks (WSN) is based on intelligent transportation systems (ITS) have emerged as a cost effective method to bear a pivotal potential to overcome some of the difficulties. This method enables a new broad range between the smart city applications along the urban sensing including various traffic safety, vehicular warning services, road state monitoring, traffic congestion control and parking management.

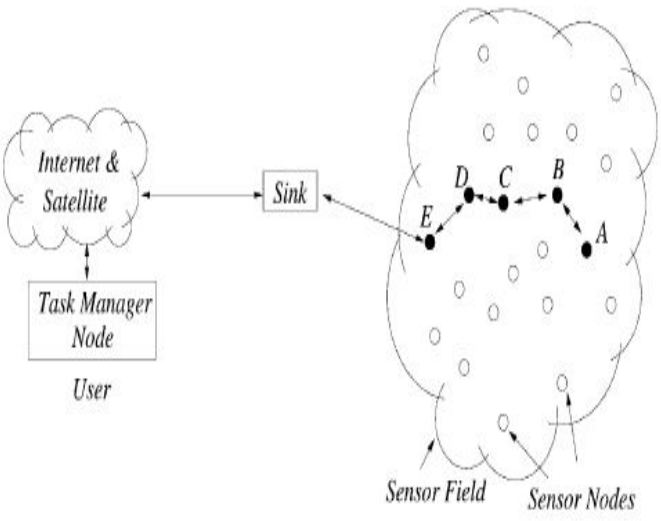

Fig.1 WSN Communication architecture

Wireless Sensor Networks consists of sensors fields and sensor nodes which are distributed in an ad hoc manner. These sensors are work with each other to sense some physical conditions and information gathered to be processed and to get relevant results.

A. Data Aggregation in WSNs

Data coming from multiple sensor nodes are aggregated if it has the same attribute of the physical phenomenon when reach the same routing node on the way back to the sink. In this fig.2 mentions that the data will be aggregated to the source from the sink.

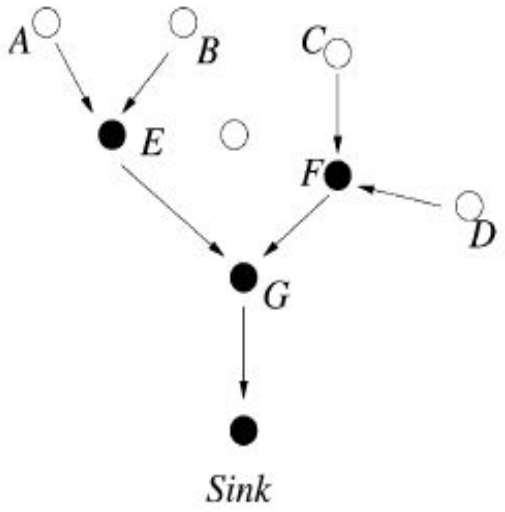

Fig.2 Data aggregation

B. Security

Wireless communications to impose more security issues namely, jamming, physical compromising of motes and criminality attacks etc. This makes the security handling mandatory for any proposed WSN based solution.

II. RELATED WORK

A. Clustering in WSNs

In clustering network the limited battery power will be difficulty in recharging the batteries in a hostile environment require that sensors will be deployed with the high density for a long lifetime of WSNs. Distributed clustering techniques are more useful in sensor network. Low Energy Adaptive Clustering Hierarchy (LEACH) [11] selects Cluster head based on the predetermined probability in order to rotate the cluster head role along with the sensors to be balance of the residual energy of the sensor network. Following the idea of LEACH protocol, a number of various protocols had presented in this literature [9], [10], and [25]. Hybrid Energy-Efficient Distributed (HEED) [13] clustering selects the cluster heads based on the residual energy of the network sensors and a secondary parameter, such as proximity to nearby neighbours. SPAN selects CHs based on that residual energy and more number of neighbours [14]. The cluster head form a network that is used to forward the data to sink. An Energy Efficient Clustering Scheme [26] allocates and selected a few number of sensors to clusters with the longer distances from source to the sink. A Fuzzy-logic method is based on the clustering approach is proposed in [2].

B. Route Optimization Technique

The goal of route optimization technique methods to achieve a path from the source to the sink but also wants to achieve the goal at a minimum cost of network, *i.e.* shortest path in terms of various hop counts among malicious node. Most of the literature method on routing method in WSNs does not have any of the special treatment for the malicious node in a FoI [1], [4], [6], [7], [31]. In this section, the proposed method is ROT in clustered sensor network to optimize the path length of node during data transmission without any extra overhead. In the early phase of ROT, a backbone sensor network will be constructed by using the proposed EHC, where the sensor is a cluster head or the member of a cluster. Consider a network of source CH i and a sink t as shown in Fig. 3. Before i send data to the sink t, it will identify the unauthorised node in network between t and itself. If there is no malicious node, i forward data to the sink t using geographic forwarding (GF) [16]. Otherwise i find a shortest path to sink (SP) to t, denoted by $\overrightarrow{i\,t}$, through the view vertices of malicious node using Dijkstras shortest path [24] algorithm. i' will be sets the view-vertices along SP as the intermediate destinations (IDs). When the data reach to the nearest CH of ID, denoted by j, ROT reruns between j and t to find a new SP. The pseudo code of ROT is described in Procedure 3.

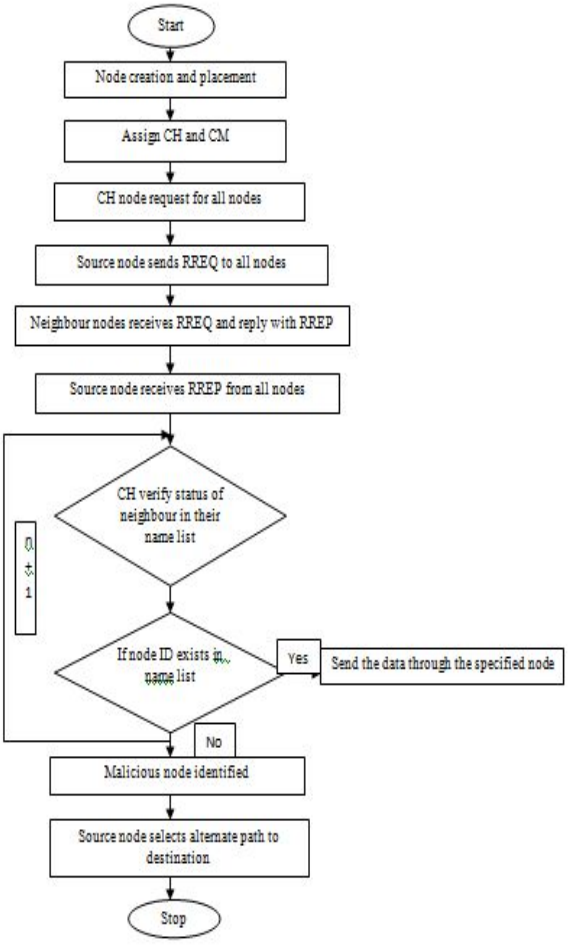

Fig.3 Flowchart of reliable geographic routing

III. SYSTEM IMPLEMENTATION

A. Network design

To create a network with the number of nodes which is a wireless sensor network and going to creating the network with the WSN specifications i.e., each node can be communicate with any other node directly to which are in coverage area of the node. Then forming one leader node which is known as traffic manger which will controls the traffic of the entire network and remaining are normal nodes. The sensor nodes are usually to be resource constrained with respect to computation capability, bandwidth, memory space, and power supply. The network users use some mobile devices to be disseminating data items into the network. The network owner is responsible for generating keying materials.

B. Monitoring the traffic

To monitor the traffic, it will be handled by the Traffic manager which is to be leader node. It is going to controls the entire network i.e., it will be monitors all the nodes and checks which are giving good response based on that it will be allow other nodes to communicating each other. Networks are assigned aggregation privileges by the trusted authorities in a PKI of the network owner. However, the network is owner may for various reasons; impersonate network users to aggregate data items.

The compromised entities are regarded as inside because they are members of the network until they are identified. The adversary controls of these entities to attack the selected network in arbitrary ways. For instance, they could be instructed to aggregate false or harmful data, launch attacks such as DoS attacks or Sybil attacks and be non-cooperative with the other nodes.

Data gathered by the individual nodes ultimately routed to the base station. A rate monitoring attack simply makes use of idea that nodes are closest to the base station that tends to forwarded more packets than the farther away from the base station. An attacker needs to only monitoring which nodes are sending the packets and follow those nodes is sending to the most packets. In time correlation attack of traffic monitoring where an adversary node can simply generates monitors and events to which a node sends its packets.

C. Route discovery process

A node wants to communicate with other node in discovery process whenever it has to find the route for forwarding the data in the network. In this route discovery process if any new node is entered means there is a chance of that a hacking node may be present. So that to avoid that hacking nodes for secure data transmission. For this reason, the nodes are maintaining a correct list known as true list, in the nodes are going to be store about their other nodes to finding the secure route. To create trust list nodes are going to create a name list known as true list, in this list they are going to store the node information's in the network which given proper response to the traffic manager. The utility of a sensor network will relay on its ability to accurately and automatically to locate each sensor in the network. A sensor network that is designed to locate faults will need to be accurate location information in order to finding of pin point of route and the location of a fault in discovery process. Unfortunately, an attacker can easily manipulate in network that are none secured information present in location by reporting the false signal strengths and replaying the signals. To check trust list whenever a node wants to send the data and it will send route request to all other nodes.

The node which are received by the route request packet will checks the node in route discovery process whether that node is present in true list or not if presented means it will be forward to other nodes and it repeats until it reaches destination. Route trust is computed by the every node for each route in routing table. It measures a reliability with a packet can reach to the destination, if forwarded by the node to particular route in network. The route will be trusts are initially unknown. RREQ's are sent by source node and the routes are established to the destination node as in GPSR.

IV. PERFORMANCE EVALUATION

A. Packet Delivery Ratio

The packet delivery ratio is a ratio of the number of packets that are received by the sink over packets to the network by the source.Fig.4 shows the overall delivery ratio for the entire duration of the simulation. It can achieve a stable performance for the entire duration.

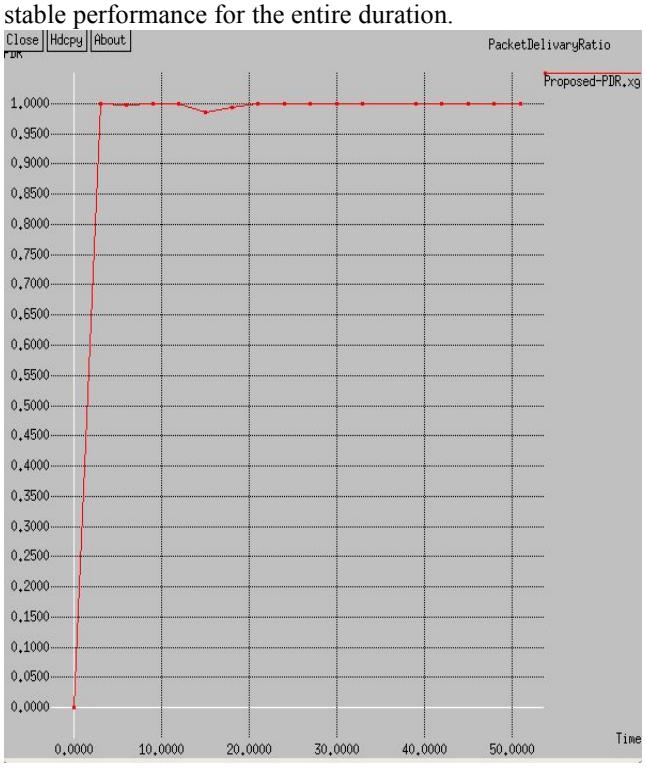

Fig.4 Packet Delivery Ratio

A. Throughput

Throughput is the total number of packets that are received by simulation time. In this fig.5 the throughput is increased in certain time. The total number of packets will be received correctly by using aggregation protocols.

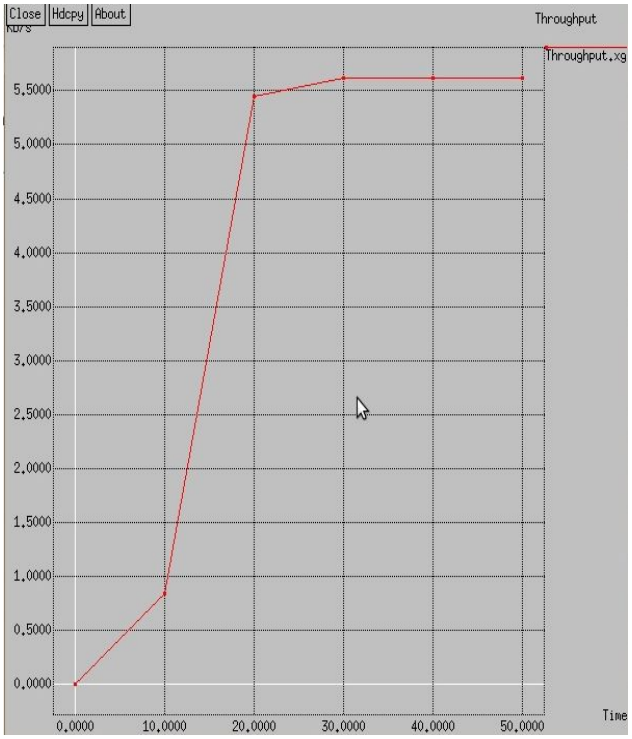

Fig.5 Throughput

A. Packet loss

The Packet loss is defined discarding of packets in a network when a router or other network device is overloaded and cannot accept additional packets at a given moment. Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. In this fig.6 mentions that Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent.

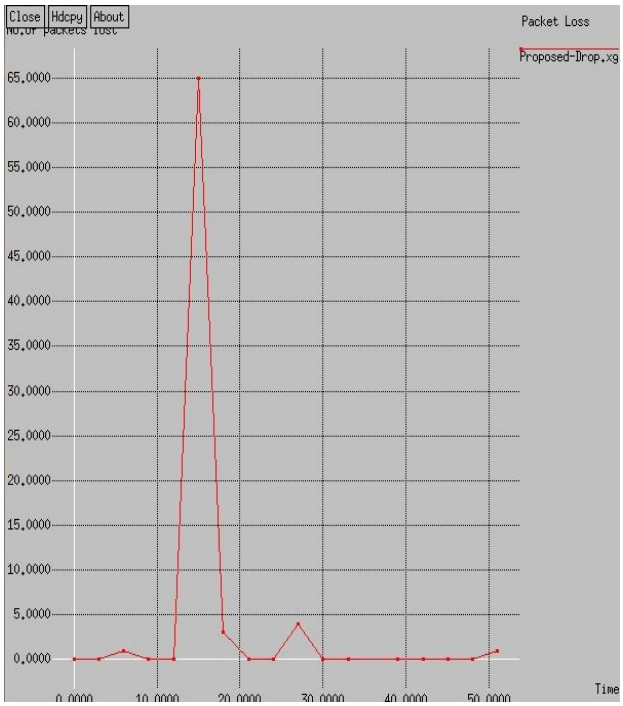

Fig.6 Packet loss

V. CONCLUSION

In this paper, by using a geographic routing scheme that enhances the security of WSN. By this method to secure routing path will be established in malicious environments. In this performance of our scheme, which improves throughput, packet delivery ratio and packet loss will be decreased. By using GPSR the reliable data transmission will be obtained and the routing path also secured.

REFERENCES

1. J. H. Lee, T. Kwon, and J. Song, "Group connectivity model for industrial wireless sensor networks," *IEEE Trans. Ind. Electron.*, vol. 57,no. 5, pp. 1835–1844, May 2010.
2. J.-S. Lee and W.-L. Cheng, "Fuzzy-logic-based clustering approach for wireless sensor networks using energy predication," *IEEE Sensors J.*, vol. 12, no. 9, pp. 2891–2897, Sep. 2012.
3. Z. Ha, J. Wu, J. Zhang, L. Liu, and K. Tian, "A general self-organized tree-based energy-balance routing protocol for wireless sensor network," *IEEE Trans. Nucl. Sci.*, vol. 61, no. 2, pp. 732–740, Apr. 2014.
4. C. Hoang, P. Yadav, R. Kumar, and S. Panda, "Real-time implementation of a harmony search algorithm-based clustering protocol for energy-efficient wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 774–783, Feb. 2014.
5. M. Tarhani, Y. S. Kavian, and S. Siavoshi, "SEECH: Scalable energy efficient clustering hierarchy protocol in wireless sensor networks," *IEEE Sensors J.*, vol. 14, no. 11, pp. 3944–3954, Nov. 2014.
6. P. T. A. Quang and D.-S. Kim, "Enhancing real-time delivery of gradient routing for industrial wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 8, no. 1, pp. 61–68, Feb. 2012.
7. J. Niu, L. Cheng, Y. Gu, L. Shu, and S. K. Das, "R3E: Reliable reactive routing enhancement for wireless sensor networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 784–794, Feb. 2014.
8. R. Xie and X. Jia, "Transmission-efficient clustering method for wireless sensor networks using compressive sensing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 806–815, Mar. 2014.
9. H. Lu, J. Li, and M. Guizani, "Secure and efficient data transmission for cluster-based wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 750–761, Mar. 2014.
10. Wei, Y. Jin, S. Vural, K. Moessner, and R. Tafazolli, "An energyefficient clustering solution for wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 11, pp. 3973–3983, Nov. 2011.
11. M. J. Handy, M. Haase, and D. Timmermann, "Low energy adaptive clustering hierarchy with deterministic cluster-head selection," in *Proc. 4th Int. Workshop MWCN*, 2002, pp. 368–372.
12. X. Zhu, L. Shen, and T.-S. P. Yum, "Hausdorff clustering and minimum energy routing for wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 2, pp. 990–997, Feb. 2009.
13. O. Younis and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 3, no. 4, pp. 366–379, Oct./Dec. 2004.
14. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," *Wireless Netw.*, vol. 8, no. 5, pp. 481–494, 2002.
15. M. Won, W. Zhang, and R. Stoleru, "GOAL: A parsimonious geographic routing protocol for large scale sensor networks," *Ad Hoc Netw.*, vol. 11, no. 1, pp. 453–472, 2013.
16. B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *Proc. 6th Int. Conf. MobiCom*, 2000, pp. 243–254.
17. Petrioli, M. Nati, P. Casari, M. Zorzi, and S. Basagni, "ALBA-R:Load-balancing geographic routing around connectivity holes in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 529–539, Mar. 2014.

18.Y. Cao, Z. Sun, N. Wang, H. Cruickshank, and N. Ahmad, "A reliable and efficient geographic routing scheme for delay/disruption tolerant networks," *IEEE Wireless Commun. Lett.*, vol. 2, no. 6, pp. 603–606, Dec. 2013.

19.T. Wang, W. Jia, G. Wang, M. Guo, and J. Li, "Hole avoiding in advance routing with hole recovery mechanism in wireless sensor networks," *Ad Hoc Sensor Wireless Netw.*, vol. 16, nos. 1–3, pp. 191–138, 2012.

20.Li, B. Zhang, and J. Zheng, "Geographic hole-bypassing forwarding protocol for wireless sensor networks," *IET Commun.*, vol. 5, no. 6, pp. 737–744, 2011.

21.P. Spachos, P. Chatzimisios, and D. Hatzinakos, "Energy aware opportunistic routing in wireless sensor networks," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2012, pp. 405–409.

22.K. Zeng, J. Yang, and W. Lou, "On energy efficiency of geographic opportunistic routing in lossy multihop wireless networks," *Wireless Netw.*, vol. 18, no. 8, pp. 967–983, Nov. 2012.

23.K. Zeng, K. Ren, W. Lou, and P. J. Moran, "Energy aware efficient geographic routing in lossy wireless sensor networks with environmental energy supply," *Wireless Netw.*, vol. 15, no. 1, pp. 39–51, Jan. 2009.

24.W. Dijkstra, "A note on two problems in connexion with graphs," *Numer. Math.*, vol. 1, no. 1, pp. 269–271, 1959.

25.B.-C. Cheng, H.-H. Yeh, and P.-H. Hsu, "Schedulability analysis for hard network lifetime wireless sensor networks with high energy first clustering," *IEEE Trans. Rel.*, vol. 60, no. 3, pp. 675–688, Sep. 2011.