ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (228-234), Month: January - March 2015, Available at: www.researchpublish.com

Effective Failure Detection Based On Round Trip Delay and Paths in Wireless Sensor Networks

E.Ponregina[1], C.R. Jerin sajeev[2]

[1]PG Student, Einstein college of Engineering, Tirunelveli, India
[2]Assistant professor, Einstein college of Engineering, Tirunelveli, India
Email ID: joneregina@gmail.com

Abstract: **Wireless sensor networks with large numbers of portable sensor nodes has potential applications in a various fields, like surveillance, home security, military operations, medical, environmental and industrial monitoring. Due to rapid growth in electronic fabrication technology it is possible to manufacture the portable sensor node at low cost with better accuracy and sensitivity. Hence large numbers of portable sensor nodes can be deployed in the field to increase the quality of service of such wireless sensor networks. The exercise to use large numbers of sensor nodes will increases the probability of sensor node failures in such WSNs. QoS of wireless sensor network is mainly affected by failure of sensor nodes. Node failure is detected by measuring Round Trip Delay time of round trip paths and comparing them with the threshold values. By reducing RTD time, accuracy of fault detection technique can be increased.**

Keywords: **QoS, RTD time, WSNs.**

1. INTRODUCTION

A wireless sensor network of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The sensor node can become faulty in WSNs due to various reasons such as battery failure, environmental effects, hardware or software malfunctions. To achieve better quality of service (QoS) by discarding the data from faulty nodes. Manually checking of such failed sensor node in WSN is difficult one.

The WSN is build by hundreds or thousands of nodes. There are some basic components that are necessary to build a network. Basic components are like memory, processor, radio transceiver, GPS, power source, and sensors as shown in fig 1.The equipment with sensors has capability for data processing and communication.

Main function of these components is to provide an environment for the packets transmission and receiving data from one node to another node through network. To achieve a good quality of service through accuracy, reliability and efficiency, detection of sensor node failure or malfunctioning is essential. Detection of faulty node by using neighbour-data analysis method. Here node trust's degree is calculated. But the algorithm is not accurate. Uses time delay based on direction of arrival estimation and confidence factor to detect faulty sensor node. It affects due to non perfect planar wave fronts.

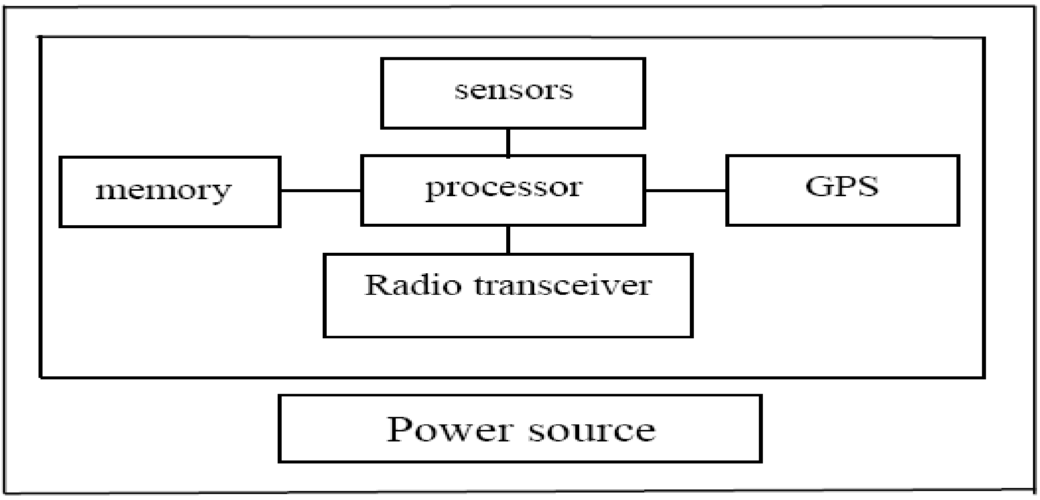


Fig 1. Basic components of a WSN node

The faulty sensor nodes identification suggested in [8] is based on comparisons between neighboring nodes and dissemination of the decision made at each node. Algorithm proposed in this method can't detect the malicious nodes. Cluster head failure recovery algorithm used in [9] to detect the faulty node has data loss problem, occurring due to transfer of cluster head. Path redundancy technique to detect faulty sensor node is suggested in [10] and [11]. Redundancy increases the energy consumption and reduces the number of correct responses in network lifetime. Excessive redundant paths in WSNs will slow down the fault detection process. In [12], link failure detection based on monitoring cycles (MCs) and monitoring paths (MPs) is presented. Three-edge connectivity in the network, separate wavelength for each monitoring cycle and monitoring locations are the limitations of this method. so the sensor node failure is detected by measuring round trip delay time of round trip paths and comparing them with the threshold value.

2. LETERATURE REVIEW

Ravindra N Duche and N.P.Sarwade, (2011) the proposed method is to detect the sensor node failure or malfunctioning with the help of confidence factors. Confidence factor of round trip path in network is estimated by using the round trip delay time. The proposed method will detect the failure in sensor node for symmetrical network conditions. The confidence factor of round trip path is computed with the help of threshold and instantaneous round trip delay time. Confidence factors of all round trip paths are stored in lookup table. Then by analyzing the status of confidence factor of all paths in the look-up table, failed or malfunctioning sensor node is detected easily.

Vivek P. Mhatre, et al, (2005) the proposed scheme consider a heterogeneous sensor network in which nodes are to be deployed over a unit area for the purpose of surveillance. An aircraft visits the area periodically and gathers data about the activity in the area from the sensor nodes. There are two types of nodes that are distributed over the area using two-dimensional homogeneous Poisson point processes; type 0 nodes with intensity (average number per unit area) λ_0 and battery energy E_0; and type 1 nodes with intensity λ_1 and battery energy E_1. Type 0 nodes do the sensing while type 1 nodes act as the cluster heads besides doing the sensing. It provides only minimum amount lifetime for sensor node.Here small amount of energy should be wasted,this is the drawback in this method.

Emad Felemban,et al, (2006) the packet delivery mechanism for QoS provisioning called Multi-Path and Multi-SPEED Routing Protocol is proposed, which spans over network layer and medium access control layer. The major goal is to provide QoS differentiation in two quality domains, namely, timeliness and reliability, so that packets can choose the most proper combination of service options depending on their timeliness and reliability requirements. For the service differentiation in the timeliness domain, the proposed mechanism provides multiple network-wide speed options extending the idea of single network-wide speed guarantee. For the service differentiation in the reliability domain, we exploit the inherent redundancy of dense sensor networks by realizing probabilistic multipath forwarding depending on packet's reliability requirement. but it consumes high energy. this is the drawback in this method.

Abolfazl Akbari et al, (2011) in this proposed scheme the unactive nodes miss their communication in network, hence split the network. For avoidance split of network a fault recovery corrupted node and Self Healing is proposed. It designs the techniques to maintain the cluster structure in the event of failures caused by energy-drained nodes. Initially, node with the maximum residual energy in a cluster becomes cluster heed and node with the second maximum residual energy becomes secondary cluster heed. Later on, selection of cluster heed and secondary cluster heed will be based on available residual energy.This method must require a self healing property that's also the drawback in this method.

Ing-Ray Chen, et al (2011) in this proposed scheme a WSN can be either source-driven or query-based depending on the data flow. In source-driven WSNs, sensors initiate data transmission for observed events to interested users, including possibly reporting sensor readings periodically. In query-based WSNs, a user would issue a query with QoS requirements in terms of reliability and timeliness. The general approach is to apply redundancy to satisfy the QoS requirement. It does not provides more detailed analysis of the effect of network dynamics on Mean Time To Failure. &This method not satisfy query QoS requirements

Arunanshu Mahapatro and Pabitra Mohan Khilar, (2012) This paper presents a distributed model to address the fundamental problem of identifying faulty (soft and hard) nodes in a WISN. The model is simple and detects faulty sensor nodes with high accuracy for a wide range of fault probabilities, while maintaining low message overhead. The message and time complexity of the proposed model is $O(n)$ which is significantly low compared to present state-of-theart approaches. It has been assumed that there are n sensor nodes non uniformly distributed in a square area of side L, which is much larger than the communication range of the sensors.

3. PROPOSED SYSTEM

The proposed method of fault detection is based on RTD time measurement of RTPs. RTD times of discrete RTPs are compared with threshold time to determine failed or malfunctioning sensor node. In order to verify the scalability of this concept, WSNs with large numbers of sensor nodes are implemented and simulated in open source software NS2.

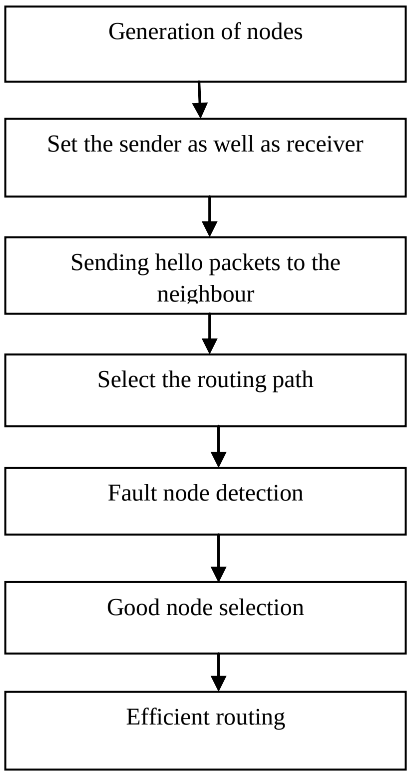


Fig 2.1 Modules overall flow diagram

In this paper first we have to generate the nodes in the open source software NS2.Then set the sender as well as receiver. After setting the sender and receiver we have to send the hello packets to the neighbour for gathering neighbour node details. The route is selected for data transmission between nodes. The route is selected based on routing protocol which selects shortest path for transmission.

The data is transmitted based on route selected by routing protocol. If the data will be lost or not reaches the destination because node failure. This fault node is identified in this module. The data will be transmitted, then we have to group the node to form the round trip path. after forming the round trip path, we have to calculate the round trip time for a corresponding round trip path. Then set the threshold value. If the round trip time greater than the threshold value means that is a malfunction node. If the round trip time is infinity means that is a failure node. after identifying the failure node the good node is selected and the data will be transmitted according to the route selected with good nodes Energy.

3.1 Round trip delay and paths analysis:

Round trip delay time of the RTP will change due to faulty sensor node. Faulty sensor node is detected by comparing the RTD time of RTPs with threshold value. The sensor node common to specific RTPs with infinity RTD time is detected as failed. If this time is higher than the threshold value then this senor node is detected as malfunctioning.

The round trip path in WSNs is formed by\grouping minimum three sensor nodes. Hence the minimum round trip delay time of RTP with three sensor node is given by,

$$\tau\text{RTD}=\tau 1+\tau 2+\tau 3 \qquad (1)$$

where $\tau 1$, $\tau 2$ and $\tau 3$ are the delays for sensor node pairs (1,2), (2,3) and (3,1) respectively. Round trip delay time for RTP with uniform sensor node pair delay is obtained by referring equation (1) as

$$\tau\text{RTD} = 3\tau. \qquad (2)$$

This is the minimum RTD time of an RTP in WSNs. Hence the efficiency of proposed method can be improved only by reducing the RTPs in WSNs.

3.1.1 Evaluation of Round Trip Paths:

The numbers of RTPs formed with ‘m’ sensor nodes is given by

$$P = N(N - m) \qquad (3)$$

Where P is the numbers of RTPs. . It is the addition of all RTD times. The equation for analysis time with P numbers of RTPs is given by,

$$\tau\text{ANL}(M)=\tau\text{RTD}-1+\tau\text{RTD}-2+\cdots+\tau\text{RTD}-P \qquad (4)$$

$$\tau\text{ANL} = \sum_i^p \tau\text{RTD} - \text{i} \qquad (5)$$

All the RTPs in WSNs are formed by selecting only three sensor nodes (m = 3). Then the round trip delay for all RTPs is approximately same i.e.

$$\tau\text{RTD}=\tau\text{RTD}-1=\tau\text{RTD}-2=\cdots=\tau\text{RTD}-P \qquad (6)$$

Equation (5) can be written with the equal RTD time as

$$\tau\text{ANL}=P*\tau\text{RTD} \qquad (7)$$

Referring (2), analysis time can be written in terms of sensor node pair delay is as

$$\tau\text{ANL}=P*3\tau. \qquad (8)$$

The maximum possible round trip paths P*M*, created by three sensor nodes per RTP are obtained by substituting m = 3 in (3) and is given by

$$P_M=N(N-3). \qquad (9)$$

Analysis time $\tau\text{ANL}(M)$, to detect the faulty sensor node using maximum RTPs is obtained by referring (8) and (9) as follows

$$\tau\text{ANL}(M)=N(N-3)*3\tau \qquad (10)$$

3.2 Optimization of round trip paths:

Fault detection by analyzing RTD times of maximum numbers of RTPs will require substantial time and can affect the performance. Therefore essential numbers of RTPs has to be selected for comparison purpose. Optimization of RTPs can be done as explained below.

3.2.1 Linear Selection of RTPs:

In order to reduce the RTPs in the fault detection analysis, instead of considering maximum numbers of RTPs, only few paths corresponding to the number of sensor nodes in WSNs are sufficient. We can select the RTPs equal to the numbers of nodes in WSNs to reduce the analysis time. RTPs selected in this way are called as linear RTPs because of the linear relationship between N and P. The linear RTPs in WSNs with N sensor nodes can be written as

$$P_L = N \qquad (11)$$

where P_L is the number of linear RTPs. Measurement of RTD times of such paths is essential. Referring (8) and (11), the analysis time $\tau ANL(L)$ for linear RTPs is given by

$$\tau ANL(L) = N * 3\tau.. \qquad (12)$$

Linear RTPs selected will be higher for large value of sensor nodes N. This will not optimize the fault detection time in case of large size WSNs. Therefore, further reduction in the numbers of RTPs is must to increase the efficiency of proposed method.

3.2.2 Discrete Selection of RTPs:

In the first level of optimization the analysis time is curtail up to certain limit. Still the numbers of RTPs are high. For WSNs with large numbers of sensor nodes the fault detection time is significantly high. So again there is need to minimize the RTPs in WSNs. In the second level of optimization, numbers of RTPs are reduced by selecting only discrete paths in WSNs. Discrete RTPs are selected from sequential linear RTPs only. They are selected by ignoring the two consecutive paths, after each selected linear path. In this way RTPs are selected in discrete steps of three as each RTP consists of three sensor nodes. The equation to select the discrete RTPs in WSNs is given by

$$P_D = Q + C \qquad (13)$$

Q and C in above equation are expressed as below

$$Q = \lfloor N/M \rfloor \qquad (14)$$

$$C = \begin{cases} 0 & if\ R = 0 \\ 1 & otherwise \end{cases} \qquad (15)$$

where Q is the quotient, m is the numbers of sensor nodes in RTP, R is remainder, N is numbers of sensor nodes in wireless sensor networks and C is correction factor to be added. Correction factor will be 0 if remainder is 0 otherwise it is 1.Analysis time $\tau ANL(D)$ required for detecting fault in discrete RTPs is obtained by referring (8) and (13) as follows

$$\tau ANL(D) = (Q + C) * 3\tau . \qquad (16)$$

The numbers of sensor nodes used in RTP are three only i.e. m = 3. Equation (16) can be written in terms of N and m as

$$\tau ANL(D)=(\_N/3\_+C)*3\tau. \qquad (17)$$

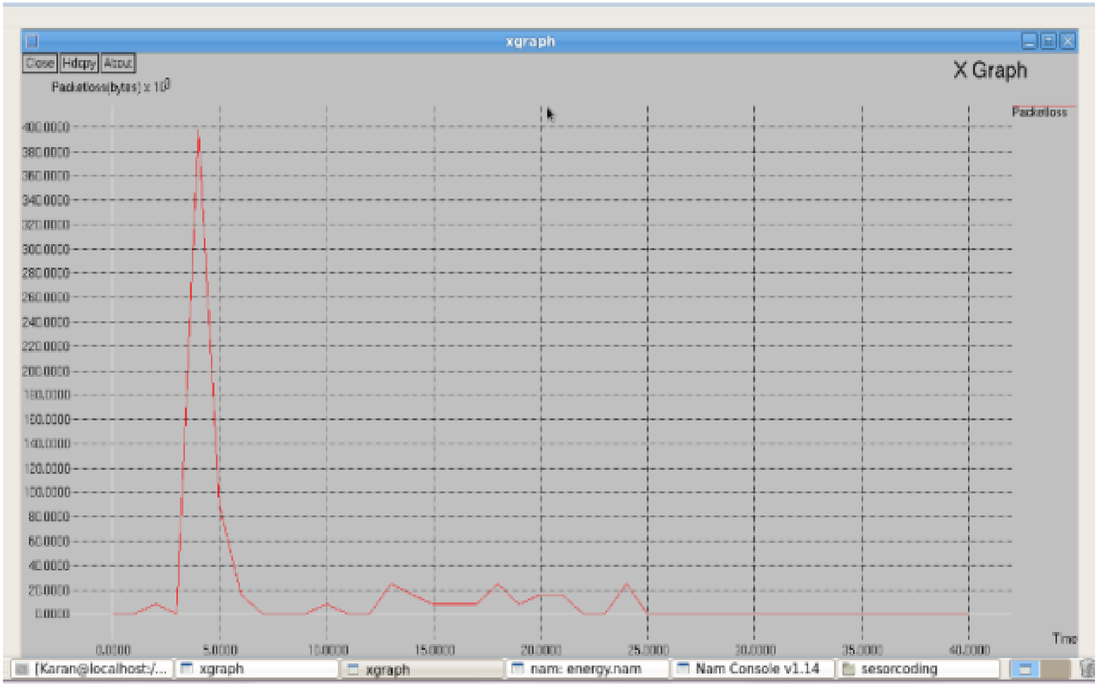
Analysis of particular selected discrete path will be sufficient to monitor the fault. Selection of discrete RTPs will save the analysis time to a large extend. Discrete RTPs obtained by using equation (16) in WSNs with different numbers of sensor nodes N are mentioned.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 1, pp: (228-234), Month: January - March 2015, Available at: www.researchpublish.com

4. RESULT & DISCUSSION

Packetloss:

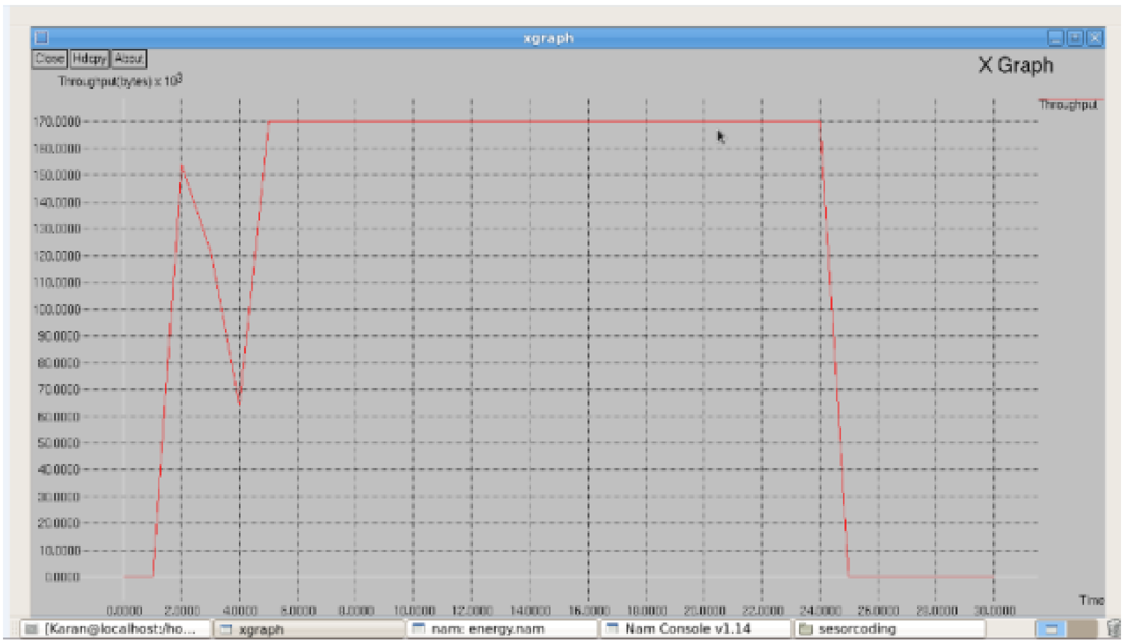
The packet loss of the network is defined as the failure of one or more transmitted data to arrival at the user.



From the simulation result the transmitted data failure is suddenly increased during the node failure time.

Throughput:

Throughput of the network is defined as how much data can be transferred from the base station to the user in the given amount of time.



From the simulation result the throughput is decreased during the node failure time. After replacing failure node the throughput is constant.

5. CONCLUSION

The proposed method is successfully implemented and tested on software. RTD time comparison of discrete RTPs is sufficient to detect the faulty sensor node. Scalability of the method has been verified by implementing it to various WSNs. Efficiency of method is excellent in case of discrete RTPs with three sensor nodes. Real time applicability of investigated method is confirmed by software results.

REFERENCES

[1] K. Sha, J. Gehlot, and R. Greve, “Multipath routing techniques in wireless sensor networks: A survey,” Wireless Personal Commun., vol. 70, no. 2, pp. 807–829, 2013.

[2] M. Asim, H. Mokhtar, and M. Merabti, “A fault management architecture for wireless sensor network,” in Proc. IWCMC, Aug. 2008, pp. 1–7.

[3] M. Younis and K. Akkaya, “Strategies and techniques for node placement in wireless sensor networks: A survey,” Ad Hoc Netw., vol. 6, no. 4, pp. 621–655, 2008.

[4] P. Jiang, “A new method for node fault detection in wireless sensor networks,” Sensors, vol. 9, no. 2, pp. 1282–1294, 2009.

[5] Chen, A. P. Speer, and M. Eltoweissy, “Adaptive fault tolerant QoS control algorithms for maximizing system lifetime of query-based wireless sensor networks,” IEEE Trans. Dependable Secure Comput., vol. 8, no. 2, pp. 1–35, Mar./Apr. 2011.

[6] A. A. Boudhir, B. Mohamed, and B. A. Mohamed, “New technique of wireless sensor networks localization based on energy consumption,” Int. J. Comput. Appl., vol. 9, no. 12, pp. 25–28, Nov. 2010.

[7] W. Y. Poe and J. B. Schmitt, “Node deployment in large wireless sensor networks: Coverage, energy consumption, and worst-case delay,” in Proc. ACM, AINTEC, Nov. 2009, pp. 1–8.

[8] M. Lee and Y. Choi, “Fault detection of wireless sensor networks,” Comput. Commun., vol. 31, pp. 3469–3475, Jun. 2008.

[9] A. Akbari, A. Dana, A. Khademzadeh, and N. Beikmahdavi, “Fault detection and recovery in wireless sensor network using clustering,” IJWMN vol. 3, no. 1, pp. 130–138, Feb. 2011.

[10] C.-C. Song, C.-F. Feng, C.-H. Wang, and D.-C. Liaw, “Simulation and experimental analysis of a ZigBee sensor network with fault detection and reconfiguration mechanism,” in Proc. 8th ASCC, May 2011, pp. 659–664.

[11] A. Mojoodi, M. Mehrani, F. Forootan, and R. Farshidi, “Redundancy effect on fault tolerance in wireless sensor networks,” Global J. Comput. Sci. Technol., vol. 11, no. 6, pp. 35-40, Apr. 2011.

[12] S. S. Ahuja, R. Srinivasan, and M. Krunz, “Single-link failure detection in all-optical networks using monitoring cycles and paths,” IEEE/ACM Trans. Netw., vol. 17, no. 4, pp. 1080–1093, Aug. 2009.

[13] R. N. Duche and N. P. Sarwade, “Sensor node failure or malfunctioning detection in wireless sensor network,” ACEEE Int. J. Commun., vol. 3, no. 1, pp. 57–61, Mar. 2012.

[14] T. W. Pirinen, J. Yli-Hietanen, P. Pertil, and A. Visa, “Detection and compensation of sensor malfunction in time delay based direction of arrival estimation,” IEEE Circuits Syst., vol. 4, no. 1, pp. 872–875, May 2004.