Medium Access Control (MAC) in Wireless Sensor Networks

Karl-F. Leiss
Betreuer: Dipl. Inf. Alexander Klein
Seminar Sensorknoten: Betrieb, Netze und Anwendungen SS2010
Lehrstuhl Netzarchitekturen und Netzdienste, Lehrstuhl Betriebssysteme und Systemarchitektur
Fakultät für Informatik, Technische Universität München
Email: leiss@in.tum.de

ABSTRACT
This paper gives an overview of the common Medium Access Controls (MAC) with respect to performance, latency, power consumption and security. Wireless MAC has to take care about harsh environment, limited power and often a big number of nodes to connect. This paper clearly emphasizes the properties of dynamic and static protocols with a short look into hybrid protocols. After explaining the fundamental aspects of wireless protocols, the main cause of energy waste as well as the limitations through the hardware will be reviewed. A survey on representative protocols is presented and the methods to lower collision probability are explained. Attacking scenarios and possible solutions are discussed at the end.

Keywords
Wireless, sensor, mac, contention, delay, latency, security

1. INTRODUCTION AND OBJECTIVES
Development of MAC in wireless sensor networks (WSN) became more and more important during the last years, since applications can benefit from wireless and energy efficient data exchange. The autonomous activity over long periods without any service access requires well designed sensor nodes. Nodes acting in an Ad-hoc (latin: for the moment) network are normally equipped with a small micro controller (uC), a radio transceiver, sensors and a battery pack. Some of the most common nodes are ScatterWeb [4], Mica 2 [9], Tmote Sky and Imote 2 [10]. The nodes preprocess and finally transmit the data. The knowledge of the hardware is especially needed in understanding the bottleneck of wireless communication. The number of nodes within a WSN and the generated traffic is variable. Therefore different solutions are necessary to cope with the data transmission. Energy consumption plays the most important role, if a node would not go to sleep, the lifetime decreases from a runtime of years to only a few days[3]. Herein comes the role of the MAC protocol which should give the best compromise in terms of throughput, latency, scalability and energy consumption. Section 3 gives a comparison of representative MAC protocols. After discussing the basics of MAC protocol design, a detailed look is taken on a particular protocol in section 4. WSN should not only be reliable but also be protected against external, unauthorized access. The term security in the contex of WSN means more than simple protection on the data. The Denial of Sleep attack will be explained in section 5.

2. MAC
First of all the term MAC has to be explained in detail. After that the basic communication issues of WSNs are reviewed.

2.1 Term definition and fundamentals
MAC is defined as the data link layer within the IEEE specified OSI model[6]. It defines the access and the arbitration of multiple nodes on a shared medium. Standards for wireless networks exist but they cannot be directly used for WSN as they are optimized for data throughput. High data throughput is accompanied by high energy consumption and less reliability of the link. The IEEE specifies the Carrier Sense Multiple Access (CSMA) approach[6]. CSMA is a basic scheme to handle the attempt of multiple nodes to send. Before data can be sent by a node the medium must be sensed. If there is no other transmission in process the node can start its own transmission. Therefore the node's transceiver has to switch from receive into transmit mode which takes between 2 and 6 milliseconds. The switching from one mode into another is called *turnaround*. The transmission delay on the wireless medium is bigger than on the wired medium. The reason is the propagation delay on the wireless medium. After the medium is sensed as free, transmission can start. If the medium is occupied a node has to wait until it is free. It is possible that two or more nodes may start their transmission in parallel on a free medium. Collisions will occur and the MAC protocol has to handle this state. In CSMA a scheduled resend is intended. Every node which detects a collision on a transmission attempt will resend the data later after a specific time interval. So the MAC protocol is occupied most of the time listening to the channel which consumes energy.

Hidden node is the naming for the 1 hop problem shown in the Figure 1. A hop is a station, the packet has to pass under its way to the receiver. Node C does not recognize a packet being sent from node A to node B. As the channel is clear for node C, it may start a transmission, too. Only node B will detect a collision but not the other ones. Exposed node problem occurs if another node D is a neighbor. Node C does not have a clear channel as it gets persistent traffic from the other nodes which results in waiting for the idle of the channel hence lowering the throughput. Listening consumes even more energy than the transmission of data. Internal setup of clock and oscillation circuit takes extra time[10].

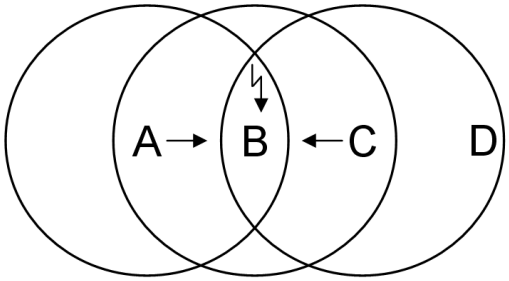

Figure 1: Hidden node problem caused by limited transmission and sensing range in WSN.

2.2 Communication issues

As discussed in the previous section, energy consumption is caused by the time duration spent on sending and receiving. Thus, the goal is to minimize this time. Nearly all WSN MAC protocols address this issue which can be divided into following sources:

- **Idle listening:** Only a small segment of the available bandwidth is really used for the raw data from attached sensors. Most of the time, the radio monitors the medium for being busy[10].
- **Overhearing:** A side effect of listening to incoming bits all the time is, that every message is processed whether the node is the intended receiver or not. Especially in dense networks where many nodes are in the transmission range of each other, the overhearing leads to a great minus in the energy asset[8].
- **Collisions:** In CSMA networks exist always the possibility of collisions even if a random backoff mechanism is used. More explanation on the backoff mechanism is given in Section 4.2. The problem is caused by the turnaround time during which no activity on the medium can be detected. Approaches for handshake like RTS/CTS [1] introduce additional overhead compared to the relatively small payload of the WSN packets [10]. Retransmitting packets can completely shut down the network's transport bandwidth in worst case.
- **Protocol overhead:** Headers for the MAC and control message data should be minimized to improve efficiency. A strategy to minimize the overhead is the aggregation of data. Buffering introduces some delay which can be compensated by reduced protocol overhead.

The first idea to improve the communication, was to listen to the channel only periodically. The problem with this idea is that a short data packet might not be recognized. Therefore a preamble at least as long as the sleep period must be put in front of the data packet. The Low Power Listening (LPL) protocol implements this approach.

[1]ready to send / clear to send

2.3 Performance limiting factors

A performance limiting factor is the Clear Channel Assessment (CCA) delay. This delay is the time a node in receiving mode needs, to clearly detect the channel state. At least eight bits have to be sampled to decide on the medium state. The delay period is 128us wide on a tranceiver with 76kbps[14]. The key parameters of three common transceivers are shown in a compressed form in the Table 1 [10]. Noticeable is the fact, that the modern Chipcon CC2420 transceiver from Texas Instruments draws more current in receiving path[14]. The specifications of the latest device, the CC2520, outperforms the CC2420 in terms of efficiency. The benefit of those newer transceivers is highlighted in Section 4.

Type	RFM TR 1000	CC1000	CC2420
Speed	10kbs	76kbs	250kbs
Sleep	2uW	100uW	60uW
Receive	12mW	36mW	63mW
Transmit	36mW	75mW	57mW
Setup	0.5ms	2ms	1ms

Table 1: WSN transceivers with their reference values

3. COMPARISON OF REPRESENTATIVE PROTOCOLS

Figure 2 classifies the most representative scheduled and random access protocols. In terms of complexity random access

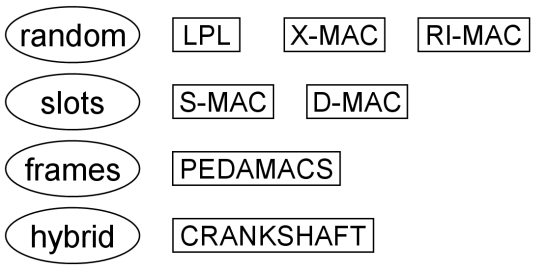

Figure 2: WSNs ordered by class

is the most simple approach. A technique called preamble sampling helps to save energy by sleeping most of the time. A wake up is periodically done to check for a preamble being sent by other nodes. Thus, the effort for carrier sense is shafted towards the sender. Slot based protocols divide their schedule into small segments. Inside these slots the message exchange can take place. Slots are the basis for frame based protocols. A frame is split into multiple slots. The slots inside a frame can have different functionality.

S-MAC

Sensor-MAC or S-MAC belongs to the slot based protocols. A fixed schedule accommodated by a sync packet, synchronizes the nodes to the slot structure. The sync packet contains the time stamp as broadcast permitting the other nodes to adjust their offset. Furthermore, S-MAC implements carrier sense and a RTS/CTS handshake to avoid collisions. Figure 3 illustrates the messaging scenario. Sender and receiver are only active during the data exchange period. It is also possible to determine slots for broadcast data. In

broadcast slots no RTS/CTS handshake exists. The message data can also be used to deploy a new schedule to the WSN which allows dynamical reconfiguration. The Carrier Sense in front of the SYNC and the RTS symbol is necessary to minimize collisions. After the Sender S has received the RTS symbol the data exchange can happen. White boxes are sent data, grey ones are received data packets[8].

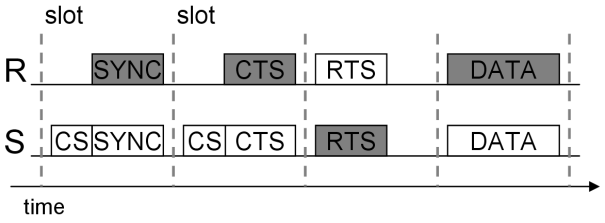

Figure 3: S-MAC slot based packet handling with carrier sense (CS)

D-MAC
Known as Datagathering MAC and a Time Division Multiple Access (TDMA) style MAC variant, D-MAC increases the usage of pure TDMA based protocols. TDMA is the opposite of CSMA. TDMA is based upon a static and predefined send/receive schedule. Slots are used for data exchange and synchronization of the nodes. In most sensor networks, the data packets from many sources are transmitted under involvement of neighbors to a sink. This topological appendage is known as convergecast traffic as the predominant part of the communication is unidirectional. The aim is to be energy efficient while achieving a low latency level. The slots are planned such that subsequent transmissions from hop to hop are appended slot by slot. Figure 4 demonstrates this scheme. During a receive period neighbors can have a

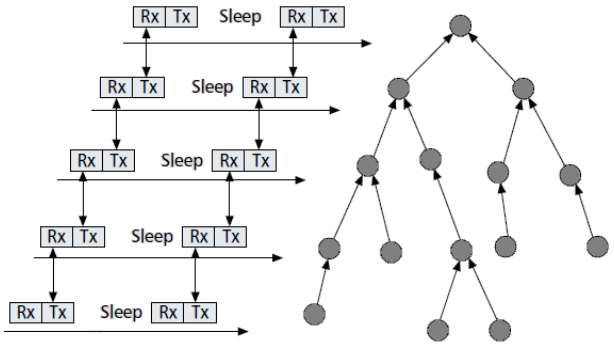

Figure 4: DMAC subsequent slot schedule beside data gathering tree

transmit period and therefore reduce the latency to the data sink. No unwanted sleep/wakeup periods are necessary for optimal latency. Every higher layer in the data gathering tree buffers data from lower nodes until next transmission slot. This is very efficient but not flexible. The drawback of D-MAC is the absence of a collision check. A collision may occur on a mobile network where nodes can move. It cannot be ensured that two or more nodes are sending within the same slot to the same receiver after they changed their place. This effect is likely to break up if the exact transmission path is not known in advance[8].

PEDAMACS
addresses a similar use case as D-MAC. The Power Effcient and Delay Aware Medium Access synchronizes the sink to all nodes implicating the deployment of a high power radio transceiver on the sink. As the sensor nodes are less powerful, a spanning tree has to be set up on initialization and nodes report back hop by hop. Once all information is gathered by the sink, it can compute the schedule based on the topology. The intended traffic pattern is convergecast. It is possible to repeat the initialization to compensate node movement or problems on the wireless link. With all the planing and setup the network is efficient but there are disadvantages. Introduced as TDMA based protocol, PEDAMACS uses CSMA during the initialization. In the initialization period are typically many broadcast frames being sent out which can lead to long initialization time. More over, PEDAMACS cannot guarante the sink will reach all nodes. Environmental circumstances may disrupt the service [8, 13].

Crankshaft
is a hybrid WSN MAC protocol, implementing both CSMA and TDMA in a new way. It is specifically designed for dense networks where the number of neighbor nodes is larger than ten. Instead of scheduling the slots of the sending node, the ones of the receiver are timed. Thus, a wake up is only necessary within the wanted receive slot. A simple algorithm allocates the receivers to the slots by node identifier modulo frame length. Crankshaft schedules the data exchange into frames which are divided into smaller slots. Two types of slots exist, broadcast and unicast slots. Broadcast slots are utilized for messages designated to all receivers, therefore all nodes have to wake up. On the other hand, unicast slots are only addressed to the receiver. Figure 5 shows a unicast slot. During the contention period in a such a slot, CSMA arbitration takes place. Sender S1 polls the channel (grey box) and starts to transmit his preamble P. Sender S2 also wants to transmit but before he has to poll the medium. Since preamble transmission from Sender S1 is already in progress, Sender S2 goes to sleep until his next scheduled slot. The intended Receiver R polls the slot, too. After the preamble is sent, the actual payload is transmitted and finally confirmed with an acknowledgment (ACK). So during the contention window all possible senders have to figure out whether they are allowed to send by using CSMA inside this TDMA scheduled unicast slot. Crankshaft reduces overhead especially for dense networks. It outperforms S-MAC [5].

X-MAC
This protocol belongs to the random access protocols shown in Figure 2. Previously talked about hybrid MAC, a step is taken to the asynchronous duty cycle protocol X-MAC. This protocol organizes the WSN such it operates in completely decoupled schedules for receiver and sender. Again, the low power listening idea together with preamble sampling is applied. The difference is that the preamble embeds the target address to save overhead and the preamble sequence is shortened. Compared to LPL in Figure 6, X-MAC uses multiple and short preambles. There are several advantages. First, the reduced energy amount spent on sending/receiving the preamble. Second, the latency drops as the receiver can answer as soon as he wakes up and does not have to wait until the end of the preamble sequence. Third, unmeant

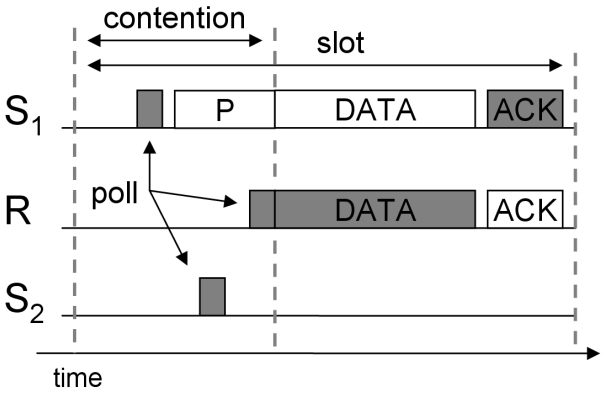

Figure 5: Crankshaft contention and message reception

receivers can go back to sleep after they got the preamble with the address information. Optionally, X-MAC offers an adaptive algorithm to adjust the duty cycle for better energy versus packet balance. With X-MAC being one of the latest protocol members in the evolution of WSN MAC, it takes into account the technological developments on the transceivers. CCA and turnaround time have great influence on the preamble gaps, therefore X-MAC suffers from older hardware [12]. X-MAC is optimized for light traffic, the scaling ratio under higher load is less optimal[15]. A nice side effect of the early ACK is the fact, that it acts as a CTS. This reduces the collision probability furthermore. A early ACK can also be sent in one of the gaps between the strobed preambles. The dotted line marks the activity period of a node. LPL has to wakeup early to get the complete long preamble. X-MAC stays active for a short time after a data transmission to listen for further preambles.

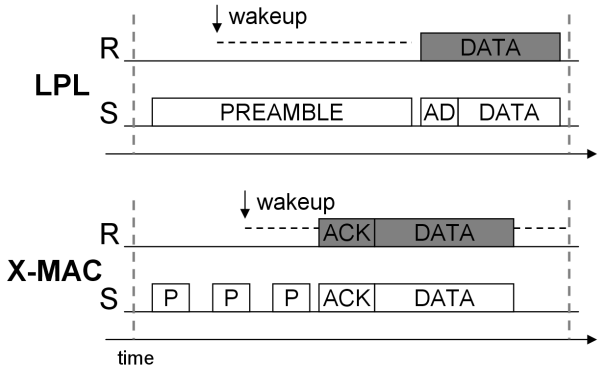

Figure 6: Difference between standard LPL and X-MAC protocol

4. PRESENTATION OF A SPECIFIC WIRELESS MAC PROTOCOL

A newer protocol has been selected to be discussed in detail. It not only implements new or different ideas, it also focuses on issues of other modern protocols like X-MAC. Most designers aim to reduce idle listening with more or less practical analysis. As shortly raised in the MAC protocol comparison before, the underlaying hardware plays a big role. A deep and critical look into **RI-MAC** will be done in the upcoming sections. RI-MAC is the abbreviation of Receiver Initiated MAC.

4.1 RI-MAC

RI-MAC belongs to the random or asynchronous protocols. The name suspects that the transmission sequence is initiated by the receiver (the sink) and not by the sender. The idea behind comes basically from infrastructure driven networks but remembering the multi-hop nature of an Ad-hoc network.

4.2 Design considerations of RI-MAC

A node, intended for receiving data wakes up based on its schedule and checks the channel for being idle. If the channel is in idle state a beacon B is transmitted by the Receiver R. Figure 7 illustrates the basic operation. Next the assignation of the beacon has to be reviewed. The beacon serves as request and as ACK for a data transmission. The Sender S wakes up to wait for a incoming beacon. The dotted line in the Figure 7 marks the active period of the transceiver. The receiver signalizes the sender the start of the data transmission. After the transmission a beacon is sent by the receiver to acknowledge the transmission. In other words, the receiver controls the medium and announces duty cycle changes by the help of the beacon.

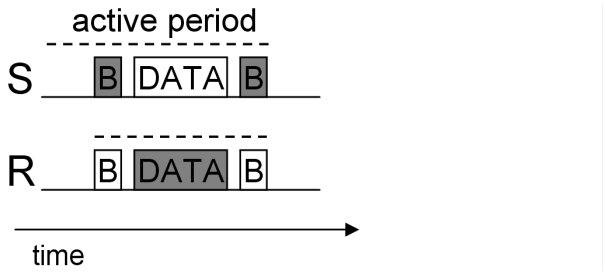

Figure 7: RI-MAC: Initiation of data exchange by the receiver R

The designers of RI-MAC have used the CC2420 radio for the implementation. This transceiver is mainly designed for IEEE 802.15.4 networks[7]. Within 802.15.4 there this a beacon format already defined. RI-MAC reuses the hardware preamble, frame length, frame control field and the frame check sequence. RI-MAC adds specific fields, the source/destination address and the backoff window (BW). Two beacon types exist in RI-MAC, a base beacon including only the source field and the extended beacon with BW and destination field. The two types can be easily divided by the receiving node due to its value inside the length field. A beacon without BW information will request the sender to start data transfer immediately.

The **backoff window** incorporates a value telling the sending nodes when they should start the transmission of their data frame. This value is computed into a time interval which the node should wait until the transmission of the next data frame. The purpose is to keep the risk of collisions on the channel low. A commonly used method to calculate the backoff time is the binary potential backoff strategy as

utilized in IEEE 802.3 e.g. Ethernet. The binary potential backoff window value is doubled on each collision. The problem on the binary potential backoff results in large waiting time on big values when the number of nodes is small. Another method is the geometrical-increasing probability distribution used in the Sift protocol [11]. A node chooses its contention slot from a geometrical distribution. Due to the nature of this distribution many nodes will pick a high slot number and a few nodes a small slot number. The smaller the chosen slot number the less the collision probability.

The difference in BW is RI-MAC being receiver orientated. After reaching the maximum BW size due to multiple collisions the receiver goes to sleep. On the sender side a missing ACK beacon within a dedicated timespan will be recognized and a counter for retransmission will be increased. The sender cancels the transmission if the predefined retry limit is reached. The detection of collisions is based on the hardware preamble bit sequence inside the beacon. If this fixed sequence is corrupted the beacon is not recognized as correct and must be sent again. Collisions on the data frames are possible but with much lower probability. Based on the backoff window value the receiver knows when to get the next data frame from a specific sender. If the received frame is outside the intended time span or the checksum is wrong no ACK will be sent back. Figure 8 shows two Senders S1 and S2 contending for transmission. As soon as the Receiver R sends a beacon B both senders will start immediately with the data transmission. The consequence is a collision. To solve the collision on the next attempt, a new beacon is sent out by the receiver. This time the beacon is populated with a backoff window value, marked with a dotted circle in the Figure 8. This value is processed by the nodes on reception and used to set the next transmission attempt for the pending data. The conflict is solved by Sender S1 doing its cycle before Sender S2 does[15].

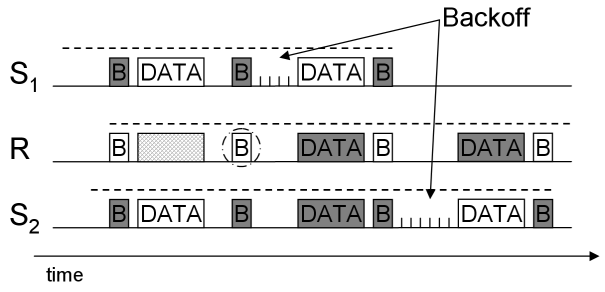

Figure 8: DATA frame transmission from contending senders in RI-MAC.

To let the beacon act as an ACK, the destination field of the beacon is set to the address of the last received data frame. Thereby the sender recognizes the beacon.

RI-MAC lacks the option to get the data directly, but there is the so called beacon on request. In networks with high traffic load or many nodes, the receivers might be active anyway. This can be adapted to process a beacon sent by sending node to tell the receiver the wish to initiate a data transfer. A beacon from a sender requests a beacon from the receiver which starts the normal frame sequence. The benefit is to use the standby activity of the transceiver on the receive side for faster data processing which helps to lower latency and energy consumption.

4.3 Evaluation of RI-MAC

The standard approach for evaluating such networks designs is to build a model for the network simulator ns-2[1]. In this paper, it was decided to concentrate on practical benchmark results as they take the CCA delay into account. Furthermore, it is not clear how an undistinguishable signal affects the protocol state if this is above the CCA threshold. The authors of X-MAC and many other protocol designers do not tackle this possible problem emerging in larger networks.

A preface to the evaluations, most comparisons reflect LPL as basis. In this context, X-MAC was chosen as representative for random access MAC protocols. The practical implementation was done on MICAz motes hardware with TinyOS. The number of nodes is twice the number of data flows. A flow is the individual traffic a receiving node has to satisfy. On increasing number of flows from every sender from one to four, the duty cycle spent on the medium increases on X-MAC while RI-MAC stays below 60%. It is clear that a higher duty cycle affects the energy consumption in proportional way.

Another interesting aspect is the classical hidden node problem. If two senders are not in the reception range of each other, the probability for packet loss at the receiving node is high and accompanied by higher duty cycle due to retransmission. The average ratio of unsuccessful transmissions with RI-MAC is about five percent lower compared to X-MAC. In contrast the results for not hidden nodes differs not much. The results were achieved by the average of ten runs [15].

As RI-MAC was designed especially for dense networks a comparison was made by using ns-2. The simulated scenario consists of a 7x7 nodes network with a sensing range of 100 to 500 meters. The 30 simulation runs trigger a series of 100 events per cycle. RI-MAC outperforms X-MAC in terms of delivery ratio. Under heavy load RI-MAC scales better than X-MAC. RI-MAC can successfully handle more concurrent flows within one transmission cycle. The wider the sensing range the less is the decrease of delivery ration of RI-MAC. Starting with the 100m range, X-MAC and RI-MAC are on the same level. At the 300m range X-MAC looses about 21% and at the 500m range about 42% [15].

5. SECURITY ASPECTS ON WIRELESS SENSOR NETWORKS

Security in general got more and more important in the last years. Many systems suffer from the beginning of their design in these questions. Likewise simple attacks can have serious impact on the operation of a system.

The weakness of WSNs is their dependency of the battery capacity. As discussed above, all protocols try to reduce energy consumption while maintaining latency and data throughput on a low level. A Tmote Sky node using two AA batteries with 3000 mAh each has got a run time of hundreds of days in sleep but only a week in receive mode. A additional problem is the self discharging of the batteries. Even if the

energy consumption of a node is very low, in the range of 0.1 to 70mW, self discharging grows to the end of the battery life cycle. Attacks to increase the energy consumption of the nodes are called Denial of Sleep attacks (DoS). Attacks on WSNs in general can be categorized into three classes:

- **Class 1: unknown protocol attack**
  This categorizes attacks, sending out high power pulses or jamming to disrupt the communication among the nodes. Jamming can also be used to generate collisions every time traffic is detected by the aggressor. More intelligent is a record of traffic and later replay. Replaying data can lead to miss detections.

- **Class 2: known protocol, untrusted traffic**
  Identifying the protocol used in a WSN by traffic analysis helps the attacker to save energy on his own node(s). The more accurate an aggressor emulates frames, the more difficult it will be for the network to detect this. Even if frames are encrypted, a receiving node has to decrypt and afterwards to dump it which wastes energy. Broadcast messages are not further proceeded by the nodes and are discarded.

- **Class 3: full access including authorization**
  Knowing the MAC protocol and it's authorization mechanism on the data link layer offers the aggressor maximum possibilities. He can send trusted traffic which cannot be sorted out by the nodes. It will be difficult to isolate such aggressor node(s) since this attack can be done random. Also wrong or even multiple source identities can be used to disturb the whole network. In this scenario not only energy is wasted, data can be manipulated. Solving the consequences of those attacks can be very cost intensive. A well timed SYNC frame in the S-MAC protocol for example, stops the nodes from entering the sleep mode. After a week the affected nodes would not respond anymore because the battery would be empty.

To prevent those attacks some techniques are listed below.

- **Strong link-layer authentication**
  Authentication at the data link layer is needed to ensure the service availability of a WSN. Using authentication on layers above the data link layer will only ensure data integrity. Broadcast frames in many protocols have got a simple structure. This frame type is well suited for an attack since all nodes receive it and the aggressor does not have to take care about specific data inside this frame. Therefor the authentication technique is important to defense the DoS and broadcast attacks[3]. TinyOS offers the TinySec component for this purpose[2].

- **Replay protection**
  To prevent recorded and replayed traffic from disturbing nodes, a table of neighbor nodes can be established in combination with sequence numbers attached to the packets. But this is not very safe at the data link layer and requires additional memory.

- **Jamming recognition**
  WSNs are resource orientated and have only a single channel radio with limited capabilities. Without a spectrum analysis it is hard to detect a jammer. Generally, jamming blocks the whole traffic, so nodes have to check the medium periodically for a free channel. A real protection cannot be done against this type of attack. It is only possible to recognized it and to go to sleep mode for longer intervals.

- **Isolation of compromised nodes**
  Detecting compromised nodes in alliance with blending the nodes out from the network is a desirable option. Therefore an asymmetric encryption approach is very effective. The negative side, asymmetric key mechanisms overload the sensor nodes processing capabilities.

Especially the early developed protocols are accessible for DoS attacks. Newer ones or ones taking security into account help to reduce the DoS issue. It widely depends on the application and its requirements which protocol and which security features to choose[3].

6. CONCLUSION

The need for dedicated MAC protocols in WSNs has been discussed under the given limitations. These limitations come from the underlaying hardware, limited battery capacity, harsh environment with a wide temperature range and a short transmission range. A wide field of applications makes it impossible to have a single solution. Many issues can be eliminated in the design phase. The decision, which protocol to choose, should not depend on a single parameter like performance or battery runtime. Especially the network size, the node allocation, possible other radio transmitters in the neighborhood and the estimated traffic pattern have to be considered.

Very popular are the dynamic protocols as they are easy to integrate. They are flexible in terms of network movement and network extension. Various implementations exist for different number of nodes under high or low traffic load. The latest protocols improve the energy efficiency again by addressing mainly the schedule and the balance between sender and receiver to lower the duty cycle. Features offered by the hardware are also taken into account.

Finally an important subject, the security, was considered. Popular and easy to adapt attack mechanisms accompanied with possible defense methods were presented. At the moment, most of the protocols are susceptible for comparatively lightweight attacks which have however great impact on the battery lifetime of a node.

7. REFERENCES

[1] The network simulator ns-2, May 2010. http://www.isi.edu/nsnam/ns/.

[2] TinyOS, May 2010. http://www.tinyos.net/.

[3] David Raymond, Randy Marchany, Michael Brownfield, and Scott Midkiff. Effects of Denial of Sleep Attacks on Wireless Sensor Network MAC Protocols. In *Proceedings of the 2006 IEEE Workshop*

on Information Assurance. United States Military Academy, 2006.

[4] Freie Universität Berlin. ScatterWeb. June 2010. http://cst.mi.fu-berlin.de/projects/ScatterWeb/.

[5] G.P. Halkes and K. Langendoen. Crankshaft: An energy-efficient mac-protocol for dense wireless sensor networks. *Faculty of Electrical Engineering, Mathematics and Computer Science Delft University of Technology, The Netherlands*, 2007.

[6] IEEE Computer Society. *802 IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*. The Institute of Electrical and Electronics Engineers, Inc., 2002.

[7] IEEE Computer Society. *802 Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*. The Institute of Electrical and Electronics Engineers, Inc., 2006.

[8] Ilker Demirkol, Cem Ersoy, and Fatih Alagöz. MAC Protocols for Wireless Sensor Networks: A Survey. *IEEE Communications Magazine*, pages 115–121, April 2006.

[9] J. Hill and D. Culler. Mica: a wireless platform for deeply embedded networks. *IEEE Micro*, 22:22–24, 2002.

[10] K. Langendoen. Medium Access Control in Wireless Networks. 2:535–560, 2007.

[11] Kyle Jamieson, Hari Balakrishnan, Y.C. Tay . Sift: A MAC Protocol for Event-Driven Wireless Sensor networks. May 2003.

[12] Michael Buettner, Gary V. Yee, Eric Anderson, Richard Han. X-MAC: A Short Preamble MAC Protocol for Duty-Cycled Wireless Sensor Networks. *SenSys, Boulder*, November 2006.

[13] S. Coleri-Ergen and P. Varaiya. Pedamacs: Power effcient and delay aware medium access protocol for sensor networks. *IEEE Trans. on Mobile Computing*, pages 920–930, May 2006.

[14] Texas Instruments. CC2420 2.4 GHz IEEE 802.15.4 / ZigBee-ready RF Transceiver, June 2004. http://www.ti.com/lit/gpn/cc2420/.

[15] Yanjun Sun, Omer Gurewitz, David B. Johnson. RI-MAC: A Receiver-Initiated Asynchronous Duty Cycle MAC Protocol for Dynamic Traffic Loads in Wireless Sensor Networks. *Department of Computer Science, Rice University, Houston, TX, USA / Department of Communication Systems Engineering, Ben Gurion University, Israel*, November 2008.