QoS in Wireless Sensor Networks: survey and approach

José-F Martínez, Ana-B García, Iván Corredor, Lourdes López, Vicente Hernández and Antonio Dasilva
DIATEL - EUIT Telecomunicación - Universidad Politécnica de Madrid
Ctra. Valencia, Km. 7, 28031, Madrid, SPAIN
{jfmartin, abgarcia, icorredor, llopez, vhernandez, adasilva}@diatel.upm.es

Abstract

A wireless sensor network (WSN) is a computer wireless network composed of spatially distributed and autonomous tiny nodes – smart dust sensors, motes -, which cooperatively monitor physical or environmental conditions. Nowadays these kinds of networks support a wide range of applications, such as target tracking, security, environmental control, habitat monitoring, source detection, source localization, vehicular and traffic monitoring, health monitoring, building and industrial monitoring, etc. Many of these applications have strong requirements for end-to-end delay and losses during data transmissions. In this work we have classified the main mechanisms that have been proposed to provide Quality of Service (QoS) in WSN at Medium Access Control (MAC) and network layers. Finally, taking into account some particularities of the studied MAC- and network-layer protocols, we have selected a real application scenario in order to show how to choose an appropriate approach for guaranteeing performance in a WSN deployed application.

Keywords: *Quality of Service (QoS), wireless sensor networks (WSN), protocols and mechanisms, performance, target tracking.*

1. Introduction

Recently there has been a great evolution in the wireless sensors domain, mainly driven by improvements in sensor hardware technology (miniaturization of components, increased ROM and RAM capacities, more energy capacity, etc). This fact, together with the new application domain possibilities being foreseen, has brought high interest in the Wireless Sensor Networks (WSN). A definition of WSN could be the following: *Networks of tiny small, battery-powered, resource-constrained devices equipped with a CPU, sensors and transceivers embedded in a physical environment where they operate unattendedly* (see figure 1). While a lot of researches and developments have been carried out in architecture and protocol design, energy saving and location, only a few studies have been done regarding network performance (i.e. Quality of Service – QoS) in WSN. We have found some works about QoS which are focused in protocols and mechanisms at MAC and network layers, and almost all of them have been tested by means of simulations. All these approaches for supporting QoS in WSN constitute a base for future works in this direction, and they are the starting point of our proposal.

The remainder of this paper is organized as follows: The most important protocols and mechanisms to provide QoS in WSN at both network and MAC layers are discussed and evaluated in section 2. Inside that section we have also included comparative charts (see Table 1 and Table 2) between the studied protocols. An approach for QoS support in WSN is depicted in Section 3 by means of a study case. Section 4 concludes this paper with an outlook on future research activities.

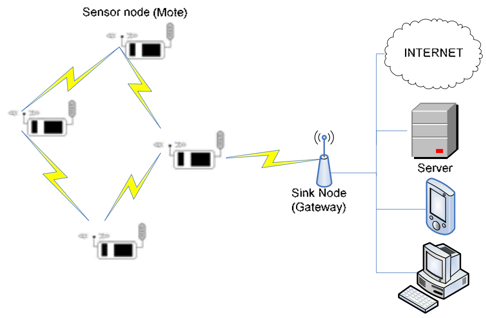

Figure 1. An example of Wireless Sensor Network

2. Providing QoS in WSNs

2.1. Network layer protocols and mechanisms

2.1.1. Directed diffusion

Directed Diffusion [1] is a data-centric and application-aware paradigm since all data generated by sensor nodes is named by attribute-value pairs. Directed diffusion, unlike traditional end-to-end routing, tries to find routes from multiple sources to a single destination which allows redundant data aggregation.

The objective of directed diffusion paradigm is to aggregate the different data coming from different sources by deleting redundancy. This particularity reduces the number of transmissions drastically, leading to two main consequences: firstly, the network saves energy and extends its time-life, and secondly, it has higher bandwidth in the links near to the sink node. This second factor could be decisive in order to provide QoS for real-time applications.

Directed diffusion is based on a query-driven model. This means that the sink node requests data by means of broadcasting *interests.* Requests can be originated from humans or systems, and they are defined as pair-values, which describe a task to be done by the network. The interests are disseminated through the network. This dissemination sets up gradients to create data that will satisfy queries towards the requesting node. When the events begin to appear, they start to flow towards the originators of interests along multiple paths. This behavior provides reliability to data transmissions in the network.

Other directed diffusion characteristic is the caching of data (generally attribute-value pair's interests). Caching can increase efficiency, robustness and scalability of coordination between sensor nodes, which is the essence of the directed diffusion paradigm.

2.1.2. SPIN

In [2] and [3] a family of adaptive protocols called Sensor Protocols for Information via Negotiation (SPIN) is proposed. These protocols do not implement any concrete QoS mechanism; they are based on an interesting data negotiation mechanism. SPIN uses this for eliminating redundant data by means of meta-data exchange. Nodes running SPIN assign a high-level name (called meta-data) to describe the data that they have collected and they perform meta-data negotiations before any actual information is transmitted. The main goal of this mechanism is similar to the typical aggregation systems. However, this mechanism has an advantage over other systems: it avoids redundant data transmissions for later processing. This way, the network increases its life time and the available bandwidth. Additionally, nodes are free from the processing load that the data aggregation implies.

Of course, the format of the exchanged meta-data has to be carefully designed in order not to make the nodes transmit very voluminous information (which again would cause waste of energetic resources). A totally general format for this metadata would probably have this problem. That is why the authors that propose SPIN do not specify a format for the meta-data, but instead they state that this format should be application-dependent in order to choose a fine-tuned set of criteria that minimizes the meta-data volume of information while serving the application functionality.

2.1.3. TEEN and APTEEN

TEEN and APTEEN, proposed in [4] and [5], have been defined for time-critical applications. These protocols are designed to work even in the event of abrupt changes in the attribute values that are being measured by the sensors. APTEEN (Adaptive TEEN) is a modification of TEEN that additionally considers the case of periodic transmissions of measurements towards the sink node. This protocol implements a very complex query system. Using this system it is possible to achieve three types of queries (historical, one-time, and persistent). All of these queries are posed by an external user through the sink node. The historical and persistent queries do not have QoS requirements. However, one-time queries have critical time constraints. In this case, for instance, the end user may want to be aware of the geographical position of a target with minimum delay. In order to achieve minimum delay, the system executes a special time slots assignment to each node using a TDMA schedule. Furthermore, APTEEN performs an important task of data aggregation, which leads to having free bandwidth and energy saving.

2.1.4. SAR

Sequential Assignment Routing (SAR), proposed in [6], is one of the first protocols for WSN that has considered QoS issues for making routing decisions. SAR makes routing decisions based on three factors: energy resources, QoS planned for each path, and the type of traffic to which the packet belongs to (types of traffic are implemented by means of a priority mechanism). SAR uses two systems for resolving reliability problems which consist in a multi-path approach and a localized path restoration (this path restoration is done by means of communications between neighbour nodes). The multi-path tree is defined avoiding nodes with low energy or QoS guarantees; taking into account that the tree root is located in the source node and the end is the sink nodes set. In conclusion, SAR will create a multi-path table whose main objective is to have energy efficiency and fault tolerance. Although this ensures fault tolerance and easy recovery, the protocol suffers from certain overhead when the tables and the node states must be maintained (refreshed). This problem is especially significant when there is a huge number of nodes.

2.1.5. SPEED

SPEED [7] is another QoS routing protocol for WSN that provides light real-time end-to-end guarantees. The QoS mechanism employed by SPEED is based on estimation procedures. The application in a node estimates the required speed for a certain delay, taking into account its

distance to the sink node. The network layer will admit the packet depending on the required speed. Moreover, SPEED will be able to recover if the network becomes congested.
The routing module in SPEED is called Stateless Non-deterministic Geographic Forwarding. (SNGF). This module implements a distributed database where a node can be selected in order to reach the speed requirement.

2.1.6. MMSPEED

MMSPEED (*Multi-Path and Multi-SPEED Routing Protocol*) [8] is a novel packet delivery mechanism for QoS provisioning. Its main goal is to provide QoS differentiation in two quality domains, *timeliness* and *reliability*: Traffic flows will be cursed with a combination of service options based on reliability and timeliness requirements. The method used by MMSPEED to obtain reliability is the typical multi-path routing, with a number of paths that depends on the required degree of reliability for the traffic flows. On the other hand, the method used by MMSPEED to obtain timeliness is a dynamic system which guarantees the packet delivery speed. MMSPEED employs localized geographic forwarding by using only local node neighbor information. The local decisions imply an inaccuracy problem, which is resolved by dynamic compensation. Thus, traffic flows requirements can be fulfilled with a high probability. With this mechanism the intermediate nodes have ability to increase the transmission packet speed to higher levels if they estimate that with the current associated speed the packet can not fulfill its delay deadline, but it could be met at higher speeds.
In order to offer the necessary functionality to the QoS mechanisms implemented by MMSPEED, a MAC protocol with a prioritization mechanism should be established. In this sense, the MMSPEED specification recommends the use of 802.11e (with several add-ons) at the MAC layer with its inherent prioritization mechanism based on the Differentiated Inter-Frame Spacing (DIFS). Each speed value is mapped onto a MAC layer priority class.
MMSPEED protocol solves many QoS issues related to real time traffic in WSN. However, many other aspects, such as network layer aggregation or handling the energy-delay trade-off, still need to be dealt with in deep in order to have good performance in a deployed WSN.

2.1.7. Energy-aware QoS Routing

In [9] the authors propose a QoS-aware protocol for real-time traffic generated by a WSN consisting of image sensors. This protocol implements a priority system that divides the traffic flows in two classes: *best effort* and *real-time*. All nodes use two queues, one for each traffic class. This way, different kinds of services can be provided to these types of traffic. Also, the protocol implements a routing mechanism based on multi-path which uses an extended version of the Dijkstra's algorithm. This makes it possible to provide certain reliability in the data transmissions. The source node chooses a route in order to achieve the end-to-end requirements and then forwards the packet to the next hop neighbor in the route. Each intermediate node classifies the received packet into real-time or best-effort. The scheduling algorithm is such that the best effort traffic cannot reduce the resources for the real-time traffic. The main disadvantage of this protocol is that it supports only one real-time traffic priority. This characteristic can be appropriate for a network with a single real-time application, but in a network with multiple applications it would be interesting to have several types of real-time traffic with different priorities.

Table 1. Comparative table of routing protocols in Wireless Sensor Networks

	Network topology	Data delivery models	Data aggregation/fusion	Traffic guarantees	Several traffic classes	Networks dynamics	Resources reservation	Scalability
Directed Diffusion	Flat	Query-driven and Event-driven	Yes	Reliability	No	Limited	Yes	Medium
SPIN	Flat	Query-driven and Event-driven	Yes (by means of data negotiation)	No	No	Limited	No	Low
TEEN and APTEEN	Hierarchical	Query-driven, Event-driven and Continuous	Yes	Certain guarantees of real time	Yes	Fixed sink	No	High
SAR	Flat	Query-driven and Event-driven	Yes	Real time and Reliability	Yes	No	Yes	Low
SPEED	Flat	Query-driven and Event-driven	No	Soft Real time	No	No	No	Low
MMSPEED	Flat	Event-driven and Continuous	No	Reliability and Real time	Yes	Limited	No	High
Akkaya 2003	Hierarchical	Event-driven and Continuous	No	Reliability and Real time	Yes	Fixed sink	No	Low

2.2. MAC layer protocols and mechanisms

2.2.1. B-MAC

B-MAC [10] stands out for its design and implementation simplicity, which has an immediate effect in memory size occupation and power saving. B-MAC does not implement any specific QoS mechanism; however, this fact is compensated by its good design. Some parts of this design are addressed to improve the efficiency for avoiding collisions, efficiency in the channel occupation at low and high data rates, the tolerance to changeable environments, or the good scalability properties. Although B-MAC was thought for monitoring applications, it is possible to take advantage of this approach in other applications such as target tracking, localization, triggered events, and multi-hop routing. Also, B-MAC has a high degree of configurability. If we have all of these characteristics in mind, we will be able to state that B-MAC is a good alternative for applications based on event-driven data delivery models with minimum delay requirements.

2.2.2. Z-MAC

ZMAC (Zebra MAC) [11] is a hybrid scheme that combines the advantages of CSMA and TDMA while isolating their weaknesses. ZMAC is characterized by an initial period in which it performs a wide time slots scheduling. In order to achieve this task, ZMAC uses DRAND, a very efficient distributed scheduling algorithm. The initial assignment of slots incurs in a high overhead, which however is subsequently amortized by a long network operation period, and eventually compensated with improvements in power saving and throughput. Z-MAC implements contention control avoiding congestion situations. Thus, under low contention it has a CSMA behavior, and under high contention a TDMA behavior. Also, this approach is robust enough for dynamic topology changes. These two characteristics are very important for applications with delay and/or reliability requirements.

2.2.3. i-GAME

The MAC protocol of the standard IEEE 802.15.4 implements a mechanism called Guarantee Time Slot (GTS). GTS tries to assign an additional time slot for applications with some delay requirements. However, this mechanism loses efficiency in WSN with a large number of nodes. In order to correct this deficiency, in [12] an implicit GTS Allocation Mechanism (i-GAME) has been proposed. The main idea of i-GAME consists on sharing the same GTS between multiple nodes, instead of being exclusively dedicated to a single node. The assignation of GTS resources is based on an admission control algorithm. This algorithm admits a request if its requirements do not exceed the available resources.

2.2.4. MAC for lineal WSN

In [13] a hard real-time MAC protocol is proposed for a network of low-cost sensors (e.g. only one frequency), deployed randomly, with no differentiated nodes (e.g. no router nodes), and without synchronization on a global clock. This protocol was though for lineal network, thus it is free of routing considerations. A sink node is situated in an extreme where it will receive all the events originated in the network. This protocol alternates two operation modes: *protected* an *unprotected*. When network is in unprotected mode, the transmission speed is near to optimal but there may be collisions. However, if it is in protected mode, the transmission speed is slower but the frames are transmitted with reliability because network will be collisions free. This characteristic can be interesting for real-time applications with critical requirements.

Table 2. Comparative table of MAC protocols in WSN

	Data aggregation/fusion	Scalability	Priority mechanisms	Energy aware	Contention - based
B-MAC	No	High	No	Yes	Yes
Z-MAC	No	High	Yes	Yes	hybrid
Watteney 2005	No	Low	Yes	No	Yes
MAC 802.15.4 with i-GAME	No	Medium	Yes	Yes	No

3. Study case: forest fire detection scenario

Inside this section we will apply the study we have presented on the protocols for QoS in WSN to a forest surveillance scenario. In this sense, we will begin by extracting the QoS-related requirements that our real-time forest surveillance application has, which will allow us later to select the network and MAC protocols that best suit these requirements. However, it is possible that these protocols will not fulfill all the necessary requirements. In that case, we will also propose which additional features must be introduced in each protocol. Inside the conclusions section we will discuss the shortcomings that in our opinion the studied protocols have and what could be corrected in future research.

3.1. Description and requirements analysis of the application for real-time forest surveillance

The application will be focused both in forest fire detection and events tracking in a natural environment (Natural Reserve), with high ecological importance.

The major objective of the application will be the early forest fire detection to avoid ecological disasters. Likewise, the application will have secondary objectives such as the detection and tracking of intruders into protected spaces to avoid illicit actions such as poaching and bonfires, among others. We could summarize these objectives as follows:

- Forest surveillance, including the detection of dangerous activities and determining the conditions that raise the risk of fires.
- Detection and location of fires.
- Fires monitoring and assist the fires extinction activities.
- Detection and tracking of intruders who accede to restricted areas.

In our forest fire detection application, sensor nodes collect measurement data such as relative humidity, temperature, infrared radiation, COx and NOx gases (these factors are necessary to detect fires and determining the forest fire danger rate). Other components of the WSN that will give support to our application are laptops and/or PDAs (supporting firemen and safety watchmen), a server, and a data base. All the WSN services will be able to be accessed by remote users through web services. The following image (see figure 2) illustrates the proposed application scenario.

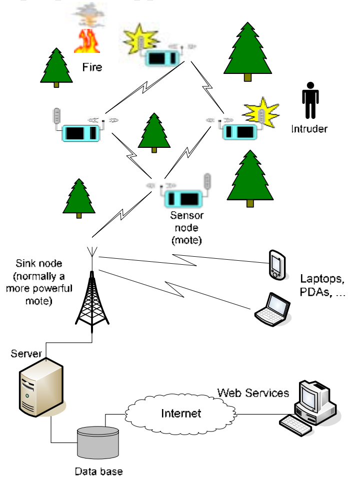

Figure 2. Forest surveillance application scenario

The sensors types, with which every sensor node will be equipped, have to be able to measure the following parameters: infrared radiation, humidity, and gases such as NOx and COx. The data gathered by all sensors will be used to determining the risk of fire at concrete moment. The infrared radiation sensor will be also used for the detection and tracking of intruders in restricted areas.

The major challenge of the proposed application is to join two critical objectives, namely habitat monitoring in forests and tracking targets in restricted areas. This is because similar applications, which combine these objectives, have not been studied in depth yet and therefore there is not much documentation about how to achieve these two objectives in a single application. Specifically, the application will have the following characteristics:

1) Topology and network dynamics*:* The WSN topology is a design parameter that should be taken into account to guarantee QoS. The selected topology for the WSN will be flat. Therefore, every node will have the same hierarchy in the WSN and the same hardware components. The hierarchy will not be necessary in the proposed network since it will use a localized geographic routing. Using this routing type has several advantages when guaranteeing QoS.

2) Geographical information*:* It will be necessary that the sensor nodes can obtain their geographical information (coordinates) in order to locate the events inside the extension of the Natural Reserve. Usually, the methods used to get this information are based on GPS [14] or distributed location services [15]. As all of WSN's nodes will have the same structure, in our case the GPS-based approach will not be used (WSN would be too expensive). Then, our WSN will implement a distributed location service. The choice of this method introduces certain overhead during the initial phase of the WSN, which could impede QoS guarantees.

3) Real-time requirements*:* Fire monitoring or target tracking reflects the physical status of dynamically changing environment, such as temperatures of forest areas or positions of moving targets. This sensory data is valid only for a limited time duration and, hence, needs to be delivered within a time deadline.

4) Unbalanced mixture traffic*:* Another characteristic of our application, which will considerably affect the QoS decisions, will be its *reactive-proactive* hybrid behaviour. The reactive behaviour will come from the fire or intruder detection, and will generate traffic to the sink node according to an event-driven delivery model. This traffic type is generated un-periodically by detection of critical events at unpredictable points in time. The proactive behaviour will come from the monitoring of the environmental status and tracking targets, and will generate traffic to the sink node according to a continuous delivery model. In accordance with this mixture of periodic and un-periodic traffic types, the selected QoS mechanisms for the WSN will be designed for an unbalanced combination of QoS-constrained traffic types.

5) Data redundancy*:* The high redundancy in the sensor data is a common characteristic in most of WSN applications. The redundancy can be considered an advantage to improve QoS since it increases the reliability and robustness of data delivery. However, it wastes a lot of energy unnecessarily. To solve this problem one possibility is using data fusion or data aggregation to maintain robustness while decreasing redundancy in the data, but these mechanisms require a high computational activity in at least several nodes (usually clusterheads). Therefore, these mechanisms also introduce delay and complicate QoS design in WSNs. We prefer to exclude these mechanisms due to the fact that our application is based on two critical objectives and the real-time requirements will prevail over the energy requirements. An alternative to data aggregation and fusion is the meta-data negotiation which is able to eliminate redundancy without introducing a lot of delay in data delivery.

6) Energy efficiency*:* An important challenge of this application will be the energy-efficiency. The large number of sensor nodes involved in the WSN and the need to operate over a long period of time (from 6 months to 1 year) will require careful management of the energy resources. However, to implement QoS mechanisms to support critical real-time traffic while at the same time saving energy is not a trivial task. The key is to distribute energy load among all sensor nodes so that the energy at a single sensor node or a small set of sensor nodes will not be drained out very soon. Nowadays, to achieve this energy distribution without compromising the QoS requirements is very difficult because the mechanisms and protocols surveyed in previous sections do not consider both possibilities at the same time.

7) Sensor data priority*:* The sensing data are not all equal in importance, i.e., they have different importance levels. For example, the data generated in a fire detection event will have more importance than the data generated in the monitoring to determine the conditions that raise the risk of fires. The QoS mechanisms will determine data delivery priorities for the different types of data present in the WSN.

As a result, the QoS support for the network will take into account almost all characteristics described above when specifying the application.

To complete the requirement analysis, we are going to extract the QoS-related requirements of the network and MAC layers of the protocol stack according to the analyzed application characteristics. The following sections help us to select the network and MAC protocols that best suite the application needs.

3.1.1. Network layer

Guaranteeing QoS for the diverse traffic types at network layer is a challenging problem due to the following characteristics of the WSN:

- Dynamic topology changes as a result of node failure, addition or mobility.
- Large scale with thousands of densely placed nodes.
- Periodical and un-periodical traffic generated by sensors with different priorities and real-time requirements.
- Possible data redundancy produced by correlated sensor nodes.

The traditional network layer methods based on the end-to-end path discovery, resources reservation along the discovered path, and path recovery in case of topological changes are not suitable for WSN with similar characteristics to ours for several reasons. To begin with, the time wasted in the path discovery is not acceptable for urgent non-periodic (event-driven) packets. In addition, it is not convenient to reserve resources for the unpredictable non-periodic packets. Even for periodic continuous flows, these methods are not practical in dynamic WSN since service disruption during the path recovery increases the data delivery delay which is not acceptable in our mission critical application. Finally, the end-to-end path based approaches are not scalable due to huge overhead of path discovery and recovery in large scale sensor networks. As an alternative to the inefficient reservation-based approaches, the network layer will include an end-to-end QoS provisioning method based on local decisions at each intermediate node without path discovery and maintenance.

To solve dynamic topology changes, the network layer will implement the already mentioned localized geographic routing. Mainly, this routing type will provide adaptability to dynamic topology changes since the nodes will not require getting the global topology information. Consequently, control packets will not be generated in a significant amount when the topology changes due to node addition, failure or mobility. The nodes in the WSN will be able to make a localized packet routing decision without global network state update or a priori path setup which will increase the network scalability and will decrease the control traffic load. On the other hand, this routing scheme is very suitable for both critical un-periodic and periodic packets due to the absence of path setup and recovery latency.

Another characteristic that should be considered by the network layer is the traffic priorities. In our WSN, the traffic priority will be characterized by two domains: reliability and timeless. The network layer will implement complex mechanisms in order to achieve this objective. For example, it could implement a priority queue system with the purpose of differentiating the traffic with different end-to-end deadlines. On the other hand, the mechanisms that will be implemented for providing reliability to the data transmissions could exploit the inherent multiple redundant paths to the final destination in a dense WSN to guarantee the required end-to-end reliability level (end-to-end reaching probability) of a packet.

Finally, the network layer will not implement a mechanism for eliminating data redundancy such as data aggregation, for two major reasons. Firstly, the in-network processing is not recommended in order to guarantee end-to-end deadlines due to the delay that is introduced by the high computational activity of these mechanisms. Secondly, the network topology will be flat (all nodes will have the same capacity), and hence, there will not be nodes capable of completing the process without using too much energy and time.

Alternatively, the network protocol will implement a method for dealing with redundant data by means of exchanging meta-data (inside the so-called data negotiation) [3]. This eliminates inefficiencies that data-aggregation mechanisms present due to the flooding and posterior processing of information. For instance, using a data negotiation mechanism, if a tracking event is detected, the location information is transmitted once and no more data is transmitted until the target moves.

3.1.2. MAC layer

The network layer alone cannot provide all the QoS requirements described above. Accordingly, the protocol stack of our WSN will have a MAC protocol capable of performing the following functions:

- Medium access control according to deadlines of each packet,
- Measurement of average delay to individual neighbors,
- Measurement of loss rate to individual neighbor,
- In addition, it could be necessary to have the capacity of performing reliable multicast delivery of packets to multiple neighbors.

Along with the functionalities described above, the MAC layer must implement mechanisms to associate each of deadlines that have been assigned by the network layer to a transmission priority level. Thus, the prioritization of the medium access will be achieved by the MAC layer. Likewise, the MAC protocol will be able to measure the average delay to individual neighbors with the purpose of forwarding the packet according to its deadline.

However, the packet forwarding will not be performed only with deadline criteria but also with reliability criteria. For this reason, the MAC protocol will measure the loss rate to individual neighbors.

The localized geographic routing used by the network layer will require transmitting control packets with the position data of the neighbours situated at least one and two hops away. For the transmission of these control packets it is necessary that the MAC layer have the capacity of reliable multicast delivery of packets.

3.1.3. Selected network and MAC protocols

Considering the mechanisms just described, the design decisions made for the network and MAC protocols in our surveillance application are the following:

From network layer perspective, we consider that the protocol to be used by the application is MMSPEED. There are several reasons to select this protocol:

- MMSPEED implements localized geographic routing which is fundamental for the network layer of our stack protocol. This mechanisms increase the network self-adaptability to dynamic changes. In addition, this protocol is suited for both periodic (real-time) and non-periodic traffic because of the routing local decisions (no path setup and failure recovery).
- MMSPEED also implements a multi-speed mechanism to assign diverse deadlines to the packets with different delay requirements. This mechanism is ideal in order to support multiple traffic types (continuous, event-driven, etc.). Its dynamic speed compensation mechanism, capable of correcting immediately small inaccuracies produced in initial routing decisions, is also very interesting.
- The routing decisions in MMSPEED are also made considering the reliability level required by the packet. In order to route considering the reliability requisite, MMSPEED has an advanced method to provide reliability to data transmissions, consisting on using the frame loss rate of the MAC layer for doing an estimation of the reliability level of each link.

However, MMSPEED lacks a method to treat the data redundancy problem. We have already mentioned that the best methods for eliminating data redundancy in our application are those based on meta-data exchange. In this sense, we are studying how to add a meta-data negotiation mechanism to MMSPEED.

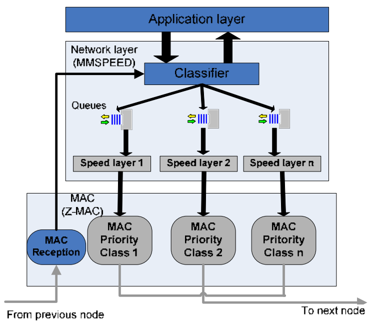

Figure 3. Structure of the priorities mechanism.

Selecting a MAC protocol that complements MMSPEED protocol is not a trivial decision. MMSPEED specification proposes an extension of 802.11e for supporting all the mechanisms implemented by the network layer. The most important of them is the priorities mechanism. However, this MAC protocol is not specific for WSNs and consequently has some deficiencies in this sense. We propose the Z-MAC protocol as an alternative to 802.11e. Although this protocol needs several additional features to be completely compatible with MMSPEED, it is an excellent base since it implements a priorities mechanism that is very appropriate for this study case. The additional features are mainly related with the abovementioned hybrid nature of Z-MAC. This nature forces the priorities mechanism to work in a different way, depending on its contention level (low level - CSMA or high level TDMA). In addition, it is necessary that Z-MAC could associate each MMSPEED's speed layer with a priority class in the MAC layer (see figure 3).

On the other hand, Z-MAC has a highly efficient contention method (which can avoid unnecessary backoff delays in the packets transmissions) and good adaptability to topology changes.

4. Conclusions and future works

In this paper we have presented a study of MAC and network layer protocols defined to provide QoS in wireless sensor networks. We have extracted the basic mechanisms that these protocols include for guaranteeing performance parameters to applications, leading to comparative charts of the different approaches.

Taking this study as a basis, we have also selected a forest surveillance application in order to show how appropriate protocols for QoS could be selected by defining the performance requirements of the application and the classification criteria considered for the study.

This research has also shown what we consider are shortcomings of the studied protocols. For instance, the MMSPEED protocol lacks a data aggregation or a (preferable) meta-data negotiation system. Other aspects that could be considered in more detail in MMSPEED are the energy-delay trade-off, and the facility of parameters interchange with MAC layer. As for the Z-MAC protocol, its initial overhead, its prioritization system and the absence of a data fusion mechanism are examples of issues that could be improved. In future works, we have the intention of modifying Z-MAC for a complete compatibility with MMSPEED.

We are currently working on the definition and posterior deployment of a WSN scenario in which a surveillance application will run. As future research, and after the functional aspects of the application are working, we plan to include performance monitoring inside this system. This will allow us to perform empirical studies regarding the influence that some of the parameters we have considered have in the quality offered to the application. At the moment, we are performing simulation experiments using J-SIM [16], which we have modified for our study case. However, its adaptation to MAC protocols is still poor and, thus, we are working to solve this problem.

5. References

[1] C. Intanagonwiwat et al., "Directed diffusion: A scalable and robust communication paradigm for sensor networks", in the Proc. of MobiCom'00, Boston, MA, August 2000.

[2] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," Proc. 5th ACM/IEEE Mobicom Conference (MobiCom '99), Seattle, WA, August, 1999. pp. 174-85.

[3] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, Volume: 8, pp. 169-185, 2002.

[4] A. Manjeshwar and D. P. Agarwal, "TEEN: a routing protocol for enhanced efficiency in wireless sensor networks," In 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, April 2001.

[5] A. Manjeshwar and D. P. Agarwal, "APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks," Parallel and Distributed Processing Symposium., Proceedings International, IPDPS 2002, pp. 195-202.

[6] K. Sohrabi, et al., "Protocols for self-organization of a wireless sensor network," IEEE Personal Comm., Vol. 7, No. 5, pp. 16-27, October 2000.

[7] T. He, J. Stankovic, L. Chenyang, and T. Abdelzaher. SPEED: A stateless protocol for real-time communication in sensor networks. In Proceedings of 23rd International Conference on Distributed Computing Systems, pages 46–55, May, 2003.

[8] E. Felemban; Chang-Gun Lee, Ekici, E. MMSPEED: multipath Multi-SPEED protocol for QoS guarantee of reliability and. Timeliness in wireless sensor networks**.** Mobile Computing, IEEE Transactions on Volume 5, Issue 6, pages 738-754, June, 2006.

[9] K. Akkaya and M. Younis. An energy-aware QoS routing protocol for wireless sensor network. In Proceedings of the Workshops in the 23rd International Conference on Distributed Computing Systems, pages 710–715, May, 2003.

[10] J. Polastre, J. Hill, and D. Culler. Versatile low power media access for wireless sensor networks. In SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 95--107, New York, NY, USA, 2004. ACM Press.

[11] Z-MAC: a Hybrid MAC for Wireless Sensor Networks; Injong Rhee, Ajit Warrier, Mahesh Aia and Jeongki Min (Technical Report, Department of Computer Science, North Carolina State University, April 2005).

[12] A. Koubâa, M. Alves, E. Tovar i-GAME: An Implicit GTS Allocation Mechanism in IEEE 802.15.4 to appear in Euromicro Conference on Real-Time Systems (ECRTS 2006), July 2006

[13] T. Watteyne and I. Augé-Blum, "Proposition of a hard real-time mac protocol for wireless sensor networks," in International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems (MASCOTS). Atlanta, GA, USA: IEEE, September 2005, pp. 532--535.

[14] B. Karp and H. Kung, "Greedy Perimeter Stateless Routing for Wireless Networks", Proc. IEEE/ACM Int'l Conf. Mobile Computing and Networking, pp 243-254, 2000

[15] T. He, C. Huang, B. Blum, J. Stankovic, and T.Abdelzaher, "Range-Free Localization Schemes for Large Scale Sensor Networks", Proc. Mobicom Conf. , 2003.

[16] Sobeih, A.; Hou, J.C.; Lu-Chuan Kung**. "**J-Sim: a simulation and emulation environment for wireless sensor networks". Wireless Communications, IEEE. Volume 13, Issue 4, Aug. 2006 Page(s):104 – 119**.**