Pithy Review on Routing Protocols in Wireless Sensor Networks and Least Routing Time Opportunistic Technique in WSN

Mohammed Salman Arafath¹, Khaleel Ur Rahman Khan², K.V.N Sunitha³

¹Dept of CSE, Keshav Memorial Institute of Technology Hyderabad, Telangana, India
²Dept of CSE, ACE College of Engineering, Hyderabad, India
³Dept of CSE, BVRIT College of Engineering, Hyderabad, India

Abstract. Nowadays due to most of the telecommunication standard development organizations focusing on using device-to-device communication so that they can provide proximity-based services and add-on services on top of the available cellular infrastructure. An Oppnets and wireless sensor network play a prominent role here. Routing in these networks plays a significant role in fields such as traffic management, packet delivery etc. Routing is a prodigious research area with diverse unresolved issues. This paper firstly focuses on the importance of Opportunistic routing and its concept then focus is shifted to prime aspect i.e. on packet reception ratio which is one of the highest QoS Awareness parameters. This paper discusses the two important functions of routing in wireless sensor networks (WSN) namely route selection using least routing time algorithm (LRTA) and data forwarding using clustering technique. Finally, the simulation result reveals that LRTA performs relatively better than the existing system in terms of average packet reception ratio and connectivity.

1. Introduction

Wireless Sensor Network (WSN) is a billion dollar market. WSN is the backbone of emerging technologies like the internet of things IoT, vehicular networks, cyber-physical systems etc. Wireless sensor networks are developed to support a huge range of applications ranging from home automation to smart battlefields [1]. Wireless sensor networks consist of a huge number of tiny sensor nodes that are arranged in spatially distributed terrain. Sensor node can sense, store, transmit and receive data from environments [2] while designing of wireless sensor network faces the major issues are energy consumption, security, and routing.

This paper targets routing part i.e. opportunistic routing and other important metrics are not focused here. Routing in wireless sensor network is one of the paramount aspects. The nitty-gritty of wireless sensor network is broadcasting nature of the network. This fact is used by the opportunistic routing.

2. Opportunistic Routing

Routing in WSN using Opportunistic routing is a newfangled paradigm to increase the network lifetime, packet delivery ratio or packet reception ratio. Routing in wireless sensor network (WSN) is an onerous task as it involves many parameters. There are many traditional routing algorithms for wireless sensor networks however it has been proven that Opportunistic routing is better and more efficient than the traditional routing [3]. If routing solution is good for WSN then it results in increased
in network lifetime and decreased in energy consumption otherwise the results will be contrary. Therefore this field has attracted many researchers.

2.1. Concept of Opportunistic Routing (OR)

WSN utilizes the shared random access wireless channel and most of the routing protocols consider this wireless medium as a limitation due to temporal variation. This shared wireless medium which was an obstruction to most of the routing protocols is an opportunity in an Opportunistic Routing (OR). The essential concept of OR it to exploit the broadcast nature of wireless medium. When OR advertise a data packet then that transmission of one node is overheard by multiple neighbour nodes which later forms the forwarder set. The crucial task of OR is to select a packet forwarder node, this is achieved by OR not by pre-selecting next forwarder node well ahead of time but the next forwarder node is selected dynamically at the time of transmission. The forwarder node is selected from the forwarder set in such a way that it is closest to the destination. The ExOR Opportunistic Multi-Hop Routing for Wireless Network [4] is the pioneer in practically implementing the OR in wireless networks as it dynamically chooses the paths on a per transmission basis in a wireless network

2.2. Pithy Review of Routing Protocols in Wireless Sensor Networks and role of OR

Networks are meant so that packets can be routed. Here our focus is WSN but there is another category of the networks known as Opportunistic Networks or Opportunistic sensor networks (Oppnets). The differentiating criterion between these two is the intermittent connection. Since OR takes advantage of Opportunistic contacts in wireless shared medium all the routing protocols in Oppnets should have the ability to withstand with the network disconnection. We may say that routing protocols in Oppnet are Opportunistic in nature and they are in the category of OR. However, the routing protocols in WSN are not opportunistic in nature because WSN is well-connected network and the intermittent connection is an exception here. Incorporating the concept of opportunity in WSN shown to the world that it has lot of improvements in term of battery lifetime, packet delivery ratio, increasing network lifetime etc; Since WSN have shared wireless medium and flooding is used to broadcast messages to the nodes in WSN the point is that we need to design mechanisms and techniques to control this flooding and we term it as forwarding. So opportunistic routing is nothing but controlled flooding by various techniques and mechanisms. Table 1 below shows in chronological order the various algorithms used in OR are nothing but controlled flooding and a mix of GPS (it is also used to control flooding messages) so that messages are not sent in the wrong direction of destination to avoid energy consumption.

Table 1. Comparison of OR Algorithms based on forwarding technique with merits and demerits

| Reference/Year | Forwarding Technique/controlled flooding | Merits and Demerits / Remarks |
|----------------|------------------------------------------|-------------------------------|
| Reference[5] 2017 | Based on Path Protected Hop by Hop Protocol. A node having no certificate avoided from the route and another path will be selected | Improved security, throughpt, energy consumption, packet overhead and network reliability. |
| Reference[6] 2017 | Based on ML probability in terms of successful delivery, dropped messages, hop counts and overhead | It outperforms PROPHET+ at cost of small buffer size and space. |
| Reference[7] 2016 | Based on combining the concept of Opportunistic routing with rateless coding and Orthogonal Frequency Division Multiple Access | It outperforms the strategy of forwarding along unique path by up to 77% |
| Reference[8] 2015 | Based on forwarder list and the nodes in the forwarder list prioritizing themselves based on optimal hop and residual energy distance | Better energy usage and increased network lifetime. Packet delivery rate is better than reference [10] |
| Reference[9] 2013 | Based on the cost metric such as social profile, social connectivity and social interaction of node | Efficient routing and increased packet delivery. |
| Reference[10] 2012 | Based on trust value(direct and indirect ) and cost distance from destination | Reduced End to End packet delay and increased in security gains. |
| Reference[11] 2011 | Based on forwarding set which in turn selected based on total expected cost TEC. TEC is calculated as min of | For each node expected cost is updated using Bellman-Ford algorithm. |
expected cost of node to be added or the prefix forwarding list

| Reference [12] | The only destination node can opportunistically receive the packet by overhearing the transmission of nodes in the traditional network and sends destination ACK to other nodes on the path. | Reduces packet duplication rate Increases throughput. |
| Reference [13] | Based on forwarder list in which nodes prioritize them based on a cost metric. Cost metric which is based on Optimal link transmission aspect, optimal path metric and node metrics. | Better throughput, improved end to end delay performances compared with traditional computer network algorithms. |
| Reference [14] | Priority candidate for the next hop among the nodes depends on priority order and delivery ratio. | Good for analyzing the performance parameters |
| Reference [15] | Always low priority nodes hear the advertisement of high priority nodes | No duplications |
| Reference [4] | It identifies the shortest path to destination and ties are resolved using delivery ratio matrix | It outperforms the best-predicted routes in number of transmissions |
| Reference [6] | Based on Geographic routing. When sender node broadcast its own and destination location the listening nodes will prioritize themselves to act as a relay node. | Analysis of performance can be done in terms of a number of hops to reach the destination. |
| Reference [17] | It uses geographic information to direct packets towards the destination. | It is reminiscent of flooding |

Figure 1. The Relative Focus on QoS Parameters by Researchers [18].

In this paper focus is only on routing taking packet delivery ratio as the important quality of service parameter according to the author of [18], as shown in figure 1 above the packet delivery is a second highest parameter and this paper is addressing the same metric as shown in the figure below which is reproduced from [18].

The data shown in figure 2 below represents the recent research and developments in the field of routing in WSN [18]. The routing protocols have been developed to face many challenges and one of them is packet reception and packet delivery, which is the prime focus of this paper. When compared with the year 2015 in 2016 the factor of developing routing solutions are fall by a factor of 5.
Figure 2. Development of Routing protocols for WSN over the time period [18].

3. Proposed Architecture
As shown in figure 3 below in order to provide efficient communication between source nodes to the destination node, clustering of the nodes will be performed and among the clusters, a cluster head is selected based on the clustering algorithm, an i.e. node which is nearest to the destination node. From the available best cluster heads the source node chooses to send the packet to cluster heads using intermediate nodes on which it trusts most. The cluster head, in turn, communicates with the destination node. For the sake of understanding in figure 3 different colors are used for selected neighboring node, cluster head, cluster member, the source node and the destination node. Similarly, the arrows in figure 3 show the available path and path selected for routing, request messages sent from cluster heads and response messages from sensor nodes. Clustering and Routing pseudo-code is given in the subsequent sections. Finally, the simulation result shows the number of data packets received is relatively better than the existing system [19].

3.1. Identifying Problems and Proposed Solutions
The author of the paper [20] proposes Establishing Stable and Reliable Routes algorithm i.e. establishing a stable and reliable route in multi-hop heterogeneous wireless sensor networks. It combines the payment and trust management with trust values and energy aware routing protocol. This routing protocol selects routing path based on trust value, which calculates trust value based on past behaviors of a node in the different time interval. This paper provides the two routing protocols Shortest Reliable Route (SRR), and Best Available Route (BAR) for reducing energy consumption in networks. However, the drawback is routing is not efficient because this algorithm calculates the trust value based on the behavior of node only. But the behavior of node may change into malicious. So it is not efficient for routing. In our proposed solution trust value is calculated based on packet reception ratio, it's efficient for routing.

The author in [21] presents the active trust routing protocol for secure routing in sensor networks. This protocol provides a quick detection of black hole attack in networks by using the trust values of nodes. Active trust algorithm significantly improves the data route access probability and ability to detect a black hole attack. However, path selection is difficult, due to source node selects only high trust value with the nearest node to the destination. The proposed solution is to select the path based on a best available path which is least routing time path.

3.2. Clustering Nodes
Clustering is the process of organizing the sensor nodes in groups. In this clustering algorithm sensor node forms the group based on least distance from the destination as shown in section 3.2.1.
Pseudo Code for Clustering Nodes. The following is the pseudo code for clustering nodes.

i. Begin
ii. Destination node gets messages from all the nodes
iii. Destination node computes minimum distance to all other best nodes
iv. Search for node closest to another node, if one of them is close to the border remove it.
v. Destination node announce the cluster head and advertise to all the nodes
vi. Cluster head is formed based on least distance with the destination and having higher energy
vii. Send data to cluster head and cluster head sends data to destination
viii. If cluster head has low energy or least distance choose which is nearest to it
ix. New cluster head will communicate with the destination node
x. End.

Figure 3. The Proposed Architecture

3.3. Routing
In routing forwarding, a packet to the intermediate node is one of the crucial decisions. To help source node to take the decision to trust the intermediate node this algorithm introduces the concept of trust value. All the intermediate nodes which can carry packet from source to cluster head may have different trust values or no trust value. The one with highest trust value will be selected for intermediate node. This trust is calculated based on packet reception ratio as shown in section 3.3.1.

Pseudo Code for Routing. The following is the pseudo code for routing.

i. Begin
ii. All nodes providing request
iii. All these requests are sent to cluster by the nodes
iv. Calculate Packet Reception ratio for all the nodes.
v. If Packet reception ratio is high then trust value is assigned
vi. Otherwise, no trust value is assigned.
vii. Sender nodes select the intermediate node based on high trust value
viii. Sender nodes sends packet to cluster head
ix. Cluster head verifies it
x. If packet is valid it moves packet to the destination
xi. Otherwise, drops the packet
xii. End

3.4. Packet Delivery Ratio
In this section packet delivery ratio on the proposed solution is described. Packet delivery ratio (PDR) is the ratio of total packets successfully sent to the source node to the total packet received by the destination node. The proposed solution results in reveals that the packet delivery ratio is better compared with the existing researches. The table 2 below depicts that when 50 nodes are taken then existing system gives 95% of packet delivery ratio whereas the proposed system gives 100% of packet delivery ratio. Similarly when 100,150 and 200 nodes are taken the respective packet delivery ratio in the existing system is 89%, 82%, and 79% respectively. However, the proposed system gives 100%,95% and 94% of packet delivery ratio for 100,150,200 nodes respectively. Figure 4 shows the aforementioned results in graphical form.

![Figure 4. Comparison of Number of packets received with the existing system [19].](image)

| Number of Nodes | Existing[19] | Proposed |
|-----------------|-------------|----------|
| 50              | 95          | 100      |
| 100             | 89          | 100      |
| 150             | 82          | 95       |
| 200             | 79          | 94       |

The proposed solutions of opportunistic routing in WSN are implemented in OMNeT++ simulation software. Omnet++ is open source. The standard IEEE 802.15.4 is designed for various supports in WSN one of them is routing also.

4. Conclusion, Future Work and Scope
In current work, we focus only on routing and packet delivery ratio. However, this paper is successful in getting the better results relatively with the existing system. Improvement in packet delivery ratio makes an attack on availability more difficult. It is possible to extend this work to incorporate security in OR (Opportunistic Routing) further the work can be extended by analyzing the replication problem and including some more data structure, it is possible to avoid replication attacks. Still, there is the scope of efficient energy management in WSN. The proposed algorithm is portable and it may be deployed in Opportunistic sensor networks to get the same results.

5. References
[1] Mohammed Salman Arafath, Khaleel Ur Rahman Khan, "Opportunistic Sensor Networks: A Survey on Privacy and Secure Routing", 2017 2nd IEEE International Conference on Anti-Cyber Crimes (ICACC), pp.41-46, 26-27 March 2017.
[2] Sukhwinder Sharma, Rakesh Kumar Bansal, Savina Bansal, "Issues And Challenges in Wireless Sensor Networks" IEEE International Conference, pp 1-5, 2013.
[3] Sanjit Biswas, Robert Morris, "Opportunistic Routing in Multi-Hop Wireless Networks" MIT Laboratory for Computer Science.
[4] S. Biswas and R. Morris, “ExOR: Opportunistic multi-hop routing for wireless networks,” in Assoc.Comput. Mach. SIGCOMM Comput. Commun. Rev., 2005, vol. 35, no. 4, pp. 133–144.
[5] Arafath, M.S., and Khan, K.U.R. ‘Incorporating privacy and security in military application based on opportunistic sensor network’, Int. J. Internet Technology and Secured Transactions, (This paper has been selected for publishing the Complete Reference will be provided soon) http://www.inderscience.com/info/ingeneral/forthcoming.php?jcode=IJITST
[6] D. K. Sharma; S. K. Dhurandher; I. Woungang; R. K. Srivastava; A. Mohananey; J. J. P. C Rodrigues, “A Machine Learning-Based Protocol for Efficient Routing in Opportunistic Networks,” in IEEE Systems Journal, vol.PP, no.99, pp.1-7 doi: 10.1109/JSYSY.2016.2630923.
[7] F. Hohmann and A. Klein, "Opportunistic Forwarding Using Rateless Codes in OFDMA Multihop Networks," 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall), Montreal, QC, 2016, pp. 1-5.
[8] Juan Luo, Member, IEEE, Jinyu Hu, Di Wu, Member, IEEE, and Renfa Li, Senior Member, IEEE “Opportunistic Routing Algorithm for Relay Node Selection in Wireless Sensor Networks” IEEE Transactions on Industrial Informatics, VOL. 11, NO. 1, February 2015.
[9] Gary K. W. Wong, Xiaohua Jia,” A Novel Socially-Aware Opportunistic Routing Algorithm in Mobile Social Networks” International Conference on Computing, Networking and Communications, Wireless Ad Hoc and Sensor Networks Symposium 2013.
[10] Jie Zhingzhong, Huan chuanhe, Xu Liya, Wang Bo, Chen Xi, Fan Xiying.”A Trusted Opportunistic Routing Algorithm for Vanet” Third International Conference on Networking and Distributed Computing 2012.
[11] Xiaohua Xu, Student Member, IEEE, Xiang-Yang Li, Senior Member, IEEE, and Huadong Ma, Senior Member.”Energy-Efficient Opportunistic Routing in Wireless Sensor Networks” IEEE Transaction on Parallel and Distributed Systems, VOL. 22, NO. 11, Nov 2011.
[12] Goo Yeon Lee and Zygmun J. Haas,”Simple, Practical, and Effective Opportunistic Routing for Short-Haul Multi-Hop Wireless Networks”, IEEE Transaction on Wireless Communication, VOL. 10, NO. 11, Nov 2011.
[13] Shih-Chun Lin and Kwang-Cheng Chen”Spectrum Aware Opportunistic Routing in Cognitive Radio Networks”. IEEE Globecom 2010 proceedings.
[14] Angela Sara Cacciapuoti, Marcello Caleffi, and Luigi Paura “A theoretical model for opportunistic routing in ad hoc networks “Ultra Modern Telecommunications & Workshops, 2009. ICUMT’09.
[15] Y. Li, W. Chen and Z. L. Zhang, "Optimal forwarder list selection in opportunistic routing." 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, Macau, 2009, pp. 670-675. doi: 10.1109/MOBHOC.2009.5336939.
[16] M. Zorzi and R.R. Rao, “Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Energy and Latency Performance,” IEEE Trans. Mobile Computing, vol. 2, no. 4, Oct.-Dec. 2003.

[17] Young-Bae Ko and Vaidya Nitin H. Location-Aided Routing (LAR) in mobile ad hoc networks. In Proc. ACM/IEEE MobiCom, pages 66-75, October 1998.

[18] A. Sarkar, T. S. Murugan, “Routing protocols for wireless sensor networks: What the literature says?”, Alexandria Eng. J., vol. 55, pp. 3173-3183, Dec. 2016.

[19] L. S. Sindhuja and G. Padmavathi, “Replica Node Detection Using Enhanced Single Hop Detection with Clonal Selection Algorithm in Mobile Wireless Sensor Networks”, HindawiResearch article, Journal of Computer Networks and Communications, pp. 1-14, 2016.

[20] Mohamed M. E. A. Mahmoud, Xiaodong Lin, and Xuemin (Sherman) Shen, “Secure and Reliable Routing Protocol for Multihop Heterogeneous Wireless Sensor Networks” IEEE Transactions on Parallel Distributed Systems, pp 1-11, 2013.

[21] Yuxin Liu, Mianxiong Dong, Member, Kaoru Ota, Member, AnfengLiu,”Active Trust Secure Trustable Routing In Wireless Sensor Networks”, IEEE Transactions on Information Forensics and Security, pp 1-14, 2016.