Mac Protocols for Wireless Sensor Networks

Hans-Christian Halfbrodt

Advisor: Pardeep Kumar

Institute of Computer Science
Freie Universität Berlin, Germany

halfbrodt@inf.fu-berlin.de

January 2010

Contents

I. Abstract

This work presents different MAC protocols for wireless sensor networks and compares them to each other. Therefore it starts with an introduction in wireless sensor networks. It will explain the important role of MAC protocols for energy saving and why currently common protocols don't fit for the actual requirements. After presenting a selection of MAC protocols their properties will be compared to each other.

II. Introduction

Motivation

Today it is possible to build very small hardware devices with wireless communication for monitoring and measuring miscellaneous values of the environment. There are a lot of application areas. One is monitoring buildings and their surrounding terrain. A common solution is to install wired sensors. Wired solutions have a continuous energy supply, but it is very expensive to lay or replace cables for them. Therefore a wireless solution with a battery which can be completely exchanged periodically is more eligible, but only if the exchange period is not too small. An other utilization for wireless sensors is medical observation. Patients, who have for example a pacemaker or comparable medical devices, want to move as free as possible, but the medical devices have to exchange information about their health status. A small wireless sensor can realize this task. It could send an emergency signal in case and with a long battery lifetime it needs less servicing. That seems more useful than a large or even wired device. Other applications can report position or traffic flow informations. This may be helpful for congestion prevention and accidents warnings. Today RFID is a common technology for product identification in warehouses. But at a container harbour are thousands of big containers to monitor. It is not possible for a worker to just go around and scan every RFID chip. Wireless sensors could provide information about container contents and status to a central instance. In agriculture sensor nodes could monitor the growth of field crops on large areas. They could check if the ground is humid and can even report statistics about the fall of rain. There are a lot of possible applications for the general concept of wireless sensor nodes, but they are limited by the technical specifications.

WSN Background

The devices are typically equipped with a processor, memory, sensors and communication devices with radio systems. All these functions can be put together in one microchip. Wireless devices are very flexible as long as the power supply, usually a battery, provides enough energy. But charging or replacing a battery can be very expensive and complicated. That is why energy saving is so important. Usually the sensor nodes don't need to stay active continuously, they only transmit data periodically. Especially wireless communication consume a lot of energy by amplifying received signals or sending data. The radio units have generally three states: Transmitting signals costs most energy. Receiving signal doesn't need the same amount of energy, but it also needs a lot. The Idle state needs (nearly) no power. To be reliable for network peers the devices have to interpret the received radio signal even if there is nothing transmitted. Based on these Informations the idea is to put the devices to sleep when they are not used and let them periodically wake up. That is not as easy as it sounds. To realize this idea the communication partners have to be synchronized at least for each single transmission. The wireless extension is managed by a media access control protocol. The task of this protocol is to transport local data to a target peer over the physical layer, the networking hardware.

Requirements for Wireless Network MAC Protocols

A Wireless Medium is a shared medium. This means one instance in the signal range is allowed to send data at most. This data can be received by one or more attendees. The MAC Protocol has to transmit given information frames over this shared medium to a network peer. To do so it is required that every network peer has an identifier. This is usually called a MAC address and has to be unique for the current network. It is even better if the address is global unique because adding or exchanging sensors in different networks might be possible. How this MAC address looks like is part of the MAC protocol definition. There should be a large range of addresses because the number of participants in the network may increase fast. The network size should be scalable, a small fixed limit of peers is not useful in general. Autonomy should be guaranteed. It would be too complicated if a human has to set up a lot of single parameters on the mac layer. It is also expected that the network is self organizing. Possibly new peers appear, others might disappear or the topology will be changed. A network has to be reliable. It is not useful if a user has no warranties for successful participation. These are basic properties which should be fulfilled by a MAC protocol.

Why WLAN IEE 802.11 is not usable for WSN

There are common MAC protocols for wireless communication. One popular is IEEE 802.11 used for wireless local area networks. WLAN is used for high speed data exchange. A typical bandwidth today is 54 Mbit per second and is theoretical possible up to 300 Mbit per second (IEEE 802.11n).

To be reliable here means especially be high available. It is not enough to say that every request will be handled eventually. Latency is important for reducing waiting periods, too. A user who requests a web page on his laptop wants to see it on his screen as soon as possible. Laptops and smart phones are typical examples for the utilization of WLAN. They have large batteries and they are easy to recharge. Because of these requirements WLAN radios are in listen mode when they are idle. Put to sleep, wake up and connect with a base station or peer would take to long and incoming traffic would not be noticed if not expected. Idle listen and receiving messages which were dropped should be avoided by sensor nodes. This is called overhearing. The devices named above are used at a limited area. They can be connected peer-to-peer or via a central access point. Sensor networks may be distributed on a larger area. It could be difficult to to provide a large number of wired access points. In sensor networks you typically have to transmit measured values. This means you have a many to one communication. These values are periodically updated. Their size is small, often a few bytes suffice. That is why the update interval is high in comparison to the time needed for transmission over the network. Most of the time there is no activity in the network. So always listening to the media would be to expensive in the view of energy costs. The basic idea is to shut the radios usually down and let them only wake up from time to time. One have to check for incoming data though. It may be possible that a node has to forward the data. Mobile phones or WLAN devices have only one hop. Sensor nodes may have many hops. For these reasons sensor nodes need specialized MAC protocols.

II. Presentation of Mac Protocols

S-MAC

This Protocol is based on the adaptive listening concept. Nodes are in sleep mode and listen periodically if there is a data transmission announced. In that way the virtual carrier sense can be used and the radio can remain turned off until the transmission of the neighbour is done. For synchronization nodes listen to and send routinely SYNC packets via broadcast. Because of the distributed ad-hoc structure there are nodes which can reach each other directly and nodes which can't. The groups of nodes which can reach each other are called virtual clusters. Nodes in the same virtual cluster synchronize each other. Nodes at borders of two clusters may have two wake up schedules. The clock drift between the peers is very small in comparison to the wakeup period. But to ensure a received message is complete nodes wait a short time value before sending. To avoid overhearing the transmission time is part of the announcement. There is no central access point, network peers communicate with each other. It follows that no instance configures the network, so every node has to detect its communication peers. Neighbour detection is expensive. A node with no neighbours performs the detection more often than a node with one or many neighbours. There is is no fairness guarantee. To prevent starvation the carrier sense time is randomized in a certain time window. It is possible that sources can't reach the destination directly. Then the data will be transmitted over multiple hops, nodes have to forward data (message passing). To reduce the latency nodes which overhear a neighbours transmission wake up short time before the end of the transmission to be prepared for message passing. Because of limited memory and possible different memory sizes in a heterogeneous network S-MAC support message fragmentation.

B-MAC

B-MAC is designed for an Ad-Hoc network of nodes with N-sender to 1-receiver transmissions. The basic idea of B-MAC is to keep the protocol simple. That allows very small implementations, an important point because of the limited available memory. Like the other protocols B-MAC uses periodically sleep/wakeup cycles. The mechanism used here is called Low Power Listening. LPL means in the wakeup time the node listens for incoming data transmissions. If there is no data received, called a “false positive”, a timeout interrupts the listen state. Otherwise the node waits for complete packet transmission. To ensure that the received packet is complete from the beginning there is a preamble time of 100ms added after the wakeup. Fairness is not guaranteed by LPL. The sleep periods of the nodes can differ to each other, B-MAC is asynchronous. When there is data to send a node switches the radio mode and starts to send an announcement. This announcement must be long enough to make sure that the receiver notices, even if the receiver starts sleeping at the beginning. Afterwards the sender transmits the target address and starts sending data. Asynchronous networks don't need complicated and expensive synchronization methods. There is no data fragmentation used in B-MAC. This would be more complicated to coordinate and B-MAC expects short messages like the ones commonly used for sensor informations. An other concept to reduce the amount of needed energy is clear channel assessment (CCA). This is used for clear channel detection. For energy reduction a better separation between signals and noise on the channel is useful. Therefore the noise must be analysed. In case of a false positive a sample was put into a queue. It makes sense to capture and analyse more than one sample because the noise caused by the environment changes continuously. An optional feature is using acknowledgements. B-MAC has an application interface for flexible configuring parameters like this. Other options are for example the check interval. A good value for this sometimes depends on the use case so this can be adjusted by a higher layer application.

WiseMAC

WiseMac is an infrastructure protocol. It assumes there is one central unit with unlimited energy supply and connection to an other high speed network e. g. Ethernet to exchange data packages. That is why this unit is called access point. Because of the independence to batteries the access point should manage the network. Therefore it has a table containing the wakeup times for every known node. That reduces the needed listening time. These times are part of acknowledgement packets send from the nodes. If the access point has information for a specific node it can be notified as soon as possible. There must be a little delay before message passing because of the possible clock drift to the nodes. The messages are expected to be short for sensor nodes. The base station handles one message after the other. Synchronized nodes would have to wait except for one node. That is why the wakeup schedules of the nodes are asynchronous. The packet header contains a frame pending bit. It indicates there is more data waiting. After sending an acknowledgement the node stays awake if the the bit is set. The sender sends the second packet ongoing to the received ACK-packet.

IEEE 802.15.4

IEEE 802.15.4 defines another mac protocol for wireless sensor networks. The protocol is based on CSMA/CA [6]. CSMA stands for carrier sense multiple access. A node which want to start a transmission first listens for a short amount of time to the media if there is traffic on the channel. The value of listen duration can be changed. If there is traffic the transmission has to wait. Otherwise the transmission can be started. The extension CA means collision avoidance. A node announces a packet transmission to its neighbours. Then the other nodes know that the channel is used. This is used by the other WSN MAC protocols and IEEE802.11, too. IEEE802.15.4 uses no RTS/CTS (request to send / clear to send) although it is a common combination. Using RTS/CTS means that the data source sends a channel request message and the destination answers with a clear / ready message. The reason for not using RTS/CTS is overhead prevention. The MAC header has only 127 bytes, so additional flags are avoided. It is possible to use peer-to-peer connections or a star topology. The default is star topology with a central instance. There are two types of nodes: Full function devices and reduced function devices. Reduced function nodes are only able to process their own data. They only have few resources like memory and small energy capacities. Full functional nodes are better equipped and can relay messages for other devices.

X-MAC

X-MAC is meant for ad-hoc structure, too. It uses asynchronous wake-up schedules like B-MAC. X-MAC tries to improve B-MAC by sending more intelligent announcements. Therefore the announcements include the target address. There is not a large announcement for a transmission, but instead short repeated messages were send. That is how the overhearing is reduced. Nodes who are not addressed as targets can go to sleep after having received one short message. An other enhancement is that there are short pauses between these preamble messages. This way the receiver hasn't to wait for the full time period and can send an Acknowledgement to inform the sending peer about its attendance and the data transmission can begin with a reduced preamble time. If a second sender observes an announcement to the same target it waits for the finished transmission and a randomized short period in addition. Then it sends its data direct without an own announcement. To ensure this process works receivers usually wait an extra amount of time for incoming data after a packet was received. This amount has to be at least the maximum randomized time of the second sender. The randomization is needed for conflict avoidance reasons. There may be others who want to communicate, too.

III. Comparison

S-MAC and B-MAC

Both, S-MAC and B-MAC, were implemented and tested [3]. For test implementation TinyOS [8] is used, a very small operation system optimized for integrated devices. It is written in C. As test hardware is Mica2 Motes used. S-MAC has a lot of features for synchronization optimization, while B-MAC seems to be more simple. That is why the implementation of S-MAC needs more memory. The test implementation by Polastre, Hill and Culler of S-MAC needs more than 6200 bytes. On the contrary B-MAC with LPL, Acknowledgements and CTS/RTS needs less than 4700 bytes. The energy consumption can be measured in energy per data (e. g. Joule per byte). If the radio device is never sleeping the energy per byte increases linear to the pause between messages because of the increased idle time. S-MAC without adaptive listening needs more energy with decreased data rate too, but compared to the idle listen mode it is only a very small rise. This can be explained by the overhead caused by synchronization and periodically media checking. Adaptive listen can reduce the energy waste in high traffic loads, but in cases of lower traffic loads the advantage is small. An important fact for a multi hop network is the latency. Latency is expected to increase with every hop. Therefore Ye, Heidemann and Estrin measured latency in comparison to the hop count (Figure 1). As expected the lowest latency occurs with no sleep. Without adaptive listen latency

rises fast. The exchange of short informations over many hops takes much time. Here adaptive listen can show a real improvement. Because of the idea of being prepared if a neighbour receives a message which he has to forward the latency increasing rate is nearly the same as by idle power on. Only at the first hop we have to wait for the listening period. There latency is the same as without adaptive listen. This causes a little shift of the overall latency with adaptive listening.
S-MACs energy consumption increases linear to the data rate. B-MACs energy use increases of course with higher data rates too, but it is below S-MACs. A reason is that B-MAC has no synchronization between the nodes, this causes a large overhead. In the test case from Polastre, hill and Cullar were up to 20 nodes used. For different variants of B-MAC depending on the number of nodes the maximum throughput decreases, while S-MAC throughput seems to be continuously with increasing node count (Figure 2). Nevertheless B-MAC without ACK and RTS-CTS is always faster for the tested range than S-MAC with unicast, while the energy consumption of B-MAC is still lower. With throughput up to 4.5 times of S-MAC it seems that B.-MAC outperforms. But this behaviour might changes for very large networks. Assuming most traffic is unicast traffic and you have a large area for these big networks, so that every node can reach only a small group of neighbours the behaviour for these small sub networks are probably the same as for a small network. One very important factor for the performance is the network topology. It might be that the performance of S-MAC in comparison to B-MAC increases if every node reaches only two neighbours like a chain.

WiseMAC and X-MAC

WiseMAC is based on the concept of IEEE802.15.4 with infrastructure topology. Because of the central communication control by the access point overhearing is minimized. Also there is no message forwarding by the nodes. That increases the lifetime of the nodes. The time spend waiting for ready peers is minimized too, because the central peer is able to listen always when it is idle. I assume WiseMAC using Acknowledgements for data transmission increase latency significantly as shown for other protocols.

X-MAC and B-MAC

X-MAC is based on the idea of B-MAC. To show the performance of X-MAC Buettner, Yee, Anderson and Han tested their implementation in comparison with a LPL based protocol similar to X-MAC. There is no direct comparison between X-MAC and B-MAC, but an LPL protocol similar to X-MAC may be comparable to B-MAC. To demonstrate the advantage of the strobed announcements Buettner, Yee, Anderson and Han set up a network where each node can reach all others. There are messages send to one destination periodically. The measured duty cycles of sending and receiving nodes are close to each other for the same protocol (Figure 3). The LPL protocol duty cycles increase significantly with the node density. Complementary the duty cycle of X-MAC increases very slow and is always below the one of LPL protocol. Because the usage time corresponds to the energy usage the result of power consumption per node in relation to the network density behave by the same scheme. This is expected from the optimized preamble communication. Nodes which are not affected in the current transmission can quickly go back to sleep. By the direct transmission of a third waiting node to the the target after a finished transmission without a preamble procedure time is reduced. Unfortunately there are no performance tests comparing this LPL protocol to X-MAC. With a reduced transmission it is expected that the latency shrinks while the throughput increases.

Conclusion

At my opinion there are many good ideas for intelligent energy reduction. But there is still optimization possible. Not only Wireless radios don't need to stay active all of the time, sensors are measuring for a short time and than they can sleep too. In these situation the whole device is idle and could go to sleep. To do so there could control mechanism accessible by the Mac protocol because typically the network is more frequently used than the sensor itself. A global control only by the operating system might cause overhead and delay. Forwarding packages consumes a lot of energy especially if there is a bottleneck in the topology. IEEE 802.15.4 proposes two types of nodes [7]. Only one of them is forwarding data. Maybe this idea can be extended. It seems that X-MAC and WiseMAC are currently good solutions, but this is only evaluated for small networks with 20 nodes or less. Tests with large networks are required to consolidate the choice of a MAC protocol for practical use. Especially for area or building observation and controlling it is possible that the number increases very fast and exceeds 20 nodes. Efficient protocols like B-MAC reduces their functionality and refer tasks to upper abstraction levels. The efficiency may decrease if the data transferred over the network increases because of the task shifting. I think there are still a lot of possibilities for improvement on MAC protocols for wireless sensor networks.

Figures

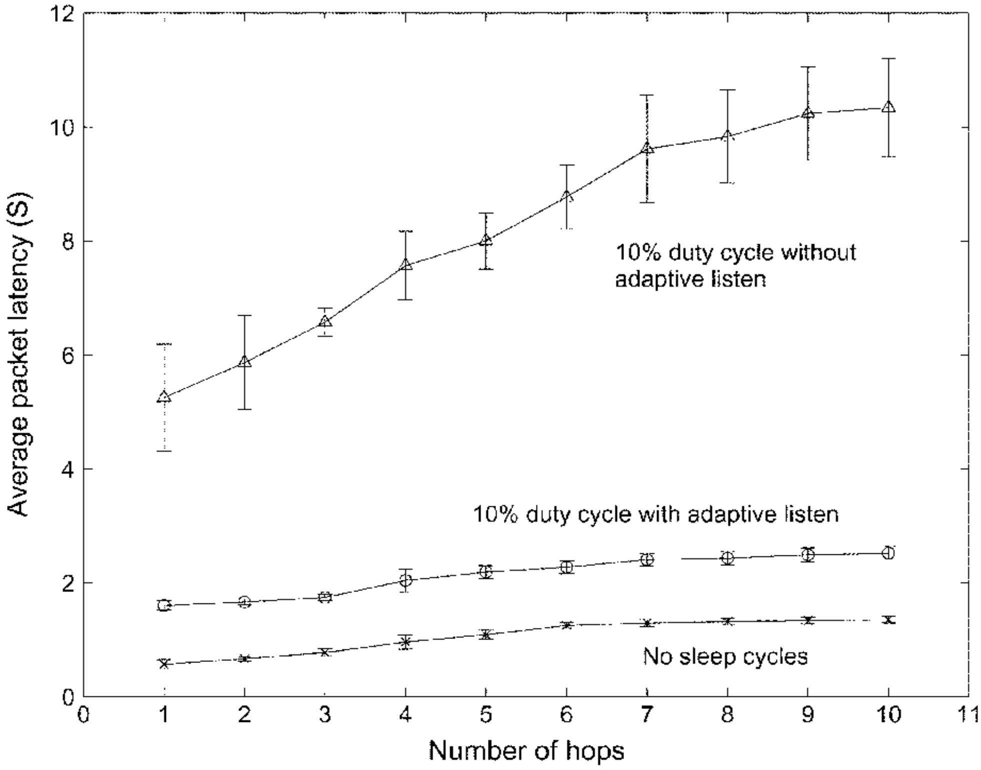

Figure 1: Latency of S-MAC with and without adaptive listening, published in [1]

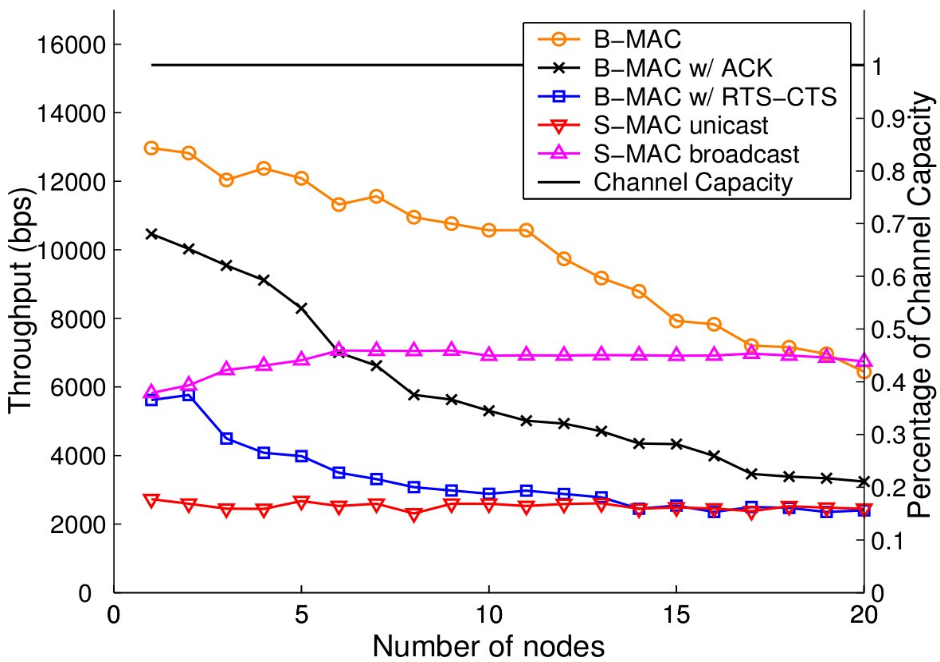

Figure 2: Throughput of S-MAC and B-MAC dependent on the Number of nodes, published in [3]

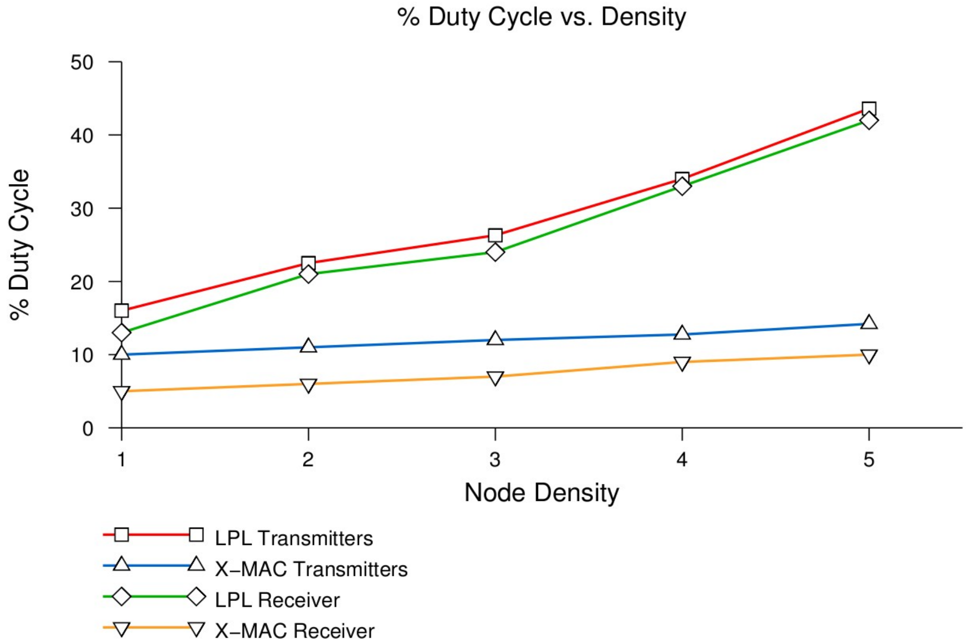

Figure 3: %Duty Cycle of X-MAC and compared LPL Protocol in dependence on Node Density, published in [5]

References

[1] W. Ye, J. Heidemann and D. Estrin, "Medium Access Control With Coordinated Adaptive Sleeping for Wireless Sensor Networks" IEEE/ACM Transactions on Networking, vol. 12, no. 3, June 2004

[2] A. El-Hoiydi and J.-D. Decotingie, "WiseMAC: An Ultra Low Power MAC Protocol for the Downlink of Infrastructure Wireless Sensor Networks", CSEM, Swiss Center of Electronics and Microtechnology, Inc., 2007

[3] J. Polastre, J. Hill and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks", SenSys'04, ACM 1-58113-879-2/04/0011, November 3-5, 2004
(cst berkley, jlh labs) ?

[4] IEEE, "Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)", IEEE Std 802.15.4-2003, 2003

[5] M. Buettner, G. Yee, E. Anderson and R. Han,"X-MAC: A Short Preamble MAC Protocol For Duty-Circled Wireless Sensor Networks", Department of Computer Science, University of Colorado at Boulder, CO [USA], May 2006

[6] B. Scheers, W. Mees and B. Lauwens, “Developments on an IEEE 802.15.4-based wireless sensor network”, Department CISS, Royal Military Academy, Belgium, published in Journal of Telecommunications and Information Technology, February 2008

[7] J.-S. Lee, “Performance Evaluation of IEEE 802.15.4 for Low-Rate Wireless Personal Area Networks”, IEEE Transactions on Consumer Electronics, Vol. 52, No.3, August 2006

[8] TinyOS Homepage, http://www.tinyos.net/, 01-15-2010