RESEARCH ARTICLE

SAMRIDDHI Volume 14, Special Issue 1, 2022 Print ISSN : 2229-7111 Online ISSN : 2454-5767

Energy Efficient Protocol for Multipath Transmission in Wireless Sensor Networks

Roshani Talmale[1*], Pranita Chaudhary[2], Sheetal Mungale[3]

[1*] Department of Computer Science and Engineering, S .B. Jain Institute of Technology, Management and Research, Nagpur, India; e-mail : roshanikambe2011@gmail.com

[2] Department of Computer Science and Engineering, S .B. Jain Institute of Technology, Management and Research, Nagpur, India.

[3] Department of Electronics and Telecommunication Engineering, S .B. Jain Institute of Technology, Management and Research, Nagpur, India.

Abstract

Energy has been a major challenge in practically all networks, particularly in terms of consumption and efficient energy utilization. Many experiments and proposals for flaw detection have been made in the past, including relevant evidence. However, academics have yet to discover the absolute solution to the pre-"fault tolerance and prevention" routing protocol. using energy efficient awareness. Therefore, there is a need to explain the definition of importance of energy efficient pre-fault detection in WSNs. We propose a disseminated important productive steering calculation for WSNs that takes mind adaptation to internal failure of the network. At that point, we propose a circulated steering calculation called "Dispersed Blame Transmission Multipath Cluster Based Protocol (DBTMCP)" approach takes into account the CHs' important use as well as their adaptation to non-critical failure. In this research, we present a protocol that selects a succeeding node in an energy-efficient manner and, in the event of its failure, restores the connectivity of the cluster's neighbours in a sensitive manner.

Keywords: Fault tolerance; Network lifetime; Wireless Sensor Networks Routing; Real-time; Energy-Efficiency; Wireless Sensor and Actuator Networks (WSANs);

SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology, (2022); DOI : 10.18090/samriddhi.v14spli01.2

Introduction

Multi-path or multi-hop networks are multi-path or multi-hop wireless sensor networks. The packet transmission in these networks is dependent on the many intermediary nodes. The data packet is sent to the destination via these intermediary nodes. Many talks on these nodes have previously been conducted through various study studies. They deal with issues like "lesser memory", "limited battery power", "computational timing" etc. In this paper, We seek for a secure and efficient routing path to transfer the incoming packet by pre-defining the fault that happens in the following node so that the preceding node detects "pre-fault detection," preserving energy and allowing for more efficient transmission.

The objective of this paper in brief is to explain the definition of importance of energy efficient pre-fault detection in WSNs. both the CHs' important use and their ability to adjust to non-critical failure.

Corresponding Author : Roshani Talmale, Department of Computer Science and Engineering, S .B. Jain Institute of Technology, Management and Research, Nagpur, India; e-mail : roshanikambe2011@gmail.com

How to cite this article : Talmale, R., Chaudhary, P., Mungale, S. (2022). Energy Efficient Protocol for Multipath Transmission in Wireless Sensor Networks. *SAMRIDDHI : A Journal of Physical Sciences, Engineering and Technology,* Volume 14, Special Issue (1), 6-12.

Source of support : Nil

Conflict of interest : None

We have proposed "Dispersed Blame Transmission Multipath Cluster Based Protocol (DBTMCP)" on order to meet the energy efficient multipath If problems are anticipated to occur, transmission without any faults is recommended. Several clustered sensor networks, as well as multipath sensor networks, have been developed in the past to improve network efficiency and dependability. The DBTMCP is made up of these two sensor networks.

Aside from these, a number of analysts have suggested using portals/transfers, which are unusual hubs. The goal of this work is to create and build a novel protocol that will result in a numerical definition for energy efficient fault mitigation, monitoring, and possibly fault removal. As a result, in order to continue with the utility of WSNs, the guiding computations should adapt to a fault tolerant perspective, particularly when some CHs frequently deliver negative acknowledgement. After a steering failure without information transmission, the computation allows a transfer hub to quickly and effectively detect the next best path from itself to the destination. Because of hub flexibility and the resulting directed packet transmission faults, non-critical failure adaption is important to ensure dependable hub correspondence. A remote sensor network (WSN) is made up of hundreds or thousands of sensor hubs that are transported physically or arbitrarily to a certain location. A WSAN is made up of sensor hubs that can detect jolts in the ground and actuator hubs that can change their surroundings.

Literature Review

There are innumerable traditions presented for sensor frameworks. First time these guiding traditions were shown in a dealt with way by Imoize, A. L et al. [1], this survey anchored all piece of coordinating tradition, request and plan. In any case, all of these core traditions have been carried out in an unsafe manner. Karlof et al. [2] depict the ambushes on different coordinating traditions and give the countermeasures. W. Heinzelman et.al. [3,4] resolves the two combined proposition; firstly, SNEP for protection, validity, respectability and freshness of data and second TESLA for confirmed telecom, anyway with the extra over head of buffering messages before key disclosure that development the torpidity and making own key chain for every single correspondence.

C. Hong-bing[5] is the first and outstandingly common thought of assembled guiding with no security. C. Th work of Intanagonwiwatet. al. and K. Kurosawa and W. Ogata[6,7] gives an efficient respond in due order regarding secure correspondence in LEACH with the help of sporadic key pre-appointment and TESLA and over-comes a segment of the attacks. Again to give effective response for secure correspondence in LEACH, Wenjing Lou and N. Nasser and Y. Chen.[8, 9, 10] has been given improved discretionary key pre-scattering plot.

Some work has been done in secure different leveled coordinating tradition; L. B. Oliveiraet. al., B. Parnoet. al. and A. Perrig, R. Szewczyk[11, 12, 13] have depicted essentialness efficient dynamic guiding tradition with get-together key organization plot, be that as it may while changing the pack head all social event keys (i.e. cover gathering and intra pack) need to determine afresh, is an overhead associated with this tradition. Z. Quan[14] is also an approach towards secure dynamic controlling which give security under center deal strike. J. G. Steiner et. al., M. Tubaishatet.al., and M. Ye[15, 16, 17] offered security against outside adversary and internal dealt center points by quality and reputation organization mechanical assemblies with extra weight of figuring and correspondence.

K. Zhang et.al., Haiying Shen et.al. andHaojun Huang et.al. [18,19,20] proposed the different leveled guiding tradition that had been executed in perspective of the efficiency. Accepting the question of security aside, there are certain specific issues in the packing tradition, such as the issue of vagrant centres and multihop routes (from the gathering go to the base station). These two topics were overshadowed in this study.

There are various multipath controlling protocols proposed in L. Chenget. al. [21], S. S. Lan et.al [22, 23], B. Karp et. al. [24] and D. Chen [25], that still exist in the present scenario, but with increased quality and reliability to the weakness of in-wrinkled imperativeness use, traffic age and overhead of keeping up the elective ways. In this paper, we overcome these issues with security as an essential issue.

Some sheltered multipath controlling traditions have also presented like; P. Boseet. al., W. Liuet. al. and Q. Chen et. al. [26, 27, 28] has proposed a tradition which is prepared for finding different center point disjoint routes from the each source center point to the normal sink (i.e. base station). H. Frey et al[29]., Q. Fang et. al [30], C. Petrioli et. al. [31] and X. Xiang [32] have executed a tradition to ensure node-to-node message transport, paying little mind to whether the sensor sort out is under unique ambush. X. Li et. al. [33] and S. Ruhrupet. al. along with X. Wang[34] both sent the neighbor information to the base station for enlisting multipath from source to sink. In INSENS, however, the base station unicasts the multipath table to each linked centre point, and SEEM fills in as a data-driven tradition, flooding the request to the framework, and the centre that responds to the inquiry will transmit an interest for the guiding route to the base station. Showing up legitimises security without relying on cryptography, whereas INSENS relies on cryptography to keep a strategic distance from diverse attackers.

Hubs, which are provisioned with additional important and bigger correspondence, extend than the ordinary sensor hubs. Second, Allude can rapidly and productively distinguish the elective ways and their lengths essentially in light of hub IDs upon a directing disappointment; past technique [18] needs to rely upon important expending steering age calculation. We perform broad investigations on the proposed calculation by recreation and contrast the outcomes and the dispersed important adjusted steering (DVAS) calculation [15], the fault tolerant bunching calculation as proposed by Gupta et al [13]. Further, a multi-way directing calculation and animportant effective multicasting calculation are proposed for intra-and between Kautz cell correspondences. In this paper, we will likely outline animportant effective steering calculation for WSNs by taking consideration of adaptation to internal failure of the CHs. Especially, the disappointment of a CH upsets the correspondence with its part sensor hubs as well as with different CHs as they are associated with steering collected information to the sink through different CHs [10]. The outcomes demonstrate that our proposed protocol and subsequent calculation performs superior to the previous calculations regarding the quantity of dead CHs, add up to important utilization of the system, the quantity of information bundle transmitted to the BS and standard deviation of residual important of the entryways amid the system lifetime. Likewise, the two techniques utilize either geological directing [7] or topological steering [8], [9], which expend a lot of important by depending on position data created by GPS or a virtual coordination strategy [10], [11], [12] or flooding to find and refresh directing ways. Along these lines, the overlay isn't steady with the hidden physical topology and multi-jump directing must be utilized for the correspondence between two neighboring Kautz hubs in MANETs. In numerous uses of WSN, CHs are picked among the typical sensor hubs, which may attack the succeeding node because of quick exhaustion for such additional node. The greater part of the directing conventions for versatile improper systems (MANETs) and WSNs treat each hub similarly and neglect to use the abilities of asset rich gadgets to diminish the correspondence trouble on low-asset sensors. The calculation depends on

1. Cost work
2. The packets that are acknowledged negatively, and
3. The separation of next-node from the BS.

The Proposed Algorithm of Energy Model

Continuing the introduction and related works in section I and II above, we start with the following parameters before proposing our new model: -

1. Action detection using sink node, which will be referred as SN (Actuator)
2. Pre-fault detection
3. Fault Tolerance

The Network Model

It's a proactive protocol, meaning that all of the routes are calculated before they're needed. The declaration is used to verify any hub at the time of neighbour location with the base station's general public key; a new unique shared key is used to communicate with the base station during the system's lifespan. At the start of the sending season, each hub has a unique ID (given by power, i.e. base station), a unique shared key (imparted to base station), and a unique base station open key. The DBTMCP is divided into five stages.

- topology development and neighbour discovery
- pairwise key circulation,
- cluster arrangement,
- data transmission, and
- re-grouping and re-direction

When sensor hubs are static, it is preferable to use table-driven convention (proactive convention) rather than receptive convention. The protected cluster based multipath steering convention is presented and illustrated in this segment (DBTMCP). Each period of the convention is depicted in depth in the following part.

Before defining the proposed protocol, we go through with the following definitions, which are based on the discussion made on the preceding sections: -

Cluster Formation

A. Neighbor acknowledgment and topology advancement: -need some clarification

1) Number of clusters (2) Number of items

As a result, k clusters of varied sizes have formed.

Algorithm:

1: Each object forms an initial cluster.

2: k' = n cluster number; 3: while (k' > k)

4: If I = 1 k', then

5: if j = 1 then k'

6: If I is equal to j,

7: compute the distance between the two nodes in each of the two clusters Ci and Cj;

8: build a distance set D and calculate the distance mean Davg and variance 2;

9: create a distance set D and calculate the distance mean Davg and variance 2;: For clusters Ci and Cj, calculate the clustering factor. Fi,j (Davg,δ2)= 1 Davg+0.5ä2

10: halt if

11: halt for

12: halt for

13: link the two clusters that correspond to Fmax

14: k'—;

15: halt while

Algorithm 2: Initialization Phase: The neighbour information must be updated at the start of this phase. After that, each node can calculate its cost on its own. Because this cost can be exchanged through CH msg messages, it will not be publicized to neighbours. As previously stated, clustering does not necessitate updating neighbour information or incurring processing expenses every time clustering is initiated. The protocol sets an initial percentage of CHs among all sensor nodes, Cprob, at the start. Cprob is set to 0.05 in this case. Each sensor node determines its own chance of becoming a CH.

Algorithm 2: CH Election (General Cluster)

(1) Cluster C nodes (2) Cluster C size: NO (3) BS location (BSx, BSy)

Cluster C's CH

1: determine Cen (XC, YC) cluster centre position;

2: for I = 1 NO

3: calculate the goal function of node I GiCH

4: finish for

5: choose the node with the highest GCHmax as the cluster C's CH;

Any most of the way center point who get the NBR Information package will perform following errands:

(1) First check the believability of the sender center by its statement.

(2) If the sender center point ID is affirmed, beneficiary center point rebroadcast the package.

(3) If the authority center point again gets a comparative package with same ID, fundamentally drops the package.

For that every center point keeps up a table, called got divide.

Thusly, it lessens the movement of the framework and extra some imperativeness of the center point. Right when the NBR Information package compasses to the BS as showed up in figure 1, BS will check the Mac for the respectability and authenticity and scrambles the neighbor information with the noteworthy shared key between sender center point and the base station. We use Mac which is made by the data and mixed by the novel shared key, with the objective that no foe can satire or control the neighbor information.

Pairwise Key dissemination

The base station can picture the right topology of the framework after receiving neighbor information from all center points of the framework and transmit a neighbor system through which the BS can determine the various paths from the BS to each source center point after applying the DFS estimation. BS must first register the secret key for each neighbor center join, or, at the end of the day, the key. A hash fills in was used to create the pairwise key, which seeks after:

Algorithm 3. Node selection algorithm (Inter Cluster)

Inputs: Cluster C consists of the following: (1) nodes (2) cluster size C: NO (3) BS's current address is: (BSx, BSy) (BSx, BSy) (BSx, BSy) (BSx, BSy) (BSx, BSy) (BSx, BSy) (BSx Cluster C's P-CH and S-CH as a result)

1st, compute Cen (XC,YC) for cluster centre position; 2nd, calculate Cen (XC,YC) for cluster centre position; 3rd,

2: in the case of I = 1 NO

3: calculate the GiCH objective function for node I;

4: as the P-CH and S-CH of cluster C, choose two nodes with GCHmax and GCHsecond-max, respectively.

5: as the P-CH and S-CH of cluster C, choose two nodes with GCHmax and GCHsecond-max, respectively.

Package form, progression number, BS ID, underwriting, ID of the objective, ID of its neighbour, mixed pairwise key for x and y, and Mac of the entire data are all included in the package configuration. Every transitional centre point that accepts this package accomplishes the following: (1) Confirms the base station's confirmation with the general society key. (2) It checks the seq no and centre point match of the package in the get allocate starting now and for the foreseeable future. If no such entry exists, save the sequence number, package create and match out of centre point, and rebroadcast the bundle; otherwise, dump it. (3) Encode the pairwise key, confirm the Mac, and transmit the mixed package proposed for the neighbour centre point with nonce and its own ID mixed if the objective centre point ID is the same as its own ID with the pairwise key, in the going with setup:

(1) Cluster C nodes as inputs (2) Size of cluster C: n (4) number of clusters to use: k NO (3) number of surviving nodes

As a result, Cluster C's dormant nodes

I = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1 = 1

2: Sidor, calculate the dormancy factor for node i. 3: complete, 4: calculate the node dormancy ratio, P 5: Sort the group of dormancy factors by size from small to large.

6: dormancy the nodes that are related to the P dormancy factors previously mentioned

Gathering Improvement

After the pairwise key dissemination, improvement of gathering is begun by the BS. Choice of the gathering head relies upon the waiting imperativeness as cleared up in EECS. We acknowledge that all center point's essentialness level are same before starting the cluster advancement. By and by BS will pick 5-8% of the centers as gathering head with the going with conditions; (1) no two bundle heads will be the neighbor of each other and (2) each cluster head have no under 7-10% of center points as neighbor. A brief span later BS unicasts the hint package (i.e. CH INT) to the gathering heads with the figured coordinating path from the CH to the BS. Allow us to acknowledge in the normal coordinating way center point I is the accompanying bounce, and after that the association of CH INT distribute according to the accompanying:

Each center point tolerating this package does the going with things: (1) Check the accompanying ricochet ID, if its proportionate as its own, decipher the Way and find the accompanying hop from the coordinating (Way) by and large drop the bundle. (2) Check the seq no in got package table, if does not exist, by then store distribute and seq no and do also changes in the package, by and large drop it. (3) Set the past hop as its own one of a kind ID and next ricochet as found in the directing (Way). (4) Store the controlling table in the memory with next and past hop as pivot to forward the data to the BS. (5) Encode the Way and seq no for next ricochet center with the pairwise key and impart the changed bundle.

Hence, when CH INT package gotten by CH, It can unscramble the Path and likewise check the data by Mac and sends an attestation (ACK) back to the BS, by following the equal directing way. After a particular time if BS won't get any attestation (ACK) from the CH, It will again enlist the way and resend the CH INT allocate. Criteria for preparing the controlling way are: (1) signify remaining essentialness of the way and (2) mean usage of the power in the way.

That is the path with more critical outstanding imperativeness and most diminutive bob check has been picked like Show up. Directly for group improvement the CHs impart the CH ADV package to promote their will. CH ADV contains the ID and CERT with the objective that recipient center point can check the affirmation. Centers, which get various promotions, will pick the CH with two criteria: (1) paying little heed to whether the pairwise key exist with the pitched ID and (2) more noticeable banner nature of the imparted advertisement.

Consequent to picking the CH, centers send their will by CH Join package with ID and a Mac with the pairwise key and a nonce. Consequent to getting the entire joining requesting, CH sends the gathering part information to the BS and makes a TDMA plan reliant on number of part center points and unicast it to each part. The extensive simulation has been carried out in different scenario. In figure no. 1 the average energy spent is shown and compared the results with traditional algorithm. Figure 2 elaborates the average number of alive nodes over the various rounds of communications and figure 3 represents the average energy dissipated in different communication scenario.

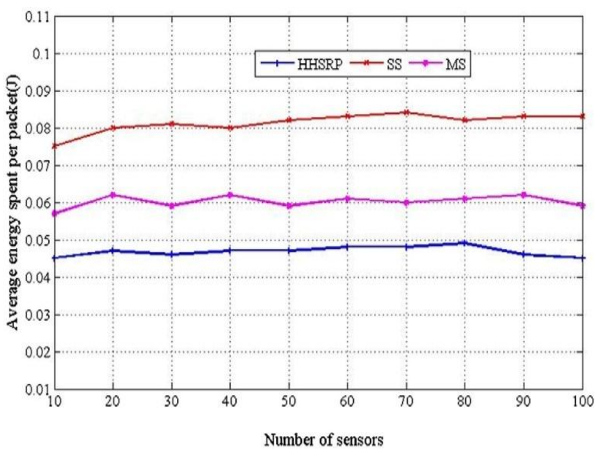

Figure 1: Average energy spent by every node

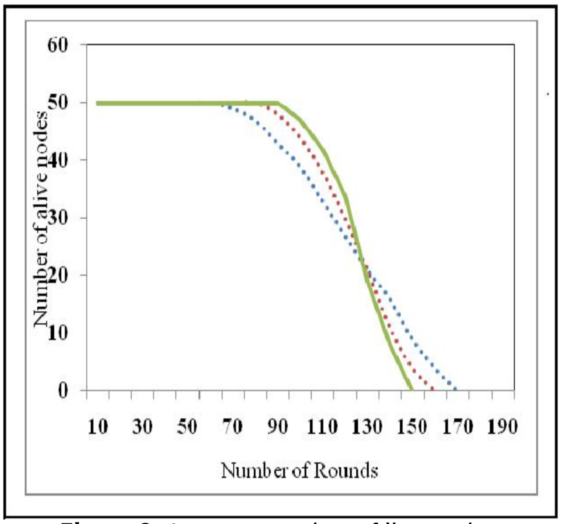

Figure 2: Average number of live nodes

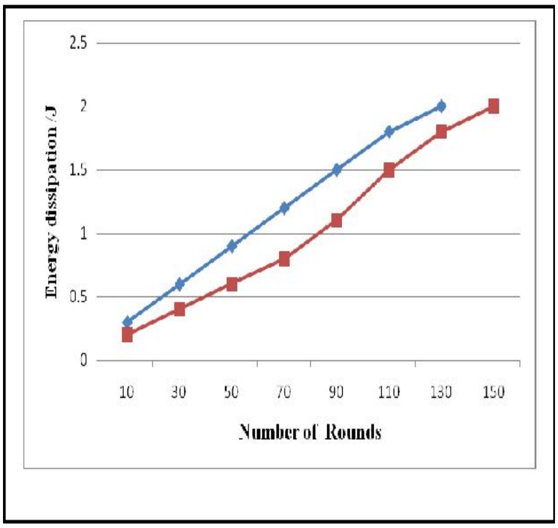

Figure 3: Average energy dissipation

In conclusion, we have examined energy challenges for all networks, particularly energy consumption and optimal utilization. We've submitted our definitions for an energy-efficient methodology, as well as detailed simulations with important data for defect detection. This study offered a novel strategy based on energy efficient awareness for "fault tolerant prevention." Finally, in this paper, we have devised a protocol that selects a successor node in an energy-efficient manner and, in the event of its failure, reverts to the previous state reestablish the connectivity of a cluster's neighbours around that node in a sensitive way.

REFERENCES

[1] Imoize, A. L., Oyedare, T. R., Ezekafor, C. G., & Shetty, S. Deployment of an Energy Efficient Routing Protocol for Wireless Sensor Networks Operating in a Resource Constrained Environment. *Transactions on Networks and Communications, 7* (1), 41. December 2019.

[2] Yongmei Wang1*, Min Zhang2 and Wanneng Shu3 An emerging intelligent optimization algorithm based on trust sensing model for wireless sensor networks. Wang et al. EURASIP Journal on Wireless Communications and Networking (2018) 2018:145.

[3] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin. Highly-resilient, energy-ecient multipath routing in wireless sensor networks. *ACMSIGMOBILE Mobile Computing and Communications Review*, 5(4):11–25, 2001.

[4] W. Heinzelman, A. Chandrakasan, , and H. Balakrishnan. Energy-e client communication protocols for wireless micro sensor networks. In *Proc. 33rd IEEE Hawaii International Conference on System Sciences*, volume vol.8, pages 4–7, January 2000.

[5] C. Hong-bing, Y. Geng, and H. Su-jun. Nhrpa: a novel hierarchical routing protocol algorithm for wireless sensor networks. *The Journal of China Universities of Posts and Telecommunications*, 15(3):75–81,September 2008.

[6] C. Intanagonwiwat, R. Govindan, and D. Estrin. Directed di usion: a scalable and robust communication paradigm for sensor networks. In *Proc. the 6th annual international conference on Mobile computing and networking (MobiCom'00)*, pages 56–67. ACM, 2000.

[7] K. Kurosawa and W. Ogata. E cientrabin-type digital signature scheme. *Designs, Codes and Cryptography*, 16(1):53–64, January 1999.

[8] Wenjing Lou. An efficientt n-to-1 multipath routing protocol in wireless sensor networks. In *In: Proc. 2nd IEEE International Conference MASS*, pages 665–672, Washington D.C., November 2005.

[9] N. Nasser and Y. Chen. Seem: Secure and energy-e cient multipath routing protocol for wireless sensor networks. *Computer Communications*, 20(11-12):2401–2412, 2007.

[10] L. B. Oliveira, A. Ferreira, M. A. Vilaa, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro. Secleach-on the security of clustered sensor networks. *Signal Processing*, 87(12):2882–2895, December 2007.

[11] B. Parno, M. Luk, E. Gaustad, and A. Perrig. Secure sensor network routing: a clean-slate approach. In *Proc. the 2006 ACM CoNEXT conference*, pages 1–13, Lisboa, Portugal, December 2006. ACM.

[12] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D. E. Culler. Spins: Security protocols for sensor networks. *Wireless Networks*, 8(5):521– 534, September 2002.

[13] Z. Quan and J. Li. Secure routing protocol cluster-gene-based for wireless sensor networks. In *Proc. The 1st International Conference onInformation Science and Engineering (ICISE2009)*, pages 4098–4102,December 2009.

[14] J. G. Steiner, G. Neuman, and J. I. Schiller. Kerberos: An authenti-cation service for open network systems. In *Proc. the Usenix Winter Conference, Berkeley*, pages 191–202, February 1988.

[15] M. Tubaishat, J. Yin, B. Panja, and S. Madria. A secure hierarchical model for sensor network. *ACM SIGMOD Record*, 33(1):7–13, March 2004.

[16] M. Ye, C. Li, G. Chen, and J. Wu. Eecs: An energy e cient clustering scheme in wireless sensor networks. In *Proc. of the IEEE International Performance Computing and Communications Conference*, pages 535–540. IEEE Press, 2005.

[17] K. Zhang, C. Wang, and C. Wang. A secure routing protocol for cluster-based wireless sensor networks using group key management. In *Proc. 4th IEEE International conference on Wireless Communications, Networking and Mobile Computing (WiCOM'08)*, pages 1–5, October2008.

[18] Haiying Shen, Ze Li, "A Kautz-Based Wireless Sensor and Actuator Network for Real-Time, Fault-Tolerant and Energy-Efficient Transmission", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 15, NO. 1, JANUARY 2016

[19] Haojun Huang, Hao Yin, Geyong Min, Junbao Zhang, Yulei Wu, and Xu Zhang, "Energy-aware Dual-path Geographic Routing to Bypass Routing Holes in Wireless Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING.

[20] L. Cheng, J. Niu, J. Cao, S. Das, and Y. Gu, "QoS Aware Geographic Opportunistic Routing in Wireless Sensor Networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1864-1875, Jul. 2014.

[21] C. Fraser, C. Kevin, S. Jose, and M. Sandra, "A Survey of Geographical Routing in Wireless Ad-Hoc Networks," IEEE Commun. Surv. Tutor., vol. 15. no. 2, pp. 621-653, 2013.

[22] S. S. Lan and C. Qian, "Geographic Routing in d-Dimensional Spaces with Guaranteed Delivery and Low Stretch," IEEE/ ACM Trans. Netw., vol. 21, no. 2, pp. 663-677, 2013.

[23] B. Karp and H. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," Proc. ACM MobiCom 2000, Boston, Massachusetts, USA, pp. 243-254, 2000.

[24] D. Chen and P.K. Varshney, "A Survey of Void Handling Techniques for Geographic Routing in Wireless Networks," IEEE Commun. Surv. Tutor., vol. 9, no. 1, pp. 50-67, 2007.

[25] P. Bose, P. Morin, I. Stojmenovic, and J. Urrutia, "Routing with Guaranteed Delivery in Ad Hoc Wireless Networks," ACM/Kluwer Wireless Netw., vol. 7, no. 6, pp. 609-616, 2001.

[26] W. Liu and K. Feng, "Greedy Routing with Anti-void Traversal for Wireless Sensor Networks," IEEE Trans. Mob. Comput., vol. 8, no. 7, pp. 910-922, 2009.

[27] Q. Chen, S. S. Kanhere, and M. Hassan, "Adaptive Position Update for Geographic Routing in Mobile Ad Hoc Networks," IEEE Trans. Mob. Comput., vol. 12, no. 3, pp. 489-501, Mar. 2013.

[28] H. Frey and I. Stojmenovic, "On Delivery Guarantees of Face and Combined Greedy Face Routing in Ad Hoc and Sensor Networks," Proc. ACM MobiCom 2006, CA, USA, pp. 390-401, 2006.

[29] Q. Fang, J. Gao, and L. J. Guibas, "Located and Bypassing Routing Holes in Sensor Networks," Proc. IEEE INFOCOM 2004, Hong Kong, China, pp. 2458-2468, Mar. 2004.

[30] C. 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.

[31] X. Xiang, X. Wang, and Z. Zhou, "Self-Adaptive On-Demand Geographic Routing for Mobile Ad Hoc Networks," IEEE Trans. Mob. Comput., vol. 11, no. 9, pp. 1572-1586, Sept. 2012.

[32] X. Li, J. Yang, A. Nayak, and I. Stojmenovic, "Localized Geographic Routing to a Mobile Sink with Guaranteed Delivery in Sensor Networks," IEEE J. Selected Areas in Comm., vol. 30, no. 9, pp. 1719-1729, Oct. 2012.

[33] S. Ruhrup and I. Stojmenovic, "Optimizing Communication Overhead while Reducing Path Length in Beaconless Georouting with Guaranteed Delivery for Wireless Sensor Networks," IEEE Trans. Comput., vol. 62, no. 12, pp. 2240-2253, Dec. 2013.

[34] X. Wang, J. Wang, K. Lu, and Y. Xu, "GKAR: A Novel Geographic K-anycast Routing for Wireless Sensor Networks," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 5, pp. 916-925, 2013.