EUROPEAN COOPERATION
IN THE FIELD OF SCIENTIFIC
AND TECHNICAL RESEARCH

EURO-COST

COST 2100 TD(09) 869
Valencia, Spain
2009/May/18-19

SOURCE: Department of Telecommunications,
AGH University of Science and Technology,
Poland

Department of Information Technologies and Communications,
Polytechnic University of Cartagena,
Spain

Competitive MAC Protocol for Azimuth Routing in Large-Scale Wireless Sensor Networks

Pawel Kulakowski
Department of Telecommunications
AGH University of Science and Technology
Al. Mickiewicza 30
30-059 Krakow
POLAND
Phone: +34 968 33 8894
Email: kulakowski@kt.agh.edu.pl

Esteban Egea-Lopez, Joan Garcia-Haro
Department of Information Technologies and Communications
Polytechnic University of Cartagena
ETSIT, Campus Muralla de Mar s/n
30202 Cartagena
SPAIN
Phone: +34 968 325314
Fax: +34 968 325338
Email: {esteban.egea, joang.haro}@upct.es

Competitive MAC Protocol for Azimuth Routing in Large-Scale Wireless Sensor Networks*

Paweł Kułakowski, Esteban Egea-López, Joan García-Haro

Abstract

This document contains a report of our recent work in the area of transmission protocols for large-scale wireless sensor networks. We analyse a sensor network where the nodes do not have any knowledge about the network topology. The nodes are only aware of their own positions and the position of the nearest sink.

We propose a MAC protocol that enables each transmitting node to choose its best neighbour to forward a data packet. All the neighbours are competing to become the forwarder using an adaptive time division multiple access scheme. The proposed MAC protocol guarantees that the best neighbour is chosen. The MAC protocol is designed to cooperate with the azimuth routing mechanism, presented during previous COST 2100 meeting in Braunschweig. Computer simulations are also reported that validate the protocol performance and allow choosing the optimal length of the MAC protocol frame.

Keywords: Wireless sensor networks, MAC and routing protocols.

I. Introduction

Wireless sensor networks (WSNs), as a research topic, are currently very intensively explored. They are considered as a solution for a large spectrum of applications, i.e. tracking patients at hospitals, gathering data from a hostile environment, controlling electronic equipment at households and many others. The variety of possible applications creates numerous problems with defining a unique standard for WSNs, as the requirements are totally different depending on the network purpose.

In this paper, we are considering communication protocols for the classical, large-scale WSN scenario. A sensor network consists of an arbitrary large number of nodes (hundreds or thousands), possibly randomly deployed. The nodes are gathering some data about the vicinity and sending it to few master-nodes, called sinks, that are distributed among the sensors. The scenario only fits to a certain group of WSNs that gather data for environmental preservation or agriculture purpose, serve in a military field to observe enemy units, measure the parameters of a polluted or inaccessible region or even explore cosmic space. However, other applications like taking caring for hospital patients or controlling household equipment require a different approach.

Taking into account the abovementioned characteristics, some objectives should be fulfilled to obtain a good communication protocol. First, the protocol should be highly scalable. Despite of the large size of the network, the protocol should be able to find a route to the nearest sink and the route shouldn't be significantly longer than the shortest path. Second, the protocol should be able to immediately adapt to network topology changes. In a sensor network, the topology can vary due to a sensor energy depletion (some nodes can practically disappear from the network), a wireless channel fading or due to node movements. The information about the

* This work was supported by Polish project grants 179/N-COST/2008/0 and DWM/MOB17/II/2008. It was also supported by Spanish grant TEC2007-67966-01/TCM (CON-PARTE-1) and developed in the framework of "Programa de Ayudas a Grupos de Exelencia de la Region de Murcia, Fundacion Seneca".

topology stored in the network quickly becomes outdated. Third, the protocol should be robust to irregular network topologies. It is very probable that, because of their large size, WSNs will be deployed randomly or quasi-randomly, e.g. with the use of airplane or helicopter. Random network topologies can result in serious routing problems, e.g. a data packet can be stuck somewhere in the network or circulate in loops. Recovery mechanisms should be implemented that help to avoid such situations. Finally, the cost constraints of sensor nodes need to be taken into account. As the number of nodes is very large, their cost should be reduced as much as possible. This puts the limits for the sensor processors complexity and the battery size. Thus, the complexity of the transmission protocols as well as the calculations performed by sensor processors should be limited. Also the number of transmitted and received packets and the overhead added by transmission protocols should be minimized to reduce the energy consumption.

We are assuming that a localization protocol exists that enables sensor nodes to calculate their own position and the position of the nearest sink. It can be realized e.g. with the aid of the sinks that could periodically transmit strong positioning signals (beacons) received by the sensors in a large neighbourhood, but this topic is out of the scope of this paper. It should be stressed that we are not assuming that the sensors are aware of their neighbours. The local topology can change frequently, as we mentioned before.

Localization ability matches well the WSN objectives. It stands behind the idea of geographic routing: a node can exploit the knowledge about its own position to forward a data packet in the proper direction. This simplifies the routing procedures. The geographic routing is a popular approach to routing problem in sensor and ad hoc networks with large amount of papers published. A good survey of this topic can be found, for instance in references [1, 2]. During the previous COST 2100 MC Meeting, we presented the azimuth routing protocol that fulfils very well the mentioned WSN objectives [3]. According to our knowledge, it is the first geographic routing protocol for WSNs that is not dependent on the nodes knowledge about their neighbours.

In this paper, we are discussing MAC protocols suitable for the large-scale WSNs. We are proposing a MAC protocol that can efficiently choose the best of its neighbours to forward a packet without any *a priori* knowledge about the neighbours. Moreover, the protocol is very simple for sensor processors and its overhead is also very limited to reduce the energy consumption. The proposed MAC protocol is designed to cooperate with the azimuth routing and meet all its requirements.

The rest of the paper is organised as follows. In Section II, we discuss the related work. The details of the MAC protocol are explained in Section III. The simulations documenting the protocol performance are described in Section IV. Finally, in Section V, we give some conclusions.

II. Related work

In the open literature, some papers can be found where MAC protocols suitable for geographic routing in WSNs are proposed. Very attractive scheme is presented in two companion papers [4, 5]. A node that wants to send a packet, monitors the radio channel and, if the channel is idle, it sends a packet with its own position data. Each neighbour node then calculates how good forwarder it is, i.e. how much could the data packet progress if the neighbour node would become the forwarder. Then, the neighbours respond to the initial packet in a time slotted scheme. In the first slot, the best possible forwarders respond, later the worse ones. If a neighbour hears that another neighbour has just responded, it suspends its own transmission. If the initial transmitter receives a single response, it transmits the data packet to that neighbours and the forwarding procedure is successfully finished. If a collision occurs, i.e. two or more neighbour nodes respond in the same time slot, the initial transmitter indicates that fact and these neighbours respond again with a probability of 50 %. This procedure enables to choose the final forwarder in one or few more extra steps.

Another solution is described in [6] and [7]. To decrease the number of exchanged overhead packets, it is proposed to omit the confirmation packets. An initial node starts with transmitting its data packet. The neighbours nodes respond in a similar time slot frame as it was in [5]. However, they respond with the same data packet, forwarding it at the same time and shortening the whole procedure. To avoid the hidden station problem, the area where the forwarding neighbours can be located is limited, so all the neighbours can hear the responses of the others. This scheme looks very promising, but it has a serious drawback. As the two nodes that are competing to forward the packet can have different group of neighbours, the entire scheme can lead to packet duplication and, as a result, to the additional energy waste and packet collisions.

All these MAC protocols have also two more shortcomings. First, they do not explain how to proceed if there are no neighbours closer to the sink than the transmitting node. Second, when a collision occurs (two neighbours respond in the same time slot), the forwarder is chosen randomly among the competitors, so it is not guaranteed that the best neighbour is selected.

III. New MAC protocol

Addressing the drawbacks mentioned in Section II, we propose a new MAC protocol that is designed to cooperate with the azimuth routing. This routing protocol implements recovery mechanisms that help to find a path to the sink if a packet reaches a node without neighbours closer to the sink. Such a situation is also taken into account by our MAC protocol. Sensor nodes do not need to be aware of their neighbours but they should know their own positions and the position of the nearest sink.

The transmission of the data packet is organised as follows. We assume there exists a super-frame structure where there is a long period of time when all the nodes are sleeping to save energy and a shorter period when they can communicate with each other. Thus, a node that has a packet to transmit waits for the time when the communication is possible and monitors the radio channel. If the channel is idle, the node starts to transmit the data packet. Then, all the neighbours can offer themselves as forwarders using a frame of N very short time slots. The length of each slot is very short, however the node that has initiated the transmission must be able to distinguish the responses in different slots. The neighbours calculate the routing metrics (according to the azimuth routing rules [3]) and respond in the appropriate slots. The metrics are normalized to the number of slots in the frame (e.g. if the frame length is 4, the maximum metric is also equal to 4). The first slot is occupied by the nodes with the best metrics, the second one – by the nodes with slightly worse metrics, etc. Depending on the nodes distribution (and their metrics), the responses can be sent in different slots. Nevertheless, sometimes there may happen that more than one response is sent in a particular slot. For the initial node, the most important is the first slot which is occupied by at least one response. If the initial node receives only one response in the first occupied slot, it answers with the confirmation to forward the packet (the confirmation packet is also very short) and the chosen neighbour continues the forwarding procedure (see the example in Fig. 1). If no responses are received, the initial node sends the request to change the routing state (according to the azimuth routing rules), then the neighbours recalculate the metrics and can respond again. If the initial node receives the message that is unable to detect, it assumes that collision has happened and sends the request to select the best neighbour among these ones that has responded in the first occupied slot. In such a situation, the next frame of N slots is created (see Fig. 2). The neighbour nodes that have made a collision in the previous frame, are now redistributed into all N slots, proportionally to their metrics. The neighbour from the first occupied slot is selected as the forwarder. If the collision occurs again, the procedure is repeated.

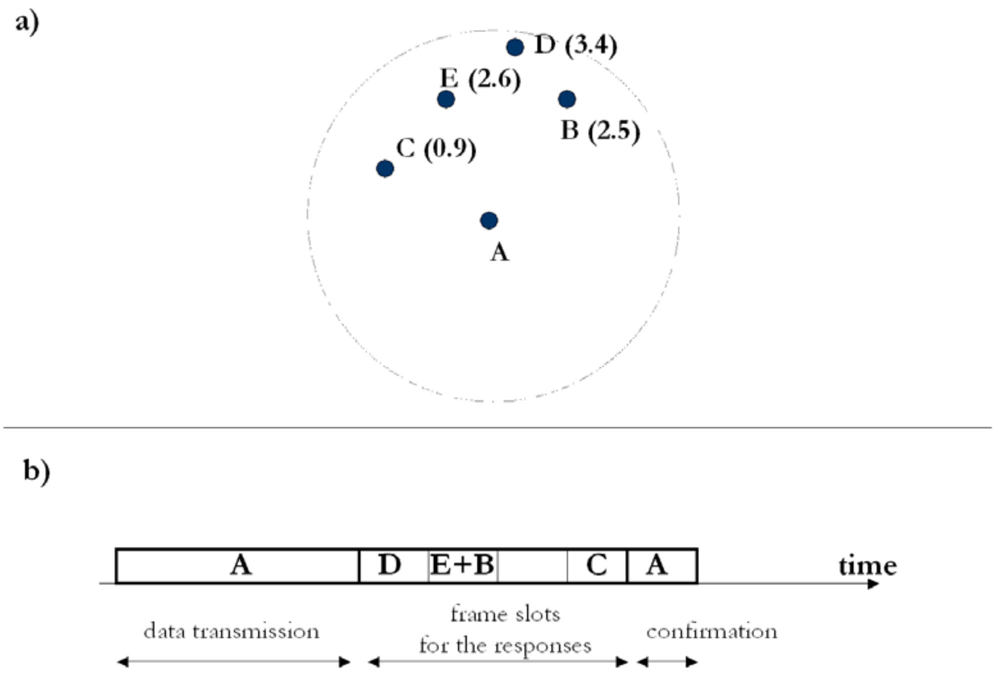

Fig. 1. An example of the forwarding procedure. In Fig. 1a. the network topology is shown. The node A initiates the transmission with a data packet, as in Fig. 1b. There are 4 neighbours, their routing metrics are given in the brackets. The time frame has 4 slots, so the metrics are normalized to 4. The nodes are distributed into the slots proportionally to their metrics. In the first slot (metrics $\in$ (3, 4)) the node D responds, as it has the best metric. In the second slot (metrics $\in$ (2, 3)), the nodes E and B respond. The node C respond in the last slot. The node A receives all the responses and sends the confirmation stating that the node D is selected as a forwarder. In this case, the collision between the nodes E and B does not disturb the selection.

Finally, in all the cases, one neighbour is chosen as a forwarder. The whole forwarding procedure requires sending one data packet and reserving at least N+1 short time slots (N slots within the time frame and 1 slot for a final confirmation sent by the initial node). If a collision occurs or the routing state needs to be changed, next N+1 short time slots need to be reserved for the communication. The response/confirmation packets that are sent in the short time slots, are probably no longer than few bytes, depending on sensors hardware.

Also, collisions may happen when two nodes initiate transmissions of different data packets simultaneously. We do not consider this issue here, but this topic is planned for our future work.

IV. Protocol performance

In order to measure the performance of the proposed MAC protocol, we implemented it in C++ and conducted computer simulations. The idea behind the simulations was to calculate the protocol efficiency, i.e. the average number of time slots needed in order to forward a data packet by a single hop.

The sensor network topology was generated randomly, with a 2-dimensional uniform distribution of the nodes and the sinks in a square area. To characterize the connectivity between sensor nodes, we use a well-known and widely used unit disk graph model [8]. This model assumes that all the nodes have the same transmission power and equal circle range called unit disk area. Under these assumptions, the entire network topology can be scaled up or down to obtain the sensor range equal to 1, independently of the transmission power and the path loss. We also assumed that sensor knew their transmission range.

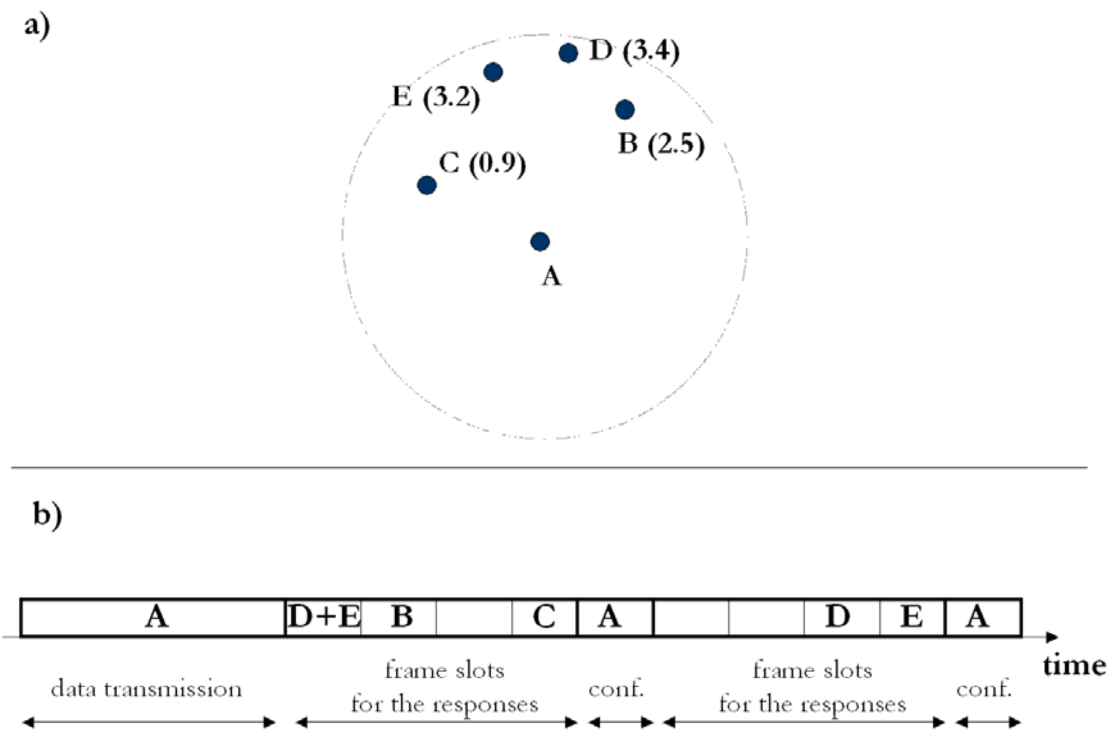

Fig.2. An example of forwarding procedure with a collision. The node A initiates the transmission sending a data packet. The neighbours respond, but there is a collision in the first slot: the nodes D and E have similar metrics. The node A sends a confirmation packet with the request to perform the selection process again. Now, only the nodes with the metrics ∈ (3, 4) compete. They are redistributed into the frame according to their metrics, the first slot: metrics ∈ (3.75, 4), in the second slot: metrics ∈ (3.5, 3.75), etc. The node D responds in the third slot (before the node E) and is selected as a forwarder.

We analysed the MAC protocol performance for the variable node density. Basically, the network consisted of 1000 nodes and 10 sinks. We were changing the area where the nodes were distributed in order to obtain different density of nodes. In the case of low-density networks, most of the nodes were not connected, i.e. there was no path between them and any sink. The simulation results were calculated only for the connected topologies. All the simulation were run 500 times.

In Fig. 3, we show the protocol performance as a function of the frame length N for different node densities. We can see that the protocol is the most efficient when the frame length is equal to 3 slots: for each case (except of very low-density networks), the number of time slots is minimal. The most critical densities are about 4 nodes per unit disk area: nearly 8 time slots are needed to forward data by a single hop. It means that 2 frames (3 slot in each frame) and 2 confirmation packets are used to select the best neighbour, in average.

To verify the protocol scalability, we also run the simulations for larger network: 10000 nodes and 100 sinks. The protocol performance for the time frame length equal to 3 slots is illustrated in Fig. 4. The results are nearly identical to the previous case with smaller network.

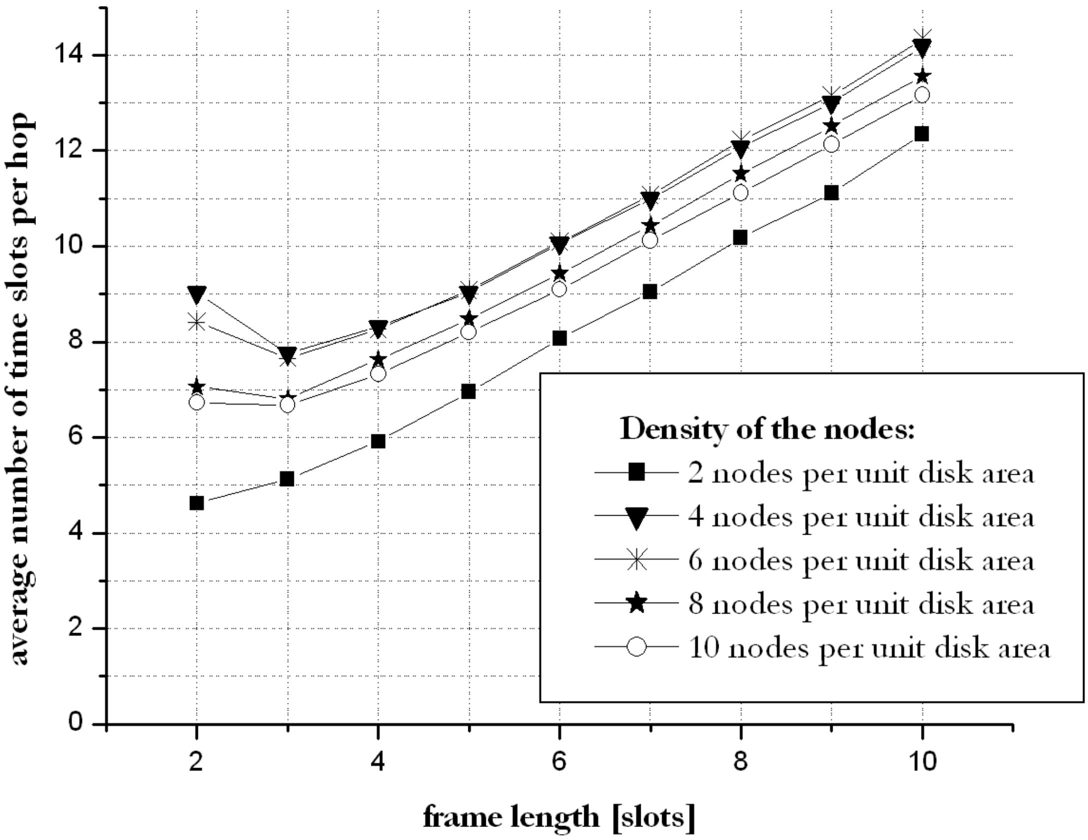

Fig. 3. The average number of time slots per a single hop a function of the frame length. The network densities from 2 to 10 nodes per unit disk area are considered. The network consists of 1000 nodes and 10 sinks.

Conclusions

In this document, we described a new MAC protocol that enabled each transmitting node to choose its best neighbour to forward a data packet. The protocol does not require any knowledge about the network topology. The nodes should only be aware of their own positions and the position of the nearest sink. The protocol is designed to cooperate with the azimuth routing.

We presented the preliminary simulation results under simplified propagation conditions. The simulations showed good protocol performance and helped to identify the optimal length of the protocol frame. As a future work, we plan to consider more complex propagation conditions and more difficult traffic scenarios, including simultaneous transmissions of multiple data packets. Modified versions of the original MAC protocol proposal will be investigated as well.

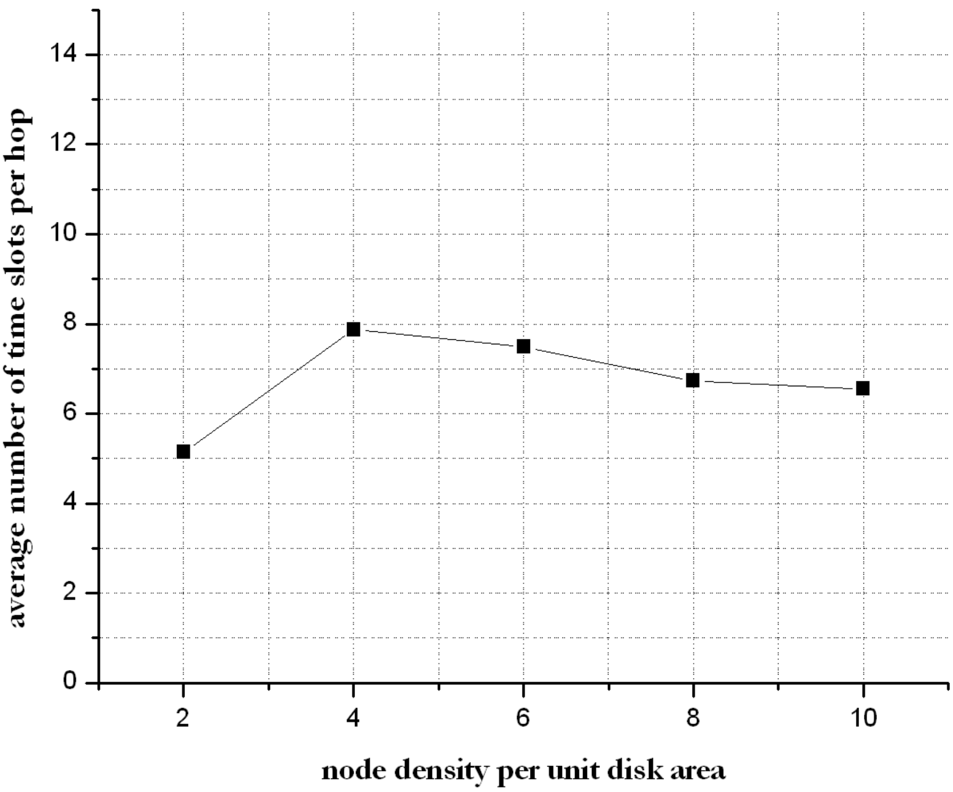

Fig. 4. The average number of time slots per a single hop a function of the node density. The frame length is equal to 3 slots. The network consists of 10000 nodes and 100 sinks.

References

[1] I. Stojmenovic (ed.), *Handbook of Sensor Networks. Algorithms and Architectures.* John Wiley & Sons, 2005.

[2] H. Karl and A. Willig, *Protocols and Architectures for Wireless Sensor Networks.* John Wiley & Sons, 2005.

[3] Pawel Kulakowski, Joan Garcia-Haro, "Alternatives to Face Routing for Localized Nodes in Wireless Sensor Networks", *COST 2100 Management Committee Meeting*, Braunschweig, Germany, 16-18 February 2009.

[4] M. Zorzi and R. R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Multihop Performance". *IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp. 337-348, October-December 2003.

[5] M. Zorzi and R. R. Rao, "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Energy and Latency Performance". *IEEE Transactions on Mobile Computing*, vol. 2, no. 4, pp. 349-365, October-December 2003.

[6] M. Heissenbuttel, T. Braun, T. Bernoulli and M. Walchli, "BLR: beacon-less routing algorithm for mobile ad hoc networks". *Computer Communications*, vol. 27, no. 11, pp.1076-1086, July 2004.

[7] H. Fussler, J. Widmer, M. Kasemann, M. Mauve and H. Hartenstein, "Contention-based forwarding for mobile ad hoc networks". *Ad Hoc Networks*, vol. 1, no. 4, pp. 351-369, November 2003.

[8] I. Stojmenovic, "Simulations in Wireless Sensor and Ad Hoc Networks: Matching and Advancing Models, Metrics, and Solutions". *IEEE Communications Magazine*, vol. 46, no. 12, pp. 102-107, December 2008.