MAC - Vergleich von Präambel-basierten Kanalzugriffsprotokollen

Joseph Wessner
Betreuer: Dr. Alexander Klein
Seminar Sensorknoten: Betrieb, Netze und Anwendungen SS2011
Lehrstuhl Netzarchitekturen und Netzdienste, Lehrstuhl Betriebssysteme und Systemarchitektur
Fakultät für Informatik, Technische Universität München
Email: wessnerj@in.tum.de

KURZFASSUNG

Mit die wichtigste Anforderung an drahtlose Sensornetze (WSN) ist die Energieeffizienz. Da die Kommunikation oftmals den größten Energieverbraucher darstellt, ist hier ein sparsamer Umgang mit den Ressource enorm wichtig. Die Wahl eines geeigneten Protokolls spielt dabei eine große Rolle um den Protokolloverhead möglichst gering zu halten. In diesem Paper werden daher die verschiedene Präambelbasierten Kanalzugriffsprotokolle LPL, X-MAC und BPS-MAC vorgestellt und miteinander verglichen. Die Schwerpunkte liegen dabei auf den Bereichen der Interferenz, Overhead, Paketverlust, Durchsatzrate, Verzögerung und natürlich der Energieeffizienz.

Schlüsselworte

LPL, X-MAC, BPS-MAC, Energieeffizienz, MAC Protokolle

1. EINLEITUNG

Media Access Control (MAC) Protokolle, im folgenden auch Kanalzugriffsprotokolle genannt, werden für die Kommunikation in WSN benötigt. In dem OSI-Schichtenmodell reihen sie sich dabei in die Sicherungsschicht direkt über der physikalischen Schicht ein. Ziel der MAC Protokolle ist die Energieeffizienz um eine möglichst lange Laufzeit der Sensorknoten zu ermöglichen. Da Sensorknoten meist über keine externe Stromversorgung verfügen, sondern auf ihre Batterien angewiesen sind muss der Energieverbrauch so weit wie möglich gesenkt werden. Um dieses Ziel bestmöglich zu erreichen spielt neben der Hardware auch die Wahl eines geeigneten MAC Protokolls eine wichtige Rolle. In dieser Arbeit werden im folgenden verschiedene MAC Protokolle und deren Vor- und Nachteile vorgestellt.

2. ENERGIEVERSCHWENDUNG

Natürlich gibt es viele verschiedene Arten unnötig Energie zu verbrauchen, die wichtigsten davon werden hier kurz vorgestellt.

2.1 Idle Listening

Mit Idle Listening bezeichnet man den Umstand, den Kommunikationskanal abzuhören, obwohl keine Kommunikation stattfindet. Da das Empfangen von Daten in der Regel mehr Energie benötigt als das Senden von Daten, stellt das Idle Listening einen nicht zu vernachlässigbaren Teil der Energieverschwendung dar. Um dieses Problem zu umgehen werden Sensorknoten oft in einen Schlafzustand versetzt, in welchem sie das Empfangsmodul deaktivieren, um möglichst viel Energie einzusparen.
Um das Idle Listening ganz zu vermeiden, müsste man also vorab wissen wann Daten gesendet werden. Dieses Problem lässt sich zwar theoretisch mit Hilfe von Zeitslots lösen, ist aber in der Praxis aufgrund zu ungenauer Zeitsynchronisation der Sensorknoten nur schwer zu realisieren.
Um die Zeit des Idle Listenings trotzdem möglichst gering zu halten, lassen viele MAC Protokolle das Empfangsmodul nur kurzzeitig aufwachen, um zu überprüfen ob momentan eine Kommunikation stattfindet. Falls keine Kommunikation stattfindet wird das Empfangsmodul wieder ausgeschaltet um Strom zu sparen. [5]

2.2 Overhearing

Anders als beim Idle Listening findet beim Overhearing eine Kommunikation statt, allerdings sind die Daten für einen anderen Empfänger bestimmt. Es werden also Daten empfangen mit denen der Sensorknoten nichts anfangen kann. Den Empfänger während des Datenstroms festzustellen erweist sich als recht schwierig. Die Folge dessen ist, dass meist erst am Ende des Datenstroms festgestellt werden kann, dass die Daten für einen anderen Empfänger bestimmt waren und dann verworfen werden.
Um das unnötige und stromraubende Empfangen nicht benötigter Daten zu vermeiden wird oft ein Header mit der Adresse des Empfängers vorausgeschickt. Wird also nach dem Empfang des Header bemerkt, dass die Daten für einen anderen Empfänger bestimmt sind, kann das Empfangsmodul sofort wieder in den Schlafzustand zurückkehren. Das unnötige Empfangen eines Headers stellt im Vergleich zu dem überflüssigen Empfangen der kompletten Daten einen recht geringen Stromverbrauch dar. [5]

2.3 Kollisionen

Kollisionen entstehen, wie der Name schon vermuten lässt, wenn zwei oder mehr Teilnehmer gleichzeitig Daten versenden. Aufgrund der Überlagerung beider Signale ist das Empfangen der Daten nur sehr schwer oder meist gar nicht mehr möglich.
Kollisionen stellen eine der größtmöglichen Formen der Energieverschwendung dar, da die Pakete erneut gesendet werden müssen. Das Erkennen einer Kollision ist erst nach dem Senden des kompletten Daten möglich, weshalb im Falle einer Kollision auch die komplette Übertragung erneut gesendet werden muss. Die Kollision wird entweder durch das Fehlen der Bestätigung über das Ankommen des Datenpaketes vom Empfänger erkannt, oder aber durch einen belegten Kanal

doi: 10.2313/NET-2011-07-1_06

nach der Übertragung.
Die Wahrscheinlichkeit einer Kollision hängt natürlich hauptsächlich von der Menge der zu übertragenden Daten und der Menge der vorhandenen Sensorknoten ab.
Um die Wahrscheinlichkeit von Kollisionen zu verringern setzten die verschiedenen Protokolle auch verschiedene Lösungsansätze um. Die einfachste Variante besteht darin, vor dem Senden zu überprüfen ob der Kanal bereits belegt ist. Dieser triviale Ansatz stößt allerdings auch sehr schnell an seine Grenzen, beispielsweise wenn 2 Sender gleichzeitig mit der Übertragung beginnen oder sich die beiden Sender gegenseitig nicht in Reichweite befinden, der Empfänger aber im Sendebereich beider Sender liegt. [5]

2.4 Auslastungsschwankungen

WSN sind fast immer großen Lastschwankungen ausgesetzt. Oft werden WSN für Messungen eingesetzt. Eine Veränderung an einem einzigen Messpunkt ist sehr unwahrscheinlich. Ändern sich aber die Messungen an vielen Sensorknoten gleichzeitig, versuchen die Sensorknoten ihre neuen Messdaten auch alle gleichzeitig zu senden. So tritt schnell eine Lastspitze auf, während in der anderen Zeit, wenn sich Messwerte nicht oder kaum ändern, fast kein Traffic entsteht.
Die eingesetzten Protokolle müssen also einerseits in der Lage sein diese vergleichsweise großen Lastspitzen zu handhaben und andererseits bei einer geringen Auslastung möglichst viel Energie sparen. [5]

2.5 Protokolloverhead

Der Protokolloverhead spielt in WSN eine große Rolle. Meistens werden in WSN nur sehr geringe Mengen an Daten versendet, so macht sich auch ein relativ geringer Overhead im Vergleich zu den Nutzdaten sehr schnell negativ bemerkbar. In anderen drahtlosen Netzwerken, wie beispielsweise dem von Laptops und Computern genutzten WLAN spielt der Overhead eine im Vergleich geringe Rolle, da in diesen Netzen der Datendurchsatz wesentlich höher ist als in WSN.
Um den Overhead zu reduzieren werden die Daten meistens gesammelt bevor sie versendet werden. Das Aggregieren der Daten erhöht in der Regel die Latenz, verringert aber auch den Overhead enorm. Da in vielen Fällen eine leichte Erhöhung der Latenz verschmerzbar ist, wird das Aggregieren der Daten oftmals eingesetzt. [5]

2.6 Over-emitting

Over-emitting beschreibt das Senden von Daten ohne dass der Empfänger die Daten empfängt. Dies tritt auf wenn sich der Empfänger im Schlafzustand befindet und sein Empfangsmodul deaktiviert hat.
Die Daten müssen also erneut gesendet werden, sobald bemerkt wird, dass sie beim Empfänger nicht angekommen sind. Im schlimmsten Fall, wenn das Ausbleiben des Empfangs nicht bemerkt wird, gehen die Daten sogar verloren. Durch unnötiges oder wiederholtes Senden von Daten, wird der Kanal auch länger belegt. Dies hat zur Folge, dass andere Knoten nicht senden können und sich so die Latenz des ganzen WSN erhöht.
Die naivste Lösung wäre natürlich, dass die Sensorknoten ihre Empfangsmodul ständig aktiviert haben und auf dem Kanal lauschen, so dass sie keine Übertragung verpassen. Aus Energieeffizienzgründen ist dies aber in den meisten Fällen keine akzeptable Lösung.
Viele MAC Protokolle setzten auf eine Präambel, die die Datenübertragung ankündigt. Durch die Ankündigung der Übertragung soll sichergestellt werden, dass der Empfänger sein Empfangsmodul nicht deaktiviert und auch wirklich auf dem Kanal lauscht wenn die eigentliche Übertragung stattfindet. Dabei wird aber vorausgesetzt, dass der Empfänger die Präambel empfängt. Dieses Problem wiederum versucht man beispielsweise mit einer sehr langen Präambel zu lösen. Die lange Präambel muss dabei so lange andauern, dass der Empfänger sie auch sicher empfängt.
Eine anderen Möglichkeit Over-emitting zu vermeiden besteht darin die einzelnen Knoten betreffend ihrer Aufwachzeitpunkte zu synchronisieren. Eine Synchronisierung des WSN stellt allerdings einen komplexeren Prozess dar, der viel Bandbreite und Rechenzeit benötigt.
So bewerten die verschiedenen MAC Protokolle die Vor- und Nachteile der Synchronisation unterschiedlich, weshalb auch verschieden aufgebaute Protokolle existieren.

3. MAC PROTOKOLLE

Alle existierenden MAC Protokolle aufzulisten würde den Rahmen dieser Arbeit sprengen, um dennoch einen Einblick in die MAC Protokolle zu erlangen werden in diesem Kapitel 3 verschiedene MAC Protokolle vorgestellt. Im folgenden werden die Protokolle LPL, X-MAC und BPS-MAC erläutert und deren Unterschiede aufgezeigt.

3.1 LPL

Bei dem Low Power Listening (LPL) Protokoll prüfen die einzelnen Knoten in gewissen Zeitabständen, ob der Übertragungskanal belegt ist. Ist der Übertragungskanal frei, können sie sofort wieder in den Schlafzustand übergehen. Falls der Übertragungskanal aber belegt ist, warten die Knoten so lange bis das Startsignal der Datenübertragung übertragen wird. Nachdem das Startsignal empfangen worden ist, können die Knoten entscheiden für welchen Empfänger die darauf folgenden Datenpakete bestimmt sind und sich gegebenenfalls wieder in den Schlafzustand begeben.
Diese Funktionsweise setzt voraus, dass die Präambel vor dem Startsignal länger andauert als die Zeitspanne zwischen zwei Aufwachvorgängen der beteiligten Knoten.

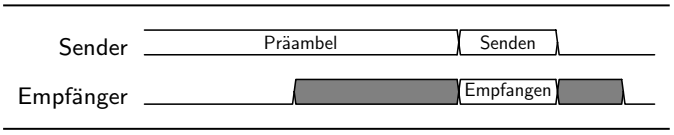

Abbildung 1: LPL Protokoll

Wie in Abbildung 1 zu sehen, beginnt der Sender damit die Präambel zu senden. Der Empfänger beginnt während der Präambel auf dem Kanal zu lauschen und erkennt dadurch, dass momentan eine Präambel gesendet wird und bald Datenpakete folgen werden, die möglicherweise für ihn selbst bestimmt sind. Dadurch ist sichergestellt, dass der Empfänger während der Datenübertragung sein Empfangsmodul aktiviert hat und dadurch die Daten auch wirklich empfangen kann. Nach dem Senden und Empfangen der Datenpakete, lauscht der Empfänger noch für eine kurze Zeitspanne ob eventuell noch weitere Datenpakete oder sogar eine andere Präambel (von einen 2. Sender) gesendet werden. Ist dies

doi: 10.2313/NET-2011-07-1_06

nicht der Fall beginnt der Knoten (Empfänger) wieder mit seinem Schlafzyklus.
Das LPL Protokoll hat zwei offensichtliche Nachteile.
Erstens wird durch die lange Präambel die aktive Sendedauer des Senders, um die meist geringen Datenmengen zu übertragen sehr lang, da Senden Strom kostet ist ein großer Overhead durch eine (im Vergleich zur Datenmenge) lange Präambel natürlich nicht wünschenswert. Auf der Empfängerseite tritt ein sehr ähnlicher unerwünschter Effekt ein. Alle möglichen Empfänger müssen die ganze Präambel abwarten bis sie entscheiden können ob sie die darauf folgenden Daten überhaupt empfangen sollen. Außer dem hohen Strombedarfs auf Senderseite, fällt auch ein hoher Strombedarf bei allen anderen Knoten an, da während der Präambel der gewünschte Empfänger nicht ermittelt werden kann.
Der zweite offensichtliche Nachteil besteht darin, dass durch die lange Präambel der Funkkanal unnötig lange blockiert wird, so dass in dieser Zeit kein weiterer Sender aktiv werden kann. [4, 1]

3.2 X-MAC

Bei der Entwicklung von X-MAC wurde besonders auf dessen Energieeffizienz geachtet. Im Gegensatz zu LPL setzt X-MAC nicht auf eine lange Präambel, um dem Empfänger die Übertragung anzukündigen, sondern auf mehrere kurze Präambelübertragungen.

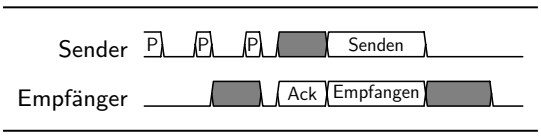

Abbildung 2: X-MAC Protokoll

Wie in Abbildung 2 dargestellt, werden mehrere kurze Präambel (P) gesendet, der zeitliche Abstand dieser Präambel muss kürzer als eine Wachphase (dunkelgrau dargestellt) des Empfängers sein, damit sichergestellt ist, dass dieser eine Präambel empfängt. Wird die Präambel vom Empfänger gelesen, schickt dieser eine Bestätigung (Ack) zurück zum Sender. Der Sender kann daraufhin mit der Übertragung der Daten beginnen. Der Empfangsmodus des Empfängers wurde durch den Bestätigungscodes Ack bereits zugesagt.
Damit nicht jeder Sensorknoten im Netzwerk den Bestätigungscode Ack sendet und damit eventuell verhindert, dass der gewünschte Empfänger über die Übertragung informiert wird, enthalten die kurzen Präambeln (P) bereits die Zieladresse der Datenpakete. Zusätzlich zur Gewährleistung, dass nur der Empfänger das Ack Signal sendet, ist es den anderen Sensorknoten auch möglich sofort nach dem Empfang einer kurzen Präambel (P) zurück in den energiesparenden Schlafzustand zu wechseln.
Das Entwicklungsziel möglichst energiesparend zu sein, wurde vor allem durch zwei Eigenschaften erreicht.
Die Sensorknoten müssen keine lange Präambel abwarten um entscheiden zu können, ob die Daten für sie oder für einen anderen Sensorknoten bestimmt sind. So können sich alle bis auf den Empfängerknoten sofort nach der Präambel wieder in den Schlafzustand begeben. Der Empfängerknoten verkürzt die Dauer der Präambelphase durch das Senden der Bestätigung.
Aber auch auf der Senderseite wird Energie eingespart. Durch die verkürzte Präambelphase wird die Sendedauer und damit die benötigte Energie verringert.
Als weiterer Vorteil sollte noch die geringere Belegungsdauer des (Funk)kanals genannt werden. Dadurch wird es weiteren Sender ermöglicht schneller auf den Kanal zuzugreifen. [1, 4]

3.3 BPS-MAC

3.3.1 Einzelne Präambel

Das Backoff Preamble-based MAC Protokoll (BPS-MAC Protokoll) hingegen ist mehr auf WSNs mit vielen Knoten ausgelegt. Da die Wahrscheinlichkeit von Kollisionen zu nimmt, je mehr Sensorknoten im Netzwerk beteiligt sind, liegt das Hauptanliegen des BPS-MAC Protokolls im Vermeiden von Kollisionen.
Trotz der Optimierung zur Vermeidung von Kollisionen kommt das BPS-MAC Protokoll ohne Synchronisation von Zeitslots oder der Speicherung größerer Datenmengen aus. Durch diesen Umstand eignet sich das BPS-MAC Protokoll auch für Sensorknoten mit begrenzter Rechen- und Speicherkapazität. So können die Kosten für BPS-MAC geeigneten Sensorknoten gering gehalten werden, was sich bei einer großen Anzahl an Netzwerkknoten, für die das Protokoll konzipiert ist, durchaus lohnt.
Im BPS-MAC Protokoll prüft der Sender zuerst ob der Kanal frei ist, ist dies der Fall sendet er eine Präambel zufälliger Länge und prüft wieder ob der Kanal frei ist. Ist der Kanal wieder frei kann der Sender problemlos seine Daten verschicken. Diese vereinfachte Darstellung stellt natürlich den optimalen Fall dar und nicht den wahrscheinlichsten.
Senden 2 (oder mehr) Sender gleichzeitig ihre Präambeln, da beide Sender den unbelegten Kanal erkannt haben, kann der Sender mit der kürzeren Präambel den anderen Sender erkennen. Wird ein anderer Sender erkannt darf die Datenübertragung natürlich nicht erfolgen, da sonst eine unerwünschte Kollision auftreten würde. Zusätzlich muss noch die Umschaltdauer vom Empfangsmodus (Rx) zum Sendemodus (Tx) und umgekehrt berücksichtigt werden. Wir nehmen im folgenden an, dass sowohl die Umschaltdauer in den Sendemodus als auch die Umschaltdauer in den Empfangsmodus jeweils eine Zeiteinheit in Anspruch nehmen. Daraus folgt, dass der (Funk)kanal mindestens für 3 Zeiteinheiten als frei erkannt werden muss um davon ausgehen zu können, dass dieser wirklich frei ist und nicht nur vorübergehend.
In Abbildung 3 werden 2 Sender dargestellt, die versuchen gleichzeitig zu Senden:

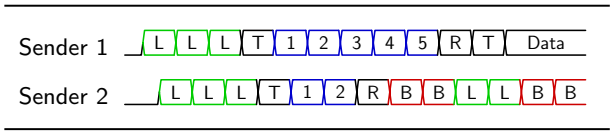

Abbildung 3: BPS-MAC mit einer Präambel

Sender 1 lauscht (L) 3 Zeiteinheiten auf dem Kanal, da der Kanal frei ist wechselt er in den Sendemodus (T) und sendet eine Präambel, die 5 Zeiteinheiten andauert (1 - 5), daraufhin wechselt er wieder in den Empfangsmodus (R), merkt dass der Kanal immer noch oder wieder frei ist, wechselt zurück in den Sendemodus (T) und beginnt mit der Datenübertragung (Data).

doi: 10.2313/NET-2011-07-1_06

Sender 2 lauscht (L) ebenfalls 3 Zeiteinheiten lang auf dem Kanal, wechselt in den Sendemodus (T) und sendet eine Präambel, die im Gegensatz zur Präambel von Sender 1 nur 2 Zeiteinheiten lang ist. Nach der Präambel wechselt auch Sender 2 wieder in den Empfangsmodus (R) zurück. Da die Präambel von Sender 1 aber noch andauert bemerkt Sender 2, dass der Kanal noch belegt ist (B). In der Zeit, die Sender 1 benötigt um in den Empfangsmodus und wieder zurück in den Sendemodus zu wechseln, wird der Kanal von Sender 2 zwar als frei wahrgenommen (L), aber kurz darauf wenn die Datenübertragung beginnt wird der Kanal wieder als belegt (B) erkannt.
So kann die Datenübertragung von Sender 1 ohne Kollision mit Sender 2 erfolgen. Sender 2 beginnt wieder mit dem Senden einer zufällig langen Präambel, sobald die Datenübertragung von Sender 1 abgeschlossen ist. Das Beispiel lässt sich natürlich auch auf mehr als nur 2 Sensorknoten, die gleichzeitig senden wollen übertragen.
Trotzdem kann es immer noch zu Kollisionen kommen, allerdings nur wenn 2 Sender gleichzeitig beginnen eine gleich lange Präambel zu senden, wie in Abbildung 4 veranschaulicht.

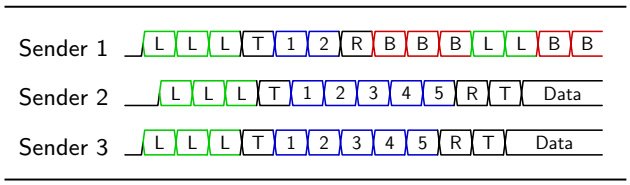

Abbildung 4: Kollision im BPS-MAC

In diesem Beispiel versuchen 3 Sender gleichzeitig Daten zu senden. Sender 1 wählt eine Präambeldauer von 2, während Sender 2 und 3 beide eine Präambeldauer von 5 wählen. Sender 1 ist also in der Lage den durch Sender 2 und 3 belegten Kanal zu erkennen und seine eigene Datenübertragung zu verschieben um eine Kollision zu vermeiden.
Sender 2 und 3 allerdings können sich gegenseitig nicht als sendewillig erkennen, da sie beide innerhalb des gleichen Zeitslots mit einer gleich langen Präambel begonnen haben. Durch diese identische Präambel erscheint beiden Sendern der Kanal als frei und sie beginnen mit ihrer Datenübertragung, die unweigerlich zur Kollision führt.
Die optimale maximale Präambeldauer hängt von der Umgebung ab. Die Anzahl der beteiligten Sensorknoten sowie die Menge der übertragenden Daten spielen dabei eine wichtige Rolle. Dennoch gilt auch bei BPS-MAC, die Wahrscheinlichkeit einer Kollision steigt mit der Anzahl der Sensorknoten und der Menge der übertragenden Daten. [3]

3.3.2 Mehrere Präambeln

Um die Wahrscheinlichkeit einer Kollision weiter zu verringern, werden ähnlich dem Schritt vom LPL zum X-MAC Protokoll, mehrere kürzere Präambel statt einer langen Präambel verwendet.

Sender 1, 2 und 3 wollen innerhalb des gleichen Zeitslots Daten versenden. Nachdem jeder Sender drei Zeitslots gelauscht (L) und keine Übertragung feststellen konnte, wechseln alle drei Sender in den Sendemodus (T). Sender 1 und

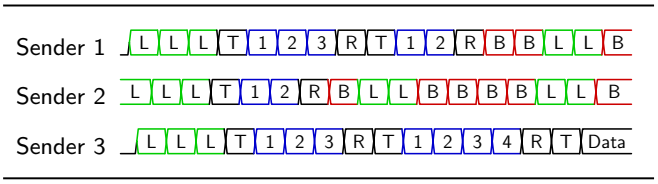

Abbildung 5: BPS-MAC mit mehreren Präambeln

3 würfeln eine Präambeldauer von 3 Zeiteinheiten (1 - 3), Sender 2 dagegen würfelt eine Präambeldauer von 2 Zeiteinheiten (1 - 2). Dadurch ist es Sender 2 möglich die Präambeln von Sender 1 und 3 auf dem Kanal festzustellen.
Sender 1 und 3 können die Präambel des jeweils anderen nicht feststellen, da beide die gleiche Präambeldauer gewählt haben.
Allerdings unterscheidet sich die Dauer der 2. Präambel von Sender 1 und 3, so dass Sender 1 die längere Präambel von Sender 3 empfängt. Durch die 2. Präambel wird in diesem Beispiel die Kollision verhindert.
Natürlich können auch hier noch Kollisionen auftreten, falls zwei Sender für jede Präambel die gleiche Dauer auswürfeln und im selben Zeitslot mit der Übertragung beginnen wollen. Allerdings sinkt die Wahrscheinlichkeit einer Kollision durch mehrere kurze Präambel im Vergleich zu einer längeren Präambel deutlich. Mit den Einstellungsmöglichkeiten für die Anzahl der Präambeln sowie der minimalen und maximalen Präambeldauer lässt sich das Protokoll für das jeweilige WSN optimal konfigurieren. Die Wahrscheinlichkeit für eine Kollision ist daher sehr gering.

4. VERGLEICH DER MAC PROTOKOLLE

In diesem Kapitel werden MAC Protokolle LPL, X-MAC und BPS-MAC bezüglich Interferenz, Auslastung (Overhead), Energieeffizienz, Paketverlust und Verzögerung miteinander verglichen.

4.1 Interferenz

Der Vergleich bezüglich der Interferenz wird in drei Teilbereichen aufgeteilt. Zuerst die klassische Kollision, bei der sich die Übertragungen von zwei oder mehr Sendern überlagern, so dass eine Unterscheidung der verschiedenen Übertragungen nicht mehr möglich ist. Außerdem wird in diesem Abschnitt noch das Hidden-Node und das Exposed-Node Problem behandelt.

4.1.1 Kollision

Kollisionen treten auf sobald ein Sender eine Übertragung beginnt obwohl bereits eine Übertragung im Gange ist. Natürlich versuchen alle 3 Protokolle eine Kollision zu vermeiden. Das LPL Protokoll benutzt eine lange Präambel um den Kanal für die darauf folgende Datenübertragung zu reservieren, so erkennt im Idealfall ein 2. Sender die Präambel und verschiebt seine eigene Übertragung nach hinten um eine Kollision mit der anderen zu vermeiden. Da aber nur eine Präambel verwendet wird, ist die Wahrscheinlichkeit einer Kollision gegenüber den anderen beiden Protokollen mit mehreren Präabeln recht hoch. BPS-MAC mit den unterschiedlich langen Präambeln bietet die höchste Wahrscheinlichkeit einer kollisionsfreien Übertragung, vor allem WSN mit höherer Knotendichte.

doi: 10.2313/NET-2011-07-1_06

Bei allen drei Protokollen steigt die Kollisionswahrscheinlichkeit mit der Anzahl der Sender und der Menge der Übertragungen.

4.1.2 Hidden-Node Problem

Das Hidden-Node Problem beschreibt folgendes Problem. Sender A und Sender B liegen in dem Sendreradius des jeweils anderen. Ebenso liegen Sender B und Sender C im gegenseitigen Senderadius. (Abbildung 6) Allerdings ist Sender C für Sender A nicht erreichbar und Sender A für Sender C nicht erreichbar. Sender A und C können also mit Sender B kommunizieren, aber nicht direkt miteinander. Daraus folgt, dass Sender C eine Kommunikation von Sender B zu Sender A erkennt, aber Sender C keine Kommunikation von Sender A zu Sender B erkennt, da sich Sender C nicht im Senderadius von Sender A befindet.

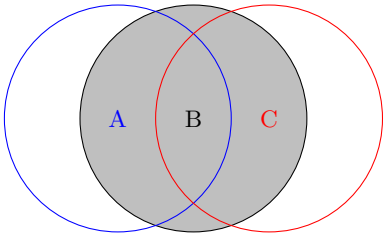

Abbildung 6: Hidden-Node Problem

Beginnt Sender C mit einer Datenübertragung, da für ihn der Kanal frei ist, aber schon eine Datenübertragung von Sender A zu B im Gange ist, kommt es zu Interferenz. Bei Sender B kommen nun gleichzeitig die Datenpakete von Sender A und Sender C an. Das Unterscheiden welche Pakete von welchem Sender kommen ist dann nahezu unmöglich. Das Ergebnis ist dann, dass weder die Übertragung von Sender A noch die von Sender C erfolgreich ist.
Für das Hidden-Node Problem bietet keines der drei vorgestellten MAC Protokolle eine zufriedenstellende Lösung, weshalb hier auch keine Empfehlung für ein bestimmtes Protokoll gegeben werden kann.
Allerdings sei angemerkt, dass ein stärkeres Signal ein schwächeres Signal oft auslöscht. Als Richtwert gilt hier eine Differenz von mehr als 3dBm um das stärkere Signal noch empfangen zu können. [2]

4.1.3 Exposed-Node Problem

Das Exposed-Node Problem beschreibt ein ähnliches Problem wie das Hidden-Node Problem, allerdings bleibt beim Exposed-Node Problem eine Übertragung aus, die eigentlich möglich wäre. Um das Exposed-Node Problem besser zu verstehen ordnen wir vier Sender so an, das jeder Sender nur seine Nachbarn erreichen kann (siehe Abbildung 7).

Sender A erreicht B, Sender B erreicht A und C, Sender C erreicht B und D, und Sender D erreicht wiederum nur Sender C. Besteht eine aktive Übertragung von Sender B zu Sender A, wird Sender C den Kanal als belegt erkennen, da sich auch Sender C im Einflussbereich von Sender B befindet. Sender C wird also keine Übertragung zu Sender D starten, da der Kanal scheinbar von Sender B belegt ist. Allerdings würde die Übertragung von Sender C zu D die andere Übertragung nicht beeinträchtigen, da Sender A nicht

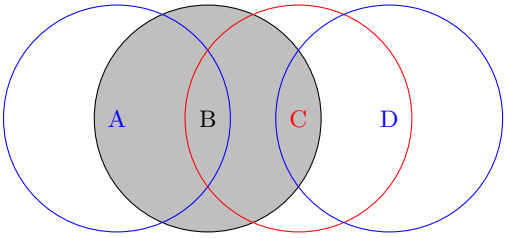

Abbildung 7: Exposed-Node Problem

im Sendebereich von Sender C liegt. Also wurde Sender A weiterhin nur die Daten von Sender B empfangen und auch Sender D wurde nur die Daten von Sender C empfangen.
Die beiden Übertragungen würden sich also nicht beeinflussen und trotzdem kommt die 2. Übertragung nicht zu stande, da Sender C den Kanal als belegt erkennt.
Auch für das Exposed-Node Problem kennt keines der 3 Protokolle eine Lösung.

4.2 Overhead

Als Overhead bezeichnet man Daten die zusätzlich zu den Nutzdaten übertragen werden. Overhead beinhaltet beispielsweise Routinginformation oder Empfängeradressen die notwendig sind um sicherzustellen, dass die eigentlichen Datenpakete auch beim Empfänger ankommen. Je größer der Overhead desto schlechter die maximale Auslastung, denn je mehr Zusatzinformationen übertragen werden müssen, umso weniger Bandbreite bleibt für die eigentlichen Daten übrig. Für ein Protokoll bedeutet dies: so wenig Overhead wie nötig.
Für WSN Protokolle ist der Overhead besonders wichtig, da hier oft mehr Overhead als Nutzdaten übertragen wird.
Vergleicht man das LPL mit dem X-MAC Protokoll wird schnell klar, dass das X-MAC Protokoll deutlich weniger Overhead produziert als das LPL Protokoll mit seiner sehr langen Präambel. Die lange Präambel des LPL kann sogar länger andauern als die darauf folgende Datenübertragung. Dieser große Overhead des LPL Protokolls führt zu einer deutlich schlechteren Auslastung des Übertragungskanals.
Obwohl das X-MAC Protokoll im Gegensatz zum LPL Protokoll schon eine deutlich bessere Auslastung bietet, eignet sich für ein höhere Übertragungsdichte BPS-MAC am besten. Da sich beim BPS-MAC Protokoll die einzelnen Sensorknoten nicht im Schlafzustand befinden, muss hier nur auf die Vermeidung von Kollisionen Rücksicht genommen werden, nicht aber auf die Aufwachzyklen. Durch das Wegfallen der Wartezeit bis der Empfängerknoten empfangsbereit ist, ist auch der Overhead beim BPS-MAC Protokoll geringer, womit sich dieses Protokoll am besten eignet, falls mit großeren Datenübertragungen zu rechnen ist.

4.3 Energieeffizienz

Wie in der Einleitung und in Kapitel 2 schon erwähnt wurde ist die Energieeffizienz oft die wichtigste Eigenschaft in WSN. Die verschiedenen Arten von Energieverschwendung wurden in Kapitel 2 schon aufgezählt.
Da das BPS-MAC Protokoll für hohes Trafficaufkommen entworfen wurde, spielt bei dem BPS-MAC Protokoll die Energieeffizienz eine untergeordnete Rolle. So lauschen alle Knoten ständig dem Funkkanal und schicken ihr Empfangsmodul nie in den Schlafzustand. Für den Energieverbrauch

doi: 10.2313/NET-2011-07-1_06

ist dieser Umstand natürlich nicht wünschenswert, deshalb schneidet das BPS-MAC Protokoll im Vergleich bezüglich der Energieeffizienz auch am schlechtesten ab.
Sowohl das LPL als auch das X-MAC Protokoll setzten auf Aufwachzyklen der Empfangsmodule. Es nutzen auch beide Protokolle Präambeln, um Datenübertragungen anzukündigen. LPL setzt dabei auf eine sehr lange Präambel, X-MAC dagegen auf mehrere Kurze. Der Vorteil der kurzen Präambeln besteht darin, dass die Präambelphase durch Senden einer Bestätigungsnachricht (Ack) des Empfängerknotens abgekürzt wird.
So wird durch die kürzere Präambelphase auf Sender- und auf Empfängerseite Energie eingespart. Außerdem enthalten die kurzen Präambeln des X-MAC Protokolls im Gegensatz zur Präambel des LPL Protokolls schon die Adresse des Empfängers, so dass alle Knoten, die nicht Empfänger sind die Präambelphase nicht abwarten müssen. Für das WSN bedeutet dies eine zusätzliche Energieeinsparung.
Im Bereich der Energieeffizienz schneidet also das X-MAC Protokoll am besten ab, weshalb es den anderen beiden Protokolle vorzuziehen ist, falls die Energieeffizienz das oberste Ziel darstellt. [1, 3]

4.4 Paketverlust

Packet Loss bezeichnet das Verhältnis zwischen den generierten und der erfolgreich übertragenen Datenpakete. Das X-MAC Protokoll bietet in fast allen Fällen eine bessere (niedrigere) Packet Loss Rate als das LPL Protokoll. [1] Die Erfolgswahrscheinlichkeit einer erfolgreichen Datenübertragung beim BPS-MAC Protokoll mit einer einzigen Präambel sinkt bereits bei einer Knotenanzahl von 10 unter 20%. Erhöht man aber die Anzahl der Präambeln des BPS-MAC Protokolls auf 5, dann beträgt die Erfolgswahrscheinlichkeit einer erfolgreichen Datenübertragung über 90 %. Liegt das Verhältnis zwischen übertragender und generierter Daten bei 10 Sendern und dem X-MAC Protokoll bei ca. 95%, erreicht das BPS-MAC Protokoll mit 5 Präambeln nahezu 100%.
Aus Sicht eines besseren Packet Loss Verhältnisses ist für dichtere Sensornetze daher sicherlich BPS-MAC die erste Wahl. [1, 3]

4.5 Verzögerung

Die Paketverzögerung spielt in WSN insoweit eine Rolle, da die Sensornetzwerke häufig eingesetzt werden um ein Ereignis zu protokollieren. Um dieses Ereignis auswerten zu können werden alle Messwerte benötigt die durch die Sensorknoten geliefert werden können. Damit die verschiedenen Messwerte zugeordnet werden können müssen sie zur gleichen Zeit ausgewertet werden. Werden nun Messwerte aufgrund der Latenz im Netz ausgebremst wird eine Zuordnung und damit verbundene Auswertung der Daten erschwert.
Wieder schneidet das LPL Protokoll am schlechtesten ab. Durch die lange Präambel wird nicht nur der eigene Messwert verzögert versendet sondern es werden auch andere Sensorknoten durch den belegten Kanal daran gehindert ihre Daten sofort weiter zu reichen.
Die verkürzte Präambelphase des X-MAC Protokolls verringert die Verzögerung deutlich. Noch weniger Latenz erreicht man mit dem BPS-MAC, da hier nicht die nächste Wachphase des Empfängers abgewartet werden muss.

5. FAZIT

Zusammenfassend kann man sagen, dass es nicht das perfekte MAC Protokoll gibt. Jedes Protokoll hat seine Vor- und Nachteile, auch wenn das BPS-MAC Protokoll in dem Vergleich als eindeutiger Sieger erscheint hat es seine größte Schwäche in der Energieeffizienz.
Da die Energieeffizienz wohl meistens das Hauptanliegen an das MAC Protokoll sein wird, greift man hier wohl besser zum X-MAC Protokoll. Das LPL Protokoll hingegen scheint nur Nachteile zu bieten und dürfte wohl in keinem Einsatzszenario die beste Wahl darstellen. Man darf dabei aber nicht vergessen, dass das LPL Protokoll das älteste der drei hier vorgestellten Protokolle ist und die anderen beiden Protokolle auf dem LPL Protokoll aufbauen.
Mittlerweile gibt es eine Vielzahl an verschiedenen MAC Protokolle, jedes für andere Anforderungen optimiert, doch selbst wenn man ein geeignetes Protokoll gefunden hat, gilt es die einzelnen Optionen, wie beispielsweise die minimale und maximale Präambeldauer im Auge zu behalten und gegebenenfalls erneut anzupassen, falls sich beispielsweise die Anzahl der Sensorknoten im Netzwerk ändert.

6. LITERATUR

[1] M. Buettner, G. V. Yee, E. Anderson, and R. 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.

[2] 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.

[3] A. Klein, J. Klaue, and J. 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.

[4] K. Langedoen. The MAC alphabet soup served in wireless sensor networks, http://www.st.ewi.tudelft.nl/~koen/macsoup/, 2006.

[5] K. Langedoen. *Medium Access Control in Wireless Networks*, volume 2, chapter 20, pages 535–560. Nova Science Publishers, July 2008.

doi: 10.2313/NET-2011-07-1_06