We are IntechOpen,
the world's leading publisher of
Open Access books
Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS
BOOK CITATION INDEX
INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

Preamble-Based Medium Access in Wireless Sensor Networks

Alexander Klein

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/48504

1. Introduction

Medium access protocols in the context of wireless sensor networks have to deal with a large number challenges resulting from hardware limitations, event-driven traffic characteristics, node density, unreliable radio links and requirements of the target application [3]. For these reasons, the design of MAC protocols is still a popular field of research [4] since protocol developers always try to optimize the communication as much as possible. A couple of years ago, the research focus was mainly laid on energy efficiency rather than Quality of Service (QoS). However, this has changed due to the technical progress which allows to employ more complex MAC protocols on the sensor nodes which suit the requirements of mission critical applications [5] and provide QoS [6].

In order to achieve energy efficient communication, the main goal of MAC protocols is to turn off the transceiver as often as possible since it is the part of the node which consumes most of its energy. Therefore, the protocols try to avoid overhearing due to the fact that overhearing is the main cause of energy consumption in duty-cycled networks. The term overhearing addresses the issue that a node receives data which is not dedicated for this node.

The medium access in duty-cycled networks can be achieved in various ways. A common approach is to make use of a Time Division Multiple Access (TDMA) based protocol which allows to efficiently use the radio resources by avoiding typical issues of energy consumption such as idle listening, overhearing, overemitting and collisions. The disadvantage of this approach is that it requires synchronization mechanisms due to the high clock drift of the low power hardware.

Another approach is represented by protocols which divide the time in common active and sleep periods. These approaches require less precise synchronization compared to their TDMA-based counterpart. However, the synchronization mechanisms still results in additional protocol overhead.

The last group is represented by random access protocols with duty-cycle support. These protocols make either use of packet retransmissions or preamble sampling to ensure that the

INTECH
open science | open minds

receiver listening to radio channel and thus able to receive the transmission. Table 1 shows an overview of preamble sampling protocols whereas the protocols are categorized according to their medium access strategy.

Strategy	MAC Protocol
Long Preamble	Aloha with Preamble Sampling [1], B-MAC [7], BP-MAC [8], CSMA with Preamble Sampling [9], LPL [2]
Short Preambles	BPS-MAC [10], CSMA-MPS [11], MFP-MAC [12], PR-MAC [13], SEESAW [14], SpeckMAC-D [15], Ticer [16], X-MAC [17]
Short Preambles with Synchronization	CSMA-MPS [11], MixMAC [18],SyncWUF [19], WiseMAC [20]
Short Preambles with adaptive Duty Cycle	BEAM [21], LWT-MAC [22], MixMAC [18], MaxMAC [23], WiseMAC(more bit) [20]
Short Preambles for Contention Resolution	BPS-MAC [10], PR-MAC [13]

Table 1. Overview of MAC Protocols using Preamble Sampling

In recent years, preamble sampling techniques became more and more popular due to the fact that they do not require additional mechanisms for synchronization. This techniques can be applied in many ways as outlined by Cano et al. [24] in their survey of preamble sampling MAC protocols. The basic principle of preamble sampling is shown in Figure 1 which is adopted from [24]. The figure shows typical preamble sampling strategies and also points out the overhearing caused by these access procedures.

The first preamble sampling approach [1] followed the access procedure as described in Figure 1.1. Nodes wake up at periodic time intervals and listen to the radio channel for a short time. If a busy radio channel is detected, nodes continue listening to the channel. Otherwise, they switch off their transceiver and wait for the next active period. Thus, a node, that wants to communicate with another node, has to send a preamble which is longer than the maximum idle period in order to assure that the receiver is listening. This approach has a clear advantage of simplicity. However, the long preamble comes with several disadvantages such as high protocol overhead and overhearing costs. As a result of the long preamble, it is likely that a large number of nodes receive a transmitted preamble and stay awake even though they are not part of the receiver group. Moreover, collisions become very costly since the retransmission of packets involves the transmission of the long preamble which increases the overhearing. The transmission of a long preamble is not supported by every low-power transceiver. Most transceivers, like the CC2420 or CC2500, only support a maximum packet/preamble size of 128 Bytes due to hardware constraints. After the transmission of a packet/preamble, the transceiver switches automatically back to receive mode which results in a gap between consecutive packets/preambles.

Later approaches [11, 16, 17, 20] introduced the mechanism of short preambles to reduce overhearing and the utilization of the radio channel. In addition, preamble sampling access strategies, which use short preambles, can be deployed on any low-power transceiver as long as the gap between two consecutive short preambles is chosen with respect to the hardware characteristics in terms of Clear Channel Assessment (CCA) delay and Turnaround Time
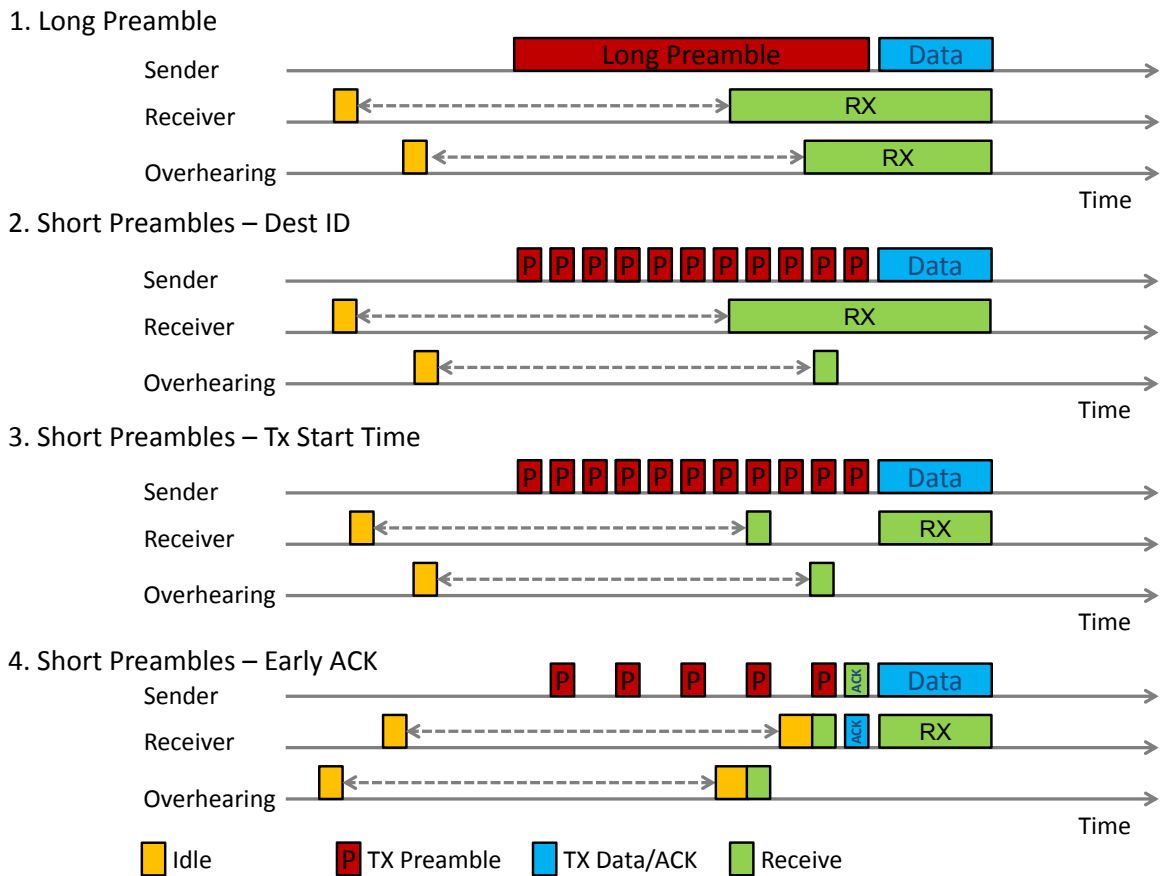
Figure 1. Overhearing in Wireless Networks depending on the Preamble Sampling

(TT). CCA delay specifies the time that a transceiver has to listen to the medium in order to determine whether the medium is busy or idle. The TT corresponds to the time interval that a transceiver requires to switch between receive and transmit mode and vice versa. Both issues and their impact on the performance of MAC protocols are discussed in Section 4.

Instead of using the preamble solely as reservation signal, it is possible to include useful information in the preamble to minimize overhearing as shown in Figure 1.2. Some protocols store the address of the destination in the short preamble which allows nodes that are not involved in the transmission to turn off their transceivers.Nevertheless, the destination node has to continue listening to the medium until the data transmission starts which represents overhead.

The protocol overhead can be further reduced if the start time of the data transmission is encoded in the preamble in addition to the destination address. In this case, it is sufficient for the destination to receive a single short preamble. The destination may than switch off its receiver until the transmission starts as outlined in Figure 1.3.

A new approach that is based on short preambles with destination information was introduced by Buettner et al. [17] in 2006. The idea of their approach is to apply a gap between consecutive preamble in order to allow the destination to respond with an early acknowledgment as shown in Figure 1.4. Upon reception of the early acknowledgment, the sender starts to transmit the data which further reduces the energy consumption of the sender and the protocol overhead.

The information in the preambles can also be used to enable synchronization [18–20], resolve contention on the radio channel [8, 13, 23] or to provide priority-based medium access for service differentiation [10]. These mechanisms are typically more complex and are therefore discussed in more detail in Section 2.

2. Survey of preamble-based MAC protocols

The number of preamble sampling MAC protocols is still increasing very fast since most of them are optimized for a certain scenario or application. In the previous section, the protocols were classified according to their used medium access scheme. Moreover, the problems of the different access schemes were highlighted and some solutions were introduced. The focus of this section lies on a more detailed description of a selection of popular preamble sampling protocols. The selected protocols either provide a basis for a large number of other preamble sampling protocols or introduce new mechanisms for contention resolution and priority-based medium access. In the following, the advantages and drawbacks of each protocol will be discussed.

2.1. CSMA-PS

The traffic load in WSNs is low compared to other wireless networks since nodes sleep most of the time to reduce their energy consumption. For this reason, nodes switch off their transceivers as often as possible since the transceiver usually is the most power-consuming part of a sensor node. Moreover, sensor nodes are often unsynchronized due to the high clock drift of the micro controllers. The CSMA-Preamble Sampling [1, 9] protocol was introduced by El-Hoiydi in 2002. The nodes in the network periodically activate their transceiver in order to listen to the medium for a short time interval. If a node senses a busy channel, it stays awake until the current data transmission has finished. Otherwise, the node switches off its transceiver and waits for the next wake-up interval. Therefore, a node transmits a preamble before its data transmission. The duration of the preamble has to be longer than the wake-up time interval to be sure that the destination node is listening to the medium. A medium access example of the CSMA-PS protocol with acknowledgments is shown in Figure 2.
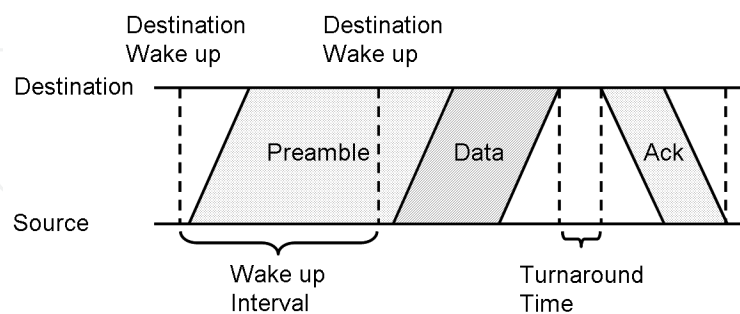

Figure 2. Medium Access Example - CSMA-PS with Acknowledgment

Acknowledgments are still required and strongly recommended for reliable data exchange due to the fact that hidden nodes may still interfere the communication. Furthermore, neighbor nodes could also disturb the current transmission if they start their own transmission during the gap between the reception of the last data packet and the transmission of the acknowledgment. The minimum gap duration is represented by the turnaround time of the

transceiver. The idea of CSMA with preamble sampling is adopted by a large number of protocols to prolong the lifetime of WSNs. Nonetheless, the performance of CSMA-PS based protocols is strongly affected by the network characteristics, the hardware limitations, and the traffic pattern. Especially, the duty-cycle and the turnaround time have a large impact on the performance of the protocol. CSMA-PS can be further improved by using scheduled wake up after transmission as introduced by Cano et al. in [22].

2.2. X-MAC

The X-MAC [17] protocol is designed for asynchronous low-power duty-cycled WSNs. It uses strobed preambles to achieve a better performance than ordinary Low Power Listening (LPL) [2] based protocols. The short strobed preambles are used instead of a single large preamble. Moreover, the short preambles contain the address of the destination. Thus, a destination node may recognize its own address immediately and transmit an acknowledgment in the next gap after the preamble which reduces the medium access delay since the originator does not need to transmit all short preambles. Figure 3 shows the difference between the medium access of LPL and X-MAC.
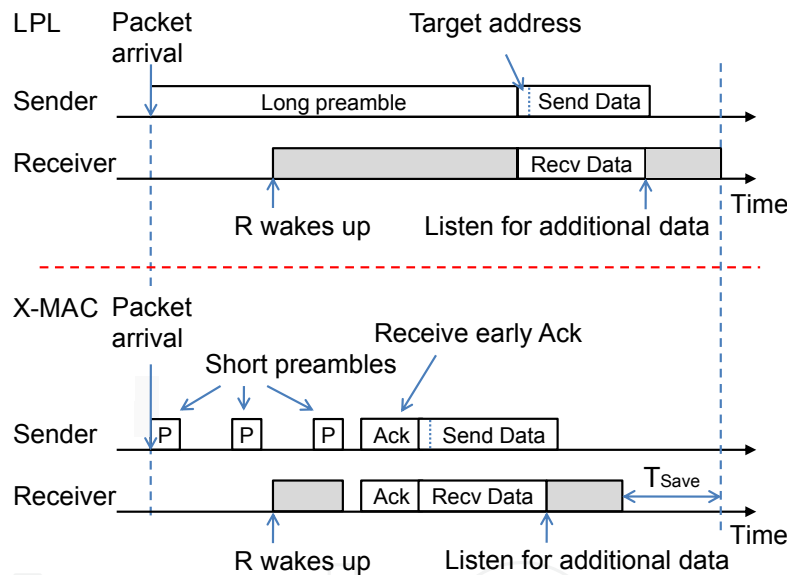

Figure 3. X-MAC - Medium Access

The advantage of X-MAC over LPL is that the destination node can respond immediately instead of listening to the whole preamble. The originating node stops the preamble transmission and starts its data transmission after receiving the early acknowledgment from the destination node during one of the gaps.

As a result, the medium access delay is reduced by approximately 50% even in the case that there is no contention on the radio channel. The difference may become larger depending on the preamble duration, the traffic load, and the packet size. The efficiency of the protocol depends on the CCA delay and the switching time of the transceiver between rx and tx mode since these hardware limitations are responsible for the length of the short preamble and the duration of the gaps. In addition, the medium access delay is strongly affected by the hardware limitations due to the fact that they also limit the length of the duty-cycle.

The protocol takes advantage from data sniffing. A destination node stays awake a short time after it has received a data transmission. Therefore, it can respond quickly with an early acknowledgment if another node wants to send packets to it. This feature may look unimportant at first glance. However, traffic patterns in WSNs are typically data-centric and event-driven. For this reason, data sniffing significantly affects the performance of the X-MAC protocol. Moreover, the acknowledgment covers the function of a CTS message if received by a node which is not the originator of the preamble. Thus, it reduces the collision probability in multi-hop networks caused by the hidden-node problem. The protocol is able to improve its energy efficiency depending on the traffic load since a node switches off its transceiver if it receives a preamble or an acknowledgment which is not dedicated for it. As a result, the corresponding node safes energy which prolongs its lifetime.

2.3. Wise-MAC

The Wise-MAC [20] protocol was developed by the Swiss Center for Electronics and Microtechnology as part of the WiseNET platform [25]. The protocol is optimized for energy efficiency in low traffic WSNs. The medium access is based on synchronized preamble sampling. In addition, the protocol is designed for infrastructure communication where more powerful and less energy-constraint nodes cover the task of base stations.

Nodes that are energy-constraint only communicate directly with the base station. In the following, these nodes are referred to as subscribers or subscriber nodes. If a subscriber node wants to transmit a packet to another node, it sends the packet to the base station. The base station transmits the packet to the destination node if the destination node is registered at this base station. Otherwise, the packet is forwarded to the corresponding base station where the destination node is registered.

In infrastructure networks, different MAC protocols and different radio channels can be used for the downlink and for the uplink since a base station will not switch off its transceiver in contrast to the subscriber nodes. Therefore, the downlink - from the base station to the subscriber nodes - represents the challenging part in low-power infrastructure WSNs due to the asynchronous sleep scheduling of the subscriber nodes. Wise-MAC is designed to optimize the downlink in terms of energy consumption and delay. It is based on preamble sampling like many other MAC protocols [1, 9]. However, the difference to other protocols lies in the fact that the base station learns the sampling schedule of its neighbor nodes. Thus, the idle listening time of the subscribers can be reduced if the base station starts to transmit the wake-up preamble in respect to the wake-up period of the corresponding subscriber. The medium access of the Wise-MAC protocol is shown in Figure 4.

Subscriber nodes sense the medium with a wake-up period of T_W. If a base station wants to transmit data to one of its subscriber nodes, it starts to transmit the wake-up preamble right before the wake-up period of the subscriber node. The transmission of a data frame is started as soon as the base station is assured that the subscriber is listening. Note that a frame may contain one or more data packets. The frame starts with the address of the subscriber. Thus, other subscribers can switch off their transceivers in order to avoid idle listening caused by overlapping wake-up intervals. The address field is followed by a data field which holds one data packet. Each frame ends with a frame pending bit to signalize to the subscriber station whether the base station has additional data frames pending for it. As a result, the energy efficiency of the protocol is increased since the subscriber is able to switch off its transceiver as
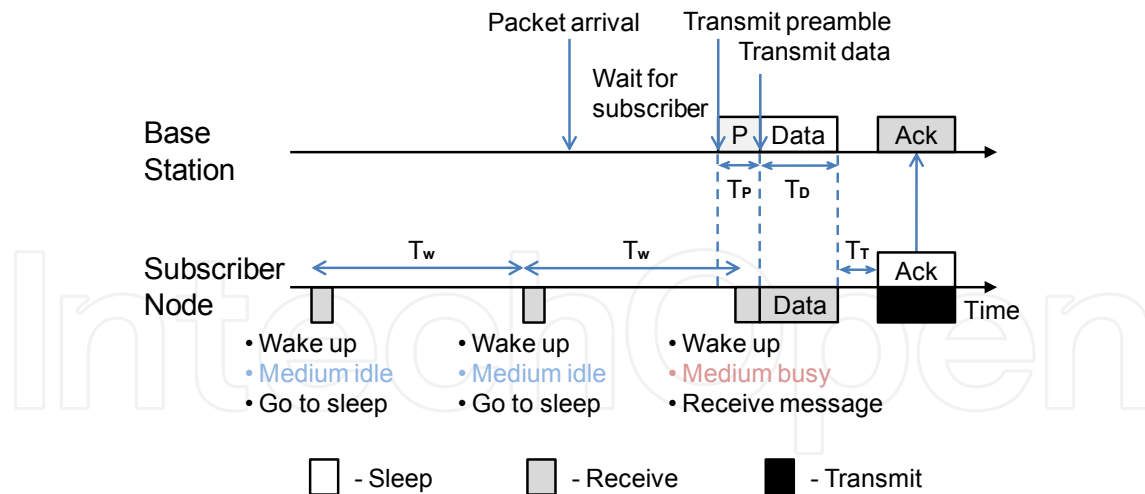
Figure 4. Wise-MAC - Medium Access

soon as possible. The subscriber node responds with an acknowledgment to the base station in the case that the base station has indicated that no additional frames are pending. The acknowledgment of the subscriber contains the information about the remaining time until the subscriber senses the medium again. This information is then used by the base station to keep its sampling scheduling information table up-to-date. The base station also stores the time when the acknowledgment was received in order to take the clock drift of the oscillator of the micro controller into account.

2.4. BPS-MAC protocol

Random access based MAC protocols are not able to reliably exchange data in dense WSNs with correlated event-driven traffic if they solely rely on the sensing capabilities of the low power transceiver due to the fact that the transceivers cannot detect a transmission that has been started within an interval that is shorter than the CCA delay and the turnaround time. The BPS-MAC protocol addresses this problem by using backoff preambles with variable length before transmitting data. The duration of the preamble is a multiple of the CCA delay or the turnaround time of the transceiver. Thus, a node is able to detect a synchronous preamble transmission of another node provided that they choose a backoff preamble with a different number of slots. Furthermore, the slot duration has to be larger or equal than the CCA delay and the turnaround time in order to leave the nodes enough time to switch the transceiver mode and/or to sense the medium. An example of the medium access procedure with two backoff sequences is introduced in Figure 5.

The example shows a scenario in which three nodes compete for the medium access. As mentioned in the previous paragraph, the BPS-MAC protocol divides the time during the medium access into time slots. A node that wants to transmit data senses the radio channel for duration of three slots. If the medium has been idle during the three slots, the node switches its transceiver from receive to transmit mode which requires an additional slot. Then, the node chooses a backoff duration and starts to transmit the backoff preamble. After the transmission of the preamble is completed, the node switches its transceiver back to receive mode and senses the medium. If a node senses a busy medium after the preamble transmission, it restarts the medium access procedure after a random number of slots. In the case that the medium is free after the preamble transmission, the node switches its transceiver back to tx
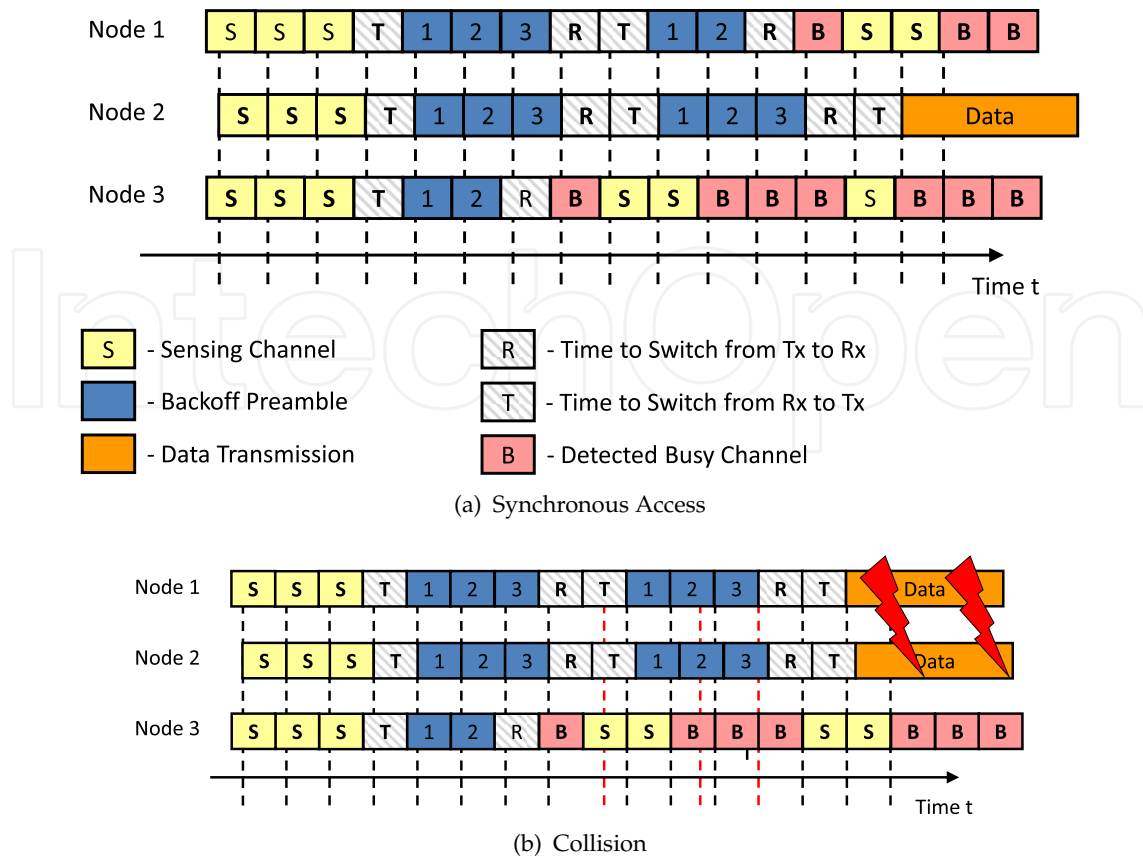
(a) Synchronous Access

(b) Collision

Figure 5. Sequential Contention Resolution

mode in order to proceed with the next sequence of the contention resolution. A node is only allowed to start its data transmission if it has sensed an idle medium after the transmission of the last backoff preamble. Note, the time between two consecutive preambles is two slots. For that reason, the nodes sense the medium for a duration of three slots at the beginning of the medium access process to assure that there is no ongoing data transmission.

The introduced procedure reduces the collision probability in case of synchronous medium access in a significant way. However, collisions may still occur if two or more nodes start their preamble transmission at the same time and chose the same number of preamble slots in every backoff sequence. Figure 5b shows a collision example for a contention resolution with two backoff sequences. The figure points out that the collision probability can be decreased by either increasing the maximum backoff duration of a single sequence or by increasing the number of backoff sequences.

Nonetheless, the backoff procedure represents protocol overhead which limits the maximum throughput of the protocol. Therefore, both parameters have to be chosen in respect to the node density and the traffic pattern. The sequential contention resolution represents an extension of the medium access procedure that is introduced in [8].

3. Implementing QoS strategies

Quality of Service requirements in the Internet lead to the development of several approaches for realizing QoS guarantees. The best known approaches are DiffServ [26] and IntServ [27].

While these protocols can be used in the global Internet, they can hardly be applied in the context of sensor networks due to multiple reasons. Sensor networks which consist of small and resource-constrained devices cannot run resource-intensive protocols that have high requirements concerning computational power, memory and bandwidth. Moreover, unreliable links and time varying channel conditions make QoS in WSNs a difficult task [28].

Instead, light-weight protocols, which require little synchronization between the nodes involved in the communication, are more suitable in this context. In order to build such light-weight protocols, simple QoS strategies need to be employed. These strategies, which can be implemented using preamble sampling protocols, should on the one hand be as simple as possible while fulfilling the requirements of a large number of applications on the other hand. In Subsection 3.1, we will discuss a number of strategies that should be implemented by a QoS approach. Afterwards, we will highlight how such an approach needs to be configured to provide the QoS strategies in Subsection 3.2. The impact of preamble transmission in multi-hop wireless networks is discussed in Subsection 3.3 by comparing the performance of the BPS-MAC protocol and Zigbee in a WSNs with high node density.

3.1. Qos strategies

3.1.1. Topology-aware

The topology in WSNs is often built from two types of nodes: few powerful nodes with little energy constraints that form a backbone and a large number of nodes with limited hardware and energy resources which use this backbone. While these backbone nodes have a distinguished special role in the network, they use the same shared medium for communication as the other nodes. This results in a situation where the backbone nodes compete for medium access with the constrained nodes. In order to avoid this, mechanisms that prioritize the medium access for backbone nodes should be implemented, which could improve the overall network performance: Since the number of backbone nodes with access priority is very small, the medium access delay for these nodes is decreased. This allows backbone nodes to forward messages faster in the WSN, thus decreasing the delay while increasing the delivery ratio. Furthermore, this strategy gives the backbone nodes control of the medium access which improves the support for data aggregation mechanisms.

3.1.2. Network-aware

WSNs have gained popularity due to their self-organizing capabilities, which allows them to be easily and randomly deployed in many scenarios. This includes scenarios where nodes can become hardly accessible, e.g. due to radioactive contamination. Such scenarios do not allow for careful sensor placement and topology architecture, but rely on the self-organization topology of the WSNs. Furthermore, some scenarios do not allow the replacement or relocation of individual nodes or the complete network. Asymmetric links or network partitioning might also make reprogramming or shutdown of nodes very difficult or even impossible.

If a user is forced, as a consequence of such conditions, to deploy a new sensor network on top of an older one, a number of problems can arise due to the shared characteristic of the wireless medium. This can limit the performance of the newly deployed network which

typically operates in the same area and on the same radio channel. Frequently transmitting older nodes will compete with the new nodes for medium access which increases the power consumption of the nodes in the newly deployed network. A priority-based medium access strategy, which allows to assign a higher priority to the newly deployed network, can mitigate the problem of co-existing networks that operate on the same frequency.

3.1.3. Traffic-aware

An increasing number of sensor networks perform different tasks at the same time. The traffic streams related to these different activities might have different priorities for a user. Thus, traffic-awareness within the MAC protocol can provide QoS guarantees for the different streams. Assume a WSN in which nodes generate traffic with different priorities, e.g. the stress and strain measurements of a structural health monitoring application, which has high QoS requirements, and temperature measurements which can be transmitted as best effort traffic. Assigning a higher priority to the traffic of the structural health monitoring than the temperature application would lead to faster forwarding of this kind of critical information.

3.1.4. Service-aware

Network and service virtualization has become an interesting topic within the last few years, with first implementations for WSNs already available [29]. Their key improvement is that they allow several different users access to the nodes and sensors in a shared manner. Resource allocation for each user on a node, e.g. computational power, memory, sensors, must be done properly in such environments, and has been studied in a variety of research work in the past years. However, as soon as the medium access has to be taken into account, the consideration of user priorities becomes a challenging task. Scheduling of packets according to priority on a single node can be easily done by applying predefined user priorities. Synchronization between users on different nodes is however very complex. The best scheduling algorithm implemented in the operating system of a node is useless if that node does not get access to the medium in order to transmit the carefully scheduled and queued packets.

3.1.5. Distance-aware

A typical WSN topology is configured in a way that allows the transmission of measured sensor data to a small number of data sinks adjunct to the network. These data sinks can then evaluate and process the data themselves or work as a gateway to another network. The topology of these networks is often arranged in a tree structure [30], which allows to take advantage from data aggregation mechanisms. While such a topology provides a number of advantages, it can be often observed that traffic load increases towards the sinks. Medium access can therefore play a critical role in these networks: A priority based medium access procedure that takes the distance to the sink into account, can support the data aggregation mechanisms to decrease the energy consumption of sensing nodes on the one hand or minimize delay on the other hand.

If nodes that are closer to the sink have a higher priority, the delay in event-based WSNs can be reduced since the node which is triggered by the event and is closest to the sink has

the highest priority. It can therefore immediately access the medium to transmit its data. In addition, lower link delays can be achieved because the priority of the transmitted packets further increases on the path towards the sink.

In scenarios where energy consumption is a major constraint, e.g. more important than the problem of high delay, a different prioritization can be beneficial. A medium access strategy, that gives nodes further away from the sink a higher priority than nodes closer to the sink, can reduce the energy consumption of the transmitting devices. The nodes that are furthest away from the sink can transmit their data immediately. Afterwards, they can turn off their transceivers at the end of the transmission, thus saving valuable energy. Furthermore, such prioritization improves the potential of data aggregation: All children of an aggregation node in the tree have a higher medium access priority than their parent. As a result, the children can transmit their data to the parent before the parent gains access to the medium in order to forward the data. Thus, the aggregation node can aggregate more messages from its children and operate more efficiently which reduces the number of medium access attempts.

3.1.6. Energy-aware

Wireless sensor nodes have very limited energy resources, which should be taken into account when prioritizing medium access. Designers of communication protocols therefore work very hard to minimize the power consumption while still meeting the given requirements. Energy-aware routing protocols, which include energy consumption into their protocol, typically aim at avoiding nodes that have little energy left. Such mechanisms have been proven to balance the traffic load and prolong the lifetime of WSNs. However, access to the medium can become a costly factor in the communication process if a node has to compete for the medium access multiple times before it can finally send its data. It can be therefore beneficial if nodes that run low on power have a higher medium access priority. These nodes can therefore save energy by the fact that their average number of medium access attempts is reduced by assigning them a higher access priority.

3.1.7. Buffer-aware

The small amount of memory represents a serious issue in WSNs. Especially, if Internet Protocol (IP) stacks are deployed on the devices since actions such as IP packet fragmentation and packet forwarding have high demands on memory. Most sensor nodes, like the TelosB, T-Mote or Mica nodes, only have as little as 8 or 10 KB of ram, which posses problems when multiple large IP packets need to be buffered before they can be forwarded. In conjunction with event-driven traffic patterns in WSNs, temporarily high traffic spikes can occur in the network. This can in turn lead to the demand for buffering several packets in some forwarding nodes. While load-balancing routing protocols can mitigate the impact of this issue in multi-hop networks, a MAC protocol which is aware of the problem can further improve the network performance. It can do this by taking the nodes' waiting queues into account: Nodes that have more packets stored in their buffers should have a higher priority, which enables them to get faster access to the medium. They can therefore reduce the amount of data in their buffers quickly, thus targeting the resource exhaustion problem already at an early stage. As a consequence, the maximum waiting queue length and share of dropped packets due to buffer overflows can be decreased.

3.1.8. Data-rate aware

The latest generation of routing protocols for WSNs, e.g. the Collection Tree Protocol (CTP) [30], apply adaptive mechanisms to cope with frequent topology changes. In general, these protocols increase their beacon transmission rate if they detect changes in their neighborhood. Topology changes usually result from interference or mobility of the nodes. The latter may lead to frequent topology changes which significantly increase the routing overhead. In dense networks, the routing overhead can even result in temporary congestion of the network. Temporary congestion can also be caused by applications which generate event-driven traffic, e.g. intruder detection. For these kinds of applications, it is important to receive information from all devices which have detected the event to gain more precise information and minimize false positives. The priority of the medium access should depend on the transmission rate of the nodes. A fair medium access can be achieved if a higher transmission rate results in a lower access priority and vice versa. Thus, nodes which rarely transmit traffic have a high probability of gaining access to the medium immediately. However, nodes that frequently transmit traffic can utilize the whole bandwidth as long as no other nodes need access to the medium.

3.1.9. Combined Strategy

Finally, it could be beneficial to have a strategy which combines the properties of the previously discussed ones. Depending on the target scenario and application, a combined strategy could further improve the performance. For example, a combined strategy could employ both the traffic-aware and buffer-aware strategy. Such a combination would represent a trade-off between the delay of high priority packets and packet loss of packets due to buffer overflows. A function which performs the trade-off calculation must be derived which calculates a priority value for each node, depending on the type of traffic that it has to forward and its current buffer fill-level.

3.2. Configuring QoS strategies

QoS strategies can be easily integrated in preamble sampling protocols since the preamble may hold additional information about the subsequent transmission. Another possibility is to encode the medium access priority in the preamble duration which is done by the BPS-MAC protocol. In the following, the an example of priority encoding is introduced which can be directly applied to the BPS-MAC protocol.

The protocol can be used in two different modes: Collision-free and prioritized contention resolution mode. Both modes result in different usages of the preamble sequences: In collision-free mode, node IDs are directly mapped onto preambles, resulting in unique preambles for each node which renders additional contention mechanisms unnecessary. In cases where preambles are not unique per node, but a priority is assigned per node group, some preamble sequences are assigned to prioritize the medium access while the others are used to resolve possible contention among nodes which have the same priority.

The decision parameter that defines the priority needs to be mapped to the length of the preamble sequence in order to configure the priority of a group of nodes. In the following we give recommendations on how the different QoS strategies that have been presented before can be implemented by choosing a certain preamble configuration. Table 2 summarizes the types of the different strategies along with the properties that should be mapped to the

sequence length. Static strategies should be configured by the user in advance before the nodes are deployed to their final location, e.g. by defining static IDs to properties. Higher property IDs yield longer preamble sequences and therefore result in higher access priorities. Mappings for static priority strategies are very straight forward: A user needs to define how

Strategy	Type	Decision parameter	Characteristics
Topology	Static	Node Type (Backbone, Constrained, ...)	Flow / traffic optimization
Network	Static	Network ID	Co-existence of networks
Traffic	Static	Application ID	Service differentiation
Service	Static	User ID	User prioritization
Distance	Dynamic	Hop count to data sink	Data aggregation
Inverse Distance	Dynamic	Hop count to data sink	Delay minimization
Energy	Dynamic	Battery fill level	Load balancing and life-time extension
Buffer	Dynamic	Buffer fill level	Fairness and reliability
Data Rate	Dynamic	Transmission rate	Fairness

Table 2. Configuration of different QoS strategies

many priority classes have to be supported. These priority classes have to be encoded onto a number of preamble sequences and the lengths of the sequences. The user may choose between providing a mapping of the priority to a single sequence or to multiple sequences, which in total use up to N slots. Let s be the number of sequences, and n_i the length of sequence i, then the total number of used slots will be:

$$N = 4 + \sum_{i=1}^{s} n_i + 2s \qquad (1)$$

since the first four slots being used for initially sensing the medium and switching from rx to tx mode, and the two pause slots between each sequence. While, at a first glance, choosing multiple sequences seems to be a bad decision due to the pause slot overhead, choosing multiple preamble sequences increases the number of priorities that can be encoded. The number of supported medium access priorities is given by the product of the maximum length in slots of each preamble sequence as shown in Figure 6. Now, consider a configuration that employs three sequences, each having a length of four slots. This configuration results in a total maximum medium access delay of 22 backoff slots according to Equation 1. If a single preamble sequence would have been chosen instead, maximum preamble duration of 18 backoff slots could be chosen to guarantee a total maximum medium access delay of 22 backoff slots. Thus, the single sequence configuration can only encode up to 18 priority classes whereas the configuration with three sequences can support up to 64 priority classes. This ratio further increases the more sequences are chosen.

3.3. Performance evaluation

The performance of MAC protocols for WSNs strongly depends on the characteristics of the network, e.g. the number of nodes, the node density, and the traffic pattern. Moreover, the
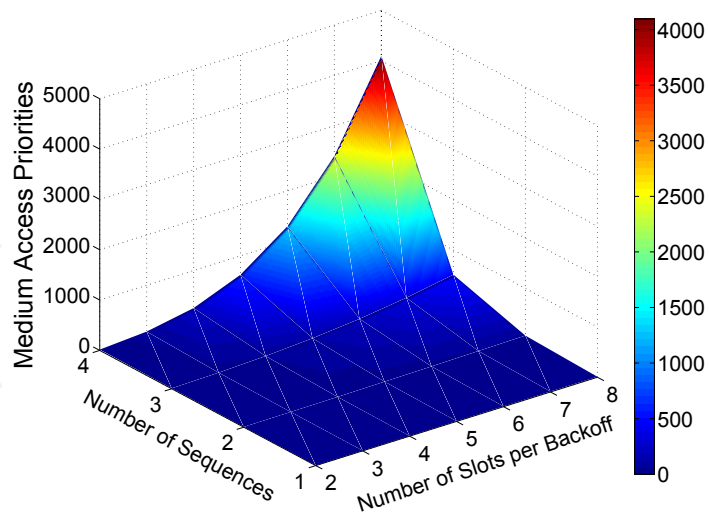
Figure 6. Medium Access Priorities depending on the Protocol Configuration

data rate and the sensing capabilities of the transceiver have a large impact on the network performance. In the following, it is assumed that the transceiver achieves a maximum data rate of 250 kb/s. Furthermore, a CCA delay and a turnaround time of 128 μs is assumed which represent typical values for low power transceivers. The OPNET Modeler [31] is used to simulate the performance of the protocols. Note that most simulation tools, like OPNET Modeler or ns-2 [32], simplify the physical layer in order to increase the simulation speed. Thus, their standard models simplify or even neglect important communication issues, e.g. the turnaround time of the transceiver and the CCA delay. For that reason, we modified the physical layer of the OPNET Modeler software such that it takes both communication issues into account. The transmission range is limited to 10 meters and the maximum interference range is set to 17 meters by modifying the so-called pipeline stages of OPNETs free space propagation model. These values reflect the average results from our first measurements with a small self-developed sensor board that uses a MSP430 micro controller and a CC2420 transceiver. The short range results from the fact that the nodes were placed inside the backrest of the seat. It is clear that these values may vary significantly depending on the position and orientation of the sensor node and the characteristics of the used antenna. Thus, the assumed values only fit to our particular example scenario.

The simulated scenario represents a typical middle-size airplane with six seats per row. A wireless sensor is placed in the backrest of each seat which monitors the state of the seat, e.g. whether the seat is occupied, the seatbelt is fastened, or the tray is secured. This information is reported periodically to a sink in the front of the plane. It has to be kept in mind that the simulated application is just an example application. There are currently a large number of applications under consideration to improve the existing flight cabin management system. A multi-hop network is required to enable connectivity between all nodes in the network due to the fact that large planes reach lengths of up to 60 meters. More powerful sensor nodes with routing capabilities are placed on the ceiling along alleyway approximately every 8 meters in order to connect the other sensors with the sink. An overview of the simulated scenario is shown in Figure 7.

The figure illustrates the high node density of up to 60 nodes.However, the large interference range has to be taken into consideration as well when specifying the application requirements.
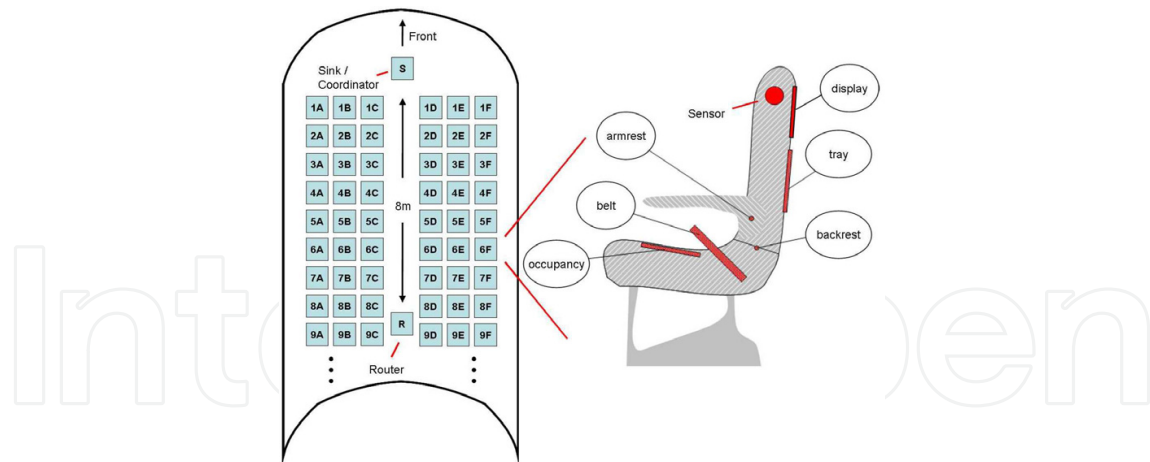
Figure 7. Overview of the Simulated Scenario

As a consequence of the high node density, the traffic pattern has a huge impact on the network performance in the simulated scenario. Data traffic is usually highly correlated in WSNs since it is often event-driven and data centric. Thus, we decided to simulate three different traffic patterns which are representative for a large number of popular intra-aircraft applications. The simulated traffic pattern are shown in Table 3. The number of (seat) rows is increased from 8 to 40 in order to find out how many nodes are supported by the protocols in the intra-aircraft scenario depending on the application. The results represent the 90 percent confidence intervals of the average end-to-end delay and packet loss that are collected from 20 simulation runs with a duration of 1000 seconds and different seeds.

The traffic pattern start after 80 seconds since the Zigbee model requires some time to build a tree topology. In addition, the traffic generation stops at 980 seconds to allow the nodes to empty their waiting queues. Thus, the packet loss is given by the fraction of generated packets and the number of packets that are successfully received by the sink. Zigbee is set to non-beacon mode. Zigbee implies network layer functionality. Thus, a directed-diffusion [33] based routing protocol is used in combination with the BPS-MAC protocol to support comparable routing functionality. The directed-diffusion based routing protocol is modified such that only routers retransmit the interest which minimizes the routing overhead. The BPS-MAC protocol uses three consecutive backoff preambles with a maximum number of four slots.

3.4. Scenario A

The introduced passenger monitoring application does not require a large amount bandwidth since some of the monitored characteristics, e.g. seatbelt fastened or unfastened, are logical. However, advanced monitoring features such as temperature or humidity can be considered. Furthermore, the sensed values are not time-critical. In scenario A, the nodes follow the low traffic pattern of application A which is introduced in Table 3. Figure 8a shows the average end-to-end delay between the nodes and the sink depending on the number of rows in the plane. The figure reveals that the end-to-end delay increases non-linearly which is the consequence of the multi-hop communication.

Moreover, the figure points out that the delay of the BPS-MAC protocol is higher compared to Zigbee if the number of rows is larger than 8. Nonetheless, the average end-to-end delay of the BPS-MAC protocol remains lower than 0.35 seconds even for the 40 row scenario which is

Pattern Name	Parameter	Distribution	Range / Values
Application A	Packet IAT	uniform	[9.99; 10.01] s
	Packet Size	constant	256 bit
	Start Time	uniform	[80;90] s
	Number of Rows	-	[8;16;24;32;40]
Application B	Packet IAT	uniform	[9.99; 10.01] s
	Packet Size	constant	256 bit
	Start Time	uniform	[80;81] s
	Number of Rows	-	[8;16;24;32;40]
Application C	Packet IAT	uniform	[3.95; 4.05] s
	Packet Size	constant	1024 bit
	Start Time	uniform	[80;84] s
	Number of Rows	-	[8;16;24;32;40]

Table 3. Traffic Pattern

(a) Delay   (b) Packet Loss
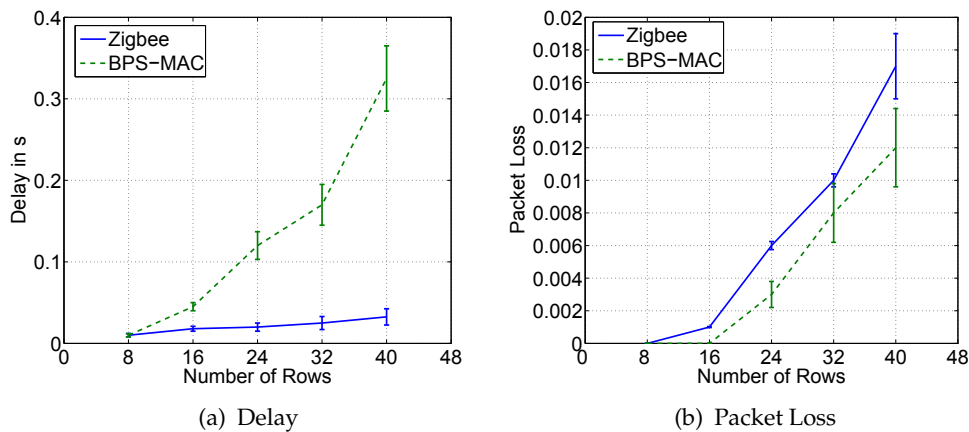
Figure 8. Application A - Performance depending on the Number of Rows

quite acceptable for this kind of application. The BPS-MAC protocol achieves a lower packet loss than Zigbee in scenario A as shown in Figure 8b due to the fact that the medium access procedure is optimized for synchronous medium access. The probability increases that two or more nodes start their data transmission within an interval that is shorter than the CCA delay of the low power transceiver in- creases with the number of nodes in the networks. As a result, the packet loss increases almost linearly for both protocols but still remains below 2 percent. Therefore, both protocols represent an acceptable solution for application A.

3.5. Scenario B

Scenario B uses almost the same traffic pattern as scenario A. The only difference lies in the fact that the offset of the traffic pattern only varies uniformly distributed by 1 second. Thus, the probability that two nodes access the medium within an interval that is shorter than the CCA delay and the turnaround time is very high. The average end-to-end delay of the different protocols depending on the number of rows is shown in Figure 9a. Both protocols achieve a low delay for scenarios in which the number of rows remains below 24. The delay sharply increases if the number of rows exceeds 24 as a consequence of the multi-hop communication and the highly correlated traffic.
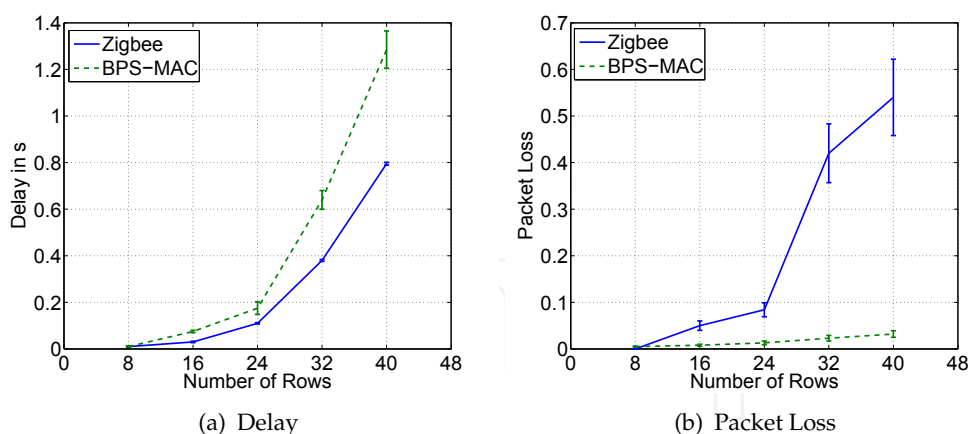
(a) Delay   (b) Packet Loss

Figure 9. Application B - Performance depending on the Number of Rows

Figure 9b shows a similar picture for scenarios with less than 24 rows. An extra ordinary high packet loss can be mentioned for the Zigbee protocol which results from the highly correlated traffic. Zigbee is not able to resolve the contention in this case due to the fact that the protocol is not addressing the problem caused by the CCA delay and the turnaround time. In contrast to Zigbee, the packet loss of the BPS-MAC remains on a low level such that it only increases to a maximum of 2 percent for the 40 row scenario.

3.6. Scenario C

In scenario C the performance of the protocols is simulated under a higher traffic load. The nodes in network generate traffic according to the traffic pattern of application C shown in Table 1. The traffic load is ten times higher than the load that is generated by application A or application B. Thus, the overall generated traffic load is 61.4 kB/s for the 40 row scenario. However, this calculation excludes the traffic that is required for forwarding data. It has to be kept in mind that some nodes require up to four hops to reach the sink in the 40 row scenario.
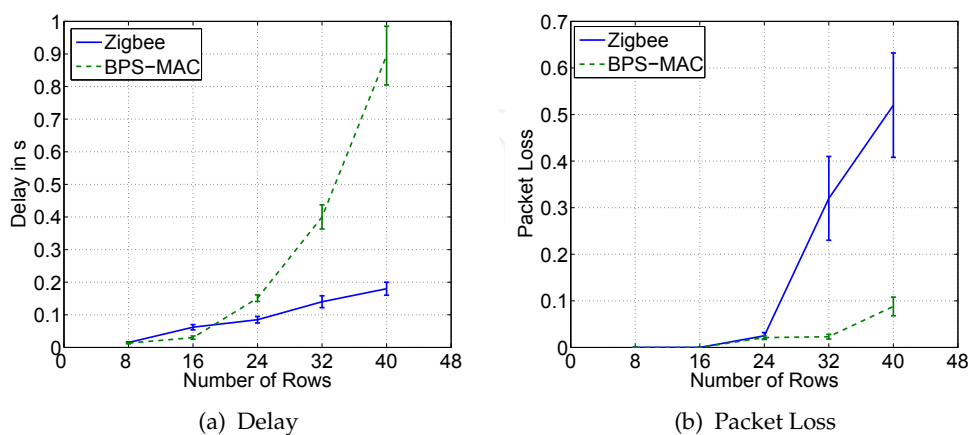

(a) Delay   (b) Packet Loss

Figure 10. Application C - Performance depending on the Number of Rows

Figure 10a shows the average end-to-end-delay in scenario C depending on the number of rows. The figure reveals that the BPS-MAC protocol achieves a slightly lower delay than Zigbee as long as the number of rows is smaller or equal than 16. The delay of Zigbee increases

almost linearly while the slope of the delay graph of the BPS-MAC protocol shows exponential characteristic. This slope results from the high utilization of the medium and the large number of nodes in the network. Nonetheless, the average delay of the BPS-MAC protocol remains below one second.

The packet loss shown in Figure 10b points out that the BPS-MAC protocol in combination with a directed diffusion based routing protocol provides a better solution than Zigbee for scenario C. The figure indicates that Zigbee is not able to handle a network that is larger than 24 rows if the nodes generate traffic according to application C. In this case, the high traffic load in combination with the correlated traffic limit the performance of Zigbee since the MAC does not address the CCA delay and the turnaround time explicitly. The packet loss of the BPS-MAC protocol increases to approximately 2 percent in the 32 row scenario which is sufficient for non-mission critical data. If the number of rows exceeds 32 the packet loss of the BPS-MAC protocol increases to 9 percent as a consequence of the high utilization.

4. Implementation issues of preamble-based MAC protocols

Two communication issues are mainly responsible for the low performance of MAC protocols in WSNs. The first issue is represented by the interval that low-power transceivers require to switch between receiving and transmitting and vice versa. Thus, the switching time which is in the following referred to as turnaround time, specifies the time between the arrival of a packet and the beginning of the corresponding response [34]. During this time interval the transceiver is not able to detect the start of other transmissions.

The second issue is called Clear Channel Assessment (CCA) delay. The CCA delay specifies the interval that a transceiver requires to detect a busy medium provided that the transceiver is already in receive mode. A transceiver is not able to reliably detect the transmission of another node if the transmission has been started within an interval that is shorter than the CCA delay. A closer look is taken on the impact of the turnaround time and the CCA delay on the MAC performance in the following two subsections.

Another factor that limits the performance of MAC protocols in WSNs is represented by the limited hardware resources. Especially, the small receive buffer and the applied operating system have to be taken into account when designing preamble sampling protocols that rely on short preamble transmissions. As a consequence of frequent short preambles, the probability of buffer overflows increases which leads to loss of information.

4.1. Impact of the turnaround time

The turnaround time of transceivers has a direct impact on the efficiency of MAC protocols. However, the impact on the performance depends on the medium access procedure which is used by the MAC protocol. The importance of the turnaround time was first addressed in [35] by Pablo Brenner. In this work, he evaluated the wireless access method and physical specification of the IEEE 802.11 standard. The same topic is discussed in more detail by Johnson et al. [34] and Diepstraten [36] who describe the effect on the performance caused by several switching aspects. Diepstraten outlines the impact that the turnaround time has on the protocol efficiency. The efficiency decreases especially in the case that a quick mutual exchange of messages, e.g. RTS-CTS messages, data packets or short preambles with early acknowledgments, between the transmitter and the receiver is required. In addition, the time that a transceiver requires to switch from receive to transmit mode represents a vulnerable

period for MAC protocols which rely on the CSMA functionality since transceivers cannot detect any transmissions that start during the switching period [37, 38]. Therefore, the developers of a preamble-based MAC protocols have to choose the gaps between consecutive preambles with respect to the turnaround time of the wireless transceiver.

4.2. The problem of clear channel assessment delay

CCA is a logical function which returns the current state of the wireless medium. It is provided by almost any low-power transceiver for WSNs in order to support CSMA functionality to the MAC layer. However, the transceivers require a certain period of time depending on their current state to reliably determine the state of the medium.

The CCA delay becomes the dominating performance limitation factor [39] for low-power transceivers which have a relatively high CCA delay compared to IEEE 802.11 transceivers. Typical low-power transceivers, like the CC2400 [40] and the CC2520 [41] (Texas Instruments) or the AT86RF231 [42] (ATMEL), have to listen to the medium for duration of 8 symbol periods to reliably detect an ongoing transmission. The chips average the Received Signal Strength Indication (RSSI) over the last 8 symbols in order to decide whether the channel is assumed to be busy or idle.

Technical aspects, like the CCA delay of low-power transceivers which have a large influence on the performance of wireless communication in sensor networks, are usually neglected. The impact of CCA delay on IEEE 802.15.4 networks is described by Kiryushin et al. [39]. The focus of their work lies on real world performance of WSNs and describes the impact of different kinds of communication aspects. Bertocco et al. [43] have shown that the performance of a wireless network can be improved by minimizing the CCA threshold. Nevertheless, the minimization of the threshold requires great knowledge of the radio channel, e.g interference and background noise, since a too small threshold will result in false positives which will significantly decrease the throughput. Thus, nodes will not transmit any data due to the fact that they falsely assume the channel to be busy. The latest generation of low-power transceivers supports different kinds of CCA methods. An intelligent cross-layer approach which takes advantage from different CCA methods is introduced by Ramachandran and Roy [44]. Their idea is to dynamically adapt the CCA method and parameters depending on the current channel conditions and the upper layer parameters.

4.3. Architecture of low-power transceivers

Wireless sensor nodes are very limited in terms of computational power and memory. The small receive buffer of low-power transceivers has to be considered when developing a preamble-based MAC protocol. Typical low-power transceivers, like the TI's CC2400 [40] and ATMEL's AT86RF231 [42], are only equipped with a 128 byte RXFIFO. The RXFIFO of the CC2500 [41] transceiver family is even limited to 64 bytes. Therefore, a received frame has to be immediately read from the FIFO in order to avoid buffer overflows caused by consecutive transmissions which would lead to loss of information. This issue can become a major problem for non real-time operating systems such as TinyOS which is only able to handle up to $\approx$170 packets per second. However, this packet reception rate only applies for small packets with a size of less than approximately 30 bytes. Moreover, there should no other time-consuming tasks be running on the sensor node. Otherwise, the packet reception rate drops down significantly as a result of the non-preemptive task scheduler.

4.3.1. Performance limitation factor - RXFIFO

In the following a brief introduction of the packet reception procedure for the CC2420 is given to provide MAC protocol designers useful information regarding the implementation. Upon detection of the Start Frame Delimiter (SFD) field, the chip begins to buffer the received data in its 128 byte RXFIFO [40]. In case the default Auto Cyclic Redundancy Check (AUTOCRC) settings are not changed, the chip replaces the first byte of the Frame Check Sequence (FCS) with a RSSI value estimated over the first 8 symbols after the SFD field. The second FCS byte is replaced by a 7 bit correlation value used for Link Quality Indication (LQI) computation and by a 1 bit field which indicates whether the frame was correctly received. The resulting data frame is shown in Figure 11.
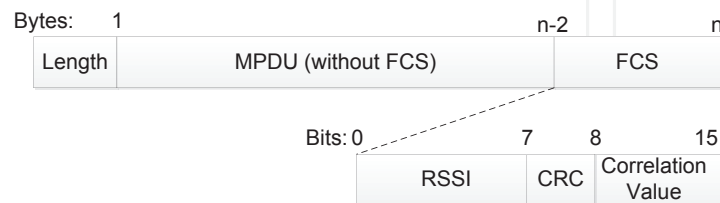

Figure 11. Data Frame in RXFIFO

The main limitation of this strategy is that damaged frames remain in the RXFIFO until they are read. In case of an overflow, the chip is not able to receive data until all correctly received frames are read and the buffer is flushed. Furthermore, the CC2420 does not protect the length field of the physical header. If the field is damaged and indicates, for example, that the stored frame is larger than the default frame size, TinyOS will *immediately* flush the buffer regardless of whether it contains correctly received frames since it does not know when the next correctly received packet starts. This means that if a MAC protocol fails to recognize a busy channel, a possible frame collision may cause correctly received frames to be flushed at the receiver before they are forwarded to the application. Listing 1 describes the reception routine in detail.

```
async event void RXFIFO.readDone (...){
    ...
    if (rxFrameLength + 1 > m_bytes_left) {
      flush ();
    }
    else {
      if ( !call FIFO.get() && !call FIFOP.get() ) {
        m_bytes_left -= rxFrameLength + 1;
      }
      if(rxFrameLength <= MAC_FRAME_SIZE) {
        // further frame processing
      }
      else {
        flush ();
      }
    }
    ...
}
```

Listing 1. Frame Length Field Processing

In general, a frame stored in the RXFIFO is read in three steps. The first step involves the interpretation of the first byte, which represents the length field, to detect the end of the frame. The second step includes the processing of the FCF header. During this phase the receiver may generate an acknowledgment when the acknowledgment request bit is set. The last step is needed to determine whether the received frame is correctly received and to signal reception to the upper layer components.

After evaluation of the length field, TinyOS tries to determine whether the received frame has a size larger than the RXFIFO. If this condition is true, the `flush()` function, which immediately erases the receive buffer, is called. Note that TinyOS uses the variable `m_bytes_left` to store the size of the buffer. This variable is initialized with a value of 128, but is decremented when an overflow occurs. With each frame which is still in the RXFIFO `m_bytes_left` gets decremented until the last incomplete frame. For this frame, the condition `rxFrameLength + 1 > m_bytes_left` is true and the queue is flushed. This action is required to enable reception of new data and reset `m_bytes_left`.

TinyOS checks whether the frame size is smaller than `MAC_FRAME_SIZE`. If the frame size is larger, the received frame is assumed to be corrupted and the RXFIFO is flushed. Thus, frames that were received correctly but have arrived after the corrupted frame will be lost.

4.3.2. Preamble transmission

Buffer overflows represent a serious problem in dense wireless sensor networks with event-driven traffic due to the fact that nodes often try to retransmit lost data. Moreover, frequent transmission of preambles increases the utilization of the medium and the probability of buffer overflows in the receiver. Before writing a packet in the receive buffer, a transceiver reads the SFD flag of a received frame. The packet is only stored in the receive buffer if the SFD flag indicates a valid frame. Otherwise, the frame is silently discarded. However, an invalid frame is still detected by transceiver. Thus, a preamble that is transmitted with an invalid SFD flag can be used as reservation signal. On the other hand, useful information cannot be stored in the preamble since receiving nodes immediately discard the frame without further evaluation. Therefore, this mechanism cannot be applied for protocols, like XMAC or WiseMAC, which store information in the preamble.

5. Conclusion

Preamble sampling protocol have many interesting characteristics which are of special interest for WSNs with their low traffic load and very limited low-power devices. In this chapter, we have discussed several preamble-based medium access strategies which either relied on long or short strobed preambles. The strategies were categorized with respect to the type of preamble (short or long), the information stored in the preamble and additional functionality such as synchronization and contention resolution. Furthermore, we outlined the impact of the different preamble sampling strategies on the energy consumption by focusing on the resulting protocol overhead. After describing the basic principles of preamble sampling, a closer look on a selection of preamble-based protocols was given. Due to the fact that preamble sampling protocols are ideal candidates for energy-constraint WSNs that require QoS support, a brief introduction on QoS in WSNs was given. Preamble sampling represents additional protocol overhead which has to be taken into account when deploying preamble-based protocols in dense wireless networks. For this reason, we compared the performance of a typical preamble sampling protocol with a CSMA-based in a large wireless network with high

node density and event-driven data traffic. The results have shown that preamble sampling protocols usually have a higher delay compared to their CSMA-based counterparts. However, the preamble sampling protocols can be optimized and configured such that they achieve a higher reliability. Sensor nodes are usually very restricted in terms of memory which increases the probability of buffer overflows that lead to loss of information. This issue can be mitigated by setting the SFD flag of preambles to invalid if no information has to be stored in it.

Acknowledgements

Author details

Alexander Klein
Network Architectures and Services - Institute for Informatics, Technical University Munich, 85748 Garching, Germany

6. References

[1] A. El-Hoiydi. Aloha with preamble sampling for sporadic traffic in ad hoc wireless sensor networks. In *Proc. IEEE International Conference on Communications ICC 2002*, volume 5, pages 3418–3423, May 2002.

[2] Jason L. Hill and David E. Culler. Mica: A wireless platform for deeply embedded networks. *IEEE Micro*, 22(6):12–24, November 2002.

[3] I. F. Akyildiz, Weilian Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. *IEEE Communications Magazine*, 40(8):102–114, August 2002.

[4] I. Demirkol, C. Ersoy, and F. Alagoz. Mac protocols for wireless sensor networks: a survey. *Communications Magazine, IEEE*, 44(4):115 – 121, April 2006.

[5] P. Suriyachai, U. Roedig, and A. Scott. A survey of mac protocols for mission-critical applications in wireless sensor networks. *Communications Surveys Tutorials, IEEE*, PP(99):1 –25, 2011.

[6] M. Aykut Yigitel, Ozlem Durmaz Incel, and Cem Ersoy. Qos-aware mac protocols for wireless sensor networks: A survey. *Comput. Netw.*, 55:1982–2004, June 2011.

[7] Joseph Polastre, Jason Hill, and David Culler. Versatile low power media access for wireless sensor networks. In *Proceedings of the 2nd International ACM Conference on Embedded Networked Sensor Systems*, SenSys '04, pages 95–107, New York, NY, USA, 2004. ACM.

[8] Alexander Klein, Jirka Klaue, and Josef Schalk. BP-MAC: a high reliable backoff preamble MAC protocol for wireless sensor networks. *Electronic Journal of Structural Engineering (EJSE): Special Issue on Sensor Network for Building Monitoring: From Theory to Real Application*, -:35–45, December 2009.

[9] A. El-Hoiydi. Spatial TDMA and CSMA with preamble sampling for low power ad hoc wireless sensor networks. In *Proc. Seventh International Symposium on Computers and Communications ISCC 2002*, pages 685–692, July 2002.

[10] Alexander Klein. Bps-mac: Backoff preamble based mac protocol with sequential contention resolution. In *Proceedings of the 4th International Conference on Multiple Access Communications*, MACOM'11, pages 39–50, Berlin, Heidelberg, 2011. Springer-Verlag.

[11] S. Mahlknecht and M. Bock. Csma-mps: a minimum preamble sampling mac protocol for low power wireless sensor networks. In *Factory Communication Systems, 2004. Proceedings. 2004 IEEE International Workshop on*, pages 73 – 80, September 2004.

[12] A. Bachir, D. Barthel, M. Heusse, and A. Duda. Micro-frame preamble mac for multihop wireless sensor networks. In *Communications, 2006. ICC '06. IEEE International Conference on*, volume 7, pages 3365–3370, June 2006.

[13] A. M. Firoze, L. Y. Ju, and L. M. Kwong. Pr-mac a priority reservation mac protocol for wireless sensor networks. In *Proc. Int. Conf. Electrical Engineering ICEE '07*, pages 1–6, 2007.

[14] Rebecca Braynard, Adam Silberstein, and Carla Ellis. Extending network lifetime using an automatically tuned energy-aware mac protocol. In *Proceedings of the Third European conference on Wireless Sensor Networks*, EWSN'06, pages 244–259, Berlin, Heidelberg, 2006. Springer-Verlag.

[15] Kai-Juan Wong and D. K. Arvind. Speckmac: low-power decentralised mac protocols for low data rate transmissions in specknets. In *Proceedings of the 2nd international workshop on Multi-hop ad hoc networks: from theory to reality*, REALMAN '06, pages 71–78, New York, NY, USA, 2006. ACM.

[16] E.-Y.A. Lin, J.M. Rabaey, and A. Wolisz. Power-efficient rendez-vous schemes for dense wireless sensor networks. In *Communications, 2004 IEEE International Conference on*, volume 7, pages 3769 – 3776, June 2004.

[17] Michael Buettner, Gary V. Yee, Eric Anderson, and Richard Han. X-MAC: A short preamble MAC protocol for duty-cycled wireless sensor networks. In *SenSys '06: Proceedings of the 4th International Conference on Embedded Networked Sensor Systems*, pages 307–320, New York, NY, USA, 2006. ACM.

[18] C.J. Merlin and W.B. Heinzelman. Schedule adaptation of low-power-listening protocols for wireless sensor networks. *Mobile Computing, IEEE Transactions on*, 9(5):672 –685, May 2010.

[19] Xiaolei Shi and G. Stromberg. Syncwuf: An ultra low-power mac protocol for wireless sensor networks. *Mobile Computing, IEEE Transactions on*, 6(1):115 –125, Januar 2007.

[20] A. El-Hoiydi and J.-D. Decotignie. WiseMAC: An ultra low power MAC protocol for the downlink of infrastructure wireless sensor networks. In *Proc. Ninth International Symposium on Computers and Communications ISCC 2004*, volume 1, pages 244–251, June 2004.

[21] M. Anwander, G. Wagenknecht, T. Braun, and K. Dolfus. Beam: A burst-aware energy-efficient adaptive mac protocol for wireless sensor networks. In *Networked Sensing Systems (INSS), 2010 Seventh International Conference on*, pages 195 –202, june 2010.

[22] C. Cano, B. Bellalta, A. Sfairopoulou, and J. Barcelo. A low power listening mac with scheduled wake up after transmissions for wsns. *Communications Letters, IEEE*, 13(4):221 –223, april 2009.

[23] Philipp Hurni and Torsten Braun. Maxmac: a maximally traffic-adaptive mac protocol for wireless sensor networks. In *Proceedings of the 7th European conference on Wireless Sensor Networks*, EWSN'10, pages 289–305, Berlin, Heidelberg, 2010. Springer-Verlag.

[24] C. Cano, B. Bellalta, A. Sfairopoulou, and M. Oliver. Low energy operation in wsns: A survey of preamble sampling mac protocols. *Computer Networks*, 55(15):3351 – 3363, 2011.

[25] C. C. Enz, A. El-Hoiydi, J.-D. Decotignie, and V. Peiris. WiseNET: An ultralow-power wireless sensor network solution. *Computer*, 37(8):62–70, August 2004.

[26] S. Blake, N. Carlson, Z. Wang, and W. Weiss. An architecture for differentiated services. RFC 2475, 1998.

[27] R. Braden, D. Clark, and S. Shenker. Integrated Services in the Internet Architecture - An Overview. RFC 1663, June 1994.

[28] A. Muneb, Umar Saif, A. Dunkels, T. Voigt, K. Römer, K. Langendoen, J. Polastre, and Z. A. Uzmi. Medium access control issues in sensor networks. *SIGCOMM Comput. Commun. Rev.*, 36(2):33–36, 2006.

[29] B. C. Donovan, D. J. Mclaughlin, M. Zink, and J. Kurose. Western massachusetts off-the-grid radar technology testbed. In *Proc. IEEE Int. Geoscience and Remote Sensing Symp. IGARSS 2008*, volume 5, 2008.

[30] Omprakash Gnawali, Rodrigo Fonseca, Kyle Jamieson, David Moss, and Philip Levis. Collection tree protocol. In *SenSys '09: Proceedings of the 7th ACM Conference on Embedded Networked Sensor Systems*, pages 1–14, New York, NY, USA, 2009. ACM.

[31] OPNET. Technologies, inc., OPNET modeler, university program, http://www.opnet.com/services/university/, May 2010.

[32] ns 2. Network simulator, http://nsnam.isi.edu/nsnam/, May 2010.

[33] Chalermek Intanagonwiwat, Ramesh Govindan, and Deborah Estrin. Directed diffusion: a scalable and robust communication paradigm for sensor networks. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 56–67, New York, NY, USA, 2000. ACM.

[34] E. E. Johnson, M. Balakrishnan, and Zibin Tang. Impact of turnaround time on wireless MAC protocols. In *Proc. IEEE Military Communications Conference MILCOM 2003*, volume 1, pages 375–381, October 2003.

[35] Pablo Brenner. The importance of the tx-rx switching time on the mac protocol, 1993.

[36] Wim Diepstraten. The importance of short rx-tx turnaround time, September 1993.

[37] G. Chalhoub, N. Hadid, A. Guitton, and M. Misson. Deference mechanisms significantly increase the MAC delay of slotted CSMA/CA. In *ICC*, pages 1–5, June 2009.

[38] A. Koubaa, M. Alves, and E. Tovar. A comprehensive simulation study of slotted CSMA/CA for IEEE 802.15.4 wireless sensor networks. In *IEEE International Workshop on Factory Communication Systems (WFCS)*, pages 1–10, July 2006.

[39] A. Kiryushin, A. Sadkov, and A. Mainwaring. Real-world performance of clear channel assessment in 802.15.4 wireless sensor networks. In *Proc. Second International Conference on Sensor Technologies and Applications SENSORCOMM '08*, pages 625–630, August 2008.

[40] Chipcon. Chipcon SmartRF CC2400 datasheet rev. 1.3, http://www.ti.com/, March 2006.

[41] Chipcon. Chipcon SmartRF CC2520 datasheet rev. 1.3, http://www.ti.com/, 2007.

[42] Atmel. AT86RF231 datasheet rev. b, http://www.atmel.com, February 2009.

[43] M. Bertocco, G. Gamba, and A. Sona. Experimental optimization of CCA thresholds in wireless sensor networks in the presence of interference. In *Proc. of IEEE EMC Europe 2007 Workshop on Electromagnetic Compatibility*, June 2007.

[44] I. Ramachandran and S. Roy. WLC46-2: On the impact of clear channel assessment on MAC performance. In *Proc. IEEE Global Telecommunications Conference GLOBECOM '06*, pages 1–5, November 2006.