FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

ZigBee WirelessHART 6LoWPAN - ein Vergleich

Seminararbeit

zur Erlangung des akademischen Grades

Bachelor of Science

im Rahmen des Studiums

Technische Informatik

eingereicht von

Thomas Frühwirth
Matrikelnummer 0927088

an der
Fakultät für Informatik der Technischen Universität Wien

Betreuung
Betreuer/in: Ao.Univ.Prof.Dr. Wolfgang Kastner
Mitwirkung: Univ.Ass.Dipl.Ing. Lukas Krammer

Wien, 23.04.2012

(Unterschrift Verfasser) (Unterschrift Betreuer/in)

Abstract

Wireless technologies are widely used in home and building automation, but not yet fully accepted in industrial automation. In both application areas wireless technologies have to overcome mayor drawbacks regarding wired technologies to compete against them. Therefore, a lot of new concepts and mechanisms were developed to guarantee reliability as well as availability and security. Depending on the destined application area, wireless protocols implement different features and mechanisms.

This thesis gives an insight into a selection of notable wireless technologies in the home and building automation domain as well as the industrial automation area. In particular, ZigBee and 6LoWPAN as well as WirelessHART are examined regarding their specific features and differences, whereby the pros and cons in the respective application area are worked out. For this purpose, these representatives are analyzed according to the open systems interconnection model.

Kurzfassung

Drahtlose Technologien finden mittlerweile sowohl in der Heim- und Gebäudeautomation als auch in der Industrieautomation Verwendung. Dennoch gibt es in beiden Bereichen noch technische Herausforderungen, die bewältigt werden müssen um einen gleichwertiger Ersatz für drahtgebundene Technologien darzustellen. Zu diesem Zweck verwenden aktuelle drahtlose Technologien neuartige Konzepte, die die Zuverlässigkeit, Verfügbarkeit sowie die Sicherheit von kabellosen Netzwerken gewährleisten. Abhängig vom konkreten Anwendungsgebiet kommen verschiedene Funktionalitäten und Mechanismen zum Einsatz.

Diese Arbeit bietet einen Einblick in die Funktionsweise von “Wireless Mesh Networks”. Insbesondere werden ZigBee, 6LoWPAN sowie WirelessHART diskutiert und deren Kommunikationsmechanismen untersucht. Die einzelnen Mechanismen der betrachteten Technologien werden den sieben Schichten des “Open Systems Interconnection”-Modells zugeordnet und ihre Vor- und Nachteile gegenübergestellt.

Inhalt

Abbildungen

Tabellen

1 Einleitung

1.1 Motivation

Bei der traditionellen Industrieautomation kommen kabelgebundene Kommunikationssysteme, wie z.B. AS-i [5], zum Einsatz. Einfache Beispiele, wie ein Beschleunigungssensor auf dem Rotor eines Elektromotors oder mobile Monitorstationen, zeigen schnell, dass kabellose Kommunikation in manchen Fällen elegantere Lösungen zulässt. Die Vorteile liegen aber auch in der Skalierbarkeit, im Speziellen beim Hinzufügen neuer Komponenten und bei der räumlichen Ausdehnung.

Probleme finden sich typischerweise bei der Sicherheit, Co-Existenz und Zuverlässigkeit der Übertragung. Ein kabelloses Netzwerk kann nicht auf eine Betriebshalle eingeschränkt werden, ein potentieller Eindringling wird also nicht erkannt. Auch andere Geräte, wie Funkgeräte, Mobiltelefone, IEEE 802.11 WLAN [6] Netzwerke und Bluetooth [7]-Geräte, nutzen kabellose Kommunikation und dürfen von anderen Protokollen nicht in ihrer Funktion beeinträchtigt werden. Umgekehrt gilt diese Regel natürlich genauso. Ein weiteres Beispiel ist die temporäre oder längerzeitige Unterbrechung des Funksignals durch Fahrzeuge, größere Bauteile oder Kräne. All das sind Probleme, die von Wireless Protokollen behandelt werden müssen.

1.2 Aufbau der Arbeit

Im ersten Kapitel werden einige schichtübergreifende Themen behandelt, in den folgenden Kapiteln werden die einzelnen Protokollschichten aller drei Protokolle anhand der OSI-Referenzmodells [8] von unten nach oben gegenübergestellt. Um den Überblick nicht zu verlieren, ist es sinnvoll, sich an Abbildung 1 zu orientieren. Es sei an dieser Stelle darauf hingewiesen, dass nicht jedes Protokoll jede dieser Schichten implementiert. Dies gilt besonders für höhere Schichten. Das darauf folgende Kapitel behandelt den Themenbereich Security. Das letzte Kapitel fasst die wichtigsten Unterschiede abschließend zusammen.

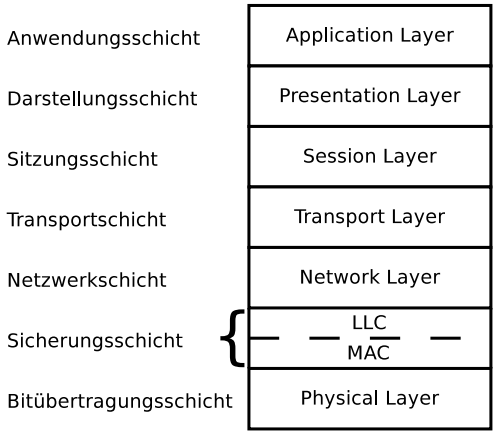

Abb. 1: OSI-Referenzmodell

1.3 WLAN

WLAN Netzwerke nach IEEE 802.11 haben sich im Office- und Privatbereich bewährt. Auf den ersten Blick wäre es daher naheliegend, diesen Standard auch im industriellen Bereich einzusetzen. Bei näherer Betrachtung wird jedoch klar, dass WLAN den Anforderungen hier nicht gerecht werden kann. Wie in Abschnitt 2.1 noch erläutert wird, ist die Sterntopologie kein geeigneter Ansatz für den Einsatz in einer industriellen Umgebung. Außerdem führt die hohe Datenrate von WLAN zu einem hohen Energieverbrauch. Ein Mobiltelefon mit aktiviertem WLAN hat nach wenigen Stunden den Akku aufgebraucht, ein batteriebetriebener Sensor in einer Industrieanlage soll im Idealfall aber Wochen oder Monate durchhalten. Im Laufe dieser Arbeit wird klar, dass in der Industrieautomation andere Anforderungen als im Office-Bereich an die Protokolle gestellt werden. Dennoch ist es sinnvoll, WLAN als einfaches Referenzprotokoll im Hinterkopf zu behalten.

2 Allgemeines

2.1 Topologie

Wie in der Einleitung erwähnt, kann eine einfache Funkstrecke in einer industriellen Umgebung sehr leicht unterbrochen werden. Dies ist aus Sichtweise der Zuverlässigkeit natürlich nicht akzeptabel. Demnach ist die im IEEE

802.11 Standard [6] beschriebene Sterntopologie äußerst schlecht für den Einsatz auf Feldebene geeignet. Der Standard definiert als weitere Möglichkeit eine Peer-to-Peer Topologie, d.h., jedes Gerät (A) kann mit jedem Gerät (B) Daten austauschen. Dies funktioniert jedoch nur solange sich Gerät B in Reichweite von Gerät A befindet. Da die Signalleistung jedes ungerichteten Funksignals quadratisch mit der Entfernung zum Sender abnimmt, ist ein solches Netzwerk in der Größe stark beschränkt. Eine bessere Topologie heißt Masche (Mesh) und kann als eine, auf höheren Schichten funktionierende, Erweiterung der Peer-to-Peer Toplogie angesehen werden. Abbildung 2 stellt die Maschen-Topologie schematisch dar. Die Kreise stehen für Netzteilnehmer, die schwarzen Kanten für ungestörte kabellose oder auch kabelgebundene Verbindungen. Bei der roten Kante handelt es sich um eine unterbrochene Funkstrecke oder um ein gebrochenes Kabel. Die Funktion des Netzwerks bleibt durch die Maschentopologie trotzdem erhalten. Die Pakete werden über eine alternative Route zum Ziel geführt.

Weiters sei erwähnt, dass die Entfernung zwischen zwei Geräten abstrakt in der Anzahl von nötigen Paketweiterleitungen gemessen wird. Jede Weiterleitung eines Pakets wird als *Hop* bezeichnet.

Vorteile der Maschentopologie:

- Netzwerke, die die Maschentopologie verwenden, können leicht in ihrer Größe ausgebaut werden.
- Durch das Hinzufügen von Routern kann auf einfache Weise sichergestellt werden, dass immer redundante Wege vorhanden sind und es keine Funklöcher gibt.
- Die Zuverlässigkeit ist sehr hoch. Sollte ein Router ausfallen, kann das Netz dies automatisch erkennen und eine alternative Route berechnen.

2.2 Aufbau der Protokollstacks

ZigBee basiert auf dem IEEE 802.15.4-2003 Standard [9]. Die von diesem Dokument behandelten Details haben sich, soweit an der betreffenden Stelle nicht anders angemerkt, jedoch in dieser Zeit nicht geändert. Außerdem ist der IEEE 802.15.4-2006 Standard [3] abwärtskompatibel. Alle Angaben sind somit für beide Versionen des Standards gültig. Näheres zum IEEE-Standard findet sich in den Kapiteln 3 und 4. 2007 wurde ZigBee PRO veröffentlicht, das den Standard von 2006 um einige Features in den Bereichen Routing und

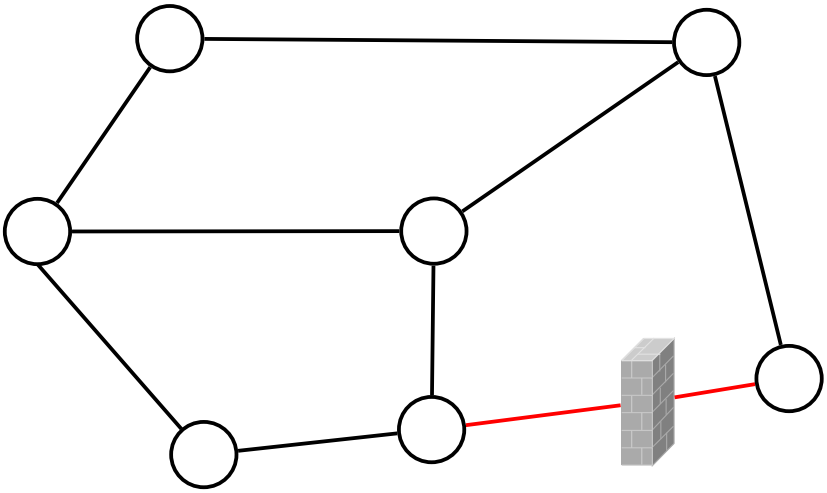

Abb. 2: vermaschtes Netz

Security erweitert. Diese Erweiterungen sind mit einem Hinweis auf ZigBee PRO gekennzeichnet.

Bitübertragungs- und Sicherungsschicht von WirelessHART orientieren sich stark am IEEE 802.15.4-2006 Standard. Sie weisen einige kleinere Unterschiede zum IEEE Standard auf, übernehmen allerdings weite Teile davon unverändert. Für Details zu den Unterschieden sei auf Kapitel 3 verwiesen.

6LoWPAN geht aus der Idee hervor, IPv6 für kleine und billige Geräte anzupassen und dabei die Idee des Internets als Verbindung unterschiedlicher Netzwerke zu erhalten. Aus diesem Grund können bei 6LoWPAN MAC- und physischer Layer getauscht werden, müssen also nicht IEEE 802.15.4 verwenden. Denkbar ist auch eine kabelgebundene Bitübertragungsschicht z.B. über Powerline oder kabellose Kommunikation im 433 MHz ISM (Industrial, Scientific and Medical)-Band. Für die Unabhängigkeit vom physikalischen Medium und der Zugriffsmethode sorgt der LoWPAN Adaption Layer. Im OSI-Referenzmodell ist dieser oberhalb des MAC-Layers anzuordnen. Im Folgenden beschränkt sich diese Arbeit auf 6LoWPAN basierend auf IEEE 802.15.4-2006.

2.3 Netzteilnehmer

ZigBee unterscheidet drei Typen von Geräten:

- Netzwerkkoordinator (Coordinator)
- Router
- Endgeräte (End Devices)

Der *Netzwerkkoordinator* ist für Managementfunktionen, wie das Verwalten von Schlüsseln und das Akzeptieren oder Ablehnen von Join-Anfragen, zuständig. *Router* erweitern die räumliche Ausdehnung des Netzwerks und sind in beliebiger Weise untereinander, mit dem Netzwerkkoordinator und mit Endgeräten verbunden. Ein dichtes Netz von Routern ermöglicht maximale Redundanz bezüglich Routen in einem Netzwerk. Fällt eine Verbindung oder ein Router aus, so wird automatisch eine neue Route ermittelt. *Endgeräte* verfügen, im Gegensatz zu WirelessHART Endgeräten, über keinerlei Routingfähigkeit. Diese Eigenschaft führt zu einem größeren infrastrukturellen Aufwand, da aufgrund der geforderten Redundanz relativ viele Router eingesetzt werden, die keinen praktischen Nutzen erfüllen. Der Vorteil liegt darin, dass die Komplexität von Endgeräten reduziert wird. Bei Endgeräten handelt es sich beispielsweise um Temperatursensoren.

In einem typischen (nicht isoloierten) 6LoWPAN-Netz finden sich

- Router,
- Edge router und
- Hosts.

Der *Edge router* verbindet das 6LoWPAN mit anderen Netzwerken. Wie später noch erläutert wird, basiert 6LoWPAN zwar auf IPv6, verwendet aber stark komprimierte Header, um unnötigen Netzwerkverkehr zu vermeiden. Die Header-Compression und -Extension erfolgt im Edge router und wird durchgeführt, wenn ein Paket das Netzwerk verlässt oder von außerhalb kommt. *Router* erledigen die typische Paketvermittlung innerhalb des Netzwerks. Unter *Hosts* werden alle möglichen Typen von Endgeräten zusammengefasst.

Im Gegensatz zu ZigBee und 6LoWPAN wird bei WirelessHART eine größere Anzahl von Gerätetypen unterschieden:

- Field Devices
- Router
- Adapter
- Handheld
- Gateway
- Access Point
- Network Manager
- Security Manager

Field Devices sind Sensoren und Aktuatoren. Auch Field Devices sind routingfähig, wodurch weniger *Router* eingesetzt werden müssen. *Adapter* ermöglichen HART Geräten den Zugang zu WirelessHART. Ein *Handheld* ist ein portables Gerät, das nur zu Inbetriebnahme- und Analysezwecken eingesetzt wird. Das *Gateway* ermöglicht einem darüberliegenden Automatisierungsnetz wie z.B. Profibus [10] den Zugriff auf Feldgeräte. *Access Points* sind direkt mit dem Gateway verbunden und binden dieses auf Seite der Feldebene in das WirelessHART Netz ein. In einem WirelessHART-Netzwerk gibt es ein Gateway und beliebig viele Access Points. *Network- und Security Manager* verwalten das Netzwerk. Sie sind z.B. für das Aufnehmen neuer Netzteilnehmer und das Verwalten und Ausgeben der Schlüssel zuständig. Gateway, AccessPoint, Network Manager und Security Manager müssen jeweils keine eigenständigen Geräte sein, sondern können auch in einem Gerät untergebracht werden. Die Kommunikation in einem WirelessHART Netzwerk findet üblicherweise zwischen einem Field Device und dem Network Manager oder dem Gateway statt. Die Messdaten werden zu einem überlagerten Automatisierungssystem geleitet, welches anschließend die Aktuatoren mit Steuerdaten versorgt. Dennoch ist auch die Kommunikation zwischen Geräten innerhalb des Netzes möglich. Ein Beispiel dafür ist die Kommunikation eines Handhelds mit einem Field Device.

2.4 Anbindung zur Außenwelt

ZigBee, WirelessHART und 6LoWPAN sind Protokolle, die auf der Feldebene angesiedelt sind. Das heißt, sie sind primär zur Bereitstellung von Kommunikationsmechanismen für rechenleistungsschwache und günstige Sensoren

und Aktuatoren vorgesehen. Sie bieten die Möglichkeit zur Anbindung an ein übergeordnetes Automatisierungsnetzwerk mit leistungsfähigeren Rechnern, die alle verfügbaren Informationen sammeln, verarbeiten und verteilen. Beispielsweise könnte ein deratiges Automationssystem Daten von Temperatursensoren sowie meteorologische Daten aus dem Internet verwenden, um Jalousien und Heizung ensprechend zu steuern.

Bei ZigBee erfolgt diese Anbindung meistens über den Netzwerkkoordinator, da dieser in der Regel über die größten Ressourcen (Rechenleistung und Speicher) aller Knoten verfügt. Prinzipiell kann aber, wie in Abbildung 3 gezeigt, jeder beliebige Knoten für diese Aufgabe konfiguriert werden.

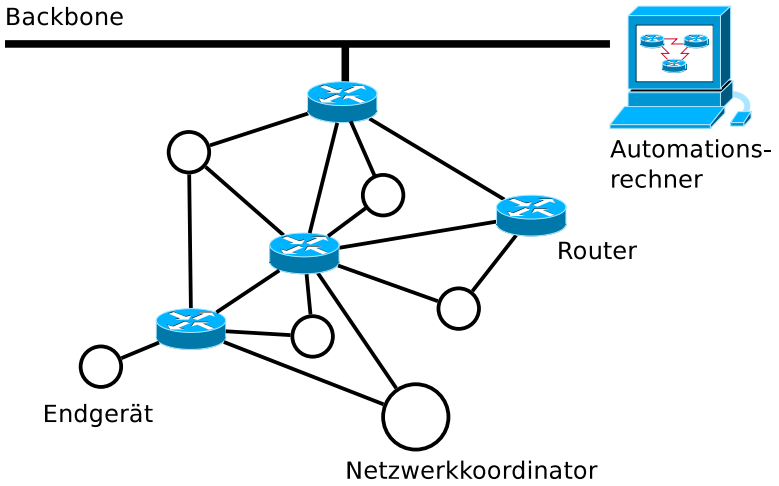

Abb. 3: Typisches ZigBee Netzwerk

Ein WirelessHART-Netzwerk wird über das Gateway mit dem Automatisierungsnetzwerk verbunden. Netzwerkkoordinator und Gateway fungieren als Übersetzer zwischen der Feldebene und der Automationsebene, implementieren also jeweils mindestens 2 vollständige Protokollstacks. Abbildung 4 zeigt ein typisches WirelessHART-Netzwerk, in das auch HART-Geräte über einen Adapter eingebunden sind.

Die Idee von 6LoWPAN ist, dass sowohl das Netwerk auf Feldebene als auch das übergeordnete Automatisierungsnetzwerk IPv6 verwenden. Auf Feldebene steht IPv6 nur in einem eingeschränkten Maß zur Verfügung. Der Edge router ist ein Vermittler zwischen einem 6LoWPAN-Netzwerk und einem IPv6-Netzwerk. Abbildung 5 zeigt die Anbindung eines 6LoWPAN-Netzwerkes an das Internet über einen Edge router. Um das aufwendige IPv6 Protokoll an die

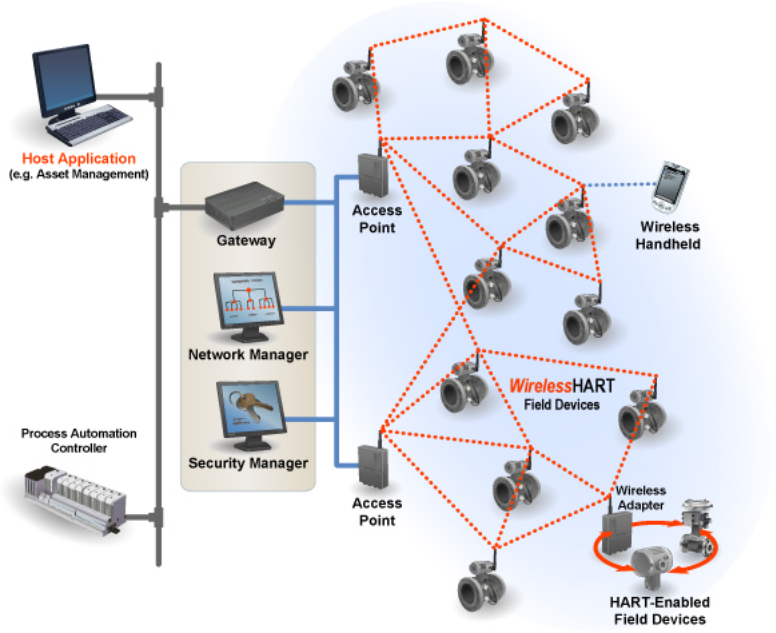

Abb. 4: WirelessHART Netzwerk mit HART Knoten und Anbindung an ein Automatisierungsnetzwerk, Übernommen aus [1]

Anforderungen eines Low power Wirless Personal Area Network, wie geringe Übertragungsraten und kleine Paketgrößen, anzupassen, wurde eine Technik names Header-Compression eingeführt. Dabei eliminiert oder reduziert der Edge router Informationen, die innerhalb eines 6LoWPAN-Netzwerkes nicht benötigt werden und fügt andererseits einem Paket, das das Netz verlässt, die ensprechenden Informationen wieder hinzu. Beispielsweise benötigt ein 6LoWPAN-fähiger Temperatursensor nicht alle 65536 verfügbaren Sockets, sondern kommt auch mit 16 aus. Aus diesem Grund verwendet das Protokoll zwei Bit, die angeben, wie viel Platz im Header für Ziel- und Quellport verwendet wird. So kann die Anzahl, der für die Ports benötigten Bits, von $32(2 * 16)$ auf bis zu $10(2 + 2 * 4)$ reduziert werden. Diese und ähnliche Maßnahmen sind in [11] zusammengefasst.

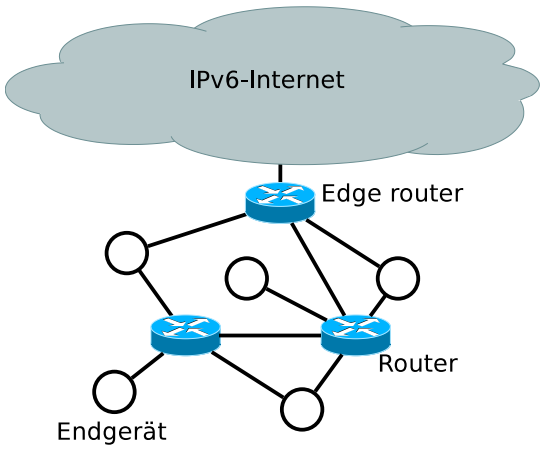

Abb. 5: Anbindung eines 6LoWPAN Netzwerks an das Internet via Edge router

3 Schicht 1 - Bitübertragungsschicht

Sowohl ZigBee also auch 6LoWPAN verwenden (zumindest als eine Möglichkeit) zur ungesicherten Übertragung einzelner Bits den IEEE 802.15.4 Standard, eine “Spezifikation für Low-Rate Wireless Personal Area Networks (WPANs)”. Dieser Standard definiert ein Protokoll für eine energiesparende, kabellose Datenübertragung mit niedrigen Datenraten im Bereich von 20 bis 250 kb/s. Besonderes Augenmerk wurde auf die Einfachheit des Protokolls gelegt, was kostengünstige, batteriebetriebene Geräte ermöglicht.

Der IEEE 802.15.4 Standard spezifiziert sowohl einen physikalischen Layer (Schicht 1) als auch einen Media Access Control (MAC) Layer, als Teil der Schicht 2. Wie in den folgenden Abschnitten ersichtlich ist, wird letzterer jedoch nicht von allen drei Protokollen gleichermaßen genutzt.

Auch wenn WirelessHART den IEEE Standard nicht gänzlich übernimmt, finden sich im Physical Layer nur wenige Unterschiede. Für eine detaillierte Liste der Unterschiede sei auf [12] verwiesen. Sofern sich an der entsprechenden Stelle kein gegenteiliger Hinweis findet, gelten für den IEEE 802.15.4 Standard beschriebene Details auch für WirelessHART.

Weitere Informationen zu IEEE 802.15.4 sind in [3] zu finden.

3.1 Verwendete Frequenzen

Alle drei behandelten Protokolle arbeiten in linzenzfreien Frequenzbändern. Die Vorteile liegen auf der Hand: Die Verwendung ist kostenfrei und bis auf wenige Ausnahmen weltweit uneingeschränkt. Der Nachteil liegt darin, dass es im 2.4 GHz Band zu Kollisionen mit WLAN oder Bluetooth kommen kann.

Der IEEE Standard definiert 16 Kanäle im 2450 MHz (2,4 GHz) Band, 30/10 Kanäle im 915 MHz Band (Amerika und Australien) und 3/1 Kanäle im 868 MHz Band (Europa). Die durch / getrennten Angaben beziehen sich auf den Standard von 2006 bzw. 2003. ZigBee ist dementsprechend auf die letztere Zahl beschränkt. Diese Kanäle können jeweils von verschiedenen Geräten parallel verwendet werden, was höhere Übertragungsraten im Netz und eine effizientere Vermeidung von Kollisionen mit sich bringt. Die Übertragungsraten in den 868 MHz und 915 MHz Bändern bewegen sich je nach verwendeter Frequenz und Modulation zwischen 20 und 250 kb/s. Im 2,4 GHz Band beträgt die Übertragungsrate 250 kb/s. [3]

Da ZigBee und 6LoWPAN den Physical Layer des IEEE Standards verwenden, stehen alle angegebenen Frequenzen zur Verfügung. Zur Verringerung von Kollisionen mit WLAN-Paketen ist es nützlich, sich auf die Verwendung der IEEE 802.15.4 Kanäle 15, 20, 25 und 26 zu beschränken. Diese Frequenzen fallen dann genau zwischen die WLAN-Kanäle 1, 6 und 11 oder in einen höheren Frequenzbereich. Abbildung 6 stellt die Bandbreite der Kanäle beider Protokolle im Spektrum dar. Bläulich markierte Kanäle überlappen sich weniger mit den erwähnten WLAN-Kanälen. [2]

WirelessHART beschränkt sich auf die Verwendung der Kanäle 11-25 im 2,4 GHz Band. Kanal 26 darf nicht in allen Ländern lizenzfrei verwendet werden und wird deshalb von WirelessHART nicht genützt. Außerdem können einzelne Kanäle z.B. bei erkannten wiederholten Störungen vom Network Manager auf eine *Channel Blacklist* gesetzt werden, um die zukünftige Verwendung zeitweise oder völlig auszuschließen. Näheres dazu ist im Abschnitt 4.1.5 festgehalten. [12]

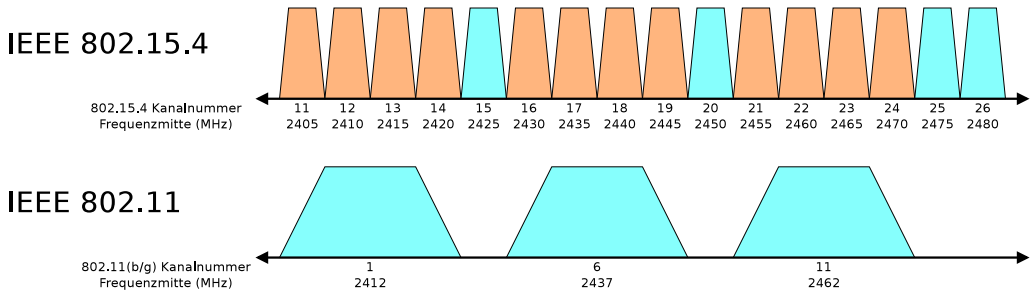

Abb. 6: Funkfrequenzen von IEEE 802.15.4 und IEEE 802.11 WLAN, Auszug aus [2]

4 Schicht 2 - Sicherungsschicht

Die Sicherungsschicht wird (von unten nach oben) in zwei Sublayer unterteilt: MAC (Media Access Control) und LLC (Logical Link Control).

4.1 MAC

Für jedes Medium, das von mehreren Geräten genutzt wird, müssen Vorkehrungen getroffen werden, um Kollisionen zu erkennen, aufzulösen oder zu verhindern. Kommt es zu einer Kollision (von Funksignalen), dann überlagern sich die Funkwellen und aus dem daraus resultierenden Signal kann keines der beiden Ursprungssignale rekonstruiert werden. Abbildung 7 stellt diesen Sachverhalt schematisch dar. Zu dem Zeitpunkt, an dem die teilnehmenden Geräte mit dem Senden beginnen, scheint das Medium aufgrund der Signallaufzeit noch frei zu sein (Teilbild A). Tatsächlich bereitet sich aber bereits eine andere Funkwelle im gleichen Funkraum aus und eine Kollision kann nicht mehr verhindert werden (Teilbild B). Erst nach der doppelten Laufzeit

des Signals durch das gesamte Medium kann davon ausgegangen werden, dass die Übermittlung kollisionsfrei abläuft. Die Erklärung für dieses Phänomen ist aus der Abbildung ersichtlich: Im ungünstigsten Fall sendet der entfernte Netzteilnehmer kurz bevor ihn das eigene Singal erreicht (einfache Laufzeit). Bis die Kollision vom zuerst sendenden Netzteilnehmer erkannt wird, vergeht noch einmal die gleiche Zeit.

ZigBee und 6LoWPAN verwenden den in IEEE 802.15.4 beschriebenen *CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance)* Mechanismus, um Kollisionen zu vermeiden. WirelessHART besitzt hierbei in Bezug auf die drei betrachteten Protokolle eine Eigenheit: Es verwendet *TDMA (Time Division Multiple Access)*, um zu verhindern, dass mehrere Geräte gleichzeitig senden, was eine deterministische und kollisionsfreie Kommunikation ermöglicht.

6LoWPAN bietet auch die Möglichkeit zur Verwendung von *Slotted CSMA/CA*, einer Mischung aus CSMA/CA und TDMA. Da diese Möglichkeit heutzutage jedoch kaum im Einsatz ist [11], wird nur 6LoWPAN mit reinem CSMA/CA betrachtet.

Im Folgenden werden die Funktionsweisen der beiden Mechanismen jeweils kurz erläutert.

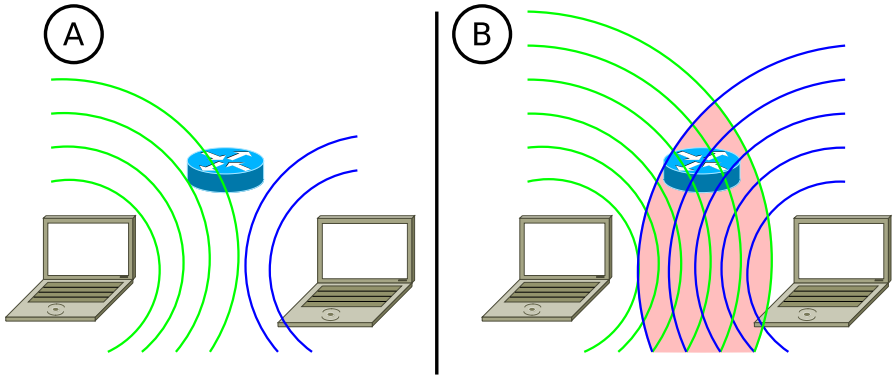

Abb. 7: Kollision zweier Funksignale

4.1.1 CSMA/CA

Beim CSMA/CA [13] handelt es sich um ein Verfahren, das den den Zugriff von mehreren Teilnehmern auf ein einziges Medium (z.B. ein Frequenzband) regelt (Multiple Access). Abbildung 8 zeigt die Funktionsweise des Algorithmus. Bevor ein Teilnehmer sendet, wartet er ein zufällige Zeit. Danach überprüft er, ob das Medium frei ist (Carrier Sense). Ist dies nicht der Fall, muss wieder einer zufällige Zeitspanne abgewartet werden und das Medium wird anschließend erneut überprüft. Dieser Vorgang wiederholt sich so lange, bis das Medium frei ist und gesendet werden kann, oder bis eine festgelegte Anzahl an Fehlversuchen überschritten wurde. In letzterem Fall wird der übergeordneten Schicht mitgeteilt, dass die Übertragung fehlgeschlagen ist. Durch dieses Verfahren sind Kollisionen sehr unwahrscheinlich. Kommt es dennoch zu einer Kollision, wird dies durch Ausbleiben der Bestätigungsnachricht (acknowledgement message) festgestellt und der Algorithmus beginnt erneut. Wie man erkennt, kann bei CSMA/CA keine garantierte Aussage über die Übertragungszeit einer Nachricht getroffen werden. ZigBee und 6LoWPAN sind also keine echtzeitfähigen Protokolle. [3]

4.1.2 TDMA

Die Idee von TDMA ist einfach: Jeder Teilnehmer darf nur zu einem bestimmten Zeitpunkt senden. Sollen beispielsweise X Temperatursensoren (S_0 bis $S_{(X-1)}$) periodisch jede Sekunde die aktuellen Temperatur zu einer zentralen Heizungssteuerung senden, so kann man vereinbaren, dass S_i genau dann senden darf, wenn $(aktuelleSekunde \bmod X) = i$. Tatsachen, wie die Ungenauigkeit von Uhren oder der Wunsch auch zu einem späteren Zeitpunkt Sensoren hinzuzufügen und entfernen zu können, zeigen jedoch, dass dieses einfache Prinzip für den praktischen Gebrauch erweitert werden muss.

4.1.3 Slots & Superframes

Zur Unterteilung der Zeit bedient sich WirelessHART sogenannten *Slots* und *Superframes*, wobei ein Superframe aus einer beliebigen Anzahl an Slots besteht. Abbildung 9 stellt den Aufbau eines Superframes grafisch dar. Jeder dieser Slots umfasst eine Zeitspanne von 10ms. Ein Superframe wiederholt sich, nachdem alle Slots abgearbeitet wurden.

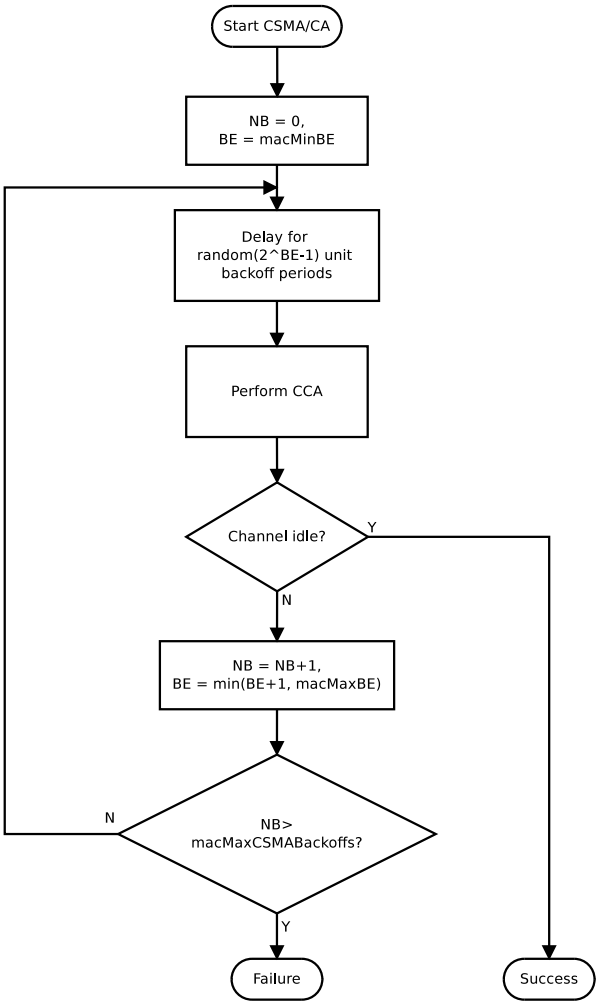

Abb. 8: Carrier Sense Multiple Access / Collision Avoidance - Algorithmus, Auszug aus [3]

Die *ASN (Absolute Slot Number)* ist eine fortlaufende Nummer, die beim Erstellen des Netzwerks auf 0 initialisiert und mit jedem abgelaufenen Slot erhöht wird. Sie hat einen Wertebereich von 0 bis 2^{40} und ist somit für jeden Slot eindeutig.

Die Zuordnung von zwei oder mehr Geräten zu einem Slot auf einem bestimmten Kanal nennt man *Link*. Werden 15 Kanäle verwendet, so gibt es in einem einzigen Slot bis zu 15 Links. Es können also 15 Sender gleichzeitig Daten an 15 Empfänger übermitteln. Diese Links können in einem einzigen Superframe oder verteilt auf mehrer Superframes definiert werden. Details dazu werden im Abschnitt 4.1.5 erläutert.

Die einzelnen Links sind bestimmten Geräten zugeordnet, die in dieser Zeitspanne entweder senden oder empfangen. Üblicherweise sendet pro Link genau eine Quelle (Source), während genau ein anderes Gerät (Ziel / Destination) empfängt. Pro Link wird ein Paket zum Ziel gesendet und dieses bestätigt den Erhalt des Pakets (ACK). Auch Broadcast-Nachrichten mit der Zieladresse 0xFFFF sind möglich. In diesen ist ein Gerät als Quelle und mehrere bzw. alle anderen Geräte als Ziel konfiguriert. Broadcast-Nachrichten werden jedoch im Datalink Layer nicht bestätigt. [4]

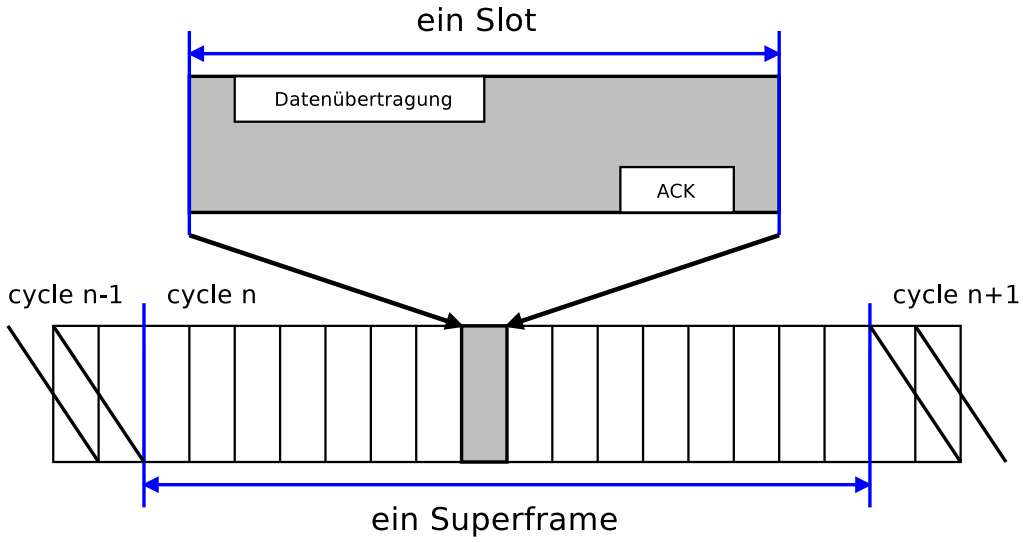

Abb. 9: TDMA Slot und Superframe, Auszug aus [4]

4.1.4 Synchronisation der Uhren

Offensichtlich müssen alle Geräte über eigene Uhren verfügen, um den richtigen Slot innerhalb eines Superframes auswählen und das Timing innerhalb der Slots einhalten zu können. Durch Ungenauigkeiten von Quarzen, Temperaturschwankungen, etc. laufen Uhren jedoch nie exakt gleich schnell und müssen deshalb von Zeit zu Zeit synchronisiert werden.

WirlessHART führt mit jeder gesendeten Nachricht und mit jedem ACK eine Synchronisation der Uhren durch. Dies hat den Vorteil, dass kein zusätzlicher Kommunikationsaufwand nötig ist. Während einer Kommunikation wird das eingehende Paket von Empfänger zeitgestempelt. Auf Grund der gespeicherten Superframe-Konfiguration kann dieser Wert mit dem erwarteten Zeitpunkt des Empfangs verglichen und so die eigene Uhr angepasst werden. Konfiguriert ein Gerät A die Uhr immer nach dem Erhalt von Paketen von Gerät B, so ist B *Time Source* von A. Diese Zuordnung wird vom Network Manager konfiguriert und darf keine Zyklen enthalten. Die als korrekt angesehene Zeit (*ultimate time*) wird vom Gateway vorgegeben und von den Access Points ausgehend im WirlessHART Netz verteilt.

Der Standard spezifiziert zusätzlich, dass ein Gerät bei Temperaturschwankungen von weniger als $2°C$ pro Minute für mindestens 30 Sekunden die Synchronisation auch ohne den Empfang von Paketen erhalten muss, was eine Uhrengenauigkeit von etwa 10ppm (parts per million) oder besser voraussetzt. Gibt es länger keine Kommunikation mit dem Gerät, so würde die Synchronisation verloren gehen. Dies muss durch das Senden einer *Keep-alive* Nachricht verhindert werden. Weitere Probleme wie die Auswirkung von mehreren Hops zum Access Point und ein detailliertes Beispiel zur Berechnung der nötigen Uhrengenauigkeit findet sich in [12].

4.1.5 Frequency Hopping

Wie bereits in Abschnitt 3.1 festgehalten, stehen alleine im 2,4 GHz Band 16 Kanäle zur Verfügung. Der regelmäßige Wechsel des physischen Kanals wird als Frequency Hopping oder Channel Hopping bezeichnet. Der Wechsel kann dabei z.B. nach jedem übertragenen Byte erfolgen. WirelessHART ändert den Kanal nach jedem Slot. Abbildung 10 veranschaulicht den Wechsel des Kanals nach jedem Slot. Zum Übermitteln von Daten ist also zusätzlich zur Information welcher Slot genutzt wird, eine Information über den verwendeten Kanal notwendig. Diese Information befindet sich im *Channel Offset*, welcher

für jeden Link vom Network Manager festgelegt wird und auf allen, zu einem Link zugeordneten Geräten, gespeichert werden muss. Damit nicht in jedem neuen Zyklus eines Superframes immer wieder der gleiche Kanal verwendet wird, berechnet sich der verwendete Kanal nach folgender Formel [4]:

ActiveChannel = (ChannelOffset + ASN) mod (number of active channels)

Die *number of active channels* ist die maximale Anzahl von Kanälen (15) weniger der Anzahl von Kanälen auf der Blacklist. Sie ist auf allen Geräten innerhalb eines WirelessHART Netzwerks ident. Das Ergebnis - der ActiveChannel - beschreibt jedoch nicht die tatsächliche Kanalnummer, sondern einen Index auf eine Liste mit aktiven Kanälen. Andernfalls können laut dieser Formel bei 12 aktiven Channels nur Kanäle mit Indizes < 12 verwendet werden, was natürlich nicht sinnvoll ist. Sind also dem gleichen Slot innerhalb eines oder auch verteilt auf mehrere Superframes mehrere Links zugeordnet, so müssen sich diese Links nur im Channel Offset unterscheiden, um eine Kollision zu verhindern.

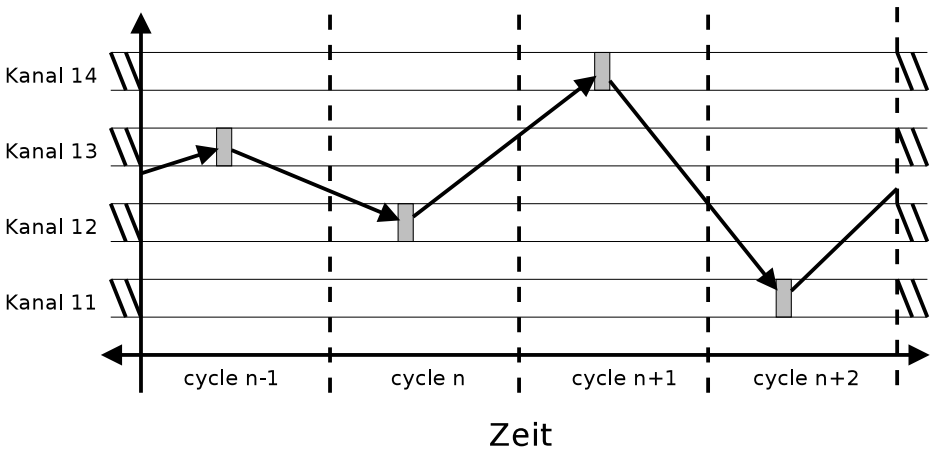

Abb. 10: Frequency Hopping, Auszug aus [4]

4.2 LLC

Die LLC (Logical Link Control) ist die hardwareunabhängige Komponente der Sicherungsschicht und verwendet den MAC Layer, um der Netzwerkschicht Dienste zum Senden und Empfangen von Paketen zur Verfügung zu stellen.

Außerdem werden erste Security-Funktionen implementiert. Mehr dazu im Kapitel 8.

5 Schicht 3 - Netzwerkschicht

Auch in einem Maschennetz müssen Pakete ihren Weg zum Ziel finden. Dafür ist bekanntermaßen die Netzwerkschicht verantwortlich. Zur Vermittlung von Paketen gibt es mehrere grundlegend verschiedene Konzepte, die im Folgenden ausführlich behandelt werden. Die Rede ist von *Source Routing*, welches von ZigBee und WirelessHART genutzt wird, den unter ZigBee und 6LoWPAN eingsetzten Verfahren *Distance-Vector Routing* und *Graph Routing*, sowie Superframe Routing als Eigenheit von WirelessHART.

5.1 Source Routing

Bei der Verwendung von Source Routing enthält die Nachricht die Zieladresse sowie die Adressen aller Knoten, über die es auf dem Weg zum Ziel geroutet werden soll. So kann jeder Knoten, den das Paket entlang eines Pfades passiert, seine eigene Adresse erkennen und das Paket an die nächste angegebene Adresse weiterleiten. Eingesetzt wird Source Routing, wenn die Routing Tabelle eines Knotens im Netzwerks nicht überlastet werden soll. Der Nachteil dieses Ansatzes ist, dass der Absender eines Pakets das gesamte Netzwerk kennen muss, um einen (optimalen) Pfad zum Ziel berechnen können. Um dies zu erreichen haben ZigBee und WirelessHART verschiedene Ansätze. ZigBee verwendet ein Route Record Kommando, welches vom gewünschten Ziel zur Quelle gesendet wird. Jedes Mal, wenn dieses Kommando einen Zwischenknoten passiert, wird dessen Adresse im Nutzdatenbereich des Paketes hinzugefügt. Die Quelle erhält somit einen vollständigen Pfad zum Ziel. ZigBee unterstützt Source Routing seit der ZigBee PRO Version. Bei WirelessHART hat der Network Manager immer Kenntnis über das gesamte Netzwerk. Im Bedarfsfall sendet er die komplette Route von einer Quelle zu einem Ziel mithilfe eines speziellen Kommandos (Write Source-Route) an den Absender des Pakets, welcher diese Information nur noch einfügen muss. [2][12]

5.1.1 Distance-Vector Routing

Beim Distance-Vector Routing tauschen die Router Informationen aus, um zu ermitteln, wie ein Paket am kosteneffizientesten von der Quelle zum Ziel transportiert werden kann. Distance-Vector Routingprotokolle sind also *selbst-organisierend* und es bedarf keines Eingriffs durch eine zentrale Instanz. Nachteilig ist jedoch, dass zur Erstellung der Routen erheblicher Netzwerkverkehr notwendig ist. Weiters gehen in die Berechnung der kostengünstigsten Route Informationen über die Verbindungsqualitäten einzelner Router ein, welche abhängig von der Distanz, Störquellen und anderen Gegebenheiten sind. Somit ist das Ergebnis dieses Routenfindungsprozesses *nicht deterministisch*, und es ist schwierig eine maximale Übertragungsdauer zu berechnen. Distance-Vector Routingprotokolle sind daher nicht echtzeitfähig.

Man unterscheidet weiters zwischen proaktivem und reaktivem Routing. Beim proaktiven Routing werden Informationen gesammelt und in den Routing-Tabellen abgelegt, schon bevor eine Route tatsächlich benötigt wird. Dies ermöglicht im Bedarfsfall eine sehr schnelle Übertragung des Pakets, führt jedoch zu großen Routing-Tabellen mit vielen nicht benötigten Einträgen. Beim reaktiven Routing sucht ein Router erst nach einer günstigen Route, wenn er das Paket weiterleiten soll. Das Vermitteln des ersten Pakets von einer Quelle zu einem Ziel nimmt also längere Zeit in Anspruch. Weitere Pakete können dank der gespeicherten Routinginformationen schneller vermittelt werden, solange diese Informationen nicht durch die Berechnung anderer Routen aus der Routing-Tabelle verdrängt werden.

ZigBee ist auf reaktives Routing beschränkt. Bei der Verwendung von ZigBee PRO kann außerdem eine Hierarchie zwischen den Routern definiert werden. Ein überlasteter Router kann dann das Paket dem ihm übergeordneten Router zur weiteren Vermittlung übergeben. 6LoWPAN unterstützt sowohl proaktive als auch reaktive Routingprotokolle. [11][2]

5.2 Graph Routing

Graph Routing wird von WirelessHART eingesetzt, um garantierte Aussagen über die Vermittlungsdauer von Paketen treffen zu können. Abbildung 11 zeigt ein kleines Netzwerk mit 2 Graphen. Der schwarze Graph führt von S1 nach D1, der orange Graph von S2 nach D2. Die Kanten eines Graphen

sind gerichtet und formen *keine Zyklen*. Alle möglichen Wege durch den gerichteten Graph münden schließlich im selben Zielknoten und haben auf Grund der Zyklenfreiheit eine maximale Länge. Die Entscheidung über welche ausgehende Kante (bzw. über welchen Link zu einem Nachbarn) der jeweilige Knoten das Paket weiterleitet, liegt bei eben diesem Knoten selbst. Dies Erhöht die Redundanz und die Flexibilität. Die Verweildauer eines Paketes im Netz ist jedenfalls begrenzt, die Vermittlung eines Pakets kann also innerhalb einer festgelegten Zeitspanne garantiert werden. Die Graphen werden vom Network Manager erzeugt und anschließend in die betreffenden Geräte geladen. Die Zuordnung von Paketen zu gespeicherten Pfaden erfolgt über die *graph ID*, die als Teil der Nachricht übertragen wird.

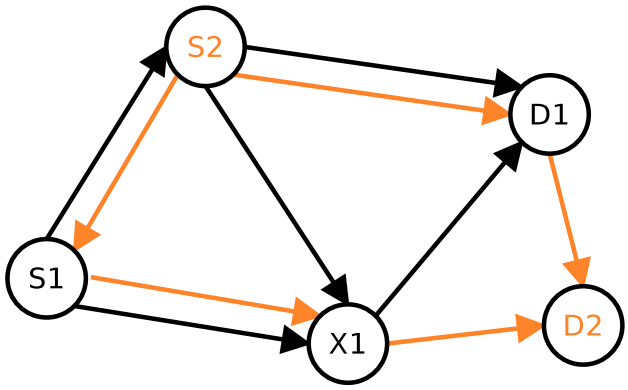

Abb. 11: Graph Routing

Eine spezielle Variante des Graph Routing ist das Superframe Routing. Ist kein Graph mit der entsprechenden Graph ID gespeichert, dann wird das Graph ID Feld der Nachricht als Superframe ID interpretiert. In diesem Fall wird das betreffende Paket an irgendeinen Nachbarn weitergeleitet, zu dem ein Link im betreffenden Superframe existiert. Der Superframe wird wieder vom Network Manager konfiguriert und in die betreffenden Geräte geladen. Tabelle 1 stellt eine zu dem orangen Graph äquivalente Superframekonfiguration dar. Die beiden im Slot 3 angegebenen Links unterscheiden sich im Channel Offset, um Kollisionen zu vermeiden.

6 Schicht 4 - Transportschicht

Das Konzept des Acknowledgements ist im OSI-Referenzmodell der Transportschicht zuzuordnen. Es wird zwischen *bestätigter (acknowledged)* und

Slotnummer	Link
1	S2 → S1
2	S2 → D1
3	S1 → X1, D1 → D2
4	X1 → D2

Tab. 1: Zu Abbildung 11 äquivalente Superframekonfiguration

unbestätigter (unacknowledged) Übertragung unterschieden. Acknowledgment stellt sicher, dass Daten über mehrere Hops erfolgreich zu ihrem Ziel transportiert werden. Bei einer bestätigten Übertragung darf das nächste Paket erst gesendet werden, wenn das Acknowledgment vom letzten Paket eingelangt ist. Dies ermöglicht eine garantierte Übertragung in korrekter Reihenfolge. Bei der unbestätigten Übertragung kann es aufgrund von verschiedenen Routen durch das Netz passieren, dass ein später gesendetes Paket früher beim Ziel ankommt.

Acknowledgment für Nachrichten ist bei ZigBee in die Anwendungsschicht integriert. Ein entsprechendes Bit in der Nachricht legt fest, ob die Bestätigung gefordert wird oder nicht. [14]

Die Ende-zu-Ende-Bestätigung von WirelessHART auf der Transportschicht unterscheidet sich grundlegend von Acknowledgement auf der Sicherungsschicht. Eine Ende-zu-Ende-Bestätigung erfolgt durch eine spezielle Nachricht, die Bestätigung der Sicherungsschicht erfolgt unmittelbar noch im gleichen Slot und nur zwischen benachbarten Geräten. Auch für Broadcast-Nachrichten z.B. zur Vergabe von neuen Schlüsseln können auf der Transportschicht Bestätigungen verlangt werden.

Die Transportschicht des 6LoWPAN Protokolls wird durch die beiden bekannten Protokolle UDP und ICMP gebildet. UDP wird dabei zur normalen Datenübertragung verwendet. ICMP Pakete dienen zur Überprüfung der Erreichbarkeit eines Hosts oder auch zur Mitteilung eines bei der Übertragung aufgetretenen Fehlers.

7 Schicht 5-7

Der Fokus dieser Arbeit liegt auf der Erläuterung von grundlegenden Konzepten, welche bei Wireless-Protokollen zum Einsatz kommen. Die Sitzungs-, Darstellungs- und Anwendungsschicht unterscheiden sich nicht von klassischen, drahtgebundenen Protokollen und werden deshalb nur kurz zusammengefasst. Zudem sind zur Verringerung der Protokollkomplexität auf Feldebene die höheren Schichten nicht streng nach dem OSI-Modell implementiert:

- Die Aufgaben der Sitzungsschicht werden in die Transport- bzw. die Anwendungsschicht verlagert.
- Der Darstellungsschicht kommt in homogenen Systemen keine Bedeutung zu.
- Die Anwendungsschicht ist für die Bereitstellung und den Zugriff auf Daten zuständig. Sie ist protokollabhängig und deshalb im Rahmen dieser Arbeit nicht weiter relevant.

ZigBee, WirelessHART und 6LoWPAN unterscheiden sich in der Implementierung von Sitzungen. Eine *Sitzung (Session)* ist eine üblicherweise private und verschlüsselte Verbindung zwischen zwei Geräten. Im ZigBee-Protokoll ist die Idee einer Sitzung in keiner Weise implementiert.

Bei WirelessHART ist diese Schicht durch Verwendung einer Session Table in die Netzwerkschicht integriert. Diese Tabelle speichert beispielsweise den Schlüssel, welcher für eine Session verwendet wird.

Um das 6LoWPAN Protkoll einfach zu halten, wurde vollkommen auf das Sitzungskonzept verzichtet. 6LoWPAN beinhaltet also keine Sitzungsschicht und ist ein vollkommen verbindungsloses Protokoll. Dies ist auch an den verwendeten verbindungslosen Transportprotokollen UDP und ICMP ersichtlich. Natürlich steht es dem Application Layer frei, sitzungsorientierte Aspekte zu implementieren, auch wenn 6LoWPAN eigentlich nicht dafür gedacht ist.

8 Security

Security ist offensichtlich ein schichtenübergreifendes Thema. Dieses Kapitel gibt deshalb einen kurzen Überblick, wie und in welchen Schichten die einzelnen Protokolle Sicherheitsaspekte implementieren.

Kabellose Netzwerke stellen besondere Anforderungen im Bereich Security, da sie in ihrer Größe nicht eindeutig abgegrenzt werden können. Ein Angreifer kann durch den Einsatz einer stärkeren Antenne auch außerhalb des normalen Operationsradius eines kabellosen Netzwerkes Informationen mitlesen oder gefälschte Pakete in das Netzwerk einschleusen.

Security umfasst vor allem die Bereiche *Authentizität*, *Integrität* und *Verschlüsselung*. Authentizität bedeutet, dass eine empfangene und geprüfte Nachricht sicher vom angegebenen Absender kommt. Die Integrität stellt sicher, dass ein Paket während der Übertragung nicht verändert wurde. Authentizität und Integrität verhindert somit, dass ein möglicher Angreifer Einfluss auf ein Netzwerk nehmen kann. Durch die Verschlüsselung wird das Mitlesen (sniffen) von übertragenen Daten verhindert.

8.1 Mechanismen

8.1.1 AES

Der AES (Advanced Encryption Standard) Algorithmus ist ein *symmetrischer block cipher*. Er verwendet zum Ver- und Entschlüsseln der Daten den gleichen Schlüssel und verarbeitet ausschließlich Blöcke mit einer Länge von 128 Bit. Die Länge des Schlüssels beträgt 128, 192 oder 256 Bit. Der Algorithmus ist in [15] detailliert beschrieben.

8.1.2 CCM*

Alle drei Protokolle verwenden in der einen oder anderen Weise den CCM* Algorithmus. CCM* ist ein im IEEE 802.15.4-2006 festgelegte Verschlüsselungsmodus, der allerdings auch von ZigBee eingesetzt wird. Er verwendet AES zur Verschlüsselung einzelner 128 Bit-Blöcke. Für diese Zwecke ist es ausreichend zu wissen, dass das Verfahren zwei Werte berechnet: Die verschlüsselte Nachricht gleicher Länge und einen Wert U zur Sicherstellung der Authentizität und Integrität, dessen Länge festgelegt werden kann. Tabellen 2 und 3 geben zum besseren Verständnis einen Überblick über einige vom CCM* Algorithmus zur Verschlüsselung verwendete Werte. Bei der Entschlüsselung müssen lediglich c und m vertauscht werden.

Symbol	Bedeutung	Hinweis
a	zusätzliche Daten zur Authentifizierung, die nicht verschlüsselt werden	-
K	der verwendete Key	-
m	die zu verschlüsselnde Nachricht	-
M	die Länge von U	-
N	Nonce, ein eindeutiger Wert der sich für den gleichen Schlüssel nie wiederholt	z.B. verwendet WirlessHART eine Kombination aus ASN und Quelladresse. Dies führt dazu, dass die letztere einer doppelt gesendete Nachricht ungültig ist.

Tab. 2: Eingabeparameter für den CCM* Algorithmus

Symbol	Bedeutung	Hinweis
c	Kombination aus verschlüsselter Nachricht und U	-

Tab. 3: Ausgabewerte des CCM* Algorithmus

8.2 ZigBee

Unter ZigBee ist der Coordinator für die Verwaltung der Schlüssel verantwortlich. ZigBee bezeichnet den Coordinator in diesem Zusammenhang als *Trust Center*. Es ist auch möglich, das Trust Center als eigenständiges Gerät zu implementieren. [2]

8.2.1 Netzwerkschicht

Zur Verschlüsselung von Nachrichten auf der Netzwerkschicht verwendet ZigBee einen *network key*. Dieser ist auf allen Geräten innerhalb eines Netzwerkes gleich. Um sicherzustellen, dass der verwendete Schlüssel nicht aus einer großen verschlüsselten Datenmenge berechnet werden kann, muss er von Zeit zu Zeit ausgetauscht werden. Dieser Vorgang ist nur automatisiert sinnvoll und wird bei ZigBee vom Trust Center durchgeführt. Es sendet den neuen Schlüssel als Broadcast-Nachricht an alle Geräte im Netzwerk. Anschließend wartet es die Bestätigung des Schlüsselerhalts aller Netzteilnehmer ab und veranlasst die Schlüsselübernahme durch eine zweite Broadcast-Nachricht. [2]

8.2.2 Anwendungsschicht

ZigBee verwendete zwei verschiedenen Typen von Schlüsseln in der Anwendungsschicht:

- link key: Diese Schlüssel sind optional. Sie können zur Sicherung von Verbindungen zwischen zwei Geräten in der Anwendungsschicht verwendet werden.
- master key: Master keys werden nie zur Verschlüsselung von Nachrichten verwendet, sondern dienen lediglich zur Erzeugung von link keys.

8.3 WirelessHART

In einem WirelessHART Netzwerk ist der Security Manager für das Verwalten von Schlüsseln zuständig. Er kooperiert dabei mit dem Network Manager in einer Client-Server Architektur. Soll zum Beispiel ein Schlüsselaustausch stattfinden, so fordert der Network Manager einen neuen Schlüssel vom Security

Manager an und verteilt diesen anschließend im Netz. Die Kommunikation der beiden Geräte untereinander ist im Standard nicht festgelegt.

8.3.1 Sicherungsschicht

WirelessHART unterscheidet zwei Schlüsseltypen im Datalink Layer:

- Well-known key: Dieser wird verwendet, wenn eine neues Gerät dem Netzwerk beitreten (joinen) will. Er ist in jedem WirlessHART Gerät fest integriert.
- Network key: Dieser wird dem Gerät nach einem erfolgreichen Join vom Network Manager zugewiesen und laufend ausgetauscht. Er wird zur Bildung des MIC verwendet.

WirlessHART verwendet den CCM* Algorithmus, um die Authentizität und Integrität einer Nachricht sicherzustellen. Dabei werden die Daten selbst nicht verschlüsselt, sondern das Ergebnisfeld U des Algorithmus unter dem Namen MIC (Message Integrity Code) dem Paket als eigenes Feld hinzugefügt. Die eigentliche Verschlüsselung der Daten findet in der Netzwerkschicht statt. Der Empfänger einer Nachricht führt den selben Algorithmus auf die erhaltenen Daten aus und vergleicht das Ergebnis mit dem MIC. Stimmen beide überein, so sind die Daten gültig und werden anschließend in der Netzwerkschicht mit Hilfe von CCM* entschlüsselt.

Der Network Manager sendet von Zeit zu Zeit eine Broadcast-Nachricht, welche den neuen Schlüssel enthält. Diese Nachricht muss von allen Geräten mittels Transport Layer Acknowledgement bestätigt werden. Der Zeitpunkt wann der Schlüssel übernommen werden soll, ist ebenfalls in dieser Nachricht durch die Angabe einer ASN definiert. [4]

8.3.2 Netzwerkschicht

Wie bereits in Kapitel 7 erwähnt, verwaltet WirelessHART einen Session Table zur Sicherung von Sitzungen. Diese ist in der Netzwerkschicht implementiert. Jede Session ist durch einen eigenen *Session Key* gesichert. Beispielszweise erhält ein Gerät beim Einbinden in das Netzwerk jeweils einen Key für Sessions mit dem Network Manager und dem Gateway und weiters zwei Keys zum Entschlüsseln der Broadcast-Nachrichten. Letztere sind auf allen Geräten gleich.

8.4 6LoWPAN

8.4.1 Sicherungsschicht

6LoWPAN schreibt die Verschlüsselung von Links innerhalb eines Netzwerkes mit einer Verschlüsselungsmethode basierend auf AES vor. Weitere Details zur Schlüsselverwaltung und -austausch sind nicht festgelegt und müssen unter Berücksichtigung des Anwendungsgebiets implementiert werden. [16]

8.4.2 IPSEc

Arbeitet eine Anwendung mit sensiblen Daten, welche über einen Edge-Router und das Internet zu einem anderen 6LoWPAN Netz bzw. IPv6-Netz übertragen werden, so muss eine zusätzliches Verschlüsselungsverfahren in den höheren Schichten verwendet werden. Beispielsweise kann IPSec zur Authentifizierung und Verschlüsselung eingesetzt werden. Für Details zu IPsec sei auf [17] verwiesen.

9 Zusammenfassung & Ausblick

Diese Arbeit hat eine Reihe von grundlegenden Konzepten vorgestellt, welche sich in energiesparenden, kabellosen Netzwerken immer wieder finden. Sie hat gezeigt, dass unterschiedliche Protokolle unterschiedliche Vorteile bieten und die Auswahl eines geeigneten Protokolls nur unter Berücksichtigung des gewünschten Anwendungsgebietes getroffen werden kann. Aufgrund der Echtzeitfähigkeit von WirelessHART ist dieses Protokoll sehr gut für die Industrieautomation geeignet. ZigBee und 6LoWPAN werden vor allem in der Home and Building Automation eingesetzt. Als Abschluss fasst Tabelle 4 die wichtigsten Unterschiede nochmals zusammen.

Themenbereich	WirlessHART	6LoWPAN	ZigBee
Netzteilnehmer	Unterscheidet eine Vielzahl von Geräten, jedes davon mit genau spezifizierten Aufgaben. Oft sind mehrere davon in ein einziges Gehäuse integriert. Jedes Gerät ist routingfähig.	Innerhalb des Netzwerkes wird nur zwischen Hosts und Core-Routern unterschieden. Edge-Router stellen eine Verbindung zur IPv6 Außenwelt her.	Der Coordinator ist für die gesamte Verwaltung des Netzes zuständig. Router stellen die Infrastruktur für Endgeräte.
Protokoll stacks	Eigenständiger Stack, untere Schichten stark basierend auf IEEE 802.15.4.	Reduzierte Version von IPv6 mit austauschbarer Sicherungs- und Bitübertragungsschicht.	Basiert auf IEEE 802.15.4, oberen Schichten auf Netzwerk- und Anwendungsschicht reduziert.
Funkfrequenz	Auf das 2,4 GHz-Band beschränkt.	Zus. Verwendung der 868 und 915 MHz Bänder (länderabhängig).	Wie bei 6LoWPAN.
MAC	Echtzeitfähig durch Einsatz von TDMA.	Verwendung von CSMA/CA zur Kollisionsvermeidung	Wie bei 6LoWPAN.
Routing	Echtzeitfähig durch Verwendung von Graph Routing. Unterstützt zusätzlich Source Routing.	Nicht echtzeitfähig wegen Verwendung von Distance-Vector Routing.	Unterstützt Distance-Vector und Source Routing.

Tab. 4: Unterschiede im Überblick

WirelessHART und ZigBee haben ihre Probleme in den Bereichen Störanfälligkeit und Security inzwischen hinter sich gelassen und sind bereit für den Einsatz in einer industriellen Umgebung. Sie werden kabelgebunde Kommunikation wohl lange nicht vollständig verdrängen, haben aber das Potential zur Koexistenz neben bestehenden Feldbussen. Die Anbindung zur darüberliegenden Automationsebene führt zu einer Transparenz des auf der Feldebenen eingesetzten Kommunikationssystems. So macht es für das Automatisierungssystem keinen Unterschied, ob ein Temperatursensor durch eine meterlange Zeidrahtleitung, ZigBee oder WirelessHART an das Netzwerk angebunden ist.

Mit 6LoWPAN wurde ein großer Schritt in Richtung Internet of Things gemacht. Die Idee ist dabei, eine große Vielfalt von Geräten mit dem Internet zu verbinden und ihnen so leichten Zugang zu Information zu verschaffen. Davon profitieren letztendlich Nutzer, die auch im Urlaub sehen können, ob sie das Licht ausgemacht und die Alarmanlage eingeschaltet haben. Und falls nicht ist dies dank 6LoWPAN fähiger Lichtsteuerung und Alarmanlage schnell erledigt. Diese Technik bietet mit IPv6 - dem Zukunftsprotokoll des Internets - eine Vielzahl von Anwendungsmöglichkeiten, die erst noch ausgeschöpft werden muss.

Nicht zuletzt werden aktuelle Entwicklungen im Bereich der drahtlosen Energieübertragung und der Verbesserung von Akkus die Nutzung von kabellosen Protokollen durch den Wegfall störender Stromkabel in vielen Bereichen weiter vorantreiben.

Referenzen

[1] *Wireless HART - How it works*, HART Communication Foundation, 2011, Stand: 2012-04-03. [Online]. Available: http://www.hartcomm.org/protocol/wihart/wireless_how_it_works.html

[2] Daintree Networks, "Getting Started with ZigBee and IEEE 802.15.4," Daintree Networks Inc., Tech. Rep., 2010.

[3] IEEE, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) (IEEE Std 802.15.4-2006)*, Institute of Electrical and Electronics Engineers, Inc., 2006.

[4] HCF, *Industrial communication networks WirelessHart communication network and communication profile (IEC 65C/532/CD:2009))*, HART Communication Foundation, 2009.

[5] IEC, *Actuator sensor interface (AS-i) (IEC 62026-2)*, International Electrotechnical Commission, 2008.

[6] IEEE, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (IEEE 802.11)*, Institute of Electrical and Electronics Engineers, Inc., 2007.

[7] Bluetooth SIG, *Bluetooth Specification Version 4.0*, Bluetooth Special Interest Group Inc., 2010.

[8] ISO/IEC, *Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model (OSI/IEC 7498-1)*, International Standards Organization/International Electrotechnical Commission, 1994.

[9] IEEE, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) (IEEE Std 802.15.4-2006)*, Institute of Electrical and Electronics Engineers, Inc., 2003.

[10] M. Felser, *PROFIBUS Manual: A collection of information explaining PROFIBUS networks.* epubli GMBH, 2011.

[11] Z. Shelby and C. Bormann, *6LowPAN: The Wireless Embedded internet.* Wiley, 2009.

[12] D. Chen, M. Nixon, and A. Mok, *WirelessHART Real-Time Mesh Network for Industrial Automation.* Springer, 2010.

[13] A. Colvin, "CSMA with collision avoidance." *Computer Communications*, vol. 6, no. 5, pp. 227–235, 1983.

[14] ZigBee Standards Organization, *ZigBee Specifiation*, ZigBee Alliance Inc., 2008.

[15] NIST, *Advanced Encryption Standard*, National Institute of Standards and Technology, 2001.

[16] N. Kushalnagar, G. Montenegro, and C. Schumacher, *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals*, 2007, Stand: 2012-04-03. [Online]. Available: http://tools.ietf.org/html/rfc4919

[17] S. Kent and K. Seo, *Security Architecture for the Internet Protocol*, 2005, Stand: 2012-04-03. [Online]. Available: http://tools.ietf.org/html/rfc4301