Performance Assessment of Congestion Control Transport Protocols for Wireless Sensor Networks

David M. Monteiro
Department of Informatics,
University of Beira Interior,
Covilhã, Portugal
david.monteiro@it.ubi.pt

Binod Vaidya
Instituto de Telecomunicações
Covilhã, Portugal
bnvaidya@co.it.pt

Joel J. P. C. Rodrigues
Instituto de Telecomunicações,
DI, University of Beira Interior,
Covilhã, Portugal
joeljr@ieee.org

***Abstract* — In wireless sensor networks (WSNs), congestion may bring about degradation of overall channel quality and increased loss rates, leads to buffer drops and enlarged delays, and tends to be disgustingly unfair toward nodes whose data has to traverse a larger number of hops. Provisioning a WSN so that congestion is an infrequent occasion is quite challenging task. This paper presents a performance comparison study focusing the most relevant congestion control transport protocols for wireless sensor networks. The main objective is to study some characteristics of these types of protocols, focus in energy saving and penalty fidelity with the help of simulations.**

***Keywords* – Wireless sensor networks; transport protocols; congestion control protocols; performance.**

I. INTRODUCTION

Nowadays, wireless sensor networks (WSNs) are widely used among people and for many situations they provide the facility to collect and process information. These networks were borne in military environment and came to the common every day life environments.

WSNs may be composed by thousands of small node devices generally with sensing capabilities. A WSN can congregate are a group of sensors and sinks that are deployed for a wide range of geographical areas, from small areas (as offices) to a large area as natural parks. These networks can be used in human body (called body sensor networks), inaccessible environments, in catastrophe situation as big storms, hurricanes, and in war scenarios.

Sensors are the most important components in these networks. This small device senses physical information, and reports to the sink for processing and storage it. The main features that it is desired to make attention in WSNs are network topology, traffic over the network, small message size, external variants and the sensor energy.

In WSNs it is necessary to use several types of protocols [1]. Physical layer protocols is responsible for collecting data, while Data Link Layer specifically a MAC (Medium Access Control) layer for transferring data between network entities as well as detecting and possibly correcting errors occurred in the lower layer. Network Layer is responsible for transferring variable length data sequences from a source to a destination, and finally Transport Layer provides transparent transfer of data between end users, providing reliable data transfer services to the upper layers. Figure 1 show a node model used in simulation and show all layers that need in a WSN simulation.

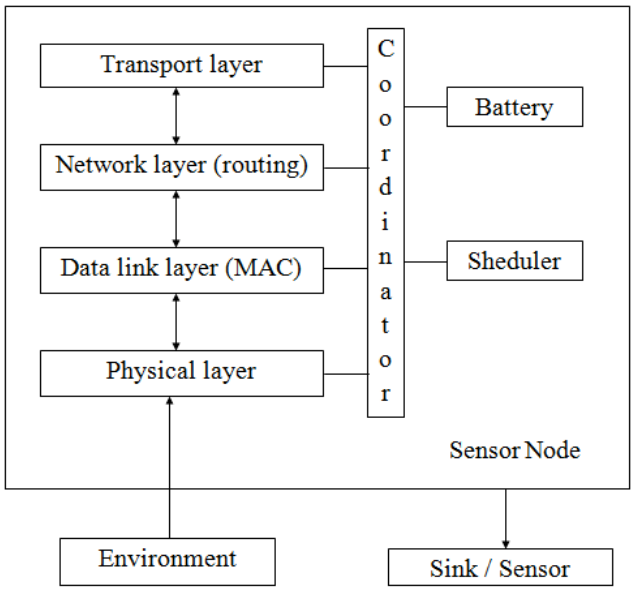

Fig 1 – A sensor node model used in the simulation.

In WSNs, congestion may cause degradation of overall channel quality and increased loss rates, leads to buffer drops and enlarged delays, and tends to be disgustingly unfair toward nodes whose data has to traverse a larger number of hops. Provisioning a WSN such that congestion is an infrequent occasion is quite challenging task.

This paper focuses on congestion control transport protocols for WSNs. These protocols are responsible for keep a smooth communication and without interruptions that can be caused by a congestion problem. The congestion

can occur in many ways like inoperability of a node and a very high rate transmission.

The rest of paper is organized as follows. Section II reviews the related literature while Section III presents a list of several protocols that was study and even about the simulation tool used for testing the protocols. Section IV evaluates the protocols referred. Finally, Section V concludes the paper and point directions for further research works.

II. Related Work

In related literature, there are many transport protocols for wireless sensor networks [2]. Figure 2 presents the most important and more developed protocols that are widely used today. WSNs transport protocols can be divided in the following three main types, taking into account their main functionalities: congestion control, reliability, and the combination of both.

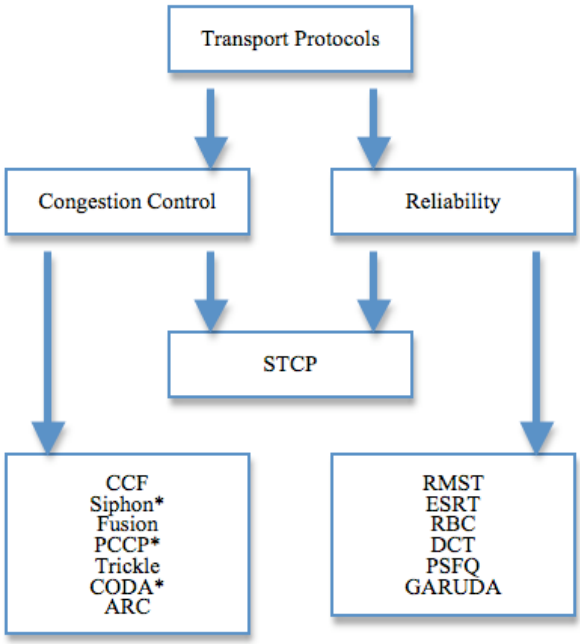

Fig. 2 - Types of Wireless Sensor Networks Transport Protocols. *Protocols related in the article.

A – Congestion Control Protocols

This section deals with some of the existing works related to the proposed Congestion Control Protocols for WSNs. In [3] the authors describe the three types of existing transport protocols, Congestion Control, Reliability and a protocol that focus the both methodologies Congestion Control and Reliability (STCP [4]). This paper includes the Congestion Control protocols such as CODA [5], Siphon [6], and PCCP [7] for our studies.

Even though all of them are congestion control protocols having different approaches for solving the congestion problem, the main aim is to control the congestion. Thus there can be three basic steps: congestion detection, congestion notification and rate adjustment.

B – Congestion Control Design

There are two main causes for occurring congestion in the wireless sensor networks. One is when the packet arrival rate exceeding the packet service rate, the main reason for that case is the proximity of the sensor nodes and the sink [8]. Another is the connection performance aspects such interference, contention and bit error rate. The congestion problem has a great impact in the energy spent by the sensors, which can lead to degradation of them, so the congestion control protocols need to be very efficient.

Congestion Detection: Unlike wired networks in WSNs proactive methods are preferred. Mechanisms such as queues length, packets service time and the ratio of packet service time over packet interarrival time at the intermediate nodes can be applied to the detection of congestion. WSN using CSMA (Carrier Sense Multiple Access) [9] and Medium Access Control (MAC) [10] and the channel loading can be measured and used as an indicator of congestion.

Congestion Notification: After congestion detection it is necessary to send the information through the sensor nodes to the base station that will receive and analysis the congestion information. There are two types of congestions, one of them use the explicit congestion notification, which uses special control messages to notify that there is a problem with the state of sending. Another is the implicit congestion notification that puts the messages in the package that nodes are sending.

Rate Adjustment: After receiving the notification, a sensor node has to adjust the transmission rate. After being resolved the congestion situation the sender can re-send rate until then.

C – CODA

Among the many transport protocols based on congestion control detection, CODA [11] as the name suggests is a protocol that continuously detect any kind of congestion and how to avoid it. This protocol is composed by three mechanisms:

Receiver-based congestion detection, a mechanism that plays an important role in the work done by this protocol because it is the mechanism responsible for detecting congestion.

Open-loop, hop-by-hop backpressure, which permits from all previous nodes to know if there is still congestion. This mechanism works with a looping message that only finishes when the congestion ends.

Close-loop, multi-source regulation is the mechanism that regulates the congestion.

Like all protocols, CODA also needs a good mechanism to detect congestion, because the process of congestion control needs much energy for the energy-aware sensors and they need to use a method of this type only that is necessary. For these there are several techniques that are used to detect congestion, the queue length is one of the mechanisms.

The load of the transmission channel is another method used to detect congestion. There is always the approximate information of the availability of the transmission channel to receive more data. When there is an overload a message of congestion notification is sent. This mechanism has a limitation in WSNs because each node is always listening when the channel is overloaded and causing a very large spent of energy.

The congestion detection method most used in WSNs is the report of reception data rate. This mechanism works as follows, the base station expects to receive packets with a certain range if the value is below the know value means that a package was lost; otherwise it sends a warning message to indicate that transmission rate is very high. For this there are measures as the waiting time between sending packets from the source to the destination.

The backpressure mechanism is a fast and effective method when congestion occurs. When congestion is detected the receiver node where congestion occurred sends a message to all neighboring nodes to indicate that no more blocks of data to send until they receive an indication to resend more data. The nodes send the message to next nodes to stop sending of data packets. *Depth of congestion* indicates the number of nodes that the backpressure message has traversed before a non-congested node is encountered.

D – Siphon

The Siphon is another congestion control protocol and it is based on the use of virtual base stations. This protocol has four mechanisms, the same as CODA and an additional that controls the congestion in a secondary network made by virtual sinks (VSs) as shown in Figure 3.

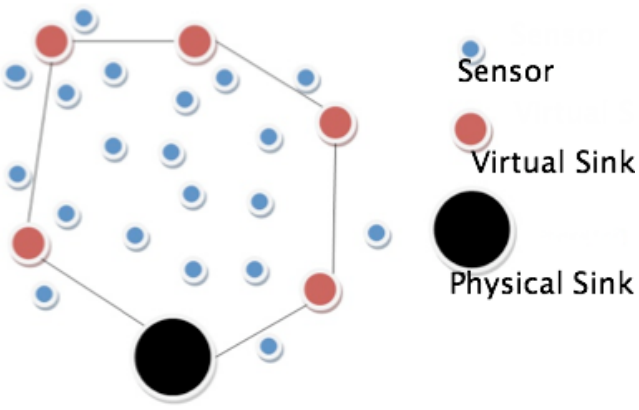

Fig 3 - An example of a network with Siphon Protocol using a secondary network.

Virtual sink discovery and visibility scope control, this protocol has virtual base stations whose main function is to prevent congestion, but there are no guarantees that the physical base stations are directly connected to the virtual base stations. If this situation is true virtual sinks detect the messages sent by a physical base station and transmit them inside the secondary network composed only by virtual sinks. These messages are normal messages to notify of the sending rate is too high or is near to occur a congestion situation. The benefit of this mechanism for sending messages through a secondary network composed only by virtual sinks is to achieve the energy cost almost zero. When virtual sinks detect some kind of notification from the base stations, they generate one byte called *signature byte* that is sent in the secondary network to notify the network that something is not being processed correctly.

There are two detection techniques in Siphon protocol: node-initiated congestion detection and physical sink initiated “post-facto” congestion detection.

In the first mechanism, all locations and levels of congestion in a node are determined. When a virtual sink observes a congestion situation near it, it sends a message that notifies that situation. The most important is that the traffic is redirected to other areas of the network so that the node can flow all the data that are causing the congestion.

In the second mechanism, the physical base stations will interfere directly in the congestion detection through monitoring the reliability and data reception quality. When these data are outside the normal range a signal is then sent to a nearby virtual sink that can transmit to the network. This method has the advantage that it is not necessary that all nodes need to make congestion detection.

The redirection of data is done using redirection bit. There are two ways of using this bit, one is enable the bit only when there is a congestion detection (on-demand redirection) and the other is the bit is always on (always-on redirection). A sensor receives a data packet with the redirection bit active, then it will forward it to the VS nearest you, if the bit is not active then the traffic goes unchanged.

If a virtual sink receives a package that has been redirected will have to send it to the near virtual sink and has recently received a message that includes a signature-byte. When everything runs normally and the virtual sinks are connected to physical base stations that receive packets they redirect the packets and will put them back on the network.

E - PCCP

PCCP protocol is another congestion control transport protocol. The main reason for the construction of this protocol is that each sensor has different priorities depending on its function or location. This protocol attempts to avoid or if it is not possible to reduce packet loss while ensuring support for multi-channel communications.

Figure 4 show a node model use in PCCP protocol, the scheduler controls the queue.

The three main features of this protocol are: intelligent congestion detection (ICD), implicit congestion notification (ICN) and priority-based rate adjustment.

The ICD mechanism used by this protocol detects congestion based on the time between transmission and arrival of the main package and the service time, time spent at the MAC layer. This method sets a new level of congestion, *d(i),* which is defined by the ratio of the average packet service time on the average time of transmission/ reception. The congestion value is to indicate the level of congestion that exists in a particular place and at any given time on the network.

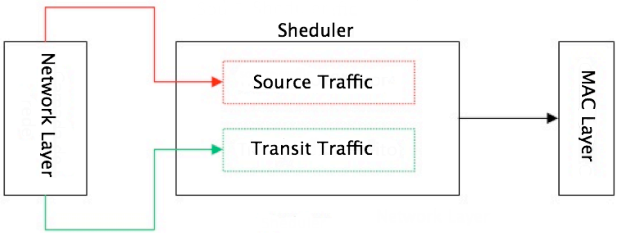

Fig 4 - A node model in PCCP protocol.

Upon congestion detection it is necessary to send a notification thus the PCCP protocol uses a mechanism called the ICN. This method is used in each node of the network. The notification mechanism is activated in one of two ways: one of the ways is that the mechanism is activated when the number of packets received exceeds the maximum, another is that the method is activated when the node receives notification of the neighboring node indicating that there is congestion in that area of the network. A node that calculates the value by adding the priority of priorities related to the existing traffic in the network, as a global will be able to monitor the best level of congestion.

The last mechanism used by this protocol is to adjust the congestion rate based on a priority system (PRA).

III. NETWORK SETUP

A – Simulation Environment

We have used the simulation method for the performance evaluation of well-known protocols such as CODA, Siphon, and PCCP. The CODA and Siphon were simulated with a same network setup while PCCP was done alone. It is due to the fact that CODA and Siphon are very similar in operation, whereas PCCP has a different mechanism.

In our simulation, star-tree and mesh topology were used. Initially the simulation in a simple linear topology was conducted to verify if the protocol algorithms are correctly implemented or not. The networks were composed by many sizes between 30 nodes to 120 nodes with interval of 10 between them. We have also simulated different physical areas with different sizes. These topologies were chosen because usually in real environments have similar placement of the nodes. We choose this number of nodes to verify which would be the behavior of networks with a large number of nodes and choose intervals of 20 nodes to have several simulations to evaluate. The transmission rate for data packets is 100 packets/second and reception rate by the sink is 500ms.

In all simulations, the same routing protocol and MAC (Medium Access Control) protocol were used. For routing the directed diffusion [12] was considered to control the distribution of the packets throughout the network and for MAC, 2 Mbps IEEE 802.11 MAC protocol [13] with some modifications included in OMNeT++ simulator.

In our simulations many tests were conducted with the above-mentioned topologies as well as all values obtained were used to evaluate the performance of the protocols. In our simulations, we used six source nodes and two sinks. Each sink is connected to three source nodes. The directed diffusion protocol chooses the best path to the data packet, so there is an energy saving by the sensor nodes.

To simulate PCCP a different topology was used because this protocol has distinct features compared to the other two. As the protocol uses a queue, it is essential to see how the queue works. A linear topology and a maximum of 60 nodes were used. In this case only the energy tax saving by the protocol was tested. The routing and MAC protocols as the same that the other two.

B – Simulation Tools

For the simulation we use the OMNeT++ v3.2 [1] that is a new simulation tool with which we can simulate almost everything. This simulator has the facility to building the network topologies in an easy way. For building simulation, there are three types of files, *NED* files to build the network topology, *C++* files to create the algorithms and the methods that the protocols use and finally the *init* files, in which all the simulation configurations as simulation time, number of sensors, the dimension of the simulation area are placed. Many simulation models can be added to the OMNeT. Each model has a specific function. The models that we used are Castalia, Mobility Framework and PAWiS. Castalia and PAWiS are exclusively created to simulate the WSNs. We have made some modifications in the models. One of the modifications is that we added codes in the MAC protocol for verifying the channel loading. The directed diffusion used is adapted because we improved it to the above-defined topologies.

IV. Results and Discussion

In this section, the simulation results are shown with the reason for each value shown in the charts. As it can be seen in the Figure 5 that Siphon has more fidelity than CODA. In the CODA protocol, the values keep around the same value in the case between 0.1 and 0.5. While the value of Siphon is basically the same that we encountered in CODA between 30 and 90 nodes, however after this, Siphon has better performance than CODA.

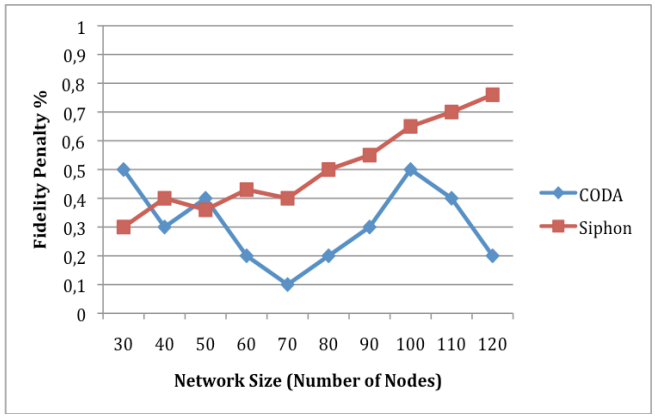

Fig 5 - A comparison between CODA and Siphon in fidelity penalty in a maximum of 120 nodes.

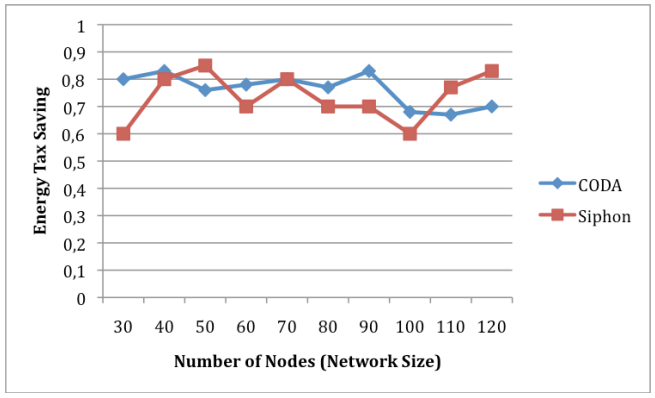

Fig 6 - A comparison between CODA and Siphon in energy tax saving in a maximum of 120 nodes.

The main reason for a better result for Siphon is that in this protocol there is a secondary network and the main responsibility of this second network is congestion control and verify the state of the network every time, so it is normal that in Siphon we get better results for this parameter. Between 70 and 100 nodes the CODA protocol has a growing because it is inside these values that it has better performance.

In the second chart as shown in Figure 6 the protocols have a very close behavior but for different reasons. In CODA there is a very high energy tax saving because CODA has the close loop mechanism and that mechanism was created for detect and resolve congestion control. Over the 100 nodes the chart show the CODA is no longer the same efficiency demonstrated at this point. The explanation for this is the same that to the fidelity penalty. This protocol has more efficiency between 40 and 90 nodes.

The main reason for the good results in Siphon is also the existence of the second network compound for virtual sinks. Here this secondary network prevents the dispend of energy by the physical sinks to resolve the problem of congestion. The only energy spent by the protocol is for the mechanism of communication between virtual sinks and physical sinks. The energy spent on the other operations is very low when compare to this action.

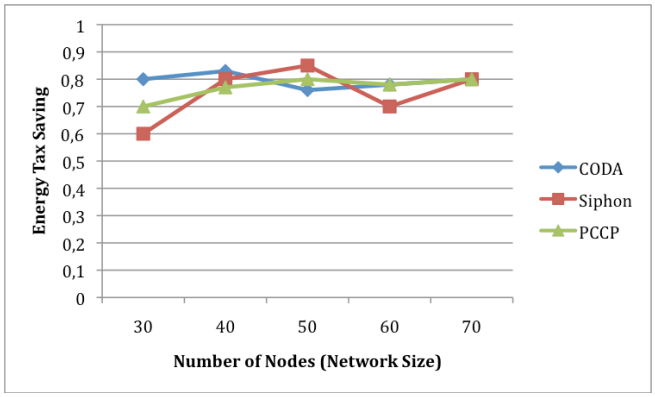

Fig 7 - A comparison between CODA, Siphon and PCCP in energy tax saving in a maximum of 70 nodes.

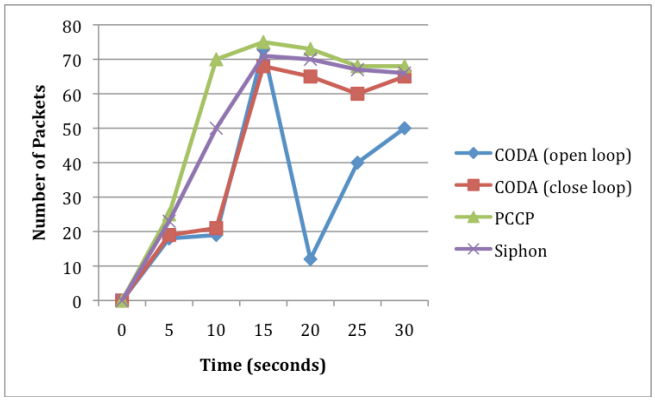

Fig 8 – A comparison between CODA open-loop, CODA close-loop, PCCP and Siphon protocols in number of packet delivery in 30 seconds.

As shown in Figure 7 the three protocols are very close, but it should be noted that PCCP was tested with a different

topology. When the network size grow PCCP has more efficiency in energy tax saving because as the packets left more time to travel in the network the queue is more smaller and the protocol can avoid or reduce the packet loss.

Another important feature that we can see in congestion control protocols is the number of delivery packets in an interval of time. Figure 8 shows the number of delivery packets between a period of 30 seconds. The chart compares the three protocols and shows two methods that was used in CODA, open-loop and close-loop. All mechanisms have similar behaviours, this happen because all have congestion control mechanisms and their operation are similar. Initially there is a low number of delivery packets, after 10 seconds there is a big increment because the number of packets into the network rise too. At 10 seconds it is visible that CODA close-loop keeps in a low value of delivery, this happen because this is the mechanism responsible for regulating the congestion, so at the first moment close-loop stabilizes the congestion. Another conclusion is in the CODA open-loop, the values show that when the congestion occurs and this is not a mechanism that control the congestion and only detect it, after 15 seconds in this mechanism the delivery falls down.

V. Conclusions and Future Work

This paper presents a study of performance of wireless sensor networks congestion control protocols. The main objective of the paper is to study the performance of some characteristics of this type of protocols specially focused on energy saving and fidelity penalty. With this study, we have accomplished the objective of understand the advantages and disadvantages of each protocol used.

As future work we aim to migration of the simulations for the new version of the simulator, OMNeT++ 4.0. The following is also the ultimate goal to find what the best advantages of existing protocols for the preparation of a new transport protocol.

Acknowledgments

Part of this work has been supported by the *Instituto de Telecomunicações,* Next Generation Networks and Applications Group, Portugal, and by the Euro-NF Network of Excellence of Seven Framework Programme of EU.

References

[1] C. Mallanda, A. Suri, V. Kunchakarra, S. S. Iyengar, R. Kannan, and A. Durresi, "Simulating Wireless Sensor Networks with OMNeT++," *LSU Simulator,* 2005.

[2] S. Hashmi, H. T. Mouftah, and N. D. Georganas, "A New Transport Layer Sensor Network Protocol," in *CCECE '06* Ottawa, pp. 1116-1119, 2006.

[3] C. Wang, K. Sohraby, M. Daneshmand, B. Li, and Y. Hu, "A survey of transport protocols for wireless sensor networks," *IEEE Network,* vol. 20, pp. 34 - 40, May/June 2006.

[4] Y. G. Iyer, S. Gandham, and S. Venkatesan, "STCP: A Generic Transport Layer Protocol for Wireless Sensor Networks," *ICCCN 2005,* pp. 449 - 454, 17-19 October, 2005.

[5] C.-Y. Wan, S. B. Eisenman, and A. T. Campbell, "CODA: congestion detection and avoidance in sensor networks," in *Proceedings of the 1st international conference on Embedded networked sensor systems* Los Angeles, California, USA, ACM, 2003.

[6] C.-Y. Wan, S. B. Eisenman, A. T. Campbell, and J. Crowcroft, "Siphon: overload traffic management using multi-radio virtual sinks in sensor networks," in *Proceedings of the 3rd international conference on Embedded networked sensor systems*, San Diego, California, USA, ACM, 2005.

[7] C. Wang, K. Sohraby, V. Lawrence, B. Li, and Y. Hu, "Priority-based Congestion Control in Wireless Sensor Networks," in *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing - Vol 1 (SUTC'06), 2006*, Taichung, Taiwan, pp. 22-31, 2007.

[8] F. K. Shaikh, A. Khelil, and N. Suri, "A comparative study of data transport protocols in wireless sensor networks," in *Proceedings of the 2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, IEEE Computer Society, 2008.

[9] S.-T. Sheu, C.-C. Wu, and P.-L. Wu, "A new contention-based CSMA protocol for star networks," in *Information Networking, 2001. Proceedings. 15th International Conference*, Beppu City, Oita, Japan, 2001, pp. 46-51.

[10] Kurtkoti and A. P. B., "Evaluation Metrics of MAC Layer in Wireless Sensor Network," in *Emerging Trends in Engineering and Technology, 2008. ICETET '08. First International Conference* Nagpur, Maharashtra, pp. 250-254, 2008.

[11] W.-R. Chang, H.-T. Lin, and Z.-Z. Cheng, "CODA: A Continuous Object Detection and Tracking Algorithm for Wireless Ad Hoc Sensor Networks," in *CCNC 2008*, Las Vegas, USA, pp. 168-174, 2008.

[12] Z. Shousheng, Y. Fengqi, and Z. Baohua, "An Energy Efficient Directed Diffusion Routing Protocol," in *2007 International Conference Computational Intelligence and Security,* Harbin, pp. 1067-1072, 2007.

[13] Y. C. Tay and K. C. Chua, "A capacity analysis for the IEEE 802.11 MAC protocol," *Wirel. Netw.,* vol. 7, pp. 159-171, 2001.