Modelling QoS for Wireless Sensor Networks

José-F Martínez[1], Ana-B García[1], Iván Corredor[1], Lourdes López[1], Vicente Hernández[1] and Antonio Dasilva[1]

[1] EUIT Telecomunicación - DIATEL
Universidad Politécnica de Madrid
Ctra. Valencia, Km. 7, 28031, Madrid, SPAIN
{jfmartin, abgarcia, icorred, llopez, vhernandez, adasilva }@diatel.upm.es

Abstract: A wireless sensor network (WSN) is a wireless network composed of spatially distributed and tiny autonomous 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. Generally, these applications have strong and strict requirements for end-to-end delaying and loosing during data transmissions. In this paper, we propose a realistic scenario for application of the WSN field in order to illustrate selection of an appropriate approach for guaranteeing performance in a WSN-deployed application. The methodology we have used includes four major phases: 1) Requirements analysis of the application scenario; 2) QoS modeling in different layers of the communications protocol stack and selection of more suitable QoS protocols and mechanisms; 3) Definition of a simulation model based on an application scenario, to which we applied the protocols and mechanisms selected in the phase 2; and 4) Validation of decisions by means of simulation and analysis of results. This work has been partially financed by the "Universidad Politécnica de Madrid" and the "Comunidad de Madrid" in the framework of the project CRISAL - M0700204174.

Keywords: Wireless Sensor Networks (WSN), QoS protocols, performance, target tracking, natural environments surveillance.

1 Introduction

Recently, we have witnessed significant evolution in the field of wireless sensors. The latest stage has been characterized by improvements in sensor hardware issues (miniaturization of pieces, increased ROM and RAM capacities, more energy capacity, etc). These facts and the new field of possibilitiess for their application have boosted interest in Wireless Sensor Networks (WSN). WSN might be defined as follows: *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.* While a good deal of research and development has been carried out in architecture and protocol design, energy saving and location, only

Please use the following format when citing this chapter:

Martínez, J.-F., García, A.-B., Corredor, I., López, L., Hernández, V., Dasilva, A., 2007, in IFIP International Federation for Information Processing, Volume 248, Wireless Sensor and Actor Networks, eds. L. Orozco-Barbosa, Olivares, T., Casado, R., Bermudez, A., (Boston: Springer), pp. 143-154.

a few studies have been done on network performance in WSN (Quality of Service – QoS).

The service provided by the network is closely related to the quality of that service. Traditional QoS requirements (usually from multimedia applications) such as bounded delays or bandwidth are not pertinent when applications are tolerant of latency or the size of the packets being transmitted is very small. Generally, packet delivery ratio is an insufficient metric in WSNs: what is important is the amount and quality of information that can be extracted from a WSN.

Some studies on QoS have focused on protocols and mechanisms for MAC and the network layer, and almost all these have been developed and tested through simulations. All these approaches for supporting QoS in WSN can constitute a base for future work in this direction, and they obviously represent the starting point in our proposal. We have already conducted work on state-of-the-art QoS in WSNs. This work has focused mainly on QoS-based protocols and mechanisms both in MAC and network layers. The results of this work can be consulted in [1].

The remainder of the paper is organized as follows:

The case study is depicted in section 2. In this section the proposed application scenario is described, as are all its QoS-related characteristics. Based on these characteristics, we have identified the QoS mechanisms which are needed both in MAC and network layers of the protocol stack. The section concludes with a selection of the most suitable protocols for MAC and network layers available in literature on WSN. The validity of decisions on QoS protocols and mechanisms is verified in section 3, with the use of simulation software to perform tests. Previously, we have designed a simulation model to which we have applied the protocols selected in section 2. Section 4 concludes this paper with an overview of future research activities.

2 Case study: QoS in forest fire detection

In this section we will apply the study we have presented on QoS protocols in WSN [1] to a forest surveillance scenario. So we will begin by extracting the QoS-related requirements from the real-time forest surveillance application, allow us to select the network and MAC protocols later that best suit these requirements. However, these protocols may not meet all necessary requirements. If so, we will also propose add-on features for each protocol. We will also create a simulation model from the application and subject it to a number of simulation tests. In the conclusions section, we will discuss what we see as the shortcomings of the protocols studied herein, and which one should be corrected in future research.

2.1 Description and analysis of requirements of application for real-time forest surveillance

The application will focus on both forest fire detection and event tracking in a natural environment (natural reserve) of great ecological importance. The main objective of the application will be the early detection of forest fires to avoid ecological disasters. Likewise, the application will have secondary objectives such as the detection and tracking of intruders within protected spaces for the prevention of illegal actions. In short, the application will be used for forest surveillance, including detection of dangerous activities and conditions that increase the risk of fires; detection and location of fires; fire monitoring and assistance in fire extinction; detection and tracking of intruders entering restricted areas.

In our forest fire detection application, sensor nodes collect measurement data, such as relative humidity, temperature, infrared radiation, COx and NOx gases. Other components of the WSN supporting our application are laptops and/or PDAs (as support to firemen and safety watchmen), a server and a data base. All WSN services will be accessible to remote users through web services. Figure 1 illustrates the proposed scenario.

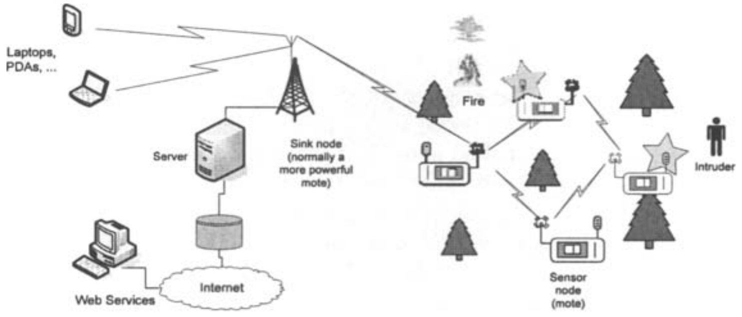

Fig 1. Forest surveillance application scenario

All sensors will be used to determine the risk of fire at a given moment. The infrared radiation sensor will also be used for the detection and tracking of intruders in restricted areas. 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 when guaranteeing QoS. The selected topology for the WSN will be flat. Therefore, every node will have the same hierarchy in the WSN as well as the same hardware components. The hierarchy will not be necessary in the proposed network since it will use a localized geographic routing.

***2) Geographical information**:* Sensor nodes must obtain geographical information – i.e., coordinates – in order to locate the events within the natural reserve. Methods commonly used to acquire this data are based on GPS [2] or distributed location services [3]. For WSNs, a GPS-based approach is too expensive, thus our WSN implements a distributed location service. However, this method adds certain overheads during the initial phase of the WSN that could impede ensuring QoS at those moments.

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

***4) Unbalanced mixture traffic**:* Another characteristic which will considerably affect QoS decisions is *reactive-proactive* hybrid behaviour. Reactive behaviour will come from fire or intruder detection, and will generate traffic to the sink node according to the event-driven delivery model. This traffic type is generated aperiodically through the detection of critical events at unpredictable points in time. Proactive behaviour will come from the monitoring of the environmental status and tracking targets, and will generate traffic to the sink node according to continuous delivery model.

5) Data redundancy: High redundancy in the sensor data is a common characteristic to most WSNs. Redundancy may improve several QoS requirements, such as reliability and the robustness of data delivery. However, this uses a large amount of energy. To solve this problem, we could use data fusion or data aggregation to maintain robustness while decreasing redundancy in the data, but these mechanisms require high levels of computational activity in at least several nodes (usually cluster-heads). Therefore, these mechanisms also add delay and complicate QoS design in WSNs. We prefer to exclude these mechanisms, as our application is based on two critical objectives, and real-time requirements will prevail over energy requirements. An alternative to data aggregation and fusion is the meta-data negotiation which is able to eliminate redundancy without introducing excessive delay in data delivery.

6) Energy efficiency: An important challenge to this application will be 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 energy resources. However, to implement the QoS mechanism to support critical real-time traffic and while saving energy is not a minor task. The key is to distribute the 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 too quickly. Nowadays, achieving this energy distribution without compromising the QoS requirements is very difficult since mechanisms and protocols do not usually consider both possibilities at the same time.

7) Sensor data priority: Not all sensing data are equal; hence they have different levels of importance. For example, the data generated in a fire detection event will have more importance than that generated in the monitoring for determining the conditions that increase the risk of fire. QoS mechanisms will determine the data delivery priorities for the different data types existing in the WSN.

As a result, QoS support for the network will take into account almost all of the aforementioned characteristics in the application specifications. The next section describes how to extract network and MAC layers mechanisms from QoS-related requirements of the protocol stack according to the application characteristics analyzed.

2.1.1 Network layer

Guaranteeing network layer QoS for diverse traffic types is a challenge, as WSN characteristics such as dynamic topology change as a result of a number of factors: node failure, addition or mobility, the large scale of a network with thousands of densely-placed nodes, periodical and aperiodical traffic generated by sensors with different priorities and real-time requirements, or possible data redundancy produced by correlated sensor nodes.

Traditional network layer methods based on end-to-end path discovery, resource reservation along the path discovered and path recovery in case of topological changes will not be suitable for our WSN: initially, the time wasted in the path discovery is not acceptable for urgent aperiodic – i.e., event-driven - packets. Moreover, it is not advisable to reserve resources for unpredictable aperiodic packets. Even for periodic continuous flows, these methods are not practical in a dynamic

WSN because service disruption during path recovery increases data delivery delay, which is not acceptable in our mission-critical application. Finally, end-to-end path-based approaches are not scalable due to excessive overheads related to path discovery and recovery in large scale sensor networks. As an alternative to 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 aforementioned localized geographic routing. This type of routing will mainly provide adaptability to dynamic topology changes, since the nodes will not require acquisition of global topology information. Consequently, no control packet will be generated in significant amounts with topology changes due to node addition, failure or mobility. The nodes in the WSN will able to take localized packet routing decisions without a global network state update or a priori path setup, thus increasing network scalability and decreasing the control traffic. Further, this routing scheme is suitable for both critical aperiodic and periodic packets as a result of no path setup and recovery latency.

Another characteristic that should be included in the network layer is 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 for the purpose of differentiating among traffic with different end-to-end deadlines. On the other hand, the mechanisms that will be implemented for lending reliability to data transmissions could exploit the inherent multiple redundant paths to the final destination in a dense WSN to guarantee the required end-to-end level of reliability (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 the aforementioned reasons. Alternatively, the network protocol will implement a method for dealing with redundant data by exchanging meta-data in so-called data negotiation [4]. This eliminates the inefficiencies generated by data-aggregation mechanisms resulting from flooding and the subsequent processing of information. For instance, if a tracking event is detected and a data negotiation mechanism is used, location information is transmitted once and no further data is transmitted until the target moves.

2.1.2 MAC layer

Not all of the aforementioned QoS requirements could be met by network layer. Consequently, our WSN protocol stack will have a MAC protocol capable of performing the following tasks: medium access control according to packet deadlines, measurement of the average delay to individual neighbours, the measurement of the rate of loss to individual neighbours. In addition to, it may be necessary to have the capacity to deliver the packet to multiple neighbours reliably.

Along with the aforementioned functionalities, the MAC layer must implement mechanisms where each one of deadlines assigned by network layer is associated to a transmission priority level. Thus, medium access prioritization will be achieved through the MAC layer. Likewise, the MAC protocol will be able to measure the average delay to individual neighbours with the purpose of forwarding the packet according to its deadline.

However, packet forwarding will be performed not only on the basis of deadline criteria but also on those of reliability. For this reason, the MAC protocol will measure the rate of loss to individual neighbours.

The localized geographic routing used by the network layer will require transmission of control packets with the position data of neighbours situated at least one or two hops away. For the transmission of these control packets, the MAC layer will require the capacity to reliably deliver multicast packets.

2.1.3...Selected network and MAC protocols

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

From network layer perspective, we believe that only a few of the protocols of surveyed in [1] could be used in our WSN. We have selected three candidates from among these protocols: MMSPEED [5], SPEED [6] and Directed Diffusion [7]. (See table 1).

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

	Network topology	Data delivery model	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
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

We selected these protocols for several reasons:

MMSPEED

→MMSPEED implements localized geographic routing, which is fundamental for the network layer of our stack protocol. These mechanisms increase self-adaptability of the network to dynamic changes as well as scalability of the network. In addition, this protocol is suited for both periodic (real-time) and aperiodic traffic because routing decisions are local (i.e., 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 for supporting multiple traffic types (continuous, event-driven, etc.). Its dynamic speed compensation mechanism, which is capable of immediately correcting small inaccuracies produced in initial routing decisions, is also quite useful.

→Routing decisions in MMSPEED are also made according to the reliability level required by the packet. To route on the basis of the reliability requisite, MMSPEED has an advanced method of lending reliability to data transmissions which involves using the frame loss rate of the MAC layer to make an estimate of the reliability level of each link.

However, MMSPEED lacks a method for dealing with 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 in the course of studying how a meta-data negotiation mechanism can be added to MMSPEED.

SPEED

→SPEED is another QoS routing protocol for WSN that provides light real-time end-to end guarantees. The QoS mechanism, which is employed by SPEED, is based on a distance to sink estimate for guaranteeing fulfillment of delay requirements. This can be an useful mechanism for prior traffic in our WSN.

→The network layer will accept the packet depending on the required speed. If the QoS mechanism verifies that it will not be capable of achieving the delay requirement for a certain packet, then the packet will be discarded before it is forwarded to a neighbor node.

→SPEED can be recovered by means of back-pressure mechanism if the network becomes congested. This feature can be decisive for ensuring that data is transported to the sink with an acceptable delay.

→Like MMSPEED, SPEED bases its routing decisions on geographic localization of sensor nodes. This routing mechanism can notably increase network scalability. The routing module in SPEED (SNGF) implements a distributed database where a node can be selected in order to attain the speed requirement.

SPEED also has several disadvantages for our WSN. First, SPEED treats all traffic classes equally. However, as we already commented, there will be at least two traffic classes (aperiodic and periodic traffic) in our WSN that will require different QoS levels in terms of reliability and delay. Secondly, SPEED does not implement any reliability mechanism, which may be necessary for critical traffic.

Directed diffusion

→ Directed Diffusion is a data-centric and application-aware paradigm. This protocol implements a mechanism based on data aggregation to eliminate redundant data coming from different sources. This particularity reduces the number of transmissions drastically, leading to two main consequences: firstly, the network saves energy and extends its life-time, and secondly, it has higher bandwidth in the links near to the sink node.

→Directed diffusion is based on a query-driven model. This means that the sink node requests data by means of broadcasting *interests.* When events begin to appear, they start to flow towards the originators of interests along multiple paths. This behavior provides reliability and robustness to data transmissions in the network.

Although Directed Diffusion includes all these optimization mechanisms, the protocol has two shortcomings in the realm of QoS: directed diffusion can neither explicitly manage QoS parameters such as delay and reliability, nor differently handle more than one traffic class.

For the MAC layer, we have established the following criteria:

First, selecting a MAC protocol that complements MMSPEED protocol is no secondary decision. MMSPEED specifications propose an extension of 802.11e for supporting all mechanisms implemented by the network layer. The most important of these is the priorities mechanism. However, this MAC protocol is not specific to WSNs and consequently bears some deficiencies as a result. We propose the Z-MAC [8] protocol as an alternative to 802.11e. Although this protocol needs several additional features to be completely compatible with MMSPEED, it is an excellent starting point because it implements a priority mechanism that is very appropriate for this case study. The additional features are mainly concerning hybrid nature of Z-MAC. The latter forces the priority mechanism to work in a different way, depending on its contention level (low level - CSMA or high level TDMA). In addition, Z-MAC must be capable of associating each MMSPEED's speed layer with a priority class in the MAC layer.

On the other hand, Z-MAC has a highly efficient contention method that can avoid unnecessary backoff delays in packet transmissions. Another distinctive feature of Z-MAC is its adaptability to topology changes.

Another MAC protocol that can be used in our WSN is B-MAC [9]. B-MAC is not a QoS-specific protocol but it does include several interesting mechanisms that can notably optimize the WSN. The features that best define B-MAC are its simplicity of design and implementation, in addition to its flexibility, allowing it to offer multiple classes of service and to adapt to any scenario.

A comparative analysis between Z-MAC and B-MAC is shown in the following table.

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

3 Simulation of application scenario

3.1 Simulation model

The following table depicts the simplified simulation model defined for the application described in section 3.1:

Table 3. Simulation Environment Settings.

Size terrain	600mx600m
Terrain morphology	A mountain of 400mx400m, centered in the terrain.
Sensor node number	176 nodes (sink included)
Radio range	80 m
Initial energy charge	1000 Joules
Bandwidth	200 Kbps
Payload	32 bytes

The sensor nodes are deployed around the mountain, distributed in four sectors (*North, South, West* and *East*). The sink node is placed at coordinate (0,0).

J-SIM is simulation software selected to implement the model. It was chosen because it is component-based, a feature that enables users to modify or improve it.

Network protocols have been configured with different parameters according to capacities. All the parameters defined for each protocol are depicted in following sub-sections:

MMSPEED

Table 4. MMSPEED parameters.

	Attaining sink probability	Max. delay (in seconds)
High priority traffic (events)	0.4	0.5
Low priority traffic (monitoring)	0.2	4

Moreover, we have defined two speed layers which have been configured with different speed levels (1000 m/s and 250 m/s, respectively).

SPEED

SPEED has been configured to ensure a delay of 0.8 seconds in all packet transmissions. Besides, the transmission speed will not have to exceed a value of 1000 m/s. These parameters are applicable to all packet types.

Directed Diffusion

Directed Diffusion can be configured with multiple parameters. The most significant parameters for the simulation tests are the following: diffusion area of interests (complete area); duration of interests (all time simulation); interest refresh (every 10 seconds).

3.2 Simulation results

Since J-SIM can only simulate the MAC protocol IEEE 802.11 (in all its variants), the results analyzed in this section are for the behavior of QoS mechanisms in network layer. At present, our work group is considering the possibility of integrating Z-MAC and B-MAC inside of J-SIM simulator.

Deadlines

-MMSPEED: The results of simulations with MMSPEED are significant in the way they show how the protocol is capable of differentiating traffic classes (see Figure 2).

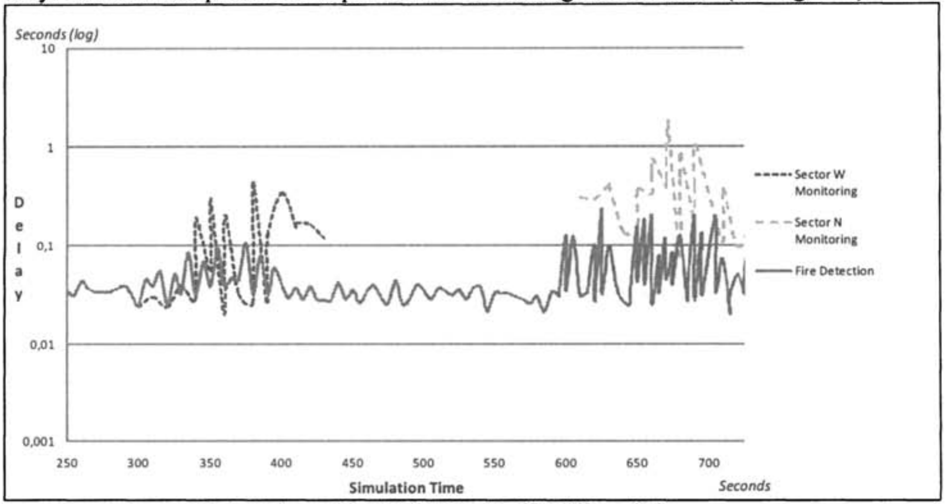

Fig 2. Delays with MMSPEED. Traffic differentiation.

When low and high-priority traffic concurs in the WSN, MMSPEED successfully supported the QoS level assigned to both traffic classes. The maximum delay configured for high-priority traffic (0.5 seconds) was never exceeded. Furthermore, the jitter (or delay fluctuation) is not excessively high, which will improve the quality of real-time data received by the application, especially if these data have been generated by the tracking of a person inside the area monitored by the WSN. In addition, low-priority traffic manages to maintain acceptable levels of delay, although the jitters are somewhat high. This fact will not lead to a decline in the quality of data obtained from monitoring, as they are not real-time data (they are generally stored in the database for later enquiries).

Figure 3 shows delays recorded in monitoring of traffic in a simulation period using SPEED and Directed Diffusion protocols. This graphic shows only a specific example, but it can be extrapolated to the complete simulation time.

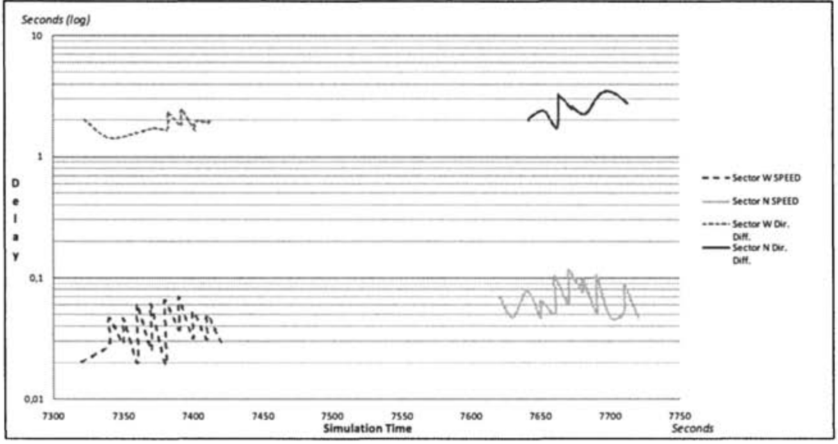

Fig 3. Delays with SPEED and Dir. Diff. Comparative graphics.

-SPEED: SPEED showed excellent performance in handling both traffic classes. The packets are never delayed more of 0.19 seconds, which is below the maximum limit allowed (0.8 seconds). SPEED also manages to maintain the jitters within an acceptable range, which is positive for real-time traffic. However, because SPEED does not differentiate between traffic classes it has to use the same amount of resources for routing both high priority traffic and low priority traffic, which is unnecessary. Any increase in monitoring traffic could seriously compromise real-time traffic.

-Directed Diffusion: According to the results, it is evident that the mechanisms implemented in Directed Diffusion are insufficient to ensure the QoS level required by the WSN, specifically with regard to delays.

Reliability

-MMSPEED: When MMSPEED initiates a packet flow to the sink following a period of inactivity, it is common for intermediate nodes to have incoherent routing information. Until MMSPEED recovers operational status, tenths of seconds to one second may elapse, during which a few packets might be discarded. However, the discarding of packets does not mean an effective loss of event notifications, as there is always a route whose nodes have information on the correct routing, and these can consequently route the packets towards the sink. In other cases, MMSPEED shows a great robustness due to its multi-path mechanism.

-SPEED: SPEED has a significant lack of reliability because it does not implement any mechanisms to guarantee that packets reach the sink node. This characteristic of SPEED means that when congestion occurs, all discarded packets will inevitably become lost packets. On the other hand, SPEED does not undergo periods of instability caused routing information inconsistencies.

-Directed Diffusion: The simulation tests with Directed Diffusion were satisfactory in terms of reliability. Although Directed Diffusion does not implement an explicit mechanism to provide reliability, it achieves an acceptable reliability level by means of a multi-path routing that selects the best paths towards the sink.

Energy consumption

During the first 12 hours of simulated time, the consumption of energy of the eight nodes closest to the sink was recorded. The results can be seen in the table 4.

Table 5. Energy consumption with each protocol.

	Average energy consumption	**Lifetime in a real WSN**
MMSPEED	3.5225 Joules/hour	9 months
SPEED	6.5056 Joules/hour	5.6 months
Directed Diffusion	0.9575 Joules/hour	3 years

The first column shows the average levels of energy consumption in the simulation period. The second column shows the lifetime of a real WSN, assuming that sensor nodes use AA alkaline batteries. It is evident that the results vary greatly.

Directed Diffusion showed the best rate of energy consumption (3 years aprox.). These good results have been obtained through use of the data aggregation mechanism implemented by Directed Diffusion. This mechanism significantly reduces the number of data transmissions, and therefore helps saves a great deal of energy.

MMSPEED achieves an acceptable lifetime (9 months) and a very good energy/delay balance. However, this lifetime could be increased if MMSPEED implemented a mechanism for reduction of redundant data (e.g. meta-data negotiation or data aggregation).

SPEED has showed the worst results in energy consumption (6 months). This is mainly due to the large number of control packets transmitted by SPEED. SPEED may be insufficiently scalable to be used in a large WSN.

Taking into account all the simulation results, we conclude that the most suitable protocol for improving performance in our WSN is MMSPEED. However, this protocol should be improved with several add-on features, which should be the subject of future research. In section below, we discuss a number of improvements that could be made to the protocol.

4 Conclusions and future work

In this paper we have presented a study of MAC and network layer protocols that have been defined to provide QoS in wireless sensor networks. We have focused on the basic mechanisms used in these protocols for guaranteeing performance parameters to applications, leading to charts comparing 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 for the protocol study.

This research has also shown what we consider to be shortcomings in the protocols. For instance, the MMSPEED protocol lacks a data aggregation or an even more 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 for parameter interchange with MAC layer. As for the Z-MAC protocol, the initial overhead, the prioritization system and its lack of a data fusion mechanism are examples of issues that could be improved. In future work, we intend to modify Z-MAC to achieve full compatibility with MMSPEED.

We are presently working on defining and subsequent deploying a WSN scenario in which a surveillance application will be run. For future research, and after the functional aspects of the application are working, we plan to include performance monitoring in the system. This will allow us to perform empirical studies of the influence of the parameters we have considered on the quality offered to the application. At the moment, we are performing simulation experiments using J-SIM [10], which we have modified for our case study. However, its adaptation to MAC protocols is still poor, and we are working to solve this problem.

5 References

1. J.F. Martínez, A.B. García, I. Corredor, L. L6pez, V. Hernández and A. Dasilva, "QoS in Wireless Sensor Network: Survey and Approach". To be published in Proc. IEEE/ACM EATIS, May, 2007
2. 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.
3. T. He, C. Huang, B. Blum, J. Stankovic, and T.Abdelzaher, "Range-Free Localization Schemes for Large Scale Sensor Networks", Proc. Mobicom Conf. , 2003.
4. 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.
5. 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.
6. 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.
7. 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.
8. 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).
9. 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.
10. 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.