der Bundeswehr
Universität München
FAKULTÄT FÜR INFORMATIK

Militärische Funkkommunikation

Prof. Dr. Gabi Dreo
Björn Stelte
Sebastian Hanigk
(Hrsg.)

Institut für Technische Informatik

Bericht 2011-02
Juni 2011

Werner-Heisenberg-Weg 39 • 85577 Neubiberg • Germany

Inhaltsverzeichnis

1 Breitbandwellenformen im Einsatz des Joint Fire Support Teams 5

Sebastian Seidel

2 ZigBee und Security 35

Caner Merten

3 DASH-7 Datenkommunikation 55

Paul Watzlawik

4 Funkkommunikation zwischen Drohnen und Bodenstation 77

Raik Kiepert

5 Drahtlose Sensornetze in der Lehre – Sicherheitsbetrachtung von ZigBee-Netzen 103

Björn Stelte

Acronyms 117

Vorwort

Ob Naturkatastrophe, humanitärer oder militärischer Einsatz: Krisen- und Katastropheneinsätze stellen die Einsatzkräfte vor zu bewältigende neue Herausforderungen. Die Einsatzführung muss schnell und sicher die richtigen Entscheidungen treffen können, diese sicher kommunizieren und die richtigen Aktivitäten einleiten. Kommunikation ist in diesem Kontext häufig überlebenswichtig.

Ziel ist die Entwicklung zuverlässiger und sicherer Verbindungen, um in Krisen- und Bedrohungslagen einen reibungslosen Informationsaustausch zwischen den Einsatzkräften zu gewährleisten. Kommunikationssysteme sollen selbst unter widrigen Kommunikationsbedingungen eine robuste und sichere Informationsübertragung gewährleisten. Hierzu bedarf es eines ganzheitlichen Forschungsansatzes. Dieser reicht von der Einsatzplanung, der Analyse von Szenaren, von den elementaren physikalischen Eigenschaften der Funkwellenausbreitung über Modulations- und Multiplexverfahren bis hin zu höheren Protokollschichten und Netzmanagement.

In diesem technischen Bericht werden einzelne Aspekte der militärischen Funkkommunikation dargelegt. Die Arbeiten sind im Rahmen des Seminars “militärische Funkkommunikation” entstanden.

Gabi Dreo Rodosek
Björn Stelte
Sebastian Hanigk

Kapitel 1

Breitbandwellenformen im Einsatz des Joint Fire Support Teams

Sebastian Seidel

Die Streitkräftegemeinsame Taktische Feuerunterstützung ist eines der aktuellen Leuchtturmprojekte der Bundeswehr. Mit ihr soll eine lagegerechte und flexible Feuerunterstützung für alle potenziellen Einsatzszenarien der Bundeswehr ermöglicht werden. Um dies zu gewährleisten, ist eine Einbindung sämtlicher Feuerunterstützungsebenen in die vernetzten Operationsführung (NetOpFü), welche laut Weißbuch 2006 eines der wesentlichen Kernziele der Transformation der Bundeswehr ist, notwendig. Somit muss auch das Joint Fire Support Team (JFST), welches direkt bei der Kampftruppe eingesetzt ist, an das System NetOpFü angebunden werden und mit allen anderen Akteuren der Feuerunterstützung kommunizieren können.
Thema dieser Seminararbeit ist eine Untersuchung der Möglichkeiten zur Kommunikation, welche sich für das JFST durch die Verwendung einer Breitbandwellenform ergeben. Dazu werden Potenzielle Einsatzszenarien für diese Feuerunterstützungskomponente entwickelt und aus diesen Szenarien Anforderungen an und entsprechende Nutzungsmöglichkeiten für die Breitbandwellenform extrahiert. So soll abschließend gefolgert werden, ob sich mit der Breitbandwellenform ein signifikanter Mehrwert für das JFST generieren lässt.

Inhaltsverzeichnis

1.1 Einleitung 7
1.2 Aufgabenspektrum der STF und des JFST 7
1.2.1 Die Streitkräftegemeinsamen Taktischen Feuerunterstützung . 7
1.2.2 Das Joint Fire Support Team 8
1.3 Technische Anforderungen an das Software Defined Radio . 10
1.3.1 Geforderte Fähigkeiten des Grundgerätes 10
1.3.2 Priorisierung der Anforderungen 13
1.4 Potenzial der Breitbandwellenform im Einsatz des JFST . . 13
1.4.1 Die Begriffe Wellenform und Breitbandwellenform 14
1.4.2 Potenzieller Nutzen der Breitbandwellenform 15
1.5 Einsatzszenarien für das Joint Fire Support Team 16
1.5.1 Szenario 1 - Unterstützung einer Panzerkompanie im Angriff . 17
1.5.2 Szenario 2 - Begleitung und Sicherung eines Konvois 19
1.5.3 Szenario 3 - Unterstützen von Kräften bei einer amphibischen Landung 22
1.5.4 Szenario 4 - Unterstützen von Infantrie im Orts- und Häuserkampf 25
1.5.5 Szenario 5 - Unterstützen von verzögernden Kräften 27
1.6 Bewertung und Schlussfolgerung 30

1.1 Einleitung

Die Grundidee einer Breitbandwellenform ist die Nutzung eines möglichst großen Frequenzspektrums bei der Funkkommunikation. Da das Joint Fire Support Team als unterste Ebene der Streitkräftegemeinsamen Taktischen Feuerunterstützung mit einer Vielzahl an Kommunikationspartner Verbindung halten muss, ist die genutzten Kommunikationstechnik von Bedeutung für den Erfolg der Feuerunterstützung. Die Realisierung und Erhaltung der Fähigkeit zur Streitkräftegemeinsamen Taktischen Feuerunterstützung ist eines der wichtigsten aktuellen Projekte der Bundeswehr und ein wesentliches Element der Einsatzfähigkeit in allen Gefechtsintensitäten und Einsatzszenarien. Aus diesem Grund soll in dieser Arbeit untersucht werden, inwieweit die Breitbandwellenform die Kommunikation des JFST verbessern kann um diese Feuerunterstützungsfähigkeit zu optimieren.
Dazu werden zuerst die Begriffe Steitkräftegemeinsame Taktische Feuerunterstützung und Joint Fire Support Team geklärt und deren Aufgaben erläutert. Danach werden kurz die Anforderungen an ein Software Defined Radio für das JFST dargestellt. Daraufhin wird der Begriff der Breitbandwellenform erläutert und eine erste Einschätzung für potentielle Nutzungsmöglichkeiten dieser Wellenform gegeben. Im Hauptteil werden mehrere Szenarien entwickelt, anhand derer eventuelle Vorteile der Breitbandwellenform für das JFST dargestellt werden. So kann abschließend eine Aussage getroffen werden ob die Breitbandwellenform einen wesentlichen Mehrwert für die Streitkräftegemeinsame Taktische Feuerunterstützung auf unterster Ebene bietet.

1.2 Aufgabenspektrum der STF und des JFST

Zunächst soll in diesem Abschnitt dargestellt werden, worin die Aufgaben der Streitkräftegemeinsamen Taktischen Feuerunterstützung (STF) und des Joint Fire Support Teams (JFST) bestehen, da es wesentlich ist das Umfeld, in welchem die Breitbandwellenform eingesetzt werden soll, richtig zu bewerten. Schließlich stellt dieses Einsatzumfeld die Bedingungen auf, denen die Breitbandwellenform schlussendlich genügen muss um einen wesentlichen Mehrwert zu erbringen. Dazu wird eine Definition vorgestellt, welche die Begrifflichkeit der Streitkräftegemeinsamen Taktischen Feuerunterstützung erläutert und das Aufgebenspektrum dieser Feuerunterstützung im Gesamtkonzept der Bundeswehr und ihrer Alliierten dargelegt. Weiter werden die Aufgaben des Vorläufers des Joint Fire Support Teams, des Artillerie Beobachtungstrupps dargestellt, da diese Aufgaben zukünftig durch das Joint Fire Support Team wahrgenommen werden sollen.

1.2.1 Die Streitkräftegemeinsamen Taktischen Feuerunterstützung

Unter Streitkräftegemeinsamen Taktischen Feuerunterstützung versteht man laut den Vorschriften der Bundeswehr folgendes:

- Streitkräftegemeinsamen Taktischen Feuerunterstützung ist die **streitkräftegemeinsame Fähigkeit** zur **gegenseitigen Feuerunterstützung** für die **taktische Ebene** von Land- Luft und Seestreitkräften sowie Spezialkräften **allen Dimensionen** des Einsatzraumes [1].

Es handelt sich hier also um eine Fähigkeit die alle Teilstreitkräfte miteinbezieht und auf taktischer Organisationsebene zur Wirkung kommt. Bereits aus dieser Definition werden einige Anforderungen deutlich, die sich aus der STF für die beteiligten Kräfte ergeben, wie die Fähigkeit teilstreitkraftübergreifend zu kommunizieren und ständig sämtliche Lagedaten aller Kräfte zur Verfügung zu haben.
Dabei umfasst das Aufgabenspektrum der Streitkräftegemeinsamen Taktischen Feuerunterstützung auf allen Ebenen folgende Tätigkeiten:

- Auswahl relevanter Ziele für die Bekämpfung durch Feuerunterstützungsmittel.
- Durchführung einer Risikoabschätzung und die Berücksichtigung von Kollateralschäden.
- Auswahl der geeigneten Wirkmittel und die Koordination dieser Wirkmittel.
- Durchführung der Anweisungen zur Zielbekämpfung.
- Auswertung der Wirkung der eingesetzten Wirkmittel im Ziel. [1]

Um diese Aufgaben erfüllen zu können benötigt die Feuerunterstützung eine Vielzahl von Informationen, welche ihr von anderen Teilen zur Verfügung gestellt werden müssen. Dazu zählen insbesondere sämtliche Lageinformationen über feindliche, eigene und neutrale Kräfte im eigenen Verantworungsbereich sowie alle Informationen über Art, Anzahl und Einsatzbereitschaft der zur Verfügung stehenden Wirkmittel.

1.2.2 Das Joint Fire Support Team

Es ist allerdings nicht Aufgabe dieser Arbeit, das Einsatzspektrum von Breitbandwellenformen in der gesamten Streitkräftegemeinsamen Taktischen Feuerunterstützung zu betrachten, sondern lediglich die Einsatzmöglichkeiten für das Joint Fire Support Team zu beschreiben. Hierbei handelt es sich um die unterste Organisationsebene der taktischen Feuerunterstützung. Ihre Aufgabe besteht im wesentlichen darin die zu unterstützenden Kampftruppen zu begleiten und in direkter Zusammenarbeit die Auftragserfüllung dieser Kräfte zu unterstützen. Es handelt sich hierbei also um ein Element, welches beweglich und direkt im Einsatzgebiet der Kampftruppen handlungsfähig sein muss.
Die Joint Fire Support Teams sollen wie folgt organisiert werden. Es ist vorgesehen, dass sie aus einer Boden-Boden und einer Luft-Boden Komponente a jeweils drei Soldaten ausgestattet mit einem Aufklärungsfahrzeug vom Typ Fennek bestehen. Dieses Fahrzeug ist noch einmal in Bild 2.1. dargestellt. Es bildet mit seinen Fähigkeiten zu Energieversorgung

und zum Transport einen wesentlichen beschränkenden Faktor für die im JFST eingesetzte Funktechnik. Die Boden-Boden Komponente führt das Team und ist für den Einsatz von Rohr- und Raketenartillerie, Seegestützter Artillerie und den behelfsmäßigem Einsatz von Kampfhubschraubern verantwortlich. Die Luft-Boden Anteile koordinieren den Einsatz von Kampfflugzeugen und primär den Einsatz von Kampfhubschraubern. Auch hier wird deutlich das eine ständige Kommunikationsmöglichkeit der beiden Komponenten mit anderen Teilen aber auch untereinander unabdingbar für eine erfolgreiche Auftragserfüllung ist. [2]

Abbildung 1.1: Bild eines Aufklärungsfahrzeuges vom Typ Fennek

Die konkreten Aufgaben des Joint Fire Support Teams entsprechen denen des Artilleriebeobachters, nur das diese beim Joint Fire Support Team für sämtliche Feuerunterstützungsmittel aller Teilstreitkräfte umgesetzt werden.Konkret sind dies die folgenden Teilaufgaben.

- Beratung des Führers Kampftruppe in Fragen der Feuerunterstützung.
- Umsetzung Unterstützungsforderungen des Führers Kampftruppe.
- Durchführung und Überwachung sämtlicher Feueranforderungen an Artillerie, Mörser, Luftfahrzeuge und seegestützte Einheiten.
- Überwachung des Gefechtsfeldes.
- Ortung und Priorisierung von Zielen für die Feuerunterstützung.
- Melden von Aufklärungsergebnissen an den Führer der zu unterstützenden Kampftruppe und die übergeordneten STF-Ebenen. [3]

Auch hier wird wieder klar ersichtlich, dass Kommunikationsverbindungen zu einer Vielzahl an Partnern und die Versorgung mit Lagedaten wesentlich für die Auftragserfüllung sind. Die Vielzahl der genutzten Funkbeziehungen des JFST wird in Abbildung 2.2. verdeutlicht. Nur sind diesmal die beschränkenden Rahmenbedingungen an die eingesetzte

Technik viel strikter als bei unbeweglichen und stationär operierenden Ebenen der STF. Der nächste Abschnitt wird auf diese Restriktionen an das technische Material genauer eingehen.

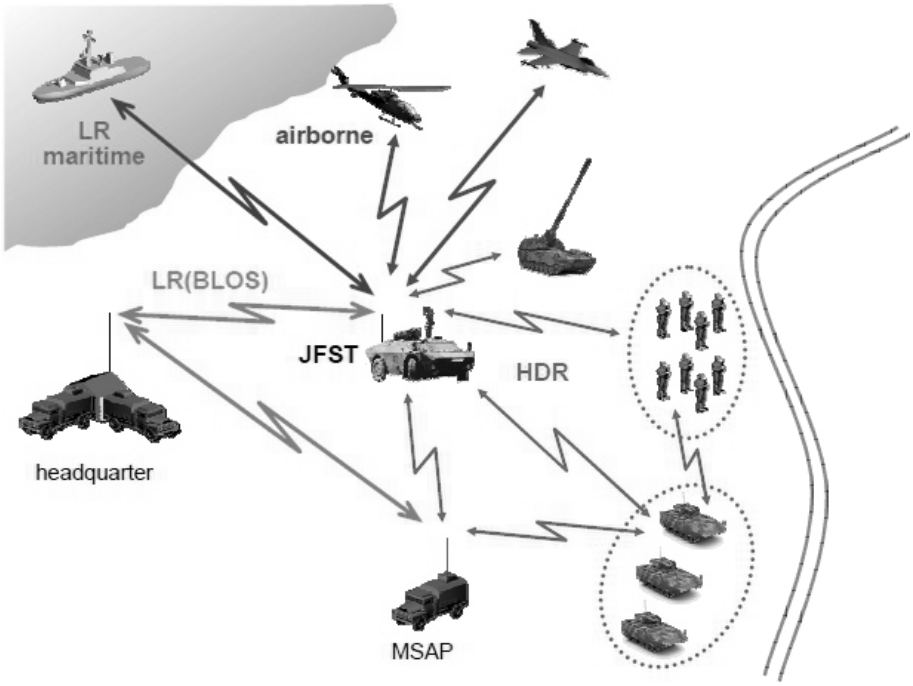

Abbildung 1.2: Kommunikationsverbindungen des Joint Fire Support Teams [4]

1.3 Technische Anforderungen an das Software Defined Radio

Dieser Abschnitt soll darlegen, welche technischen Anforderungen und Rahmenbedingungen an die Realisierung eines Software Defined Radio (SDR) gestellt werden, welches durch das Joint Fire Support Team genutzt werden kann. Zwar ist das Anforderungsprofil an ein solches Gerät nicht Kerninhalt dieser Arbeit, doch lassen sich aus den Anforderungen an das Gesamtgerät auch einige Bedingungen für die Breitbandwellenform ableiten.

1.3.1 Geforderte Fähigkeiten des Grundgerätes

Die eigentlichen Anforderungen an das Gerät existieren bereits und sind vollständig in der Leistungsbeschreibung SVFuA von Dr. Walter Maydl aufgelistet. aus diesem Grund werden hier nur noch einmal die für das Joint Fire Support Team wesentlichsten Anforderungen aufgeführt und erläutert.

Das Software Definded Radio muss **multibandfähig** sein. Es soll in der Lage sein sowohl im HF-, VHF- und UHF-Bereich zu arbeiten. Insbesondere werden folgende Anforderungen gestellt [5]:

- Bereitstellung der Wellenformen Thales SEM 70/80/90.
- Bereitstellung der Wellenform des Infanterist der Zukunft (IdZ).
- Bereitstellung der gebräuchlichen NATO Flugwellenformen.

Durch die Bereitstellung dieser grundlegenden Wellenformen soll die Interoperabilität zwischen der Funkausstattung des Joint Fire Support Teams und der Funkausstattung der zu unterstützenden Kräfte und der Wirkmittel gewährleistet werden.

- Bereitstellung von High-Data-Rate, Long-Range, Anti-Jam und Low-Probability-of-Detection Wellenformen.
- Realisierung eines schnellen und einfach durchzuführenden Wechsels der angesprochenen Wellenformen.

Durch diese Wellenformen und den schnellen Wechsel dieser soll die Funktionssicherheit des Gerätes gewährleistet werden, auch wenn feindliche Kräfte zur elektronischen Kampfführung aktiv sind oder ungünstige äußere Bedingungen wie starke Bebauung vorhanden sind.

Weiterhin soll das eingesetzte Software Defined Radio **plattformübergreifend** arbeiten können. Es ist wesentlich das sowohl Sprache als auch Daten, Link-Kommunikation, sowie ID-gestützte Kommunikation möglich sind.Dabei sind die folgenden Bedingungen wesentlich [5]:

- Fähigkeit zur Verarbeitung von Daten-Nachrichten (ADLER II).
- Fähigkeit zur Verarbeitung von Link-Nachrichten (Link 11/16/22).
- Unterstützung des IP-Protokolls.

Mit diesen Funktionalitäten soll garantiert werden, dass die Funkausstattung auch sämtliche benötigten Nachrichtenformate wie erforderlich verarbeiten und an eventuelle angeschlossene Geräte weiterleiten kann. Die Vernetzung in welche das Gerät später eingebunden werden soll ist in Abbildung 2.3. dargestellt.

Darüber hinaus soll ein **multinational interoperables Sicherheitskonzept** durch das SDR unterstützt werden. Hierzu werden folgende Funktionalitäten gefordert [5]:

- Möglichkeiten zur Verschlüsselung und Authentisierung.
- Erkennen von Störern und Abhörversuchen des Funkverkehrs.

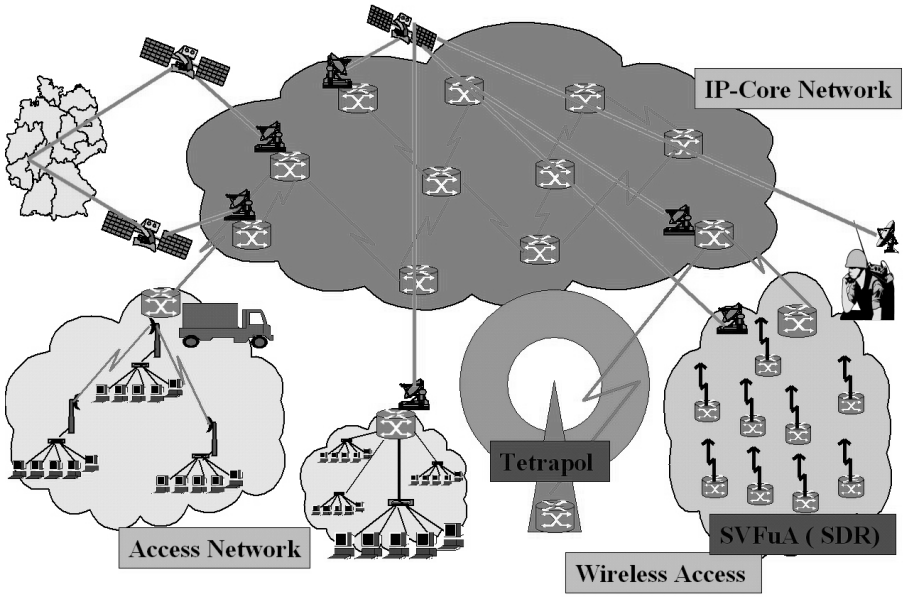

Abbildung 1.3: Vernetzung der SVFuA-Kommunikationsbeziehungen [5]

- Möglichkeiten zur Funkstille.

Auch diese Maßnahmen sollen die Funktionssicherheit sowie die eigene Daten- und Informationssicherheit und Vertraulichkeit garantieren. Es ist allerdings momentan noch kein endgültiges Sicherheitskonzept beschrieben, welches diese Anforderungen multinational für die NATO realisieren soll.

Eine **harte Echtzeitfähigkeit** des ganzen Systems wird ebenfalls gefordert. Für eine vernetzungsfähige Breitbandwellenform (BBWF) muss für eine Ende zu Ende Verbindung über 5 Knoten die Einweglaufzeit maximal 500ms betragen und die Einweglaufzeit einer Sprachübertragung mit mindestens 5 intermittierenden Knoten darf 150ms nicht überschreiten. Insbesondere ist ein Gleichzeitigkeitsbetrieb von Breitbandwellenformen auf mehreren Linien zu gewährleisten. Nur so kann gewährleistet werden, dass zeitkritische Anwendungen wie Feueranforderungen effektiv ausgeführt werden können [5].

Auch eine hohe **Durchhaltefähigkeit** (Einsatzdauer) des Funkgerätes sowie eine signifikante **Robustheit** gegen Umwelteinflüsse werden von dem Gerät verlangt. **Flexible Möglichkeiten zur Einrüstung** in verschiedene Trägersysteme ist eine weitere Forderung. So soll die Hardware mit der 24V Bordspannung operieren können, aber auch sowohl von Seiten der Energieversorgung als auch der Halterung und des Platzbedarfs in verschiedenen Trägersystemen der Bundeswehr nutzbar sein. Die minimale Vorraussetzung ist eine Nutzung in den Fahrzeugen vom Typ Fennek, wünschenswert wäre die Möglichkeit des infanteristischen Einsatzes. Dies beschreibt deutlich den Wunsch nach Flexibilität bei den Einsatzmöglichkeiten des Grundgerätes.
Schlussendlich ist auch die Möglichkeit, das SDR in der **Bewegung in Betrieb** zu neh-

men gefordert. Hier soll das Gerät auch bei 160 km/h Geschwindigkeit noch voll Funktionsfähig sein, was besonders an die IP-Fähigkeit hohe Ansprüche stellt [5].
Dies ist nur ein Ausschnitt der wesentlichsten Leistungskriterien des Grundgerätes, auf welchem auch die Breitbandwellenform eingesetzt werden soll. Eine vollständige Beschreibung findet sich in der Leistungsbeschreibung SVFuA von Dr. Walter Maydl und kann ergänzt werden durch die Studie BBWF und IFM für das SDR Bw von Rhode und Schwarz.

1.3.2 Priorisierung der Anforderungen

Angesichts des umfangreichen Anforderungskataloges an das Grundgerät des Software Defined Radio ist die Frage berechtigt, in welcher Reihenfolge all diese Anforderungen priorisiert werden sollen. Dies ist besonders in anbetracht der Tatsache naheliegend, dass sich einige der Anforderungen bei der Realisierung gegenseitig beschränken. So ist unter Anderem der geforderte hohe Funktionsumfang und die hohe Durchhaltefähigkeit des Gerätes nur auf Kosten der Forderungen nach einem möglichst flexiblen Einsatz auf nahezu allen Plattformen und der damit verbundenen Restriktion in Volumen und Gewicht umzusetzen.
Eine Priorisierung in dem Sinne, dass man zuerst nur bestimmte Funktionalitäten umsetzt und gegebenenfalls sich ausschließende Funktionalitäten verwirft ist allerdings nicht möglich, da alle angegebenen Anforderungen notwendig sind, um ein brauchbares Grundgerät zu entwickeln. Vielmehr ist es notwendig alle Anforderungen bis zu einem festgelegten Grenzwert zu realisieren, so das ein kritisches Maß an Einsatztauglichkeit für das Gerät garantiert werden kann. Das bedeutet, dass Ziel der Entwicklung des Software Defined Radio für die Streitkräftegemeinsame Verbundfähige Funkgeräteausstattung ist die Realisierung einer möglichst großen Schnittmenge aller festgeschriebenen Anforderungen, nicht das Erreichen von Spitzenleistungen in einem einzelnen Bereich zulasten anderer Anforderungen. Dies mag aufgrund der teilweise gegenläufigen Forderungen schwer sein, aber nur so kann durch das Software Defined Radio auch ein wesentlicher Mehrwert in der Kommunikation erzeugt werden. Es ist zum Beispiel unabdingbar, dass alle angesprochenen Wellenformen nutzbar sind und das Grundgerät trotzdem in ein Fahrzeug vom Typ Fennek einrüstbar ist.
Diese Feststellung ist auch im Weiteren wichtig für die Breitbandwellenform an sich, da auch bei dieser widerstreitende Anforderungen auftreten können und auch hier ist es möglicherweise sinnvoller nicht nur eine priorisierte Anforderung zu verfolgen, sondern eine möglichst große Schnittmenge an Funktionalitäten umzusetzen. In späteren Abschnitten werden die hier aufgeführten Forderungen soweit sie für die Breitbandwellenform von Bedeutung sind noch einmal aufgegriffen.

1.4 Potenzial der Breitbandwellenform im Einsatz des JFST

In diesem Abschnitt soll vorgestellt werden, was eine Wellenform im Allgemeinen und was die Breitbandwellenform im Besonderen ist. Weiter wird betrachtet, welchen potenziellen

Nutzen die Breitbandwellenform hat und wie man diesen Nutzen zur Generierung eines Mehrwertes für das Joint Fire Support Team nutzen kann.

1.4.1 Die Begriffe Wellenform und Breitbandwellenform

Zunächst wird hier geklärt was allgemein unter einer **Wellenform** zu verstehen ist. Dazu sei folgende Definition gegeben:

- Eine Wellenform ist die gesamte **Funk-und Kommunikationsfunktionalität**, die in einem Funkgerät **zwischen der Ein- und Ausgabe** von Sprache, Daten und Video an der **Benutzerschnittstelle** und dem **Signal auf der Antenne** realisiert ist [6]. Sie beinhaltet somit alle Umwandlungen, die auf Informationen bei der Übertragung angewendet werden, sowie die dazugehörigen Rückumwandlungen beim Empfänger [7].

Die Wellenform beschreibt also die Behandlung von Sprache, Daten und Videos Zwischen der Benutzerschnittstelle eines Funkgerätes und dem Versenden und Empfangen des Signals über die Antenne. Dazu können Formatumwandlungen, Verschlüsselung oder die Wahl der später genutzten Sendefrequenz gehören. Demzufolge werden die informationstechnischen Funktionalitäten eines Funkgerätes durch sie maßgeblich mitbestimmt.

Da nun der Begriff einer Wellenform geklärt ist wird es Zeit den Begriff der Breitbandwellenform zu definieren. Aus der Definition der Wellenform wird bereits ersichtlich, dass die Breitbandwellenform aufgrund ihrer Eigenschaften erheblich die kommunikationstechnischen Funktionalitäten eines Software Defined Radio mitbestimmt. Diese Eigenschaften werden mit der folgenden Definition dargestellt:

- Die Breitbandwellenform ist eine **Wellenform**, welche auf einer **großen Spanne von Frequenzen** arbeitet. Dabei handelt es sich meist um einen zusammenhängenden Abschnitt auf dem Frequenzband, wobei die **Bandbreiten der einzelnen Kanäle sehr groß** gewählt werden. Die Datenübertragung wird mit Hilfe sogenannter Spreizbandverfahren realisiert. Hierbei werden die Daten geteilt und auf verschiedenen Frequenzen übermittelt [8], [9].

Das wesentliche Charakteristikum an der Breitbandwellenform ist die Tatsache, dass sie auf einer großen Frequenzspanne arbeitet. Es gibt allerdings mehrere Ansatz diese Frequenzspanne auszunutzen. Das Code Division Multiple Access Verfahren (CDMA) teilt die so verfügbare Bandbreite auf mehrere Teilnehmer auf, wodurch diese Teilnehmer entsprechende Daten, Sprache oder Videos empfangen können. Das Frequenzsprungverfahren hingegen nutz die hohe Bandbreite um um bei der Übertragung häufige Frequenzwechsel vorzunehmen. Dies ermöglicht es die Funkkommunikation relativ sicher vor Abhörung oder Störung durchzuführen. Ein drittes Verfahren ist Wideband Code Division Multiple Access (WCDMA). Hier wird die Breitbandübertragung genutzt um besonders hohe Datenraten zu erreichen. [9]

Es wird also ersichtlich, dass das Merkmal der großen Frequenzspanne der Breitbandwellenform für verschiedene technische Funktionalitäten genutzt werden kann. Im Weiteren soll aufgezeigt werden, welche Funktionalitäten für die Nutzung im Software Defined Radio des Joint Fire Support Teams potenziel in Betracht kommen und welchen Mehrwert sie dort realisieren können.

1.4.2 Potenzieller Nutzen der Breitbandwellenform

Es wurde bereits genannt, welche Möglichkeiten es gibt das große Frequenzspektrum der Breitbandwellenform auszunutzen. Noch einmal zusammengefasst sind dies:

- Das Erreichen von hohen Datenraten bei der Datenübertragung durch WCDMA.
- Das Kommunizieren mit verschiedenen Teilnehmern mittels CDMA.
- Die Härtung der eigenen Kommunikation gegen Störung und Abhörung mittels Frequenzsprungverfahren.

Gleicht man diese Funktionalitäten mit den Bedingungen ab, welche das Joint Fire Support Team an seine Kommunikationsverbindungen stellt, so ergeben sich folgende potenzielle Nutzungsmöglichkeiten für die Breitbandwellenform im Einsatz zur Streitkräftegemeinsamen Taktischen Feuerunterstützung durch das JFST:

- **Fördern der Verfügbarkeit aller benötigten Lageinformationen.**
  Das Joint Fire Support Team benötigt ständig aktuelle Lageinformationen über eigene, feindliche und neutrale Kräfte in seinem Verantwortungsbereich. Da diese Informationen sich ständig sehr kurzfristig ändern und eine Vielzahl von Einzelereignissen beschreiben ist es notwendig, dass Lagedaten von signifikanter Größe nahezu in Echtzeit übertragen werden können. Beides kann durch hohe Datenraten bei der Übertragung unterstützt werden. Hier ist demnach die Möglichkeit gegeben, durch die Verwendung einer Breitbandwellenform und WCDMA Die Versorgung des JFST mit Lagedaten sicherzustellen. Je mehr Daten übertragen werden, desto länger dauert auch die Übertragung aller Daten. Da eine harte Echtzeitfähigkeit für die Feuerunterstützung notwendig ist, muss beim Umfang der zur Verfügung gestellten Daten ein akzeptabler Grenzwert gefunden werden.
  Der Einsatz einer Breitbandwellenform unter Nutzung von WCDMA ist folglich für das Joint Fire Support Team potenziell lohnenswert.
- **Fördern der Kommunikation mit allen Wirkmitteln und der Kampftruppe.**
  Um das volle Spektrum der Feuerunterstützung nutzen zu können, muss das Joint Fire Support Team in der Lage sein sowohl mit der zu unterstützenden Kampftruppe als auch mit allen verfügbaren Wirkmitteln und dem Joint Fire Support Coordination Team zu kommunizieren. Nur so kan gewährleistet werden, das wirklich eine optimale Feuerunterstützung durchgeführt wird. Die Breitbandwellenform ermöglicht

die Kommunikation verschiedener Teilnehmern mittels CDMA. So können sowohl Boden- als auch Luft- und Seegestützte Unterstützung angefordert werden. Durch ein ständiges Übermitteln der Feueranforderungen an die übergeordnete Feuerunterstützungsebene sowie an alle Wirksysteme ist es außerdem möglich eventuelle Fehler besser zu erkennen und zu korrigieren.

- **Fördern sicherer und zuverlässiger Kommunikation.**
  Durch die Anwendung von Frequenzsprungverfahren wird ein Mithören des Funkverkehrs und damit auch der Feueranforderungen sowie ein gezieltes Stören der Funkkommunikation erschwert. Dies verbessert zum einen die Funktionssicherheit der Feuerunterstützung, denn ohne Kommunikation zu den Wirkmitteln kann kein Feuer angefordert werden. Zum anderen erhöht dieser Punkt auch die Effizienz des Joint fire Support Teams, da eigene Feueranforderungen nicht abgefangen und feindliche Kräfte nicht vor dem eigenen Feuer gewarnt werden können. Auch die Koordination mit den zu unterstützenden Teilen der Kampftruppe ist deutlich effizienter mit funktionstüchtiger Kommunikation durchzuführen, da das JFST so nicht nur auf vorherige Absprachen angewiesen ist, sondern auch Lageangepasst reagieren kann.

Auf den ersten Blick werden aus der Verwendung einer Breitbandwellenform für das Joint Fire Support Team einige Vorteile deutlich. Im folgenden Abschnitt soll anhand von fünf typischen Szenarien herausgearbeitet werden, ob diese Vorteile wesentlich für den Einsatzwert des Joint Fire Support Teams sind und wie weit die entsprechenden Eigenschaften der Breitbandwellenform mindestens ausgeprägt sein müssen um diese Vorteile zu wahren.

1.5 Einsatzszenarien für das Joint Fire Support Team

Es werden nun fünf Lageausschnitte beschrieben, welche typische Einsatzszenarien des Joint Fire Support Teams skizzieren. Jeder Ausschnitt gliedert sich dabei in 3 Phasen. Anhand dieser kurzen Szenarien soll dann begründet werden, welchen Nutzen die Breitbandwellenform im konkreten Einsatz für das Joint Fire Support Team hat und welche Spezifikationen sie dafür mindestens aufweisen muss. Auf eine vollständige Lagedarstellung zu den einzelnen Lagen soll hier aufgrund des Aufwandes und des mangelnden Nutzens für die Analyse verzichtet werden. Die Basis für die hier entwickelten Beispiele bilden die Feuerunterstützungsvorschriften der Bundeswehr, die Vorschriften für Close Air Support der Nato, die Ausbildungsunterlagen der Offizierschule des Heeres in Dresden sowie das COALWNW Scenario Package 3 und das Konzept der Breitbandwellenform für das SDR Bw von Rhode und Schwarz. Die taktischen Zeichen sind gegeben durch die APP-6 Military Symbols for Land Based Systems der NATO. Die Geländekarten für die taktischen Dartsellungen wurden Google Maps entnommen.
Weiterhin wird darauf verwiesen, dass die hier dargestellten Szenarien sich rein auf das Joint Fire Support Team beziehen und deshalb keine Feuerunterstützung für spezielle Operationen oder ähnliche Anwendungen berücksichtigen. Wenn in den folgenden Szenarien von Blenden, Vernichten, Zerschlagen oder Stören gesprochen wird, so handelt es sich dabei um die Namen konkreter Feueranforderungen an die Wirkmittel der eigenen

Feuerunterstützung.

1.5.1 Szenario 1 - Unterstützung einer Panzerkompanie im Angriff

- **Phase 1**

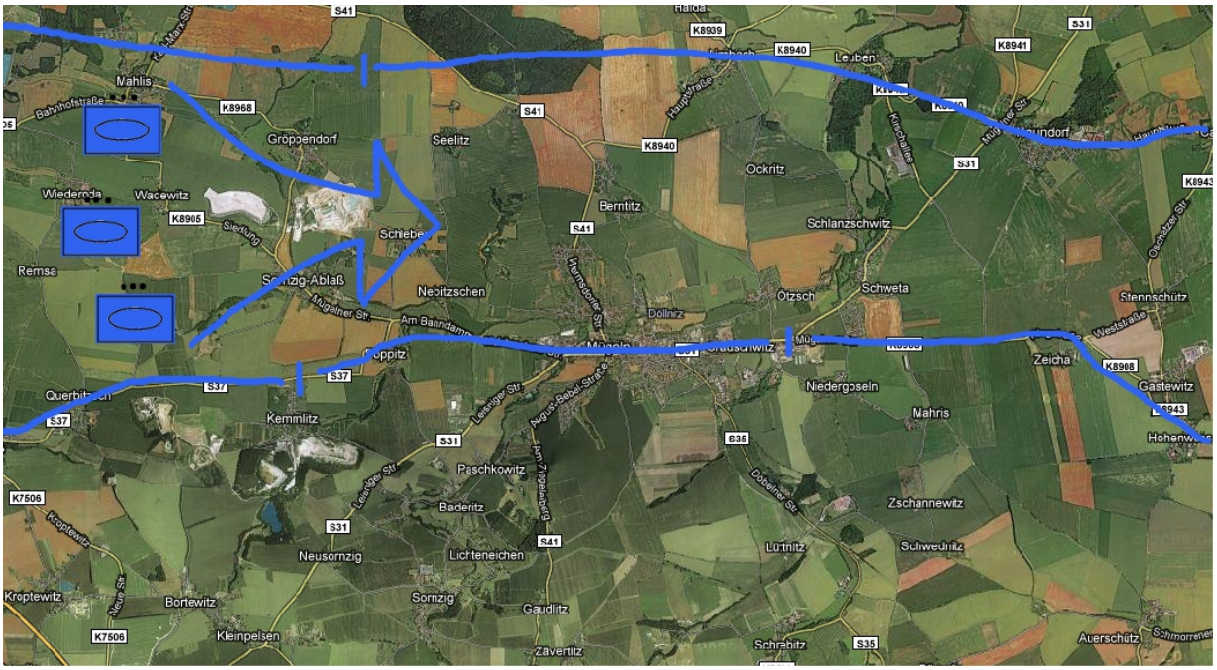

Abbildung 1.4: Unterstützung einer Panzerkompanie im Angriff - Phase 1

Das Joint Fire Support Team befindet ist mit einer Panzerkompanie im Angriff auf Zusammenarbeit angewiesen und befindet sich beim rechts eingesetzten Zug eingegliedert. Während Kompanie und JFST sich in der Angriffsbewegung befinden, informiert das JFST den Kompaniechef, welcher sich beim links eingesetzten Zug befindet, über zusätzliche zur Verfügung stehenden Wirkmittel, welche gerade durch das Joint Fire Support Coordination Team zugewiesen wurden.
Ein Aufrechterhalten der Funkverbindung zu den übergeordneten Feuerunterstützungsebenen und zum Führer Kampftruppe auch in der Bewegung ist also notwendig.

- **Phase 2**
  Während die Kompanie weiter Angreift, wird der links eingesetzte Zug aus bewaldetem Gelände von Panzerabwehrraketen beschossen. Da der Kompaniechef den Angriff weiter fortführen will meldet er dies dem Joint Fire Support Team und fordert bei diesem Feuerunterstützung an. Das JFST leitet die gemeldeten Informationen in einer Wirkungsanforderung an die eigene Artillerie weiter, welche darauf hin ein Zerschlagen auf die angegebenen Koordinaten feuert. Die Panzerkompanie kann den

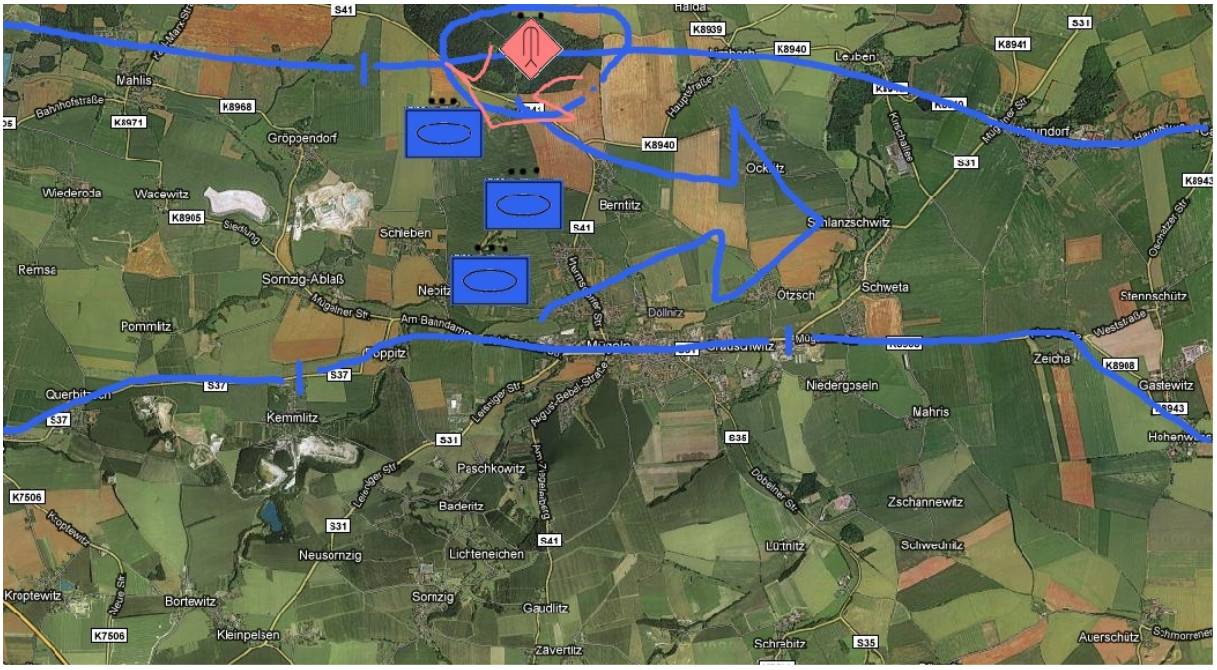

Abbildung 1.5: Unterstützung einer Panzerkompanie im Angriff - Phase 2

Angriff ungehindert fortsetzen.
Hier ist ein Aufrechterhalten der Funkverbindung zu den Wirkmitteln der eigenen Artillerie und zum Führer Kampftruppe in der Bewegung notwendig. Weiter ist eine ständige Echtzeitaktualisierung der Lagedaten notwendig um schnell reagieren zu können.

- **Phase 3**
  Kurz vor erreichen des Zwischenzieles führen zwei feindliche Panzerkompanien einen Gegenangriff in die linke Flanke der angreifenden Panzerkompanie durch. Da es sich hier um überlegenen Feind handelt entscheidet das Joint Fire Support Team in Absprache mit dem Kompaniechef Feuerunterstützung anzufordern. Die linke der feindlichen Kompanien soll durch einen Feuerauftrag Vernichten an die eigene Artillerie mittels SMART-Munition bekämpft werden. Bei der rechten feindlichen Kompanie ist dieses Vorgehen aufgrund der bereits eingetretenen Verzahnung mit einem eigenen Zug nicht möglich. Deshalb fordert der Forward Air Controller des JFST eigene Kampfhubschrauber an und weist diesen die feindlichen Kampfpanzer als Ziel zu. Nach erfolgreicher Bekämpfung der beiden feindlichen Kompanien kann der Angriff fortgesetzt werden.
  Die ständige Echtzeitaktualisierung der Lagedaten ist auch in dieser Phase ein entscheidendes Kriterium für die Handlungsfähigkeit des JFST. Zusätzlich muss hier die störungs- und verzögerungsfreie Funkkommunikation zum Kompaniechef der Panzerkompanie, den Wirkmitteln der eigenen Artillerie und den verfügbaren Kampfhubschraubern garantiert werden um erfolgreich zu sein.

Auswertung Szenario 1:
In diesem Szenario wird der ganze Einsatz des JFST in der Bewegung durchgeführt. Die

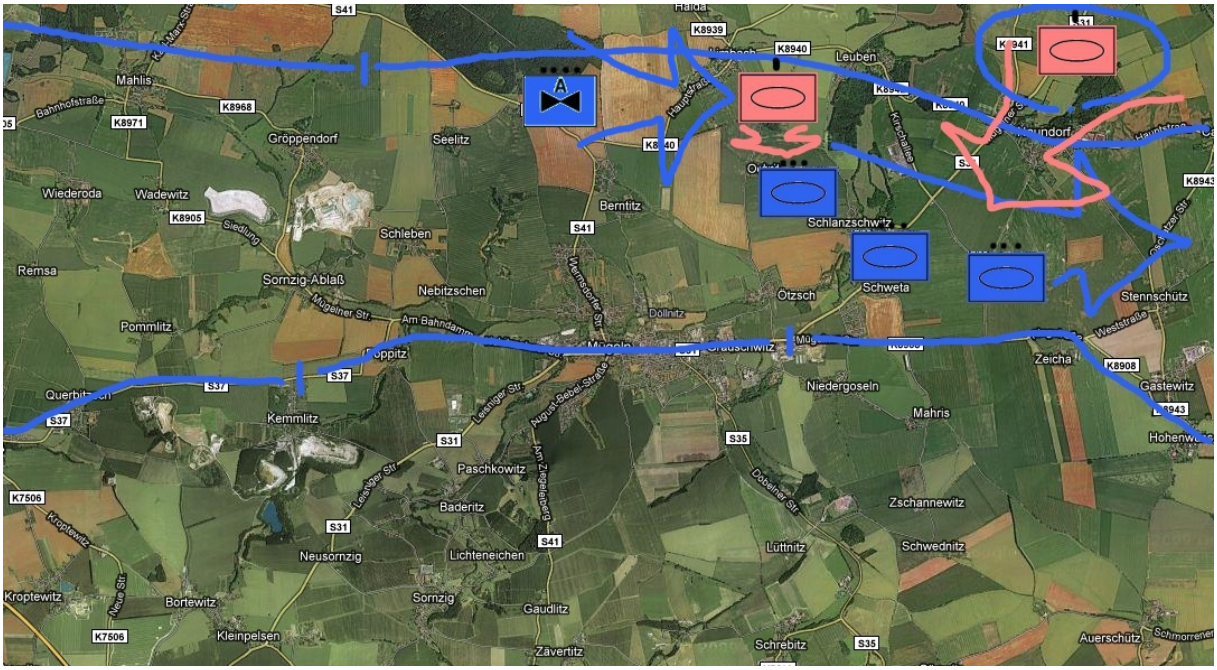

Abbildung 1.6: Unterstützung einer Panzerkompanie im Angriff - Phase 3

Kommunikation muss also auch während der Bewegung bis mindestens zur Höchstgeschwindigkeit des Fahrzeugs Fennek aufrecht erhalten werden. Da die Reaktion auf ständige Lageänderungen eine konstante Echtzeitversorgung mit Lagedaten erfordert muss über die Breitbandwellenform auch eine entsprechend hohe Bandbreite zur Verfügung gestellt werden, um alle Informationen aus dem FüInfoSys H rechtzeitig zu erhalten und lageangepasst reagieren zu können. Da eine ständige Koordination und ein individueller Informationsaustausch mit der Kampftruppe und dem Joint Fire Support Koordination Team notwendig sind, muss die Bretbandwellenform auch die entsprechenden Funkverbindungen zu diesen Teilen realisieren können. Darüber hinaus muss auch die Verbindung zu den Wirkmitteln der Artillerie und den Kampfhubschraubern gehalten werden. Die Frequenzen all dieser Teilnehmer müssen also über das Gerät einzubinden sein. Diese Kommunikation muss auch bei feindlichen Störversuchen aufrecht erhalten werden, das das JFST sonst nicht handlungsfähig ist. Es ist also wünschenswert wenn trotz der anderen hohen Anforderungen die Möglichkeit des Frequency Hopping über die Breitbandwellenform realisiert werden kann.

1.5.2 Szenario 2 - Begleitung und Sicherung eines Konvois

- **Phase 1**
  Das Joint Fire Support Team befindet sich eingegliedert in den zu sichernden Konvoi, welcher sich im Marschband nach Norden bewegt. Plötzlich tritt an der linken Flanke des Konvois Feind auf und nimmt den Konvoi mit Panzerabwehrraketen unter Feuer. Der Konvoiführer entscheidet sich durchzubrechen und den Feind gleichzeitig mit eigenen Feuerunterstützungsmitteln zu bekämpfen und stellt eine entsprechende Anforderung an das Joint Fire Support Team. Der Forward Air Controller des JFST

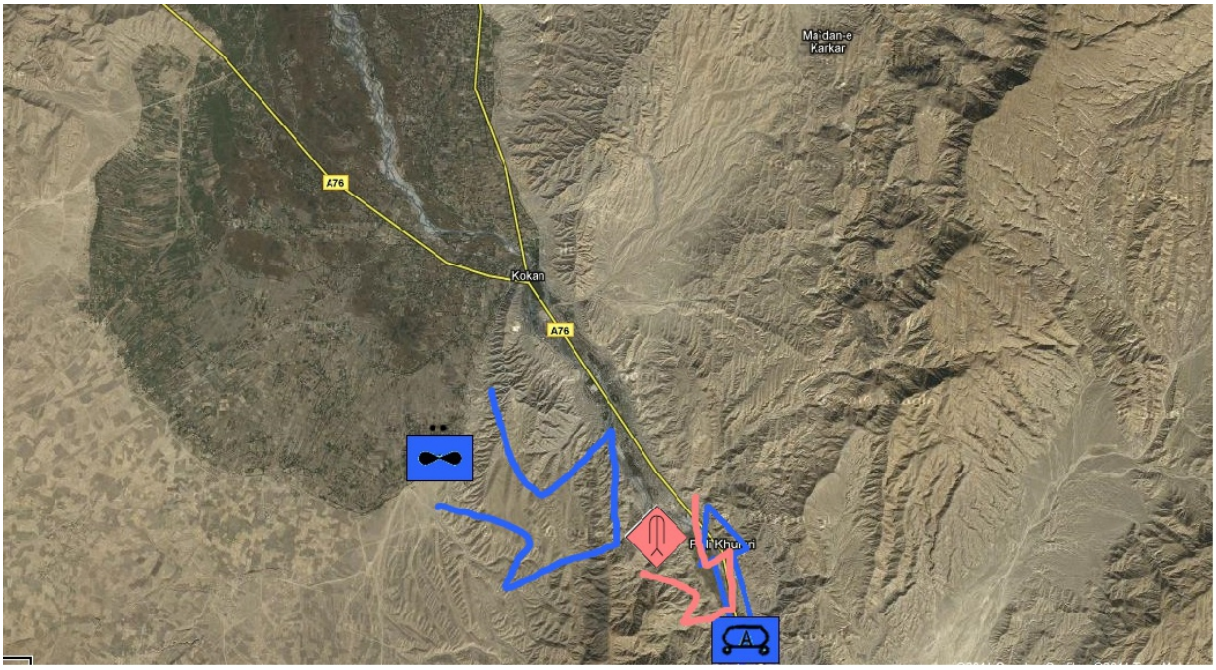

Abbildung 1.7: Begleitung und Sicherung eines Konvois - Phase 1

koordiniert einen Close Air Support alliierter Kampfflugzeuge zum Angriff auf den Feind während der Konvoi wie geplant durchbricht.
In dieser Situation sind die Störungsfreie Funkkommunikation zum Konvoiführer und zu den Kampfflugzeugen der Alliierten absolut notwendig für die Auftragserfüllung.

- **Phase 2**
  Plötzlich kommt der Konvoi zum stehen, die Vorhut meldet das der Feind eine Straßensperre errichtet hat. Auf der rechten Flanke taucht feindliche Infantrie in gut ausgebauten Stellungen auf und nimmt den Konvoi unter Beschuss. Mithilfe der Lagemeldungen entscheidet das Joint Fire Support Team in Absprache mit dem Konvoiführer das Deckungsfeuer des Konvois mit eigenen Kampfhubschraubern zu unterstützen, bis die Sperre beseitigt ist un der Marsch fortgesetzt werden kann. Der Forward Air Controller des JFST koordiniert die Kampfhubschrauber dementsprechend.
  Zu den wichtigen Faktoren für das Joint Fire Support Team gehören in dieser Phase wieder die Garantie der Störungsfreie Funkkommunikation zum Konvoiführer und zu den eigenen Kampfhubschraubern sowie die ständige Versorgung mit Lageinformationen in Echtzeit

- **Phase 3**
  Während der Marsch fortgesetzt wird klärt die Vorhut links der vorgesehenen Marschroute feindliche Infantrie und Panzerabwehrraketen auf und meldet dies umgehend dem Konvoiführer. Dieser entscheidet den Marsch auf einer Ausweichroute fortzusetzen und weist das Joint Fire Support Team an das Ausweichen mit Mitteln der

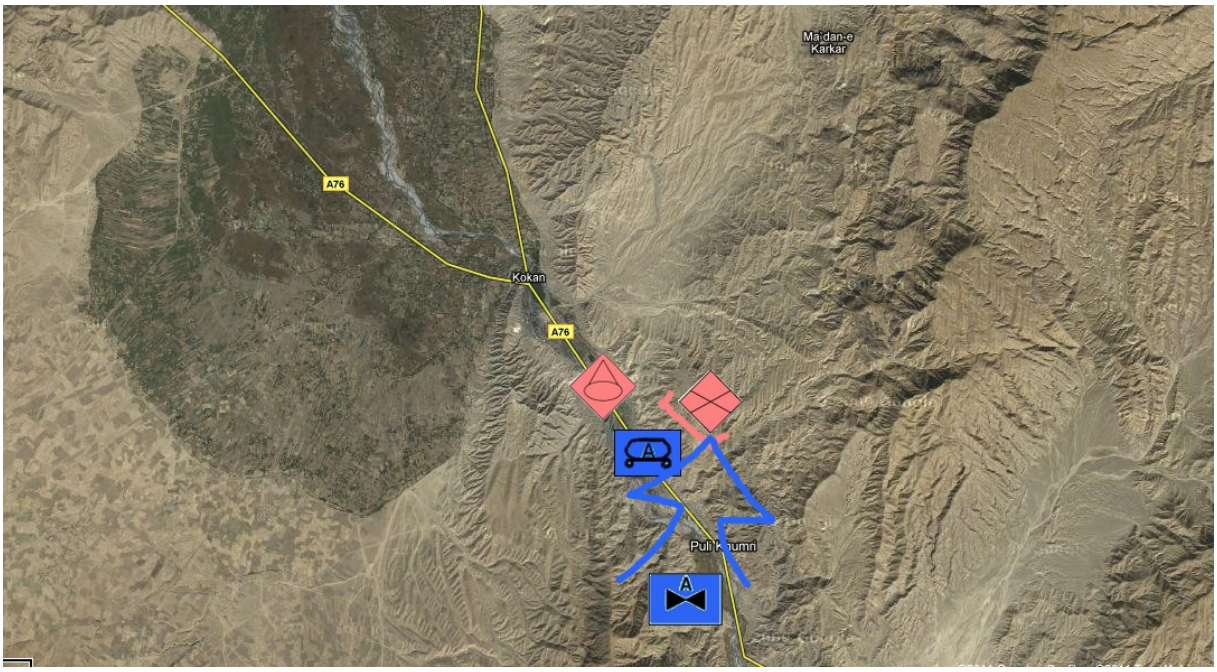

Abbildung 1.8: Begleitung und Sicherung eines Konvois - Phase 2

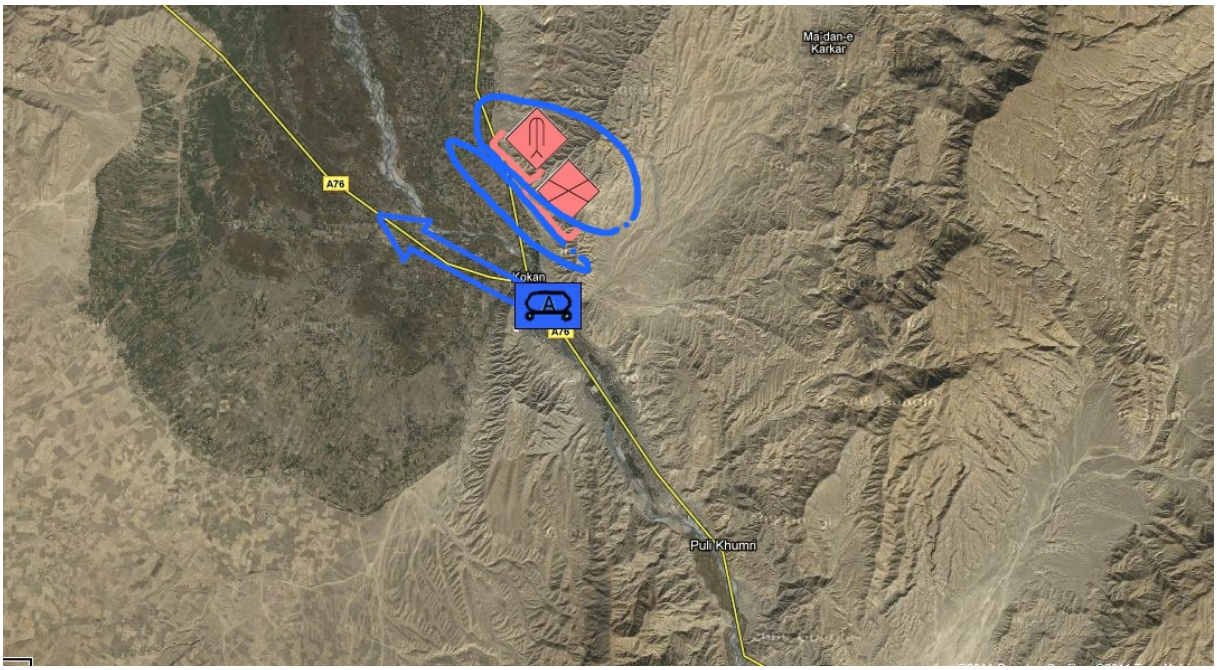

Abbildung 1.9: Begleitung und Sicherung eines Konvois - Phase 3

Feuerunterstützung zu decken. Das Joint Fire Support Team erhält die Koordinaten der feindlichen Kräfte aus den Lageinformationen und fordert von der mittlerweile in Reichweite befindlichen eigenen Artillerie ein Blenden vor sowie ein Stören auf der Position des Feindes an. Der Konvoi nutzt dieses Deckungsfeuer und weicht auf die alternative Marschroute aus.
Die ständige Versorgung mit Lageinformationen in Echtzeit, das Sicherstellen der Funkverbindung zum Führer des Konvois sowie die störungsfreie Kommunikation mit den Wirkmitteln der eigenen Artillerie müssen in dieser Phase erfüllt werden um diese Vorgehensweise umsetzen zu können.

Auswertung Szenario 2:
Auch in diesem Szenario ist das JFST in ständiger Bewegung eingesetzt, auch die Kommunikation wieder in der Bewegung bis mindestens zur Höchstgeschwindigkeit des Fahrzeugs Fennek gearantiert werden muss. Die Reaktion auf ständige Lageänderungen erfordert wieser eine konstante Echtzeitversorgung mit Lagedaten über die Breitbandwellenform und demzufolge auch eine entsprechend hohe Bandbreite, um alle Informationen aus dem FüInfoSys H rechtzeitig zu erhalten. Gerade bei Konvoioperationen kann nie exakt vorausgeplant werden, weshalb diese Bedingung hier von besonderer Bedeutung ist. Die Breitbandwellenform muss auch die Kommunikation mit allen Konvoiteilnehmern, insbesondere dem Konvoiführer, sowie mit den Wirkmitteln der eigenen Artillerie, den Kampfhubschraubern und alliierten Luftfahrzeugen gewährleisten. Entsprechend müssen von der Breitbandwellenform alle benötigten Frequenzspektren sowie ein multinationales Kommunikationskonzept unterstützt werden. Diese Kommunikation muss auch bei feindlichen Störversuchen aufrecht erhalten werden, weshalb die Möglichkeit des Frequency Hopping über die Breitbandwellenform zur Härtung der eigenen Funkverbindungen gegen solche Angriffe wieder neben den anderen Anforderungen realisiert werden sollte.

1.5.3 Szenario 3 - Unterstützen von Kräften bei einer amphibischen Landung

- **Phase 1**
  Das Joint Fire Support Team bezieht eine Beobachtungsstelle südwärts des Gefechtsstreifens der zu unterstützenden alliierten Kräfte, welche die Landung durchführen. Als erstes müssen die feindlichen Luftabwehrstellungen bekämpft werden, damit die alliierten Kampfflugzeuge gegen weitere feindliche Kräfte in der Landungszone vorgehen können. Dazu stellt das Joint Fire Support Team eine entsprechende Wirkungsanforderung an die alliierte Marine und übermittelt dieser die Koordinaten der betreffenden Stellungen, um diese mit Raketen zu bekämpfen.
  Hier ist die Störungsfrei Kommunikation mit den alliierten Seeeinheiten wesentlich.

- **Phase 2**
  Da die feindlichen Luftabwehrstellungen nun bekämpft wurden, kann der Forward Air Controller des Joint Fire Support Teams die Zieldaten der feindlichen Stellungen an die alliierten Kampfflugzeuge übermitteln und deren Waffen ins Ziel lenken.

Abbildung 1.10: Unterstützen von Kräften bei einer amphibischen Landung - Phase 1

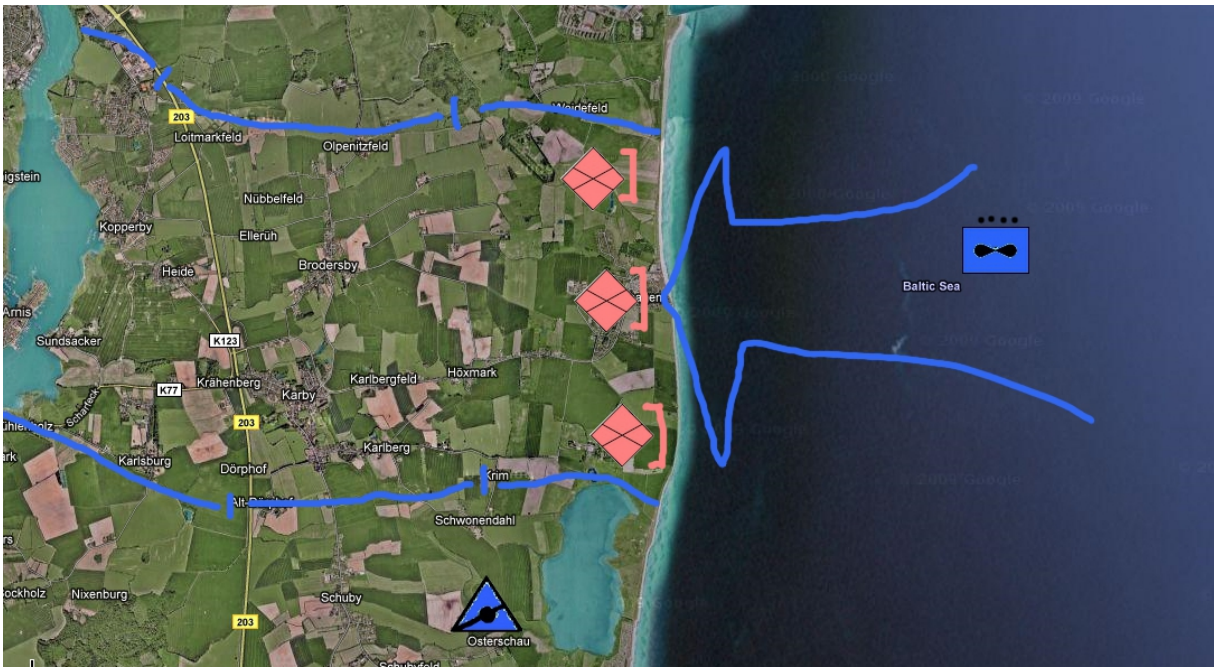

Abbildung 1.11: Unterstützen von Kräften bei einer amphibischen Landung - Phase 2

Die störungsfreie Kommunikation mit den alliierten Kampfflugzeugen ist in dieser Phase wichtig.

- **Phase 3**

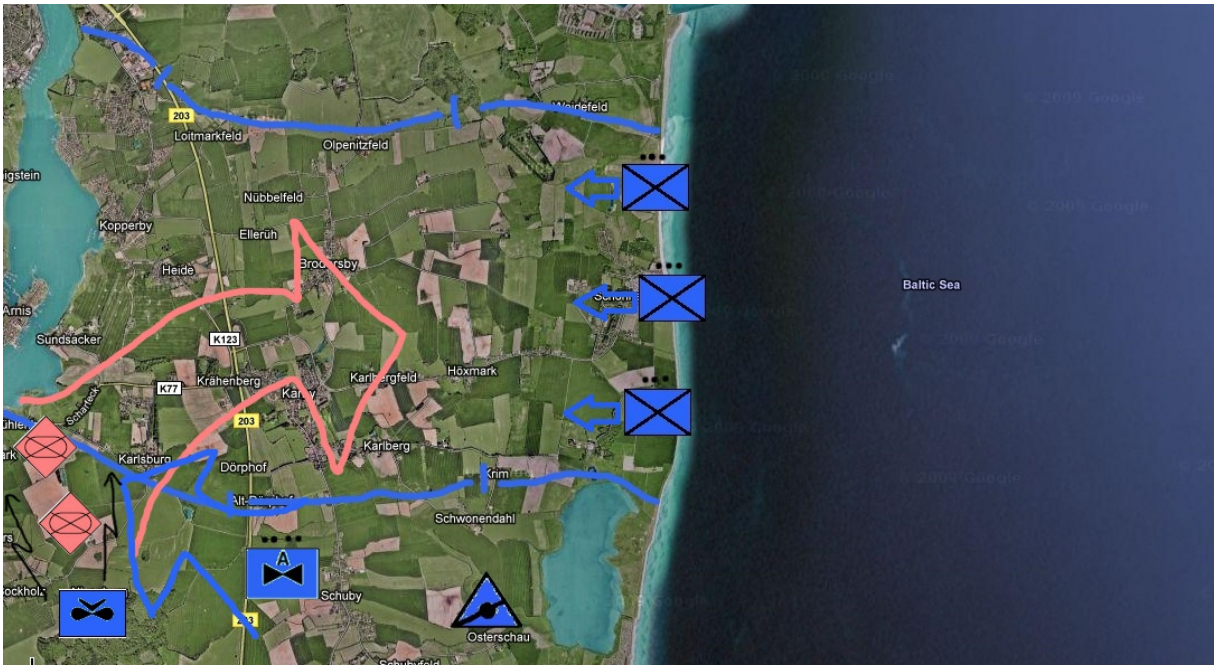

Abbildung 1.12: Unterstützen von Kräften bei einer amphibischen Landung - Phase 3

Während die alliirten Infantriekräfte landen erhält das Joint Fire Support Team von der eigenen Drohnenaufklärung die Meldung, das sich feindliche Panzergrenadierkräfte im Angriff auf die landende Infantrie befinden. Diese Meldung wird umgehend an den Kompaniechef der alliierten Infantrie weitergeleitet, welcher beim Joint Fire Support Team Feuerunterstützung anfordert, da sich seine eigenen Kräfte noch nicht zur Verteidigung einrichten konnten und ihm momentan keine eigenen Feuerunterstützungsmittel zur Vefügung stehen. Der Forward Air Controller des Joint Fire Support Teams fordert daraufhin eigene Kampfhubschrauber an und weist diesen den angreifenden Feind als Ziel zur Bekämpfung zu. Dafür nutzt er die stets aktualisierten Lagedaten der eigenen Drohnenaufklärung.
Für diese Phase sind eine Vielzahl an Faktoren aus sicht der Kommunikation wichtig. Die ständige Versorgung mit Lageinformationen in Echtzeit ist ebenso von Bedeutung wie die störungsfreie Kommunikation mit den alliierten Infantriekräften und der Funkverbindung zu den eigenen Kampfhubschraubern.

Auswertung Szenario 3:
Da hier zum größtenteils mit alliierten Kräften zusammengearbeitet wird ist es wichtig, dass die Funkkommunikation nach einem multinational nutzbaren Konzept strukturiert ist. Das JFST muss mit allieerten Luftfahrzeugen, Seeeinheiten und Infatriekräften sowie mit dem eigenen Joint Fire Support Coordination Team in Funkverbindung stehen, weshalb wieder ein Einsatz der Breitbandwellenform mit verschiedenen Frequenzbändern

gefordert ist. Um die Lageübersicht zu wahren und übergeordnete Aufklärungsmittel effektiv nutzen zu können muss auch eine ständige Lageaktualisierung in Echtzeit spätestens in der kritischen Phase der Landung der alliierten Kräfte gewährleistet werden. Deshalb ist für die Breitbandwellenform wieder die Datenübertragung mit hoher Datenrate in Echtzeit gefordert, um eine Sicherung der landenden Kräfte realisieren zu können. Wie in jedem anderen Fall sollte auch hier noch vorhandenes Potenzial zur Härtung der eigenen Funkkommunikation mittels Frequenzsprung Verfahren genutzt werden, wenn die geforderten Grenzwerte der anderen Anforderungen dadurch nicht gefährdet werden.

1.5.4 Szenario 4 - Unterstützen von Infantrie im Orts- und Häuserkampf

- **Phase 1**

Abbildung 1.13: Unterstützen von Infantrie im Orts- und Häuserkampf - Phase 1

In der ersten Phase des Szenarions muss zunächst der Anmarsch der eigenen Infantriekräfte vor den feindlichen, in Stellung befindlichen Kräften nordwärts der eigenen Teile gedeckt werden, so das diese den westwärtigen Feind in Stelluzng angreifen können. Dazu fordert das Joint Fire Support Team in Absprache mit dem Führer der Infantrie zwei Blenden vor den Stellungen der feindlichen Kräfte im Norden an, welches durch die eigene Artillerie umgesetzt wird. Zuvor vergewissert sich das Joint Fire Support Team mittels der aktuellen Lageinformationen das sich keine Zivilisten auf der Straße aufhalten.
In dieser Phase müssen die störungsfrei Funkommunikation zur eigenen Infantrie sowie zu den Wirkmitteln der eigenen Artillerie gewährleistet sein. Auch eine ständige Versorgung mit Lageinformationen in Echtzeit ist wieder notwendig.

- **Phase 2**

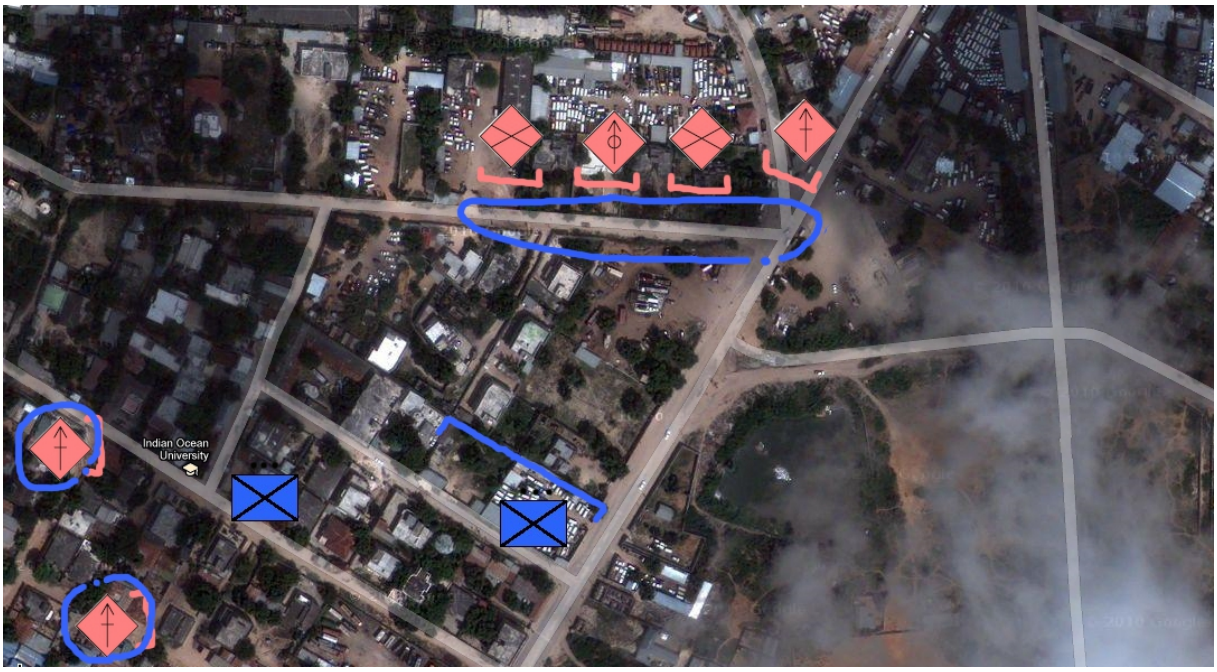

Abbildung 1.14: Unterstützen von Infantrie im Orts- und Häuserkampf - Phase 2

Nachdem die feindlichen Kräfte in Stellung durch die eigene Infantrie bekämpft wurden wird das weitere Vorrücken dieser Infantrie aber durch zwei feindliche Scharfschützen in Stellung erschwert. Eine Bekämpfung dieser Scharfschützen ist nicht möglich, da deren Stellungen zu gut befestigt sind. Der Führer Infantrie fordert deshalb Feuerunterstützung beim Joint Fire Support Team an, welches nach vorheriger Lageprüfung auf Zivilisten in den Zielgebäuden an die eigene Artillerie eine Wirkungsforderung zur Punktzielbekämpfung mittels GMLRS stellt. Währenddessen gehen nachrückende eigene Infantriekräfte unter dem Schutz des anhaltenden Blendens in Stellung Richtung Norden, um die gesamte Operation in dieser Richtung abzusichern.
Die störungsfrei Funkommunikation zur eigenen Infantrie und zu den Wirkmitteln der eigenen Artillerie ist auch in dieser Phase wieder von Bedeutung. Die ständige Versorgung mit Lageinformationen in Echtzeit wird ebenso wieder benötigt, um eventuelle Kollateralschäden zu minimieren.

- **Phase 3**
  Nachdem die feindlichen Scharfschützen eleminiert wurden kann die eigene Infantrie unter Sicherung der nachgeführten Kräfte weiter vorrücken. Dabei werden sie weiter durch das Joint Fire Support Team unterstützt und von diesem mit aktuellen Lageinformationen versorgt.

Auswertung Szenario 4:
In diesem Szenario ist wieder die Nutzung der Breitbandwellenform zur Kommunikation mit den Joint Fire Support Coordination Team, der eigenen Infantrie sowie den Wirkungsmitteln der eigenen Artillerie über mehrere Frequenzbänder gefordert. Darüber hinaus ist

Abbildung 1.15: Unterstützen von Infantrie im Orts- und Häuserkampf - Phase 3

auch die ständige Echtzeitversorgung mit Lagedaten, gerade von Drohnen und andern Aufklärungsmitteln, über die Breitbandwellenform mittels hoher Datenraten von Bedeutung, um in dem unübersichtlichen, urbanen Gelände rechtzeitig auf plötzlich auftretenden Feind reagieren zu können. Wieder ist nach Möglichkeit die Härtung der eigenen Funkkommunikation gegen Störung über Frequency Hopping anzustreben. Zusätzlich gibt es in diesem Szenario zwei Besonderheiten. Zum ersten erfolgt der Einsatz des JFST abgesetzt, da die eigene Infatrie begleitet werden muss. Das bedeutet, dass die Breitbandwellenform entweder von einem Grundgerät aus nutzbar sein muss, welches ein einzelner Soldat ohne größere Einschränkungen tragen kann, oder das eine Nutzung über ein tragbares Funkgerät im Relaybetrieb möglich ist. Zum zweiten muss die Breitbandwellenform in der Lage sein mit Störeffekten aufgrund der verstärkten Bebauung wie Abschattung oder Beugung zurecht zukommen.

1.5.5 Szenario 5 - Unterstützen von verzögernden Kräften

- **Phase 1**
  Das Joint Fire Support Team ist in diesem Szenario mit einer Panzergrenadierkompanie in der Verzögerung auf Zusammenarbeit angewiesen und beim links eingesetzten Zug der selbigen Kompanie angegliedert. Zu Begin der ersten Phase haben die eigenen Pionierkräfte eine Panzerminensperre im rückwärtigen Raum des Verzögerungsstreifens verlegt und melden diese weiter. Diese Meldung erreicht auch das Joint Fire Support Team durch eine kontinuierliche Abfrage und Weitergabe von Lagedaten. Weiter klärt das Joint Fire Support Team vorrückenden überlegenen Feind mit zwei feindlichen Panzerkompanien auf und entscheidet in Absprache mit dem Kompaniechef, diesen mittels Feuerunterstützung zu bekämpfen. Dazu werden

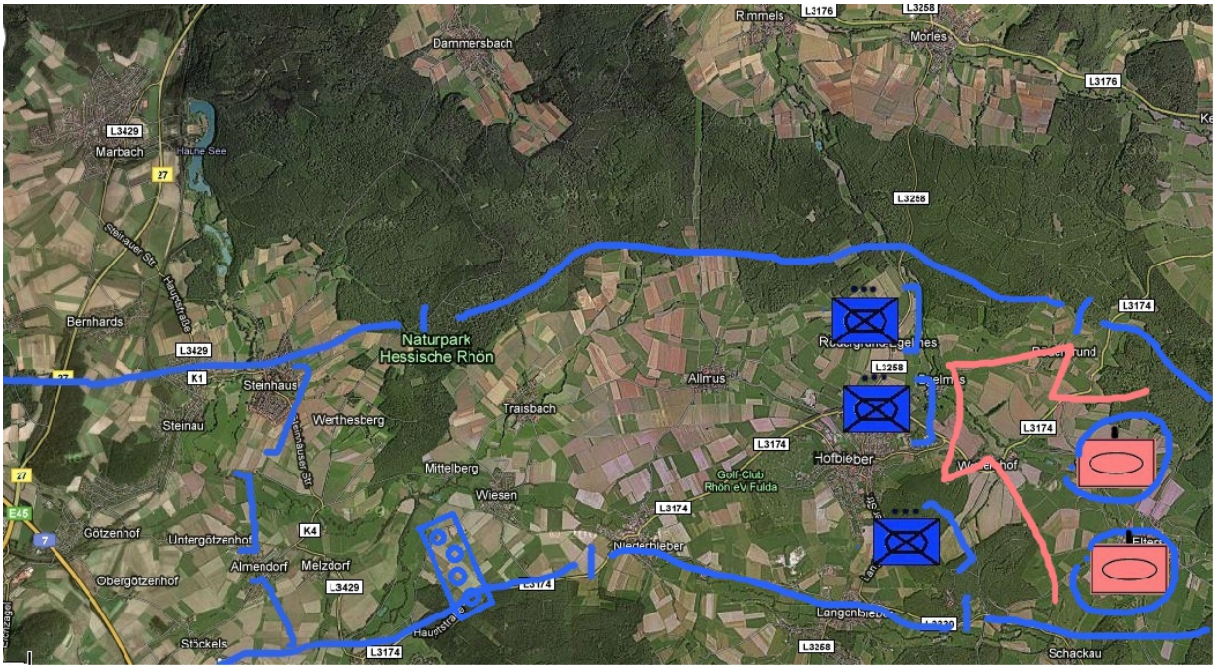

Abbildung 1.16: Unterstützen von verzögernden Kräften - Phase 1

zwei Wirkungsanforderung Vernichten mit SMART-Munition an die eigene Artillerie gesendet.
Um eine erfolgreiche Auftragserfüllung zu garantieren ist hier störungsfreie Funkommunikation zum Kompaniechef und zu den Wirkmitteln der eigenen Artillerie zu garantieren. weiter wird auch wieder eine ständige Versorgung mit Lageinformationen in Echtzeit gefordert.

- **Phase 2**
  Der Kompaniechef meldet das die vorderen Verzögerungsstellungen nicht mehr zu halten sind und entschließt sich mit seiner Kompanie überschlagend in die rückwärtigen Stellungen auszuweichen. Da weiterhin feindliche Kampfpanzer im Angriff sind fordert er beim Joint Fire Support Team Feuerunterstützung zur Verzögerung dieser Kräfte an. Das JFST entscheidet sich in der Angriffsrichtung ein Kombiniertes Blenden und Stören durchführen zu lassen und gibt eine entsprechende Feueranforderung an die Wirkmittel der eigenen Artillerie weiter. Sobald das Feuer liegt meldet das Joint Fire Support Team dem Kompaniechef dies und Koordiniert mit ihm das Ausweichen.
  Die Anforderungen bleiben gleich denen in Phase 1 störungsfreie Funkommunikation zum Kompaniechef und zu den Wirkmitteln der eigenen Artillerie sowie eine ständige Versorgung mit Lageinformationen in Echtzeit

- **Phase 3**
  Der Kompaniechef der Panzergrenadiere meldet dem Joint Fire Support Teamwenn alle seine Teile erfolgreich ausgewichen sind. Notfalls erkennt das Joint Fire Support Team dies auch an den kontinuierlich übermittelten Lageinformationen. Nun wird

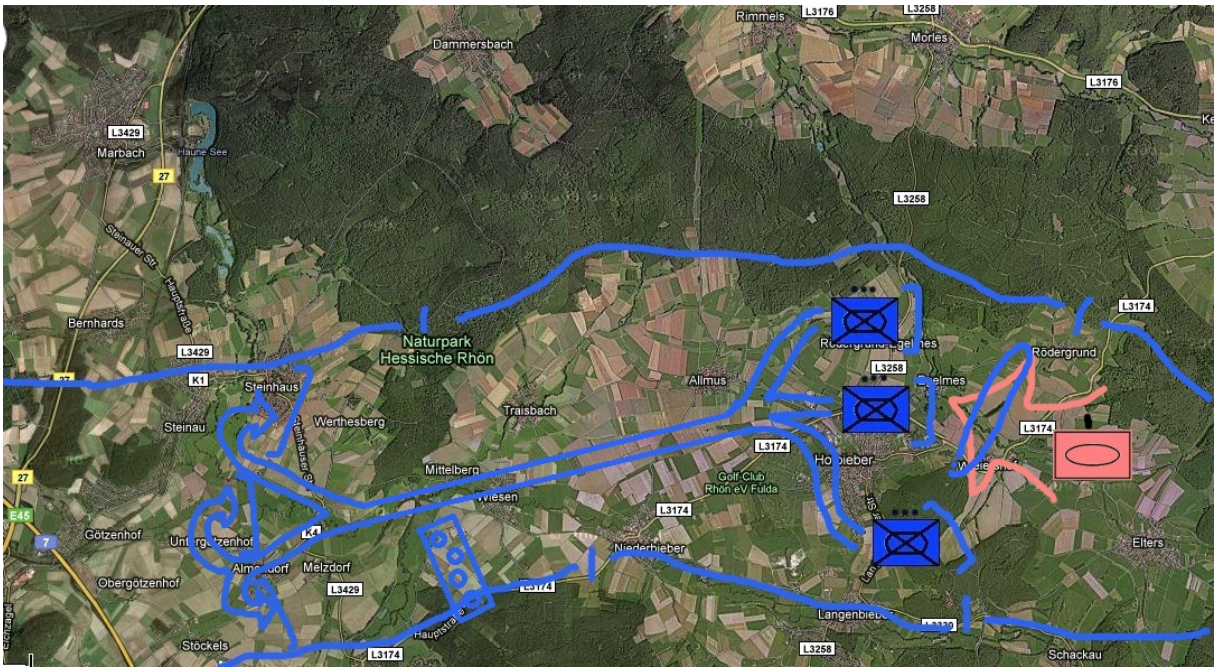

Abbildung 1.17: Unterstützen von verzögernden Kräften - Phase 2

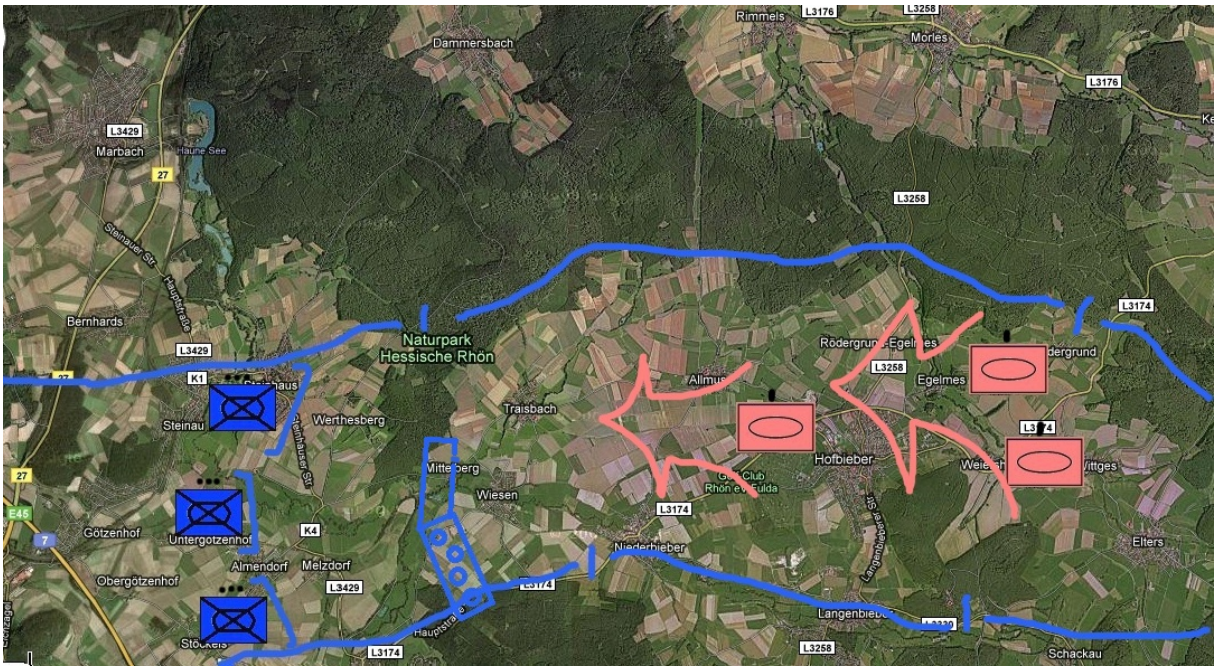

Abbildung 1.18: Unterstützen von verzögernden Kräften - Phase 3

an die eigene Raketenartillerie die Anforderung gesandt möglichst schnell die vorher teilverlegt Minensperre mittels dem Verschuss von Wurfminen zu komplettieren und so die nachdringenden feindlichen Panzer vor der Minensperre zu stauen, damit diese weiter von den Panzergrenadieren und der eigenen Feuerunterstützung bekämpft werden können.
In dieser Phase sind ebenfalls die Anforderungen der vorangegangenen beiden Phasen zu beachten. Besonderer Bedeutung kommt durch das Ausweichen dem ständigen Aktualisieren der Lage des Joint Fire Support Teams zu, da nur so die Minensperren rechtzeitig verschlossen werden kann ohne eigene Teile abzuschneiden.

Auswertung Szenario 5:
Die Anforderungen, welche aus dem Szenario 5 entstehen entsprechen denen aus dem Szenario 1. Der einzige marginale Unterschied ist, dass in diesem Szenario ein besonderer Schwerpunkt auf der ständigen Versorgung mit Lagedaten in Echtzeit liegt, da der Koordinationsaufwand bei der Verzögerung relativ groß ist. Auch muss damit gerechnet werden, dass die eigene Feuerunterstützung überproportional häufig genutzt wird, da die verzögernden Kräfte meist deutlich schwächer sind als die angreifenden feindlichen Kräfte.
Hintergrundquellen für die aufgestellten Szenarien: [1], [3], [5], [10], [11], [12], [13], [14]

1.6 Bewertung und Schlussfolgerung

Im vorherigen Abschnitt wurden aus den fünf beschriebenen Szenarien bereits einige Nutzungsmöglichkeiten der Breitbandwellenform für den Einsatz des JFST herausgestellt. Diese stimmen größtenteils mit den in 2.4.2. angenommenen Nutzungsmöglichkeiten der Breitbandwellenform überein. In diesem Abschnitt sollen die erarbeiteten Nutzungsmöglichkeiten noch einmal aufgelistet und beschrieben werden. Anhand dieser Auflistung soll danach eine Einschätzung erfolgen und begründet werden, ob der Einsatz der Breitbandwellenform im Grundgerät des Software Defined Radio des JFST einen Mehrwert für den Einsatzwert des JFST darstellt.

Folgende Nutzungsmöglichkeiten wurden in Abschnitt 2.5. für die Breitbandwellenform im Einsatz des JFST festgestellt:

- **Die Verbesserung des Lagebewußtseins des JFST und damit eine optimierung seiner Reaktions- und Entscheidungsfähigkeit.**
  Durch die Nutzung der Breitbandwellenform auf der sogenannten letzten Meile im FüInfoSys H kann mittels WCDMA und den daraus resultierenden hohen Datenraten bei der Datenübertragung eine umfassende Übertragung von Lagedaten mit harten Echtzeitkriterien gewährleistet werden. Dazu muss folgende Anforderung erfüllt werden:

  – Die Breitbandwellenform muss in der Lage sein, genügend Bandbreite und damit eine ausreichend hohe Datenrate für die Anbindung an das FüInfoSys H zur Verfügung zu stellen um alle Lagedaten aus diesem, welche im Interessenbereich des JFST liegen, in nahezu Echtzeit an das JFST übertragen können.

- **Die Kommunikation mit allen wesentlichen eigenen Teilen unter Verwendung von möglichst wenig Hardware.**
  Das Kommunizieren mit verschiedenen Teilnehmern mittels CDMA stellt eine Möglichkeit dar, auf einem gemeinsam genutzten Frequenzband unterschiedliche Nutzdaten zu versenden. So kann das JFST mit dem eigenen Joint Fire Support Coordination Team, der zu unterstützenden Kampftruppe und den eigenen Landgestützten Wirkmitteln Verbindung halten. Weiterhin können verschiedene seegestützte Einheiten sowie Luftfahrzeuge Koordiniert werden. Deshalb wird folgende Anforderung gestellt:

  – Die Breitbandwellenform muss in der Lage sein, sowohl im HF- als auch im UHF- und VHF- Bereich zu arbeiten. Weiter soll sie auf dem gleichen Frequenzband zum einen Daten, Sprache und Videos für das Joint Fire Support Coordination Team, die Kampftruppe und die Artillerie und zum anderen für mehrere Seeeinheiten und mehrere Luftfahrzeuge getrennt versenden und empfangen können. Darüber hinaus ist die Fähigkeit zur Verarbeitung von Link-Nachrichten zu gewährleisten.

- **Der Schutz der eigenen Funkkommunikation gegen Störung und Abhörung seitens feindlicher Kräfte.**
  Durch die Nutzung des Frequenzsprungverfahrens auf der großen Bandbreite, welche durch die Breitbandwellenform realisiert wird, ist es möglich das Abhören und Stören des eigenen Funkverkehrs durch feindliche elektronische Kampfführung zu erschweren. Dadurch kann die Funktionssicherheit und Effizienz der zu leistenden Feuerunterstützung optimiert werden. Hierfür wird folgende Anforderung formuliert:

  – Die Breitbandwellenform muss in der Lage sein, auf einem möglichst großen Frequenzspektrum die eigene Kommunikation mit der maximale Anzahl möglicher Sprünge zu realisieren, die ohne Einschränkung der vorher genannten Funktionalitäten möglich sind.

- **Weitere Forderungen.**
  Für den Einsatz der Breitbandwellenform durch das JFST muss auch garantiert werden, das eine Verwendung dieser Wellenform in der Bewegung möglich ist und die Kommunikation auch bei auftretender starker Bebauung oder anderen Geländeeinflüssen Aufrechterhalten werden kann. Hierfür werden folgende Anforderungen formuliert:

  – Die Breitbandwellenform muss bei Geschwindigkeiten bis zur Höchstgeschwindigkeit des Fahrzeugs Fennek genutzt werden können und muss mit einer entsprechend hohe Sendeleistung einsatzbar sein, um auch weiter entfernte Kommunikationsteilnehmer wie das Joint Fire Support Coordination Team oder die eigenen Wirkmittel trotz einschränkendem Gelände erreichen zu können.

Damit sind auch die jeweils zu erfüllenden Mindestgrenzwerte in den gewünschten Funktionalitäten der Breitbandwellenform beschrieben. Ähnlich wie bei der Realisierung des Grundgerätes des Software Defined Radio ist auch hier darauf zu achten, das nicht ein Bereich zu lasten anderer Funktionalitäten besonders ausgeprägt umgesetzt wird. Stattdessen ist es wichtig das die geforderten Grenzwerte bei allen Funktionalitäten erreicht

werden, da nur so mit der Breitbandwellenform ein maximale Mehrwert erreicht werden kann. Weiter ist zu beachten, das die Anforderungen an das Grundgerät aus den Szenarien hier nicht noch einmal aufgeführt wurden, weil sie nicht der Schwerpunkt dieser Arbeit sind, diese aber dennoch beachtet werden müssen um ein brauchbares Gesamtsystem zu entwickeln. Die entsprechenden Anforderungen existieren aber bereits und wurden mit Bezug auf das JFST in 2.3.1. bereits genannt.
Die Nachteile der Umsetzung dieser Ideen sind zum einen, dass man die Schwächen des IP Protokolls, welches für das FüInfoSys H genutzt werden soll, beheben oder umgehen muss um die Kommunikation auch sicher gestalten zu können. Zum zweiten ist die Entwicklung eines solchen Systems sehr komplex und kostenintensiv, so das man für eine akzeptable Realisierung entsprechende finanzielle Mittel, Zeit und technisches KnowHow aufbringen muss. Können diese Probleme jedoch beherrschbar gemacht werden ist der Einsatz der Breitbandwellenform wie gerade dargestellt mit erheblichen Vorteilen verbunden.

Schlussfolgerung:
Wenn man die Eingangs genannten Aufgaben des JFST betrachtet, wird sofort klar das eine stabile Kommunikation und ein stets aktuelles Lagebewußtsein für die Auftragserfüllung der Feuerunterstützung elementar sind. Dies sind auch die Punkte, welche durch die Verwendung der Breitbandwellenform in der Funkausstattung des JFST optimiert werden können. Die Möglichkeit durch eine hohe Bandbreite stets in nahezu Echtzeit alle neuesten Lagedaten zu bekommen steigert die Reaktionszeit des JFST auf plötzliche Lageveränderungen signifikant und wirkt sich positiv auf die Planung der Feuerunterstützung sowie auf die Koordination mit Kampftruppe und Wirkmitteln aus. Eine Bereitstellung von Kommunikationsverbindungen zu allen beteiligten Partnern des JFST ist unerlässlich für die Realisierung der Streitkräftegemeinsamen Taktischen Feuerunterstützung. Da das JFST jedoch maximal den Fennek als Transportfahrzeug zur Verfügung hat ist das mitführen von einer Vielzahl an Funkgeräten zur Kommunikation nicht zweckmäßig und würde darüber hinaus die personelle Struktur eines einzelnen JFST schwer belasten, schlimmstenfalls sogar überlasten. Deshalb ist die Lösung dieses Problems mit einem einzigen Gerät empfehlenswert, wozu die Breitbandwellenform beitragen kann. Schlussendlich ist die Funktionssicherheit der Kommunikation ebenfalls absolut notwendig um ein handlungsfähiges JFST zu erhalten. Die Breitbandwellen könnte auch auf diesem Gebiet von Nutzen sein.
Es ist also festzustellen, dass der Einsatz der Breitbandwellenform den Einsatzwert des JFST erheblich steigern kann und somit einen signifikanten potentiellen Mehrwert für die Feuerunterstützung beinhaltet. Demnach sollte die Entwicklung und Nutzung dieser Wellenform vorangetrieben werden.

Literaturverzeichnis

[1] KGv STF: *Streitkräftegemeinsame Taktische Feuerunterstützung*, 2008

[2] Hptm. Christoph Mahlstedt: *Joint Fire Support im Lehrübungsblock Nord 2009* Zu Gleich - Zeitschrift der Artillerietruppe 2/2009, 2009

[3] HDv 266/200: *Die Feuerunterstützungsorgane der Artillerie*, 2006

[4] Dr. Henrik Schober: *Konzept der Breitbandwellenform für das SDR Bw* Studie BBWF und IFM für das SDR Bw, Rohde und Schwarz, 2007

[5] Dr. Walter Maydl: *Leistungsbeschreibung SVFuA* Anlage A1, 2008

[6] *Joint Programm Executive Office: Joint Tactical Radio System* URL:`http://jpeojtrs.mil` Stand 06.04.2011

[7] Dr. Walter Maydl: *Software Defined Radio* Vortragsfolien IT-Amt der Bundeswehr,

[8] Laurence B. Milstein: *Wideband Code Division Multiple Access* IEEE Journal on Selected Areas in Communications, Ausgabe 18(8), 2000

[9] Marcus Knüpfer: *Ad-Hoc Network (MANET)* Militärische Funkkommunikation, Band 3, 2009

[10] ATP-3.3.2.1(B): *Tactics, Techniques and Procedures for Close Air Support and Air Interdiction)*, 2009

[11] *Ausbildungsunterlagen der Offizierschule des Heeres in Dresden*, 2007-2008

[12] Lt Col. Phil Baker: *COALWNW Scenario Package 3*, 2009

[13] APP-6A: *Military Symbols for Land Based Systems*, 1999

[14] *Google Maps* URL:`http://maps.google.de/` Stand 13.04.2011

Kapitel 2

ZigBee und Security

Caner Merten

Das seit 2004 spezifizierte Funkprotokoll ZigBee ist der momentane Standard bzgl. Kommunikation in low-power Netzen, wie bspw. Sensornetzen. Seit letztem Jahr sind mehr und mehr Schwachstellen des Protokolls bekannt geworden. So hat z. B. das KillerBee Framework eindrucksvoll gezeigt, dass mittels einfacher Methoden ein ZigBee Netz kompromittiert werden kann. Die Arbeit soll einen Überblick über die in der Literatur veröffentlichten Schwachstellen geben und abschließend in einer kurzen Zusammenfassung eine grobe Einteilung der Schwachstellen in Gefährdungsklassen aufstellen.

Inhaltsverzeichnis

2.1 Einführung 37
2.2 Protokolle 38
2.2.1 IEEE 802.15.4 38
2.2.2 ZigBee 41
2.3 Gefahren 44
2.3.1 Schlüsselmanagement 44
2.3.2 Funkübertragung im Allgemeinen 46
2.3.3 Replay 47
2.3.4 Verfügbarkeit und Störanfälligkeit 47
2.3.5 Identitätsdiebstahl eines gültigen Netzwerkgerätes 48
2.3.6 Diebstahl eines ZigBee-Gerätes 49
2.4 Bewertung 51
2.5 Fazit 52

2.1 Einführung

ZigBee ist der Name für einen Protokollstapel, der von einer Allianz, bestehend aus rund 350 Firmen entwickelt wird. Diese Firmen kommen aus dem zivilen Sektor und decken die Bereiche von Mikroprozessorherstellung über Softwareentwicklung bis hin zum Stromversorger ab. Die Allianz wird von 12 Firmen (ember, emerson, freescale, Itron, Kroger, Landis+Gyr, Philips, Reliant Energy, Schneider Electric, STMicroelectronics, Tendril, Texas Instruments) maßgeblich geführt, dazu kommen noch weitere Mitglieder (wie z.B. Intel at&t, Atmel, Electrolux, LG, OKI). Das Ziel deren Bestrebungen ist es, einen Standard zu entwickeln, um ein Netzwerk zum Überwachen, Steuern und Vermessen der realen Welt mithilfe von Kleinstcomputer zu betreiben. Die primären Anforderungen richten sich hierbei auf eine kostengünstige Produktion der Geräte, diese sollen möglichst langlebig sein und ohne externe Stromversorgung auskommen. Im Gegensatz zu anderen Implementierungen im Wireless Personal Area Networks (WPAN) Bereich kommt es hier nicht auf hohe Datenübertragungsraten an, stattdessen soll das Netzwerk möglichst flexibel reagieren können. Zu den typischen Anwendungsbereichen von ZigBee gehören:

- Heim- und Gebäudeautomatisierung: Steuerung der Beleuchtung, Regelung der Klimaanlage, Zugangssysteme, Steuerung von Produktionsabläufen
- Unterhaltungselektronik: Fernbedienung aller Geräte, intelligente Interaktion zwischen Geräten (Herunterregeln der Lautstärke bei einem eingehenden Anruf)
- Medizintechnik: Überwachung von Patienten und Umwelteinflüssen, Unterstützung bei einer Ferndiagnose
- Energieverteilung: Steuerung von elektrischen Verbrauchern, genauere Vorhersage über den Stromverbrauch für Energieversorger
- Telekommunikation: Standortbezogene Dienstleistungen, Micro-Payment, Werbung, Datenübertragung

Keine der aufgelisteten Bereiche entspricht einem klassischen militärischen Anwendungsbereich. Jedoch muss unter dem Aspekt des Cyberwars oder dem des Terrorismus auf wesentliche Grundpfeiler der zivilen Infrastruktur Rücksicht genommen werden. Hier spielt wiederum ZigBee eine immer größer werdende Rolle. Zumal wird bei der Einführung neuer Systeme beim Militär auch die Benutzung ziviler Techniken zur Kostenreduzierung und Interoperabilität in Erwägung gezogen. Die zunehmende Integration elektronischer Systeme in unser alltägliches Leben fordert eine gründliche Betrachtung der Sicherheit der dahinterliegenden Mechanismen. Vor allem bei Sensor- und Steuernetzen ist die Integrität der übertragenen Daten von erheblicher Bedeutung, die Störanfälligkeit des Netzwerkes ist bei zeitkritischen Anwendungen ebenfalls substanziell.

2.2 Protokolle

2.2.1 IEEE 802.15.4

Dieser Standard regelt den Datenaustausch in WPAN auf den beiden untersten Schichten (PHY/MAC) des OSI-Modells. Ziel war es, eine Möglichkeit zu schaffen, mit geringen Kosten äußerst Strom sparende Hardware drahtlos miteinander zu verbinden, unter der Bedingung innerhalb der lizenzfreien Bänder zu funken. Die Frequenzen für den weltweiten Betrieb liegen im Bereich von 2,4 bis 2,48 GHz, in Europa innerhalb von 868.0 - 868.6 MHz und in den USA innerhalb von 902.0 - 928.0 MHz. Im 2,4 GHz Bereich konkurrieren viele verschiedene, privat genutzte Anwendungen, die häufigsten sind Bluetooth™ und Wi-Fi™. Wi-Fi™ nutzt dabei einen von elf 22 MHz breiten Kanälen, meistens jedoch einen der drei Überlappungsfreien (1;6;11 bzw. 1;7;11). Hier wäre es möglich, dass durch geschickte Wahl eines 5 MHz Kanales ein störungsfreier Betrieb aufgenommen werden kann, jedoch sieht der Standard keine Erkennung von fremden Signalen vor. Die Sendeleistung von WLAN Stationen ist meistens um ein Vielfaches höher als die eines IEEE 802.15.4 Gerätes, dadurch ist die Überlagerung von Signalen wahrscheinlich. In den beiden anderen Frequenzbändern des IEEE 802.15.4 Standards muss im industriellen Sektor mit Störungen gerechnet werden, aber für den privaten Bereich bieten sich diese Kanäle an, sofern die zu übertragende Datenmenge begrenzt ist.

Tabelle 2.1: Übersicht Frequenzbänder

	Frequenz in MHz	Kanäle	Datenrate kbit/s	Verfahren
weltweit	2400 - 2480	16	250	Quadrature Phase Shift Keying (QPSK)
Europa	868.0 - 868.6	1	20	Binary Phase Shift Keying (BPSK)
US	902.0 - 928.0	10	40	BPSK

Für die grundsätzliche Funktion eines nach dem Institute of Electrical and Electronics Engineers (IEEE) Standard spezifizierten Netzwerkes werden die sogenannten Full Functional Device (FFD) und möglicherweise noch zusätzliche Reduced Functional Device (RFD) benötigt, diese lassen sich entweder in einer Sterntopologie oder als Peer-to-Peer-Netzwerk organisieren. In einer Sterntopologie kommunizieren FFDs und RFDs mit dem PAN Coordinator, es gibt keine direkte Verbindung zwischen den einzelnen Geräten. Bei einem P2P-Netzwerk dürfen die Geräte auch untereinander Kontakt aufnehmen. Eine Abwandlung ist das Netzwerk in Baumstruktur, hierbei sind die RFDs die Blätter, die restlichen FFDs stellen als Router Kontakt zum PAN Koordinator her.

Dabei sind FFD für den Aufbau und den Betrieb des Netzwerkes vorgesehen, ein RFD dient der bedarfsorientierten Anwendung. FFDs haben die Möglichkeit untereinander zu kommunizieren, wohingegen RFDs nur mit einem FFD in Kontakt treten können. Der Standard sieht vor, dass ein FFD zu einem PAN Coordinator wird, sofern es selbst das erste Gerät innerhalb eines Netzwerkes ist. Damit übernimmt es die Verwaltung des WPAN, darin eingeschlossen sind die Integration neuer Teilnehmer, die Vertretung des Netzwerkes mithilfe des PAN Identifier (PAN-ID) oder die Konfliktbewältigung aufgrund von Interferenzen im Frequenzbereich. Um möglichst Strom sparend dieses Netzwerk zu betreiben,

kann zur Koordination des Netzwerkes ein sogenanntes Beacon Frame verschickt werden; alle anderen Geräte synchronisieren sich damit und wachen regelmäßig zum Empfang dieses Frames auf. Darin enthalten ist u. a. die Identifikation des Netzwerkes, somit können die Empfänger entscheiden, ob sie darauf reagieren. Zusätzlich ist in diesem Beacon Frame hinterlegt, ob weitere Daten für ein bestimmtes Gerät vorliegen. Somit werden nur die eigentlichen Daten übertragen, sofern sie angefordert werden; optional ist es möglich, dass die Endgeräte auf eine Bestätigungsmeldung verzichten.
Zur Absicherung eines Netzwerkes stehen eine Access Control List (ACL) und sieben verschiedene Sicherheitsdienste zur Verfügung, von denen aber nur AES-CCM-64 und None implementiert werden müssen. Ein jedes Gerät hat eine ACL mit bis zu 255 Einträgen (möglich wäre auch nur der default Eintrag), darin sind für jeden Eintrag die Adresse des zu kontaktierenden Gerätes, der benutze Sicherheitsdienst, der verwendete Schlüssel, der letzte Initialvektor und der Nachrichtenzähler gespeichert. Ein besonderer Eintrag ist der sogenannte default Eintrag, dieser dient zur Absicherung der Nachricht bei unbekannten Geräten, hier wird ein einheitlicher Schlüssel im Netzwerk benötigt. Bei ausgehenden Nachrichten wird der unter der Adresse verwendete Schlüssel und Initialvektor unter Berücksichtigung des Sicherheitsdienstes verwendet, bei eingehenden Nachrichten wird der Nachrichtenzähler verglichen, ist der Zähler in der Nachricht kleiner als der gespeicherte Wert, so wird die Nachricht verworfen. Es ist nicht verboten, einen Schlüssel für mehrere Einträge zu verwenden, hier kann auf Grund des Advanced Encryption Standard (AES) zu einer Schwäche in der Verschlüsselung kommen.[10] Zusätzlich definiert der Standard keine Routinen für die Schlüsselverwaltung, dies muss von den übergeordneten Schichten implementiert werden.
Der Initialvektor (auch number used once (nonce) genannt) setzt sich aus der Absen-

Tabelle 2.2: Aufbau Initialvektor

1 byte	8 byte	4 byte	1 byte	2 byte
Flags	Source adress	Frame Ctr	Key Ctr	Block Ctr
Flag	Absenderadresse	Paketzähler	Schlüsselzähler	Blockzähler

deradresse, einem statischen Flag Field und drei verschiedenen Zählern zusammen (frame counter, key counter, block counter). Der Frame Counter identifiziert das Paket und wird von der Hardware verwaltet, dabei wird nach jedem empfangenen Paket der Zähler erhöht. Falls der Zähler nicht mehr inkrementiert werden kann, muss ein Fehler ausgegeben und die Verschlüsselung eingestellt werden. Der Key Counter hingegen wird von der Anwendungsschicht genutzt und kontrolliert, eine Erhöhung dieses Wertes findet beim Erreichen der Inkrementierungsgrenze des Paketzählers statt. Beide Zähler sollen das wiederholte Verwenden eines identischen Initialvektors verhindern. Der Block Counter organisiert die Auswahl der Bits, die für die Entschlüsselung der Nachricht benötigt werden.

- Zugangskontrolle & Integritätsprüfung
  Hiermit ist gemeint, dass keine unbefugten Geräte an einem Netzwerk teilnehmen dürfen. Die Netzwerkmitglieder müssen erkennen können, ob eine Nachricht von einen legitimierten Sender kommt und falls nicht, die Nachricht verwerfen. Ebenso muss die Integrität der Nachricht sichergestellt werden, ansonsten könnte eine Manipulation unentdeckt bleiben, obwohl die Nachricht als von einem korrekten Netzwerkmitglied versendet gilt. Hierfür wird eine Message Authentication Code (MAC)

eingefügt, dies kann als eine verschlüsselte Prüfsumme betrachtet werden. Es ist auf Grund der Einfachheit der Hardware notwendig, eine symmetrische Verschlüsselung zu verwenden, dadurch wird erwartet, dass beide Kommunikationspartner über den gleichen Schlüssel verfügen.

- Vertraulichkeit
  Um eine Vertraulichkeit zwischen zwei Partnern zu gewährleisten, wird meistens die zu übertragende Nachricht verschlüsselt. Die Verschlüsselung soll einerseits sicherstellen, dass der Klartext nicht bekannt wird, aber auch, dass keine grundlegenden Informationen aus dem Chiffre abgeleitet werden können. Sollte eine Nachricht zweimal verschlüsselt werden, so darf die Ausgabe nicht übereinstimmen, ansonsten ist die semantische Sicherheit gefährdet. Zur Prävention wird ein Initialvektor (nonce) mit in den Verschlüsselungsvorgang einbezogen, dieser verändert sich nach jeder Verwendung. Der Nonce wird dabei häufig im Klartext übertragen.

- Sequenzkontrolle
  Es wird ein gültiges Paket mitgeschnitten und dann wieder ins Netzwerk eingespeist. Der Empfänger der Nachricht kann bestätigen, dass dieses Paket von einem legitimen Netzwerkmitglied versendet wurde. Um das wiederholte Senden von bereits versendeten Nachrichten zu verhindern, wird ein Zähler genutzt, der nur inkrementiert werden kann. Beim Empfang einer Nachricht wird dieser Zähler erhöht, sollten danach Pakete empfangen werden, deren Nummer kleiner oder gleich ist, wird das Paket verworfen.

Tabelle 2.3: Sicherheitsdienste in IEEE 802.15.4

Identifikation	Name des Sicherheitsdienstes	Zugangs-kontrolle	Verschlüs-selung	Integritäts-prüfung	Sequenz-kontrolle
0x00	None				
0x01	AES-CTR	X	X		X
0x02	AES-CCM-128	X	X	X	X
0x03	AES-CCM-64	X	X	X	X
0x04	AES-CCM-32	X	X	X	X
0x05	AES-CBC-MAC-128	X		X	
0x06	AES-CBC-MAC-64	X		X	
0x07	AES-CBC-MAC-32	X		X	

Die Sicherheitsdienste setzen alle auf den AES (bis auf None, dieser versendet Daten ohne jegliche Absicherung), der Counter Mode (CTR) Dienst verschlüsselt die Nutzdaten, fügt den Nachrichten- und Schlüsselzähler hinzu und versendet dieses Paket im Nutzdatenbereich. Cipher Block Chaining (CBC)-MAC fügt am Ende des Nutzdatenbereichs einen Integritätswert an, sodass die Daten und der MAC Header verifiziert werden können. Der Zahlenwert eines Sicherheitsdienstes gibt die Länge des MAC in Bits an. Der Empfänger berechnet ebenfalls den Integritätswert und vergleicht diesen dann mit dem in der Nachricht enthaltenden. Der Sicherheitsdienst CCM nutzt im ersten Schritt CBC-MAC um den Integritätswert zu erstellen, dann werden die Nutzdaten mit CTR verschlüsselt. Ebenfalls gibt hier der Zahlenwert die Länge des Integritätswertes an.

Die einzelnen Anwendungen müssen explizit die Verwendung eines Sicherheitsdienstes verlangen, ist dies nicht der Fall, so kommt keiner (None) zum Einsatz. Die Sequenzkontrolle ist in jedem Sicherheitsdienst optional.

2.2.2 ZigBee

Es gibt drei verschiedene Versionen, sie wurden 2004, 2006 und 2007 veröffentlicht, jedoch wird in jeder auf die IEEE-Norm 802.15.4 von 2003 verwiesen. Bei der im Jahre 2007 veröffentlichten Version wird zwischen zwei Leistungsvarianten (Standard, Pro) unterschieden. Die Pro Variante wird als primäres Implementierungsziel angegeben, die Standardvariante nur als garantierte Kompatibilitätsschnittstelle zwischen dem Protokollstapel von 2006 und 2007. Genauere Leistungsbeschreibung im Absatz 2.3.1. In der weiteren Betrachtung im Rahmen dieser Seminararbeit fällt das Initialprotokoll von 2004 heraus, da es mit den nachfolgenden Versionen nicht kompatibel ist und auch nicht im kommerziellen Bereich genutzt wird.
Der Aufbau eines Netzwerkes ist ähnlich dem, der im IEEE Standard vorgesehen ist. Jedoch können die FFDs drei unterschiedliche Rollen annehmen: Coordinator, Router oder ZigBee End Device (ZED). Der Coordinator entspricht dem PAN Coordinator, das ZED entspricht dem RFD, der Router stellt ein Bindeglied zwischen ZED, anderen Routern und dem Coordinator dar. Die Router verwalten bestehende und suchen zusätzliche Routen, um auch bei einem Ausfall eines Knotenpunktes die Daten weiterleiten zu können, damit übernehmen sie die Eigenschaften des PAN Coordinators ohne die Möglichkeiten der Administration. Der ZigBee Coordinator kann zu den prädefinierten Aufgaben noch die Aufgabe des Trust Centers übernehmen oder aber diese Aufgabe an ein Gerät delegieren. Das Trust Center organisiert das Schlüsselmanagement für das ihm zugehörige Netzwerk. Laut Vorgabe sollen alle Mitglieder eines Netzwerkes nur ein Trust Center kennen und benutzen, dementsprechend sollte auch nur ein aktives Trust Center im Netzwerk existieren. Zur Absicherung kann ein zweites Trust Center von Coordinator bestimmt werden, welches dann beim Ausfall des Ersten einspringt und dessen Funktionen übernimmt. Gateways stellen eine Brücke zwischen dem ZigBee-Netzwerk und anderen Netzwerken dar und führen notfalls auch Protokollkonvertierungen durch, sie stellen aber wie das Trust Center auch keinen eigenen Typus dar, sondern sind meistens ZEDs, die besonders grundlegende Funktionen zum Betrieb eines Netzwerkes bereitstellen.
Das ZigBee Protokoll definiert die Vermittlungsschicht (Network Layer (NWK)) als Verbindung zwischen der Application Layer (APL) und der Media Access Control (MAC) Schicht; die Application Support Sub-Layer (APS), das ZigBee Device Object (ZDO) und das Application Framework sind Teil der APL, der Security Service Provider (SSP) ist aus beiden Schichten (NWK und APL) verfügbar.

- Application Framework
  Um die verschiedenen application objects auf einem einzigen ZED integrieren zu können, müssen diese, falls gefordert, über eine Kommunikationsmöglichkeit verfügen. Hierfür definiert der ZigBee Standard verschiedene Anwendungsprofile (Building Automation, Remote Control, Smart Energy, Health Care, Home Automation, Input Device, Retail Services, Telecom Services, 3D Sync), diese dienen als garantierte Mindestschnittstelle für andere Anwendungsprofile. Jeglicher Datenaustausch

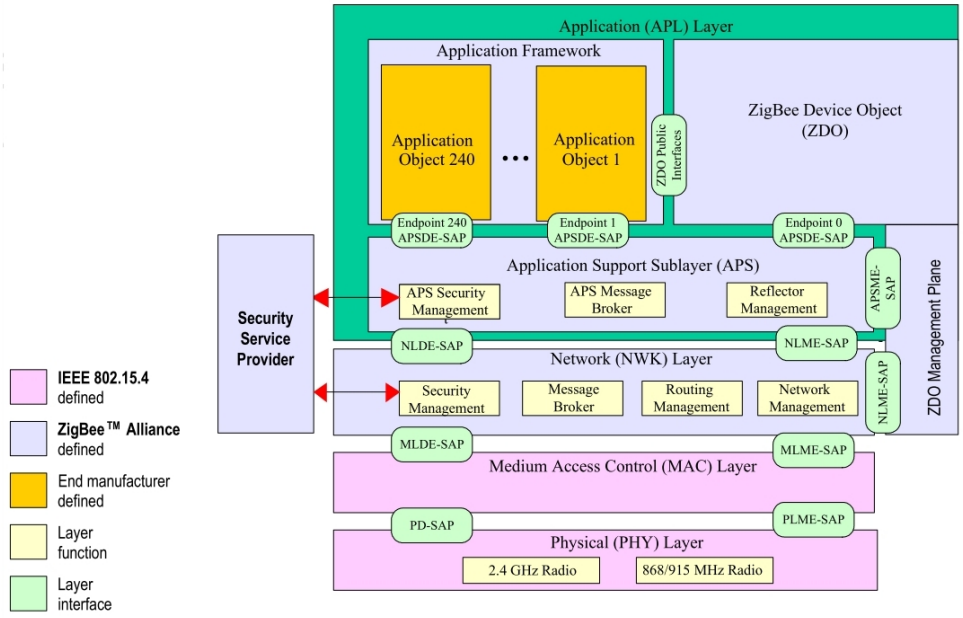

Abbildung 2.1: ZigBee Stack [1, S.30]

erfolgt über diese Anwendungsprofile, ein direkter Austausch unter den verschiedenen application objects ist nicht vorgesehen.

- ZigBee Device Object
  Das ZigBee device object ist ein spezielles application object und dient der Initialisierung und Verwaltung des ZEDs. Dafür bestimmt es u. a. den Typ des ZEDs (Coordinator, Router, ZED). Ein für jedes Gerät identisches Anwendungsprofil (ZigBee Device Profil (ZDP)) gibt auf Anfrage die unterstützten Anwendungsprofile oder den Gerätetyp bekannt oder stellt die Schnittstellen zur Verwaltung der in der APS definierten Tabellen bereit.

- APS
  Die APS stellt die Verbindung zwischen NWK Layer und dem Application Framework her, die Aufgaben der Schicht belaufen sich auf das Filtern von Paketen an nicht benutzten Endpoints und falsch klassifizierten Paketen, deren Profil nicht mit dem des Empfängers übereinstimmt. Für die end-to-end Kommunikation werden die Acknowledgement with retries generiert und deren Duplikate bei Störungen gefiltert. Zusätzlich müssen die zwei lokalen Tabellen (binding, APS group) und die lokale adress map gewartet werden. Die binding Tabelle koordiniert die Verbindung der eigenen Endpoints zu den Endpoints anderen ZEDs, die APS group Tabelle organisiert die Zusammenfassung von application objects auf dem eigenen und möglicherweise noch anderen Geräten. Die adress map verknüpft lediglich die vom NWK Layer vergebenen Adressen mit denen aus der MAC Schicht.

- NWK Layer
  Die Vermittlungsschicht übernimmt das Routing und die Verwaltung der Netzwerkinformationen, dafür teilt es jedem Gerät eine Netzwerkadresse (16bit) zu, die sich von der im IEEE Standard vorgesehenen unterscheiden kann. Die Adresse ist

abhängig von der Topologie des Netzwerkes und ob durch die MAC Schicht die erweiterten Netzwerkadressen verwendet werden. Da nur Router und der Coordinator neue Routen finden können, sind diese auch für den Erhalt korrekter Routingtabellen verantwortlich; bei jedem Passieren eines solchen Gerätes wird ein Wert (Radius) dekrementiert, erreicht dieser den Wert 0, so wird das Paket nicht mehr weiter geleitet.

- Security Service Provider
  Der Security Service Provider stellt für die APS und die NWK Schicht die Methoden der Sicherheitsdienste zur Verfügung.

- MAC
  Die MAC Ebene stellt die direkte Verbindung zwischen unmittelbaren Nachbarn her und integriert intelligente Zugriffsverfahren auf die unterste Schicht.

- PHY
  Die physikalische Schicht bietet den Zugriff auf die Schnittstelle zum direkten Transportmedium, in diesem Fall Funk.

2.3 Gefahren

Die nachfolgend beschriebenen Gefahrenpotenziale beziehen sich sowohl auf den IEEE 802.15.4 Standard als auch auf ZigBee. Die einzelnen ZigBee Anwendungsprofile schreiben den Umfang und die Verwendung der einzelnen Sicherheitsdienste vor, bei den vom Hersteller entwickelten Anwendungsprofilen gibt es keine Zusicherung über die Einhaltung seiner Versprechen. Hierbei gibt es auch Anwendungsprofile (Home Automation), die auf Grund der Nutzbarkeit keine Planung des Netzwerkes oder gar Sicherheitsüberlegungen vorsehen. Die Standards selbst fordern keine zwingende Nutzung von Sicherheitsdiensten, hier bleibt es dem Entwickler überlassen, diese zu nutzen bzw. zu implementieren. Einige Hardwarehersteller setzen sich zudem über die Bestimmungen im IEEE 802.15.4 hinweg und implementieren nicht den AES-CCM-64 Sicherheitsdienst oder nutzen ACL Listen mit ein oder zwei Einträgen;[10] der ZigBee Standard selbst fordert nicht die explizite Nutzung der vorhandenen Sicherheitsdienste auf MAC Ebene, damit entfällt das zwingende Integrieren dieser Funktionen durch den Hersteller.[4, S.16] Durch nicht präzise formulierte Anforderungen innerhalb der Standards und der Ausrichtung auf äußerst kostengünstige Produktion entstehen Brüche im Sicherheitskonzept der beiden Standards, die Angriffspunkte werden in den nächsten Abschnitten näher erläutert.

2.3.1 Schlüsselmanagement

Da der IEEE Standard 802.15.4 keine Bedingungen bezüglich einer Schlüsselverwaltung stellt, sondern diese Aufgabe den übergeordneten Schichten überlasst, wird hier nur die Umsetzung innerhalb des ZigBee Stacks betrachtet.
Die Spezifikation des ZigBee-Protokolls setzt für die Sicherheit des Netzwerkes auf die korrekte Initialisierung der Geräte, die richtige Implementierung von Zufallsgeneratoren und sichere Aufbewahrung des Schlüsselmaterials. Zusätzlich wird der Gedanke des Open-Trust Modells angeführt, dies bedeutet, dass gemeinsames Schlüsselmaterial von den verschiedenen Schichten auf einem Gerät benutzt werden kann, somit gibt es nur eine sichere Gerät-zu-Gerät-Verbindung. Daraus muss ein Vertrauen der verschiedenen Anwendungen auf einem Gerät und der einzelnen Schichtimplementierungen gegenüber einander folgen. Die Sicherheit in einem ZigBee-Netzwerk wird maßgeblich von zwei verschiedenen Schlüsselarten bestimmt:

- Link Key
- Network Key

Dabei sichert der Link Key (128bit) die Kommunikation zwischen genau zwei Geräten ab, wohingegen der Netzwerkschlüssel (128bit) für die Broadcast Kommunikation genutzt wird. Für den Empfänger ist immer ersichtlich, um welchen Nachrichtentyp es sich handelt. Die Anwendungsprofile können auf jeder Ebene die Verschlüsselung fordern, somit kann ein auf der APL Schicht gesichertes Paket zusätzlich auf der NWK Schicht verschlüsselt werden. Es sind drei verschiedene Modi definiert, um Schlüssel an die Geräte zu verteilen. Hierbei wird zwischen dem Vorkonfigurieren (durch den Hersteller oder Nutzer),

dem Versenden und zusätzlich für den Link Key dem Generieren differenziert. Für das Generieren von Link Keys benötigen zwei Geräte einen gemeinsamen Master Key. Dieser wird niemals selbst zur Verschlüsselung eingesetzt, lediglich die per Symmetric Key Key Establishment (SKKE) erzeugten Link Keys dienen diesem Zweck. Für die Aushandlung eines Link Keys wendet sich der Initiator an das Trust Center. Dieses verschickt an den Initiator und den Empfänger den für die beiden gemeinsamen Master Key (verschlüsselt mit dem entsprechenden Link Key (Initiator<->Trust Center) und (Empfänger<->Trust Center)). Daraus wird dann per 4-Wege-Handschlag von den zwei Endgeräten ein Sitzungsschlüssel abgeleitet.
Einer der wesentlichen Schwachstellen innerhalb der ZigBee Spezifikation ist das Fehlen einer präzisen Bestimmung zur sicheren Übertragung des Schlüsselmaterials bei der Initialisierung neuer Netzwerkteilnehmer. Laut Vorgabe ist es auch möglich, diese Daten unverschlüsselt und somit ungesichert zu übertragen. Daraus folgend kann das Netzwerk nur als sicher betrachten, wenn bei der Installation und Initialisierung aller Teilnehmer keine dritte Partei Zugriff auf die übertragenden Daten hatte. Ein zusätzliches Authentifizierungsverfahren existiert nicht; sind die je nach Sicherheitsvorgabe zu besitzende Schlüssel bekannt, gilt das Gerät als vertrauenswürdig.
Zudem existieren zwei verschiedene Sicherheitsstufen für die Schlüsselverwaltung. Der Standard ("Residential" in 2006) beinhaltet die Absicherung der NWK Schicht durch den Network Key, die zentrale Kontrolle dieses Schlüssels sowie dessen Aktualisierung und die Benutzung von Ersatzschlüsseln. Für die Spezifikation von 2007 wurde die Unterstützung von Link Keys in der APS Schicht übernommen. Im High-Security Modus (nur verfügbar in 2007 Pro) stehen mehrere Optionen zur Absicherung des generellen Schlüsseltransportes zur Verfügung. Dabei werden mithilfe einer Einweg-Funktion aus dem (Trust Center) Link Key Schlüssel erzeugt, die zum sicheren Transport von Master und Link Key (key-load key) und dem Network Key (key-transport key) dienen. Abhängig vom gewählten Modus speichern die ZigBee Geräte nur den Netzwerkschlüssel (Standard) oder zusätzlich den Master Key und Link Key für jede end-to-end Verbindung (High Security). Dies setzt einen erheblichen Speicherplatz voraus, den RFDs auf Grund der Kosten und des Energieverbrauches normalerweise nicht haben dürften. Der ZigBee 2006/2007 Stack sieht maximal 31101 Geräte innerhalb eines Netzwerkes vor, bei ZigBee 2007 Pro sind es 65540, damit beläuft sich die Speicherkapazität bei einem vollvermaschtem Netzwerk und einer Schlüssellänge von 128bit auf ein bis zwei Mbyte Speicher. Realistischer dürften aber pro FFDs zwischen 20 bis 30 und für ein RFD maximal 10 Verbindungen sein, damit werden auch für die Schlüsselaufbewahrung zwischen 320Byte und einem kByte gebraucht.
Für den High-Security Modus ist es möglich, Geräte mit der Trust Center Adresse und einem initialen (Trust Center <-> Gerät) Master Key zu versehen, im Standard Modus kann der aktuelle Netzwerkschlüssel vorkonfiguriert werden. Alternativ kann der jeweilige Schlüssel auch ungesichert über das Netzwerk übertragen werden. Jedoch akzeptiert ein Gerät nur einmal den ungesicherten (Schlüssel-)Transport, danach wird nur noch über gesicherte Verbindungen kommuniziert. Eine massive Einschränkung bei der Übertragung des Schlüsselmaterials liegt darin, dass viele Geräte keine entsprechenden Optionen zur manuellen Eingabe (serielle Schnittstelle, DIP-Schalter) besitzen. Hier könnte sich eine technische Erweiterung des Trust Center anbieten, bei dem der Schlüsselaustausch direkt zwischen Trust Center und neuem Gerät stattfindet. Der Austausch würde zwar immer noch unverschlüsselt erfolgen, aber durch geeignete Maßnahmen ließe sich aber ein Abhören der Kommunikation verhindern. Eine mögliche Umsetzung wäre die Konstruktion

einer Box, in der das zu initialisierende Gerät gelegt wird. Entsprechend der Frequenzen von ZigBee ist die Box nach außen hin abgeschirmt, im Inneren befindet sich eine Antenne, die direkt mit dem Trust Center verbunden ist.

2.3.2 Funkübertragung im Allgemeinen

Liegt in der Verantwortung von IEEE 802.15.4, da dieser Standard für die unterste (physikalische) und die unmittelbar darüberliegende Schicht (MAC) im OSI-Modell verantwortlich ist.
Prinzipbedingt breiten sich elektromagnetische Wellen radial aus, dies lässt sich durch z. B. eine Richtfunkanlage vermindern. Soll nun vermieden werden, dass eine Funkübertragung mitgehört werden kann, so muss der physischen Zugang zur Funkverbindung verhindert werden. Dies ist aber bei Funk aufgrund des enorm großen, zu überwachenden Raumes so gut wie unmöglich. Von daher sollten die per Funk übertragenden Daten verschlüsselt werden, sodass aufgrund der Benutzerfreundlichkeit nicht auf den Richtfunk zurückgegriffen werden muss, aber doch garantiert werden kann, dass die übertragenen Informationen gegen unberechtigten Zugriff geschützt sind. Durch den Standard ist eine Sendeleistung von 0,5 mW bis 10mW vorgesehen, dabei sind Reichweiten von bis zu 100 Metern möglich (optimale Voraussetzungen). Im 2,4 GHz ISM-Band darf nach deutschem Recht auch mit 100mW gesendet werden, sofern eine Bandspreiztechnik zum Einsatz kommt. Innerhalb von Gebäuden fehlt jegliche Beschränkung der Sendeleistung.[11] In den meisten Fällen wird von einer 1mW Sendeleistung ausgegangen, dies entspricht einer durchschnittlichen Reichweite von 10 Metern. Damit überschreitet ein ZigBee-Netzwerk aber möglicherweise die Grenzen des Raumes, in dem es genutzt werden soll. Hier wäre eine genaue Planung zum Einsatz und Unterbringung der Router notwendig. Diese Vorsichtsmaßnahmen an sich schützen aber nicht vor dem gezielten Abhören mithilfe einer Richtantenne oder dem Erstellen eines Bewegungsprofils einzelner Netzwerkteilnehmer. In der Verbindung mit Ort und Uhrzeit lässt sich ein detailliertes Bewegungsprofil eines Gerätes erstellen, da die MAC Adresse unverschlüsselt übertragen wird, hierbei wird zwischen zwei möglichen Adressen unterschieden. Die Geräteadresse wird durch 64 bit lange Zahl dargestellt und ist eindeutig, die möglicherweise zugeteilte MAC Geräteadresse dagegen nur 16 bit lang und nicht eindeutig. Zusätzlich gibt es noch eine ebenfalls 16 bit lange Netzwerkadresse, die von der NWK Schicht vergeben ist und nicht mit der MAC Geräteadresse übereinstimmen muss, aber kann. Sofern der Sicherheitsdienst None oder AES-CBC-MAC auf MAC Ebene gewählt wurde, kann auch diese Adresse erkannt werden. Im Falle von 2007 Pro wird die Netzwerkadresse zufällig vergeben und folgt somit keinem Vergabemuster anhand der Topologie wie im normalen Standard. Inwieweit dies eine Gefahr für die Sicherheit ist, kann nur unter Berücksichtigung der Anwendungen bewertet werden. Sollten bestimmte ZED personenbezogene Funktionen bereitstellen, so muss bei der Planung betrachtet werden, wie stark eine mögliche Verletzung der Privatsphäre zu bewerten ist.
Eine weitere Möglichkeit, Funkübertragung zu schützen ist das Frequenzsprungverfahren. Hierbei wird die Frequenz zufällig gewechselt, sodass ein Angreifer im Unklaren darüber ist, auf welchem Kanal die nächsten Daten übertragen werden. Dies setzt die Integration eines Verfahrens voraus, sodass nicht erraten werden kann, welcher Kanal als nächstes genutzt wird. Der IEEE Standard sieht aber keine Implementierung dieses Verfahrens zur

Absicherung der Kommunikation vor, der zu verwendende Kanal wird bei der Einrichtung eines PANs vom Coordinator für die Dauer des Betriebes festgelegt. ZigBee selbst unterstützt das Wechseln des Kanals im laufenden Betrieb durch eine optionale Erweiterung, wird aber nur in 2007 Pro funktionstüchtig spezifiziert; es soll aber niemals als Absicherheit des Netzwerkes dienen, sondern nur die Störresistenz erhöhen.

2.3.3 Replay

Der ZigBee und der IEEE 802.15.4 Standard bieten Maßnahmen gegen Replayattacken. Jedoch sind diese Konzepte nicht zu einander kompatibel, es bestehen jeweils eigene Lösungen für die MAC, NWK und APL Schicht.
Bei diesem Szenario wird ein oder mehrere Paket(e) mitgeschnitten. Da die Pakete verschlüsselt sind, ist der genaue Inhalt unbekannt. Dieser Informationsmangel ist nicht weiter hinderlich, da der Angreifer einfach durch wiederholtes Senden bestimmter Mitschnitte die Auswirkungen in der realen Welt beobachtet. Dagegen wurde im IEEE 802.15.4 Standard der Message Integrity Check (MIC) eingeführt, der auf den Integrity Check Values (ICV) von 802.11b beruht. Diese Methode fügt eine fortlaufende Nummer im MAC Header hinzu (MAC Header-> Auxiliary Security Control -> Frame Counter). Damit soll verhindert werden, dass Pakete mehrfach gesendet werden können. Die vom Nutzer eingesetzte Anwendung muss diese Funktionen aber explizit fordern.
Hierin liegt nun ein wesentlicher Schwachpunkt der ZigBee Implementierung. Die Spezifikation sieht nicht vor, auf die vorhandenen Security Suites des IEEE 802.15.4 Standards zurückzugreifen. Zwar bieten die Sicherheitsmaßnahmen auf der Netzwerkebene sowie der APS eigene Schutzvorrichtungen gegen Replay-Attacken, dies verhindert jedoch nicht einen Angriff auf MAC-Ebene. Ein erfolgreicher Replay wird damit nicht möglich sein, sofern die von ZigBee integrierten Vorrichtungen korrekt arbeiten, gleichwohl kann es zu einem Denial of Service kommen (siehe 2.3.4). Ist es dem Angreifer jedoch gelungen, in das bestehende Netzwerk integriert zu werden (siehe 2.3.5), so ist eine Replay ähnliche Attacke durchführbar. Ab diesem Zeitpunkt ist es von erheblicher Bedeutung, wie restriktiv die einzelnen Geräte auf Daten reagieren.

2.3.4 Verfügbarkeit und Störanfälligkeit

Dieses Szenario beschreibt das Verhalten eines ZigBee-Netzwerkes unter internen und externen Einflüssen. Dabei wird die MAC Schicht im ersten Abschnitt betrachtet, im zweiten die NWK Schicht.
Durch den Betrieb innerhalb der ISM-Bänder muss mit Störungen gerechnet werden, da einige andere, häufig genutzte Dienste (Wi-Fi™ 802.11b/g, Bluetooth™ 802.15.1) ebenfalls auf diesen Frequenzen arbeiten. Das Direct-Sequence-Spread-Spectrum (DSSS) Verfahren wird zum Verhindern schmalbandige Störungen genutzt. Vor allem im industriellen Bereich ist mit Maschinen (Pumpen, Lüfter, Motoren, Generatoren, Schweißgerät) zu rechnen, deren elektromagnetischen Verhalten massiven Einfluss auf die genutzten Frequenzen nimmt, sodass es auf Grund des Carrier Sense Multiple Access with collision Avoidance (CSMA/CA) Verfahren zu einen Denial of Service (DoS) kommt. Ein Gerät

wird zuerst auf dem entsprechenden Kanal auf Datenverkehr achten, dabei betrachtet es die Amplituden auf dieser Frequenz. Nun kann es dazu kommen, dass die Frequenz fälschlicherweise als benutzt interpretiert wird, weil das Hintergrundrauschen dementsprechend als Aktivität gewertet wird. Durch die breitbandige Abstrahlung mancher Maschinen kann nun der Fall eintreten, dass das Gerät jeglichen Sendeversuch einstellt, weil alle benutzbaren Frequenzen als in Gebrauch interpretiert wurden. Der gleiche Effekt lässt sich auch mit herkömmlichen ZigBee-Geräten erzielen, wenn auf den im IEEE Standard definierten Kanälen gesendet wird. Entgegen der unbeabsichtigten Beeinflussung ist es immer möglich, das komplette Frequenzband mit einem Störsender absichtlich zu blockieren, dies lässt sich auch nicht verhindern. Daraus folgt, dass eine zeitkritische Anwendung derart robust konzipiert sein muss, sodass eine Fehlfunktion ausgeschlossen werden kann. Diese (effektive, aber nicht sonderlich elegante) Art des Angriffes lässt sich sehr einfach erkennen, da das komplette Netzwerk ausfällt. Hingegen ist ein gezieltes Stören einzelner Pakete weit aus unauffälliger und kann automatisch erfolgen.[5]
Des Weiteren sieht die ZigBee Spezifikation bei einen PAN-ID oder Kanalkonflikt keine eindeutige Lösung vor, somit bleibt es dem Hersteller überlassen, eine geeignete zu finden. Falls nun ein Gerät mit der identischen PAN-ID oder auf dem gleichen Kanal funkt, so sollte der Coordinator des beeinflussten Netzwerkes reagieren und eine neue ID oder neuen Kanal auswählen. (Alternativ wird die/der alte PAN-ID/Kanal beibehalten und die damit einhergehende Störung in Kauf genommen). Erst in der Spezifikation 2007 Pro wird ein Wechsel der PAN ID und des Kanals bei einer Störung ermöglicht, ansonsten kann dies nur bei Initialisierung des Netzwerkes geschehen. Dies kann ein Angreifer ausnutzen und einen DoS herbeiführen, in dem er die gleiche PAN-ID oder den gleichen Kanal auswählt. Möglicherweise kann hier auch ein Identitätsdiebstahl (siehe 2.3.5) stattfinden, die Gefahr besteht dann, wenn einzelne Netzwerkteilnehmer sich mit dem Coordinator verbinden, der mit der gleichen PAN-ID arbeitet, aber eine höhere Signalstärke aufweist.

2.3.5 Identitätsdiebstahl eines gültigen Netzwerkgerätes

Dieses Szenario bezieht sich auf die MAC, NWK und APL Schicht; da die ZigBee Spezifikation nicht die Verwendung der ACL vorsieht, wird der Fall für die MAC Ebene nur nachrangig betrachtet.
In diesem Fall würde der Angreifer sich für ein anderes, im Moment nicht aktives Gerät ausgeben. Ist das Netzwerk auf einen Betrieb ohne vorher konfigurierte Authentifizierungen ausgelegt, so könnte der Angreifer mit den aktuellen Schlüsseln versorgt werden. Hier muss bei der Absicherung auf der MAC Ebene die Aufmerksamkeit auf die ACL gelegt werden, da in dieser vermerkt sein muss, ob dieses Gerät dem Netzwerk bekannt ist (und somit über einen gültigen Schlüssel verfügen muss). Wird auf die Verwendung der ACL verzichtet, findet aber eine Absicherung auf dem NWK und/oder auf der APS Schicht statt, so muss mithilfe des Trust Centers ermittelt werden, ob das Gerät schon über die notwendigen Informationen verfügt. Falls dieses Gerät jemals eine abgesicherte Verbindung zum Trust Center abgebaut hat, so existiert ein Link Key. Kann nun mit diesem Link Key vom Trust Center ausgehen eine Verbindung zu dem Gerät aufgebaut werden, so ist das Gerät nicht ersetzt worden. Scheitert der Verbindungsaufbau, so sollte das Trust Center den Beitritt dieses Gerätes ab sofort dauerhaft verweigern und einen entsprechenden Hinweis für die Administration hinterlegen.

Ein Gerät darf per Definition nur einmal mit einem Schlüssel in Klartext initialisiert werden, so muss ein trojanisches Gerät auffallen, sofern es nicht über den aktuellen Netzwerkschlüssel verfügt. Dieser Fall kann aber auch eintreten, sofern ein Gerät zum Energie sparen im Tiefschlaf war, während das Trust Center den Austausch des aktuellen Netzwerkschlüssels durchführte. Hierfür sieht die 2007 Pro Spezifikation einen Ersatzschlüssel vor, der genutzt wird, sobald das Gerät feststellt, dass der alte Schlüssel nicht mehr zur Kommunikation mit dem bestehenden Netzwerk genutzt werden kann. In einem Standard Netzwerk wird der neue Netzwerkschlüssel per Broadcast verteilt, in einem High Security Netzwerk per Link Key gesicherter Kommunikation. In einem Standard Netzwerk besteht nun wieder die Gefahr der ungesicherten Übertragung eines Netzwerkschlüssels, da der Austausch per Broadcast "verschlafen" wurde. Wird das trojanische Gerät sofort oder dann aktiviert, sobald das zu ersetzende Gerät den Netzwerkschlüssel im Klartext erhalten hat, kann dieser Angriff erfolgreich verlaufen, da nun der Network Key per Sniffing bekannt ist, aber kein Master oder Link Key existiert.
In Verbindung mit dem Diebstahl eines Gerätes (siehe 2.3.6) kann dies aber zu einer wesentlich größeren Gefahr werden. Falls es gelingt, alle notwendigen Informationen zu erhalten, kann ein bestehendes Gerät gegen ein Manipuliertes ausgetauscht werden. Bei korrekter Ausführung ist dieser Austausch kaum nachweisbar. Sofern das injizierte Gerät korrekt arbeitet, dessen bauliche Bestimmungen dem Original entsprechen und der Unterbringungsort keine Veränderungen aufweist, besteht kein offensichtlicher Grund, die Echtheit des Gerätes anzuzweifeln. In Anbetracht der einzelnen Aufgabe von FFDs ergeben sich daraus sehr prekäre Sicherheitslücken. Falls ein FFD die Funktion eines Routers übernommen hat, so besteht die Gefahr eines Man-in-the-Middle Angriffes. Damit kann der mit dem Netzwerkschlüssel abgesicherte Verkehr abgehört oder manipuliert werden, vorstellbar sind das Versenden über ungünstige Routen oder das komplette Verwerfen von Nachrichten. Ist jedoch der Coordinator kompromittiert, so ist das komplette Netzwerk gefährdet, da in den meisten Fällen Coordinator und Trust Center auf demselben Gerät integriert sind. Falls dies nicht der Fall ist, kann der Coordinator sich als neues Trust Center bestimmen. Es wäre möglich, dass GPRS/UMTS-Gateways integriert werden, die den kompletten Datenverkehr ins Internet weiterleiten oder von dort neue Instruktionen entgegennehmen, notfalls kann der Coordinator die Topologie zu einem Sternnetzwerk verändern, somit muss jegliche Kommunikation über den Coordinator abgewickelt werden. Bei einem erfolgreichen Ersetzen des Trust Centers besteht nun die Gefahr, dass die bestehenden Sicherheitsrichtlinien heruntergestuft werden, hier wäre ein Verbot der end-to-end Verschlüsselung auf der APL von erheblicher Bedeutung. Unter dieser Bedingung könnte nun jeder Datentransfer eingesehen und manipuliert werden, ohne dass es dafür wirksame Gegenmaßnahmen gäbe.

2.3.6 Diebstahl eines ZigBee-Gerätes

Dieses Szenario ist weder dem IEEE 802.15.4 noch dem ZigBee Standard anzulasten, jedoch bestünde in der ZigBee Spezifikation die Möglichkeit, für bestimmte Sicherheitsstufen eine geeignete hardwaretechnische Umsetzung durch die Hersteller zu fordern.
Ein Angreifer könnte versuchen, ein zu einem Netzwerk gehörendes Gerät zu entwenden, um hardwareseitig die Schlüssel zu extrahieren. Dabei wird ausgenutzt, dass die einzelnen Geräte auf Anfragen antworten. Über eine Triangulierung kann der Ort des

ZigBee-Gerätes aufspürt werden und der Angreifer kann es dann entwenden bzw. direkten physischen Zugriff erhalten. Bei diesem Angriff spielt die korrekte Implementierung durch den Hardwarehersteller eine große Rolle. Da das erklärte Ziel der ZigBee Vereinigung unter anderem auch eine kostengünstige Produktion von Endgeräten ist, muss hier besondere Aufmerksamkeit auf die Auswahl von RFDs gelegt werden. Diese Geräte sollen möglichst einfach und kostengünstig sein, gleichzeitig stellt die Sicherheit nicht die größte Priorität dar. Somit ist es wahrscheinlich, dass die Hersteller schon bekannte Hardwarekomponenten verwenden. Möglicherweise existieren dafür schon Schaltpläne, sodass eine genaue Analyse durch den Angreifer möglich ist, im schlimmsten Fall sind auch schon Schwachstellen dokumentiert, die die einzelnen Komponenten z. B. in einen Debug-Modus versetzen. Ist dies der Fall, so bekommt der Angreifer mit sehr wenig Aufwand zügig Zugriff auf die gespeicherten Daten, und damit auch auf die Schlüssel. Es ist unwahrscheinlich, dass die Daten ständig verschlüsselt in RAM und ROM sowie beim Datentransfer vorliegen. Damit ergeben sich Möglichkeiten, auf die Daten im Klartext zuzugreifen.[6]
Dieses Szenario ließe sich vermeiden, wenn die Hardwarehersteller unbekannte Komponenten verwenden würden, die ihre internen Daten jederzeit verschlüsselt verarbeiten. Dies dürfte aber den Stromverbrauch sowie die Kosten von RFDs massiv in die Höhe treiben. Dagegen ist die Option, die Komponenten der Geräte gegen direkten Zugang zu schützen, weit aus einfacher und kostengünstiger. Hier böte es sich an, die Platinen mit Epoxidharz zu vergießen. Dies würde zwar keinesfalls den direkten Zugriff verhindern, jedoch sind die Verfahren äußerst kostspielig, um die einzelnen Komponenten freizulegen.[8] Im Rahmen der von ZigBee definierten Einsatzgebiete ist dies eine angemessene Reaktion auf die Forderung, einen erfolgreichen Angriff durch den Diebstahl eines Gerätes zu verhindern. Für Gateway, Trust Center und den Coordinator sollten andere Schutzmaßnahmen ergriffen werden, diese Geräte sind wie für eine Infrastruktur relevante Dinge grundsätzlich gegen unautorisierten Zugriff zu schützen. Bei Routern und Geräten, die nicht in einem überwachbaren Bereich installiert sind, sollte die Option in Erwägung gezogen werden, sie genauso wie RFDs zu schützen. Das würde aber auch jeglichen Versuch einer Reparatur verhindern.

2.4 Bewertung

Betrachten man die im vorangegangenen Kapitel gemachten Überlegungen, so kommt man zu dem Schluss, dass ein ZigBee-Netzwerk erst einmal als sicher zu betrachten ist. Diese Annahme setzt aber auf verschiedene Voraussetzungen auf. Eine ausführliche Planung des Netzwerkes und dessen Sicherheitsrichtlinien müssen vor der Inbetriebnahme eines solchen Netzwerkes erfolgen. Damit kann verhindert werden, dass ein Schlüssel im Klartext an neue Netzwerkmitglieder übertragen wird, einhergehend werden auch alle weiteren Angriffe, die auf diesen Angriff als Initialhandlung setzten, verhindert. Der AES unter Nutzung eines 128bit Schlüssels soll für eine ausreichende Sicherheit bis 2030 sorgen, [2, S.81] unter dieser Bedingung ist ein langfristiger Schutz gegenüber BruteForce-Attacken gegeben.
Sollte ein Angreifer aber anderweitig in den Besitz des Schlüsselmaterials gelangen, so sind kaum interne Maßnahmen gegen Missbrauch möglich. Eine hardwarebasierte Identifikationsmöglichkeit für ein bestimmtes Gerät wie bei Computern ein TPM-Chip ist nicht vorgesehen. Hier sind die Hersteller gefordert, Geräte zu produzieren, bei denen ein Angriff auf die Hardware unrentabel ist.
Als real existierendes Beispiel dient das MGM City Center in Las Vegas. Dieser Gebäudekomplex beinhaltet ein Hotel mit 4000 Zimmern. Hier wurde ein ZigBee-Netzwerk aufgebaut, welches über 10.000 Thermometer, 5.000 Touchscreens und 7.500 andere Geräte einbindet. Dieses System erkennt den einzelnen Besucher und seine Vorlieben und konfiguriert das Hotelzimmer dementsprechend. Es können sich Dinge wie die Raumtemperatur, Helligkeit der Lampe, TV-Sender oder Mahlzeiten gemerkt werden. Diese Dinge werden dann bei einem weiteren Besuch als Referenz genutzt und sollen so dem Besucher eine Exklusivität vermitteln. Es ist nicht bekannt, wie das Netzwerk oder die Netzwerke organisiert sind, auf Grund der Größe dürfte aber 2007 Pro zur Anwendung kommen. Vorstellbar wäre pro Etage ein Coordinator, sodass unter einer Baum Topologie für jedes Zimmer ein dedizierter Bereich geschaffen wird.
Nach dem Standard von 2006 "Residential" wäre es durch das Erlangen des Netzwerkschlüssels möglich gewesen, den kompletten Netzwerkverkehr einzusehen. Mit dem Standard von 2007 wurde dann der Link Key für die APS Schicht eingeführt, somit wäre bei Anwendung dieser Option nur noch ein Abhören der Broadcast Kommunikation möglich gewesen. Dies hätte je nach Größe des Netzwerkes immer noch für massiven Schaden sorgen können. Es ergibt sich bei einem erfolgreichen Einsatz eines "Trojaners" (siehe 2.3.5) ein begrenztes Aktionsfeld für den Angreifer, sofern intelligente Vorkehrungen getroffen wurden. Auch hier ließen sich wieder die mit dem Network Key verschlüsselten Nachrichten einsehen, sowie direkte Verbindungen zu anderen Geräten aufbauen. Ginge man davon aus, dass ein Thermometer erfolgreich durch einen Trojaner ersetzt worden wäre, darf dann das Thermometer an den Stellmotor der Heizung direkte Anweisungen erteilen? Hier liegt es in der Verantwortung der Hersteller, Optionen in die einzelnen Anwendungsprofile zu integrieren, sodass die einzelnen Geräte nur von logisch verbundenen Führungsgeräten instruiert werden können.
Unbeeinträchtigt davon bleibt das Beeinflussen durch einen Störsender. In dem Fall des Hotels stellt dies einen gravierenden Angriff auf Existenz dar, da bei einem Ausfall des Netzwerkes kein Ersatz vorgesehen ist. Hier müsste mit einem erheblichen finanziellen Schaden gerechnet werden, da dieses Hotel in seiner Verkaufsstrategie diese interaktiven

Hotelzimmer als Argument benutzt.
Nach aktuellem Stand sind jedoch keine wirksamen Maßnahmen integriert worden, so ist auf der Source Konferenz im April 2010 von Joshua Wright durch das von ihm entwickelte Framework KillerBee gezeigt worden, dass bestehende Netzwerke häufig das Schlüsselmaterial an neue Geräte im Klartext übertragen. Zusätzlich dürften keine Absicherungen bezüglich Replayattacken genutzt worden sein, da von ihm erwähnt wird, diese Attacken erfolgreich eingesetzt zu haben. Unter der zu Hilfenahme eines Hardware Debugging Tools von Travis Goodspeed konnte bei einem ZigBee-Gerät der RAM ausgelesen werden, obwohl der Chip dies nicht gestattete. In Kombination mit mitgeschnittenen Daten konnte daraus das Schlüsselmaterial abgeleitet werden.[6]

2.5 Fazit

Betrachtet man die zunehmende Verbreitung von ZigBee basierten Lösungen, so muss die Frage gestellt werden, inwieweit man den Systemen vertrauen kann. Der Einfluss auf den durch diese Netzwerke gesteuerten Alltag ist schon jetzt nicht unerheblich. Jedoch sind die bisherigen Implementierungen (hauptsächlich im kommerziellen Bereich) durch Fachleute vorgenommen worden, dies reduziert das Risiko, unbewusst Sicherheitslücken integriert zu haben. Hierbei stellt sich aber die Frage, wie die Folgen im privaten Bereich zu bewerten sind. Grundsätzlich bietet der ZigBee Stack Schutzmaßnahmen, die einen sicheren Betrieb gewährleisten können, bisher werden diese aber nicht zwingend gefordert. Hier wäre eine verpflichtende Vorgabe durch den Standard sinnvoll und nicht wie bisher durch die einzelnen Anwendungsprofile. Einige Anwendungsprofile (Smart Energy 2.0) sollen in Zukunft die Sicherheitsdienste von IEEE 802.15.4 nutzen, sowie umfangreiche Authentifizierungsmöglichkeiten (X.509 Zertifikate) bieten [2, S.84]; diese Optionen setzen wie bisher eine gründliche Planung des Netzwerkes voraus. Hier ist es fraglich, ob der Heimanwender bei der Vernetzung seiner Geräte genügend Fachexpertise und Interesse mitbringt; selbst bei der Integration durch einen Handwerker wird eine Sicherheitsanalyse nur selten zum Leistungsspektrum gehören.
Es ist kein grundsätzliches Problem von ZigBee, das die Masse der Anwender nur wenig Interesse an Datenschutz hat, die Sicherheit der Funktionalität unterordnet, Einfachheit gegenüber Konfigurationsmöglichkeiten bevorzugt. Hier sollte sich die Allianz verpflichtet fühlen, dem Anwender ein Produkt zu präsentieren, dass seinen Ansprüchen gerecht wird, aber nicht seine Sicherheit vernachlässigt. Hierbei spielt es nach meiner Ansicht keine Rolle, welche Funktion die Daten erfüllen, jegliche Daten sind grundsätzlich zu schützen.

Literaturverzeichnis

[1] ZigBee Alliance. *The ZigBee Specification 2007 V.r17* , 17. Januar 2008, verfügbar auf http://zigbee.org

[2] ZigBee Alliance. *ZigBee Smart Energy Profile 2.0 Technical Requirements Document Ver. 0.5 rev. 14* , 11. Dezember 2009, verfügbar auf http://zigbee.org/Standards/ZigBeeSmartEnergy/Version20Documents.aspx

[3] IEEE Std 802.15.4-2003. *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs)* , Oktober 2003, verfügbar auf http://standards.ieee.org

[4] Ken Masica. *Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Enviroment (Entwurf)*,Homeland Security , April 2007

[5] Ryan Speers / Ricky Melgares. *ShmooCon 2011 "ZigBee Security: Find, Fix, Finish."*,Dartmouth Trust Lab, Dartmouth Januar 2011, verfügbar auf http://www.cs.dartmouth.edu/ rspeers/

[6] Joshua Wright. *KillerBee: Practical ZigBee Exploitation Framework*, Source , 2010, verfügbar auf http://sourceboston2010.blip.tv/file/3567619/

[7] David Gascón. *Security in 802.15.4 and ZigBee networks* , Februar 2009, verfügbar auf http://www.sensor-networks.org

[8] Christiane Rütten. *magazin für computer und technik - "Panzerknacker - Sicherheit von USB-Sticks"*, heise, Hannover 22/2010

[9] Markus Gerstner. *ZigBee - Bachelor Seminar Paper*, TU Wien, Wien 2010

[10] Naveen Sastry/David Wagner *Security Considerations for IEEE 802.15.4 Networks*, University of California, Berkeley Oktober 2004, verfügbar auf http://en.scientificcommons.org/43301853

[11] ZVEI- Zentralverband Elektrotechnik- und Elektronikindustrie e.V. *Koexistenz von Funksystemen in der Automatisierungstechnik*, ZVEI-Fachverband Automation, Frankfurt a.M. November 2008, verfügbar auf http://zvei.org/automation

Kapitel 3

DASH-7 Datenkommunikation

Paul Watzlawik

Die DASH7-Funktechnologie soll in den kommenden Jahren bisher vorhandene und etablierte Protokolle ersetzen. Das Departement of Defense lies dieses Protokoll zur verbesserten Nutzung von drahtlosen Sensornetzen entwickeln und stellt dabei auch den größten finanziellen Anteil. Durch das neue Kommunikationsprotokoll soll unter anderem die Reichweite und die Batterielebensdauer erheblich gesteigert werden. Unter optimalen Bedingungen konnten auch bereits Reichweiten von bis zu zehn Kilometern erreicht werden und auch der Energieverbrauch wird im Vergleich zu herkömmlichen Protokollen um das Zehnfache unterschritten.

Aufgrund dieser viel versprechenden Eigenschaften befasst sich diese Arbeit genauer mit dem Protokoll DASH7. Es werden Anwendungsbereiche für dieses Protokoll aufgezeigt und abschließend wird es mit ZigBee, eines der derzeit etablierten Protokolle, verglichen.

Inhaltsverzeichnis

3.1 Einleitung und Problemstellung 57
3.2 Sensornetze 57
3.2.1 Drahtlose Sensornetze 58
3.2.2 Anwendungsszenarien für drahtlose Sensornetze 58
3.2.3 Anforderungen an Sensornetze 60
3.2.4 Aufbau eines WSN 62
3.3 ZigBee 64
3.3.1 Aufbau des Protokolls 65
3.3.2 Arbeitsweise ZigBee 66
3.4 DASH7 67
3.4.1 ISO 18000-7 67
3.4.2 Arbeitsweise DASH7 69
3.5 Vergleich der Protokolle 70
3.5.1 Vergleichskriterien 70
3.5.2 Vergleich 71
3.6 Schluss 72
3.6.1 Bewertung 72
3.6.2 Zusammenfassung und Ausblick 73

3.1 Einleitung und Problemstellung

Die Technik der drahtlosen Sensornetzwerke wurde ursprünglich für den militärischen Gebrauch entwickelt. Im Laufe der Zeit wurden die verschiedenen Anwendungsmöglichkeiten auch für kommerzielle Zwecke entdeckt. So kam es zur Entwicklung von Protokollen zur Nutzung von drahtlosen Netzen, wie zum Beispiel ZigBee oder IEEE 802.15.4. Diese Protokolle sollten die immensen Anforderungen, wie Energieeffizienz, Umgang mit hohen Fehlerraten, möglichst lange Übertragungsdistanzen oder verschiedene Sicherheitsaspekte, an ein solches Netzwerk erfüllen. Seit Januar 2009 fördert das U.S. Verteidigungsministerium die DASH7-Funktechnologie, die dann Ende 2009 durch ein Konsortium aus Industrie und Forschung spezifiziert wurde. Diese neue Technik soll nun in den kommenden Jahren bisher vorhandene und etablierte Protokolle des Bereichs der drahtlosen Sensornetze, wie beispielsweise ZigBee, ersetzen.
Diese Arbeit wird sich mit der Technologie des DASH7-Protokolls beschäftigen und es mit Protokollen wie ZigBee vergleichen. Ziel ist es dabei festzustellen, ob das DASH7-Protokoll den Anforderungen an die Kommunikation im Umfeld von Sensornetzen gerecht wird und wie es im Vergleich zu ZigBee abschneidet. Dazu wird im Verlauf der Arbeit zunächst in 3.2 geklärt, was unter einem drahtlosen Sensornetzwerk zu verstehen ist. Es werden dabei die einzelnen Generationen der drahtlosen Sensornetze vorgestellt und anschließend werden mögliche Einsatzgebiete für solche Netzwerke betrachtet. Daraus entstehen dann Anforderungen, die an ein solches Netz gestellt werden, welche danach auch betrachtet werden. Wenn dies alles geschehen ist wird dann die Arbeitsweise von drahtlosen Sensornetzen erläutert. Im Folgenden Abschnitt 4.7.2 dann das ZigBee Protokoll behandelt. Dies war in den letzten Jahren eines der wichtigsten Protokolle auf dem Markt war und setzt auf dem IEEE 802.15.4 Standard auf. Bevor in Abschnitt 3.5 ein Vergleich zwischen Developers' Alliance for Standards Harmonization of ISO 18000-7 (DASH7) und ZigBee stattfinden kann muss DASH7 selbst aber noch näher beleuchtet werden. Dazu wird in Abschnitt 3.4 zunächst der ISO 18000-7 Standard betrachtet werden müssen, bevor dann das Protokoll selbst erläutert werden kann. Um einen Vergleich der beiden Protokolle durchführen zu können müssen zunächst Vergleichskriterien gefunden werden anhand welcher dann im weiteren Verlauf des Abschnitts 3.5 eine Gegenüberstellung stattfinden kann. Nach dem Vergleich wird dann eine Bewertung von DASH7 vorgenommen werden. Die Arbeit endet mit einer Zusammenfassung und einem Ausblick mit Abschnitt 3.6.

3.2 Sensornetze

Ihr Siegeszug begann in den Achtziger Jahren des vergangenen Jahrhunderts. Die Rede ist von Sensornetzen. Waren sie anfangs nur für das Abhören und zur Überwachung von Personen gedacht, wurden jedoch schnell weitere Möglichkeiten zum Einsatz dieser Netze gefunden. So verwundert es nicht, dass sie schnell an Bedeutung gewannen und auch heute noch eine zentrale Rolle sowohl beim Militär als auch in kommerziellen Anwendungen spielen. In den folgenden Abschnitten werden Drahtlose Sensornetze (Wireless Sensor Network) (WSN), ihre möglichen Einsatzszenarien und daraus entstehende Anforderungen an sie betrachtet.

3.2.1 Drahtlose Sensornetze

Unter einem drahtlosen Sensornetz versteht man ein Rechnernetz von Sensorknoten die über Funk kommunizieren. Sensorknoten sind dabei winzige („Staubkorn“) bis zur Größe von Schuhkartons kommunizierende Computer, welche mittels Sensoren ihre Umgebung überwachen. Sie bauen dabei Infrastrukturbasierte- oder sich selbst organisierende Ad-Hoc-Netzwerke auf. WSN greifen somit auf Konzepte aus Radio-frequency identification (RFID)-Systemen sowie auf Konzepte aus Mobile Ad-Hoc Networks (MANet) zurück. Sie unterscheiden sich aber dennoch von beiden Systemen, da sie im Gegensatz zu MANet stark in ihrer Hardware beschränkt sind und anders als bei RFID-Systemen ein Netzwerk mit mehreren Knoten bilden.[1, 17]
WSN können in drei Generationen kategorisiert werden. Zur ersten Generation gehörten einzelne Sensoren, die noch von Hand verbracht werden mussten. Das daraus entstandene Netzwerk war meist vorkonfiguriert. Das wiederum führte dazu, dass das Netzwerk sehr unflexibel und starr war. Erweiterungen ließen sich nur schwer und in der Regel nur durch den Administrator selbst einbringen. In der zweiten Generation konnten die einzelnen Sensorknoten bereits zwischen einander kommunizieren und somit auch kollaborieren. Leider mussten die einzelnen Sensoren auch hier per Hand an ihren Einsatzort gebracht werden. WSN der zweiten Generation waren daher ebenfalls meist vorkonfiguriert. Die Netzwerke die aus ihnen entstanden sind waren meist sternförmig.[1, 6, 17]
Am interessantesten aber sind die Sensornetze der dritten Generation. Sie können auf verschiedenste Arten verbracht werden. So ist es zum Beispiel möglich sie durch einen Flugzeugabwurf oder auch durch Artillerieverschuss an ihren Bestimmungsort zu bringen. Dies erweitert erheblich das Gebiet in dem sie potentiell eingesetzt werden können und auch ihr Einsatzspektrum wird dadurch erweitert. Ein WSN kann dabei mehrere hundert bis tausend Sensorknoten umfassen. Welche sich dann selbst organisieren und flexible Netzwerke bilden. Diese Netzwerke sind dabei auch noch skalierbar, so dass problemlos weitere Knoten hinzugefügt oder entfernt werden können. Die Sensorknoten der dritten Generation bilden so ein so genanntes Multi-Hop Netzwerk, dass durch seine In-Netzwerkverarbeitung und Aggregation besticht.[6]
Auch wenn es im Bereich der WSN noch einige Probleme, wie beispielsweise die Energieversorgung, zu lösen sind, so sind sie doch in vielen kommerziellen und militärischen Gebieten von großem Interesse und bieten ein außerordentliches Potenzial [2, 6]. Dazu werden in den folgenden Abschnitten ein paar wenige Möglichkeiten zum Einsatz von WSN aufgezeigt und erläutert.

3.2.2 Anwendungsszenarien für drahtlose Sensornetze

Die Anwendungsbereiche für WSN sind sehr vielfältig. Sie werden zur Überwachung von Maschinen, in der Medizin oder aber auch in der Landwirtschaft eingesetzt [1, 18]. Dies sind aber bei weitem nicht alle denkbaren Einsatzmöglichkeiten. So könnten WSN im zivilen für die Überwachung einer Chemiefabrik, eines Waldbrandes oder aber auch zur Steuerung eines intelligenten Gebäudes, welches dadurch Heizung, Klimaanlage und Belüftung je nach Tageszeit, Außentemperatur und Anwesenheit von Bewohnern regelt, genutzt werden. [1]

In diesem Abschnitt werden zwei mögliche Einsatzszenarien, davon eins kommerziell und eins militärisch, behandelt und somit das Potenzial von WSN aufgedeckt.

Zivile Anwendung

Ein typisches Einsatzgebiet eines WSN stellt die Beobachtung von Tieren dar. Diese werden nicht durch die Sensornetzwerke gestört und können so bestens in ihrer natürlichen Umgebung beobachtet werden. Hierzu gab es bereits Versuche mit Sensornetzen der ersten Generation, welche getarnt als Baumstumpf in den Urwald verbracht wurden. Sie dienten dazu Elefanten in ihrer natürlichen Umgebung zu beobachten und waren mit Bewegungssensoren ausgestattet. Angeschaltet waren sie dementsprechend nur, wenn sich vor ihnen etwas bewegte. Dies half dabei Energie zu sparen. Die durch die Sensorknoten gewonnen Daten mussten damals noch per Hand ausgelesen werden. Hier ist jedoch der Schritt zur Ausstattung mit einem Funksender nicht mehr weit und relativ einfach zu realisieren.[2, 9]
Aus diesem Beispiel ergeben sich aber noch weitere Einsatzmöglichkeiten zur Überwachung der Tiere. So könnten die Wanderrouten der Tiere sowie deren Zahl oder die Anzahl der Populationen in einem Gebiet bestimmt werden. Dazu wären, wie in Abbildung 3.1 zu sehen, langlebige mit Bewegungssensoren ausgestattete Sensorknoten nötig.

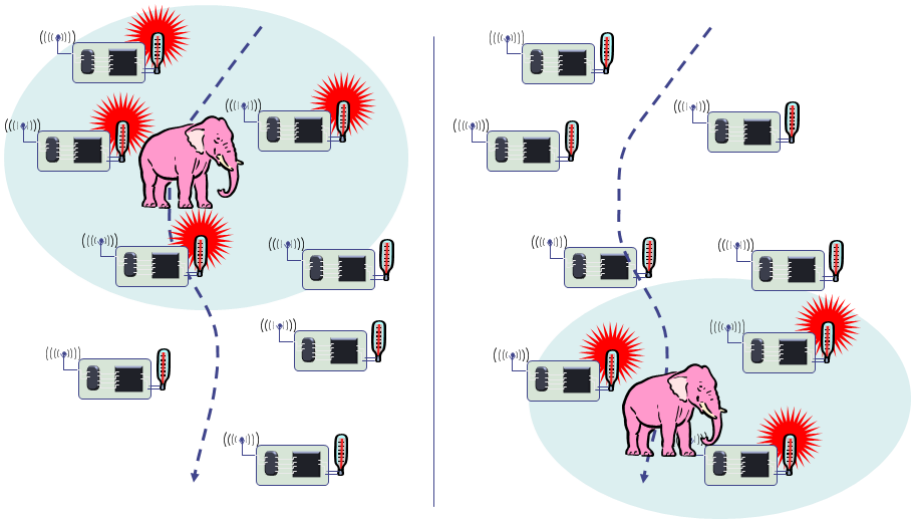

Abbildung 3.1: Drahtloses Sensornetz zur Überwachung von Tierwanderrouten [6]

Militärische Anwendung

Für den Einsatz im Militär liegen die Vorteile von WSN klar auf der Hand. Hier geht die Verwendung von drahtlosen Sensornetzen einher mit einer signifikanten Steigerung der Sicherheit der Soldaten. So können durch WSN, ähnlich wie bei den Elefanten, die Marschrouten der feindlichen Truppen oder aber ein Feldlager überwacht werden. Durch diese Möglichkeit, kann die Anzahl der eingesetzten Soldaten stark reduziert werden. Gleichzeitig können durch die Sensoren auch die Kommunikation des Gegners entweder

abgefangen und mitgehört oder zumindest gestört werden. Durch das Abhören kann sogar eine Informationsüberlegenheit erzielt werden, welche im Falle eines Gefechts zu einem Wirkungsvorteil werden könnte. Es bleibt also fest zu halten, dass der Einsatz von WSN in militärischen Einsätzen ein sehr nützliches Werkzeug darstellen könnte und eine Vielzahl von weiteren interessanten Einsatzmöglichkeiten bietet.[6]

3.2.3 Anforderungen an Sensornetze

Aus den vielfältigen Möglichkeiten zum Einsatz von Sensornetzen ergeben sich ganz bestimmte Anforderungen für diese. Aufgrund der großen Unterschiede in den Szenarien resultieren aber auch die unterschiedlichsten Anforderungen an ein WSN. Prinzipiell sind die Anforderungen eher anwendungsbezogen und somit auch sehr schwer global zu formulieren. Es lassen sich aber dennoch einige Kriterien feststellen, durch die drahtlose Sensornetze vergleichbar werden. Zu den typischen Anforderungen gehören hier: ein niedriger Preis, Energieeffizienz, lange Lebensdauer, Selbstkonfigurierbarkeit, Skalierbarkeit, Quality of Service, Robustheit, Fehlertoleranz, Sicherheit, Mobilität und Umweltverträglichkeit.[6]

Niedriger Preis:
Der Preis eines Knotens sollte einen bestimmten Wert nicht überschreiten. Drahtlose Sensornetze können in einigen Szenarien mehrere hundert bis tausend Knoten groß sein. Bei solchen Größen wären Preise von hundert Dollar oder mehr pro Sensorknoten zu hoch. Nach einigen Überlegungen sollte ein einzelner Knoten nicht mehr als einen Dollar kosten. Der Peis lässt sich aber nicht allein an der Größe eines einzelnen Knotens ausmachen. Hier muss die Leistungsfähigkeit und Funktionalität beziehungsweise die Erfüllung anderer Anforderungen mit einberechnet werden.[6]

Energieeffizienz:
Ein sehr großes Problem stellt die Energieversorgung dar. Hier soll eine möglichst gute Ausbeute erreicht werden um eine möglichst lange Überwachungsdauer gewährleisten zu können.[6]

Lange Lebensdauer:
Die Lebensdauer geht einher mit der Energieeffizienz. Es ist daher von besonderer Bedeutung, dass ein WSN mit beschränkter Energieversorgung so lange wie nur möglich betrieben werden kann um seinen Auftrag wahrzunehmen.[6]

Selbstkonfigurierbarkeit:
Durch die Möglichkeit, dass ein WSN per Flugzeugabwurf oder Artillerieverschuss verbracht werden kann ist es kaum möglich das Netzwerk vorher zu konfigurieren. Aus diesem Grund muss ein Knoten über Mechanismen verfügen, welche es ermöglichen sich mit den anderen Knoten des Netzwerkes zu organisieren. Dies wird durch die Protokolle geregelt. Aber auch weitere Ereignisse wie Knotenausfälle müssen dabei beachtet werden und eine Möglichkeit der Rekonfiguration gegeben sein.[6]

Skalierbarkeit:
Mit der Skalierbarkeit wird der Umgang eines Netzwerkes mit der Anzahl der Knoten

beschrieben. Unter einer guten Skalierbarkeit versteht man, dass es für ein WSN egal ist, ob es hundert oder tausend Knoten enthält. Auch diese Eigenschaft ist abhängig von den Protokollen. In Netzen in denen die Anzahl der Knoten fix ist wird keine Skalierbarkeit benötigt.[6]

Quality of Service:
Im Zusammenhang mit WSN beschreibt Quality of Service (QoS) weniger die „klassischen", „Low-Level QoS-Parameter" wie Jitter, Bandbreite oder Verzögerung. Viel mehr werden die „High-Level QoS-Parameter" abhängig von subjektiven Qualitätsmerkmalen beschrieben. Darunter fallen beispielsweise Ereigniserkennung, Ereignisklassifizierungsfehler, Verzögerungen in der Ereigniserkennung oder die Genauigkeit.[6]

Robustheit:
Unter Robustheit wird zum einen die physische Robustheit verstanden. So sollten die einzelnen Sensorknoten einen möglichen Flugzeugabwurf, oder einen Artillerieverschuss auch überstehen können. Zum anderen ist es aber auch notwendig, dass das Netzwerkprotokoll so gestaltet ist, dass ein Ausfall eines Knotens nicht zum Zusammenbruch des gesamten Netzes führen kann.[6]

Fehlertoleranz:
Die Fehlertoleranz geht einher mit der Robustheit. Sie bezeichnet dabei den Umgang mit häufig auftretenden Störungen und Interferenzen, die typischerweise in der drahtlosen Kommunikation auftreten.[6]

Sicherheit:
Sicherheit ist gerade in kritischen Anwendungen, bei denen sensible Daten über das Netzwerk verschickt werden sollen von besonderer Bedeutung. Sie spielt gerade für militärische Anwendungen eine herausgehobene Rolle. Hier muss ein Knoten sowohl physikalisch geschützt sein, als auch in der Übertragung von Daten. Es muss gelten, dass für sicherheitsrelevante Daten die Authentizität, Integrität und Vertraulichkeit nicht verletzt sind. Diese Bedingungen stehen aber in Kontrast zu Anforderungen wie Lebensdauer, Ressourcenknappheit und Energieeffizienz, so dass hier ein guter Mittelweg gefunden werden muss.[6]

Mobilität:
Für ein WSN werden drei Arten der Mobilität unterschieden. So gibt es zum einen die Knotenmobilität, die, wie der Name schon sagt, vorliegt wenn sich die Knoten während des Betriebs des Netzwerks bewegen sollen. Zum anderen gibt es noch die Datensenkenmobilität. Hierunter wird verstanden, dass sich nur die Datensenken bewegen, die Netzwerkknoten selbst bewegen sich aber nicht (Beispiel: Waldbrand). Als letzten Punkt der Mobilität ist die Ereignismobilität zu nennen. Hier muss durch einen Knoten erkannt werden, ob das von ihm gemessene Ereignis bereits früher durch einen anderen Sensor gemessen wurde und daraus ableiten können, dass sich das Ereignis bewegt. Ein WSN muss mit allen drei Arten der Mobilität umgehen können.[6]

Umweltverträglichkeit:
Wenn nicht die Möglichkeit besteht die Sensorknoten wieder einzusammeln, sollte die

Umweltverträglichkeit bedacht werden. Hier sollte geprüft werden, ob ein Sensorknoten eventuell Schadstoffe enthält oder aber ob ein Tier durch fressen eines Knotens verenden könnte.[6]

Für den Einsatz in militärischen Szenarien kommen noch spezielle Anforderungen hinzu. So sollen solche Netze eine schnelle Einsatz- und Aufklärungsbereitschaft, eine hohe Redundanz gegenüber Einzelausfällen von Sensorknoten, eine Befähigung für den Langzeitbetrieb und eine gesicherte Aufklärungs- und Kommunikationsfähigkeit haben.[2, 5] Diese werden hier nur kurz genannt. Weitere Informationen darüber können gern in [7] nachgelesen werden.

3.2.4 Aufbau eines WSN

Dieser Abschnitt soll erläutern, wie nun ein WSN aus Sensorknoten aufgebaut wird. Dazu wird zunächst der Aufbau eines Sensorknotens erläutert und dann in groben Zügen der Aufbau eines drahtlosen Sensornetzes erklärt.

Aufbau eines Knotens

Wie bereits im letzten Abschnitt dargestellt worden ist, sind Sensornetz und dementsprechend auch die Sensorknoten sehr anwendungsspezifisch und müssen einen guten Kompromiss zwischen den einzelnen Anforderungen finden. Im Allgemeinen ist der Aufbau eines Knotens aber immer gleich. In Abbildung (3.2) wird der typische Aufbau eines Knotens

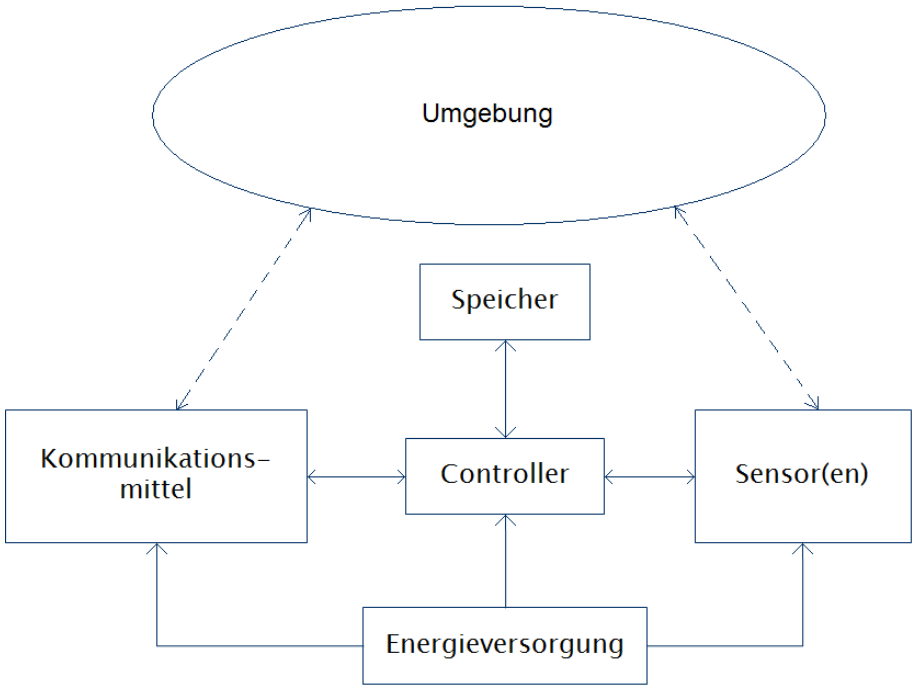

Abbildung 3.2: Aufbau eines Sensorknotens [6]

gezeigt. Er besteht aus den fünf Komponenten: Controller, Speicher, Sensoren, Energieversorgung und Kommunikationsmittel.

Controller:
Er stellt den Kern eines Sensorknotens dar. Durch ihn werden die Daten von den Sensoren verarbeitet und versendet. Gleichzeitig erhält er auch Daten anderer Sensorknoten. Der Controller führt verschiedene Programme, wie Signalverarbeitungs- und Kommunikationsprotokolle und Anwendungsprogramme, aus. Er ist somit der Hauptprozessor des Knotens. Oftmals kommen hier Microcontroller zum Einsatz. Diese haben Vorteile durch ihre Flexibilität und ihren niedrigen Energieverbrauch. Alternativen zu Microcontrollern sind Digitale Signalprozessoren (DSP), Feldprogrammierbare Gate Arrays (FPGA) oder Anwendungspezifische Integrierte Schaltkreise (Application specific integrated Circuits) (ASIC).[1]

Speicher:
Der Speicher wird benötigt um Programme und Daten zu speichern. Hierzu werden in der Regel unterschiedliche Arten von Speichern verwendet. Für die Sensordaten und Pakete die von anderen Sensorknoten kommen wird Random Access Memory (RAM) benötigt. Dieser hat aber den Nachteil, dass er flüchtig ist und ohne eine Energieversorgung alle Daten verliert. Deshalb wird der Programmcode typischerweise in Electrically Erasable Read Only Memory (EEPROM) oder Flash-Speicher gespeichert. Trotz seines höheren Energieverbrauchs und seiner längeren Zugriffszeiten wird der Flash-Speicher in den meisten bisher gebauten Sensorknoten bevorzugt.[1]

Sensor(en):
Für einen Sensorknoten können ein oder mehrere Sensoren verbaut werden. Unterschieden wird hier in drei Arten von Sensoren. Die passiv, omnidirektionalen Sensoren, die passiv, gerichteten Sensoren und die aktiven Sensoren. Passiv heißt in diesem Zusammenhang, dass die Umwelt durch den Sensor nicht beeinflusst wird. So messen die passiv, omnidirektionale Sensoren einen physikalischen Wert in ihrer Umwelt. Die Art der Messung ist dabei „richtungslos“. Typische Anwendungen für solche Sensoren sind Thermometer, Lichtsensoren oder Feuchtigkeitssensoren. Gerichtete Sensoren sind ebenfalls passiv, jedoch haben sie eine klare Richtung für ihre Messung. Als Beispiel für einen solchen Sensor kann man hier die Videokamera nennen, die mit einer bestimmten Richtung Bilder aufnimmt. Unter aktiven Sensoren verstehen wir Sensoren, welche ihre Umwelt beeinflussen um eine Messung durchführen zu können. Beispiele hierfür sind das Sonar und das Radar. Sie senden Signale aus und empfangen die Rückmeldungen aus ihrer Umwelt.[1]

Energieversorgung:
Die Energieversorgung stellt eine besondere Herausforderung dar. Hier gibt es unterschiedliche Möglichkeiten. So kann zwischen wieder aufladbaren (kurz: Akku) und nicht wieder aufladbaren Batterien unterschieden werden. Nicht wieder aufladbare Batterien haben hier den Vorteil des höheren Energievolumens, falls es keinen Auflade-Mechanismus gibt. An die Batterien werden im Allgemeinen sehr hohe Anforderungen gestellt, da die Belastungen stark schwanken. Es reicht also nicht aus, wenn eine Batterie nur unter optimalen Bedingungen eine lange Lebensdauer hat. Akkus hingegen machen Sinn wenn es eine Möglichkeit der Wiederaufladung gibt. Dies ist beispielsweise durch Photovoltaik möglich. Ziel

wird es sein völlig autarke Knoten zu entwickeln, welche sich selbständig vollständig aufladen können.[1]

Kommunikationsmittel:
Durch das Kommunikationsmittel wird die Art der drahtlosen Kommunikation beschrieben. Dafür gibt es grundsätzlich mehrere Möglichkeiten. So können beispielsweise optische Kommunikation, Schallwellen und Funktechnik genutzt werden. Von den drei Möglichkeiten ist die Funktechnik bei der Nutzung der Luftschnittstelle im Vorteil, da hier relativ hohe Reichweiten, akzeptable Fehlerraten und ein recht geringer Energieverbrauch erzielt werden können. Für die Übertragung unter Wasser sind wiederum Schallwellen besser geeignet. Die größte Bedeutung kommt aber dennoch der Funktechnik zu.[1]

Aufbau des WSN

Wie in jedem anderen Netzwerk gibt es auch bei den WSN Quellen und Senken. Unter einer Quelle versteht man in diesem Zusammenhang die Knoten, die mit Hilfe ihrer Sensoren ein Ereignis wahrgenommen und entsprechend ihrer Programmierung verarbeitet haben um diese nun über ihr Kommunikationsmittel zu versenden. Senken sind die Computer im Netzwerk, welche genau diese Daten empfangen sollen. Dies können sowohl andere Knoten, als auch in Reichweite des Netzwerks befindliche Computer oder aber über ein Gateway angeschlossene Computer sein.[6]
Das Kommunikationsmittel stellt den größten Energieverbraucher dar. Aus diesem Grund versucht man die Sendeleistung so gering wie möglich zu halten. Dies gelingt am besten durch den Aufbau von Multi-Hop Netzwerken, ähnlich wie bei den mobilen Ad-Hoc Netzwerken. In den meisten Szenarien gibt es fast nie den Fall, dass es nur eine Quelle und eine Senke gibt. Häufig ist es der Fall, dass ein oder mehrere Ereignisse durch verschiedene Knoten erfasst werden. Somit kann es dazu kommen, dass viele Quellen an nur eine Senke senden. Aber auch die umgekehrte Variante ist möglich, so dass eine Quelle an mehrere Senken sendet. Das komplizierteste Szenario stellt dementsprechend der Fall dar, dass es mehrere Quellen und Senken gibt. Dies aber ist der häufigste Fall. Ein weiteres Problem stellt die Mobilität der WSN dar. Wenn sich eine Senke bewegt, muss das durch das Sensornetz erkannt und auch dementsprechend reagiert werden.[6]
Wie zu sehen ist, ist die Netztopologie und der Aufbau eines WSN stark anwendungsbezogen. Aus diesem Grund werden auch an die jeweiligen Protokolle besondere Anforderungen gestellt. Zwei dieser Protokolle werden im Folgenden näher betrachtet.

3.3 ZigBee

ZigBee stellt einen Funknetz-Standard dar. Er setzt als Kommunikationsprotokoll auf Layer 3 des Open Systems Interconnection (OSI)-Referenzmodells auf. PHY- und MAC-Layer basieren hierbei auf den denn Institute of Electrical and Electronics Engineers (IEEE)-Standard 802.15.4 [11]. Dieses Kapitel befasst sich zunächst mit dem Aufbau des ZigBee-Protokolls und im Folgenden wird der Aufbau eines Netzes durch die Nutzung von

ZigBee erläutert. Die Informationen für diesen Abschnitt stammen aus der Spezifikation von ZigBee aus dem Jahr 2008 [10] und aus [8] sowie [11].

3.3.1 Aufbau des Protokolls

In Abbildung 3.3 ist der genaue Aufbau des ZigBee Protokollstack zu sehen. Er nutzt wie eben beschrieben die den IEEE-Standard 802.15.4 auf Layer 1 und 2 und setzt dann ab dem Networklayer darauf auf und erweitert diese um ein Framework für Anwendungen. ZigBee zielt darauf ab, günstige und interoperable Produkte für Funknetze zu er-

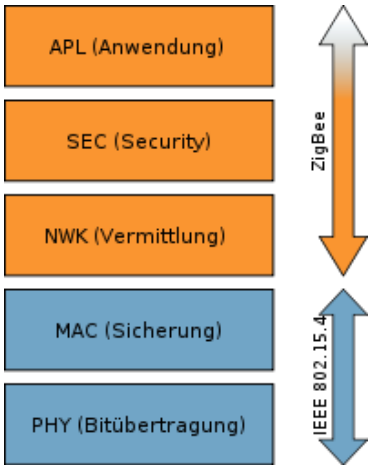

Abbildung 3.3: ZigBee Protokollstack [15]

möglichen. So werden durch diesen Standard Übertragungen von Sensoren und Geräten ermöglicht, welche von zehn bis hundert Meter reichen können. Typische Einsatzgebiete für dieses Protokoll sind wartungsfreie Funkschalter sowie Funksensoren mit beschränkter Energieversorgung in schwer erreichbaren Gebieten, aber auch eine Vernetzung von Haushaltsgeräten. ZigBee unterstützt insgesamt drei Topologien. Die Stern-, die Baum- und die vermaschte (mesh) Topologie. Interaktionen zwischen den einzelnen Architekturschichten sind dabei auf wenige Schnittstellen beschränkt. Im Folgenden werden die einzelnen Layer näher betrachtet und ihre Eigenschaften herausgestellt.

PHY-Layer:
IEEE 802.15.4 ist gedacht für Anwendungen die nur niedrige Bitraten bei gleichzeitig geringem Energieverbrauch benötigen. Durch den Standard werden die Frequenzen aus den Industrial, Scientific and Medical (ISM)-Bänder verwendet. Gegen Störungen greift er auf Direct Sequence Spread Spectrum (DSSS) zurück.

MAC-Layer:
Als Übertragungsverfahren werden durch Medienzugriffsschicht ein *unslotted mode* und ein *slotted mode* definiert. Allgemein werden sie auch als *non-beacon-enabled* oder *beacon-enabled* bezeichnet. Versendet werden die Daten durch die Knoten mittels Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA). Daraus folgt, dass vor jeder Übertragung geprüft wird, ob der Übertragungskanal frei ist. Ist dies nicht der Fall wird eine

zufällige backoff-Zeit gewartet. Die backoff-Zeit im slotted mode wird dabei durch die Synchronisation auf die beacons koordiniert.[8]
IEEE 802.15.4 unterscheidet dazu zwischen Full Function Device (FFD) und Reduced Function Device (RFD). Das FFD kann dabei als Koordinator den Zugriff auf das Übertragungsmedium organisieren. Um eine feste zeitliche Übertragungsspanne (superframe) einzugrenzen werden durch den Koordinator periodisch bestimmte Signale, so genannte beacons versendet. Andere Knoten können sich daraufhin auf den superframe synchronisieren. Die Zeitschlitze, aus denen ein superframe besteht, werden dazu in eine Wettbewerbsphase und eine Wettbewerbsfreie Phase unterteilt. Wobei in ersterer CSMA/CA wie beschrieben stattfindet und in letzterer Phase den Knoten durch den Koordinator feste Zeitschlitze zugeteilt werden.

NWK-Layer:
Die Netzschicht wird von ZigBee in die Network Layer Management Entity (NLME) und die Network Layer Data Entity (NLDE) unterteilt. Dabei ist das NLDE für das topologiebezogene Routing und das Erzeugen von Nachrichten (PDUs) zuständig. Das NLME dagegen bietet verschiedene Funktionalitäten, wie ein Gerät zu konfigurieren, ein Netz aufzubauen oder einem Netz beizutreten. Weiterhin ist es auch in der Lage Neighbor and Route Discovery durchzuführen. Schnittstellen zur Medienzugriffs- und zur Anwendungsschicht werden sowohl durch NLME als auch von NLDE definiert.[10]

Sowohl ZigBee als auch IEEE 802.15.4 stellen dem Entwickler abgestufte Fähigkeitsprofile von Geräten zur Verfügung. So kann unterschieden werden zwischen Endgerät, Router und Koordinator, wobei letztere immer FFDs sind. Durch diese drei Arten von Geräten werden unterschiedliche Rollen beim Aufbau eines Netzes besetzt. Die eigentlichen Endgeräte kommen hierbei mit wenigen Ressourcen aus. ZigBee kann diese Geräte direkt durch eindeutige 64-Bit Gerätebezeichner oder aber indirekt über 16-Bit Netzschicht-Adressen adressieren.

3.3.2 Arbeitsweise ZigBee

Wie findet jetzt aber die Netzerkennung und das Neighbor Discovery statt? IEEE 802.15.4 unterstützt bereits eine hierarchische Clusterstruktur. In dieser Struktur gibt es einen Koordinator für das Personal Area Network (PAN) und weitere Koordinatoren für Teilnetze. ZigBee nutzt dies aus. Durch den Standard werden bereits Assoziationen zwischen Geräten unterstützt, welche zum Bilden der Cluster-Hierarchie für das organisierte Time Division Multiple Access (TDMA) dienen. Im Folgenden wird hier die Baumtopologie betrachtet, da die anderen in ZigBee möglichen Topologien nur Abwandlungen dieser Topologie sind. Eine Verschlüsselung und Authentifizierung für ZigBee-Nachrichten kann auf der Netzschicht über symmetrische Blockchiffre (AES) durchgeführt werden.

Vor dem Aufbau eines PAN durch den Koordinator, der dieses Netz auch verwaltet, wählt dieser einen Kanal mit geringem Rauschen aus. Auf diesem Kanal dürfen keine anderen Netze senden. Anschließend versendet er periodisch beacons die Adresse des Netzes, die die so genannte PAN-ID enthalten. Knoten die noch keinem Netz zugehörig sind hören alle

Kanäle auf diese beacons ab. Ein Knoten der bereits Teil eines Netzes ist wird durch ZigBee als parent und ein beitretender Knoten als child betrachtet. Das Beitreten zu einem Netz findet dann ähnlich dem Neighbor Discovery statt. Nach dem erkennen eines Netzes sucht der neue Knoten in seiner Nachbarliste nach einem geeigneten parent-Knoten und fragt bei diesem an, ob er dem Netz beitreten kann. Dies geschieht über eine Assoziation auf der Medienzugriffsschicht oder aber über eine explizite ZigBee-join-Nachricht.
Nachbarlisten werden von allen ZigBee-Knoten geführt. In ihnen werden alle in Reichweite befindliche Knoten mit deren Netzwerk-weiten Adressen, die Art des Geräts, die geschätzte Verbindungsqualität und das Alter des Eintrags geführt. Die Größe einer solchen Liste kann aus Gründen der Implementierung aber auch begrenzt sein. Empfängt nun ein Knoten von irgendeinem anderen Gerät eine Nachricht, so wird der dazu gehörige Eintrag aktualisiert und das Alter des Eintrags zurückgesetzt. Endgeräte können Router und Koordinatoren an den reglmäßig versandten beacons erkennen. Router tauschen untereinander noch zusätzlich link-status-Nachrichten aus und können Routingpfade über einen route-discovery-Mechanismus finden. Hier kooperieren die Knoten miteinander um optimale Pfade von einem Knoten zu einem anderen zu finden.

Die Vergabe der Netzschicht-Adressen kann in ZigBee auf zwei unterschiedliche Arten geschehen. Man unterscheidet hier zwischen der verteilten Adresszuordnung, bei der jeder parent-Knoten einen zugewiesenen Satz an Netzadressen hat und der stochastischen Zuordnung, bei der die Geräte sich selbst eine zufällige Adresse zuordnen. Beide Vergabemechanismen können aber problematisch sein. Während bei der verteilten Zuordnung irgendwann alle Netzadressen vergeben sind und keine weitere Knoten mehr über einen bestimmten parent eintreten können kann es bei der stochastischen Zuordnung zu Adresskonflikten kommen, da sich zwei Knoten zufällig die gleiche Adresse geben können.

3.4 DASH7

DASH7 ist eine neue Technologie für WSN und steht für Developers' Alliance for Standards Harmonization of ISO 18000-7 (DASH7). Es wurde ursprünglich (beginnend ab 2009) für das Militär entwickelt wird aber zunehmend auch für andere, auch kommerzielle, Zwecke eingesetzt um dort Protokolle wie ZigBee oder IEEE 802.15.4 zu ersetzen. In diesem Abschnitt werden der Aufbau des Protokolls und später der Verbindungsaufbau zwischen den RFID-Einheiten durch dieses beschrieben.

3.4.1 ISO 18000-7

Das DASH7 Protokoll nutzt die International Organization for Standardization (ISO) 18000-7 Norm. Diese regelt die Kommunikation von RFID-Einheiten. Man unterscheidet bei diesen Einheiten zwischen Reader (Leser) und Tag (Etikett). Der Reader ist ähnlich einem Barcodescanner, der Informationen aus einem Strichcode eines Etiketts (Tag) liest. Nur ist in diesem Fall keine direkte Sichtverbindung nötig. Der ISO 18000-7 Standard ist verglichen mit seinen Gegenstücken ein eher junger Standard. Durch ihn wird das Physical layer communication protocol definiert, welches die Übertragung zwischen Reader und

Tag unter Nutzung der Luftschnittstelle als Kanal gewährleistet.[3, 12]
ISO 18000-7 ist ein offener Standard, der für das lizenzfreie 433 MHz ISM-Band entwickelt wurde. Dieses Band ist weltweit verfügbar und liegt im Ultra High Frequency (UHF)-Bereich von 433,906 - 433,933 MHz. Die Nutzung dieses Bandes führt zu einer sehr guten Energieeffizienz. ISO 18000-7 muss für Kommunikationen, anders als andere Protokolle für WSN, keine Sessions aufbauen. Dafür nutzt es ein symmetrisches Protokoll[4]. Durch dieses ist es möglich sowohl Reader als auch Tag als low power devices zu implementieren, da ihre Funktionen nahezu identisch sind (siehe Abb. 3.4). ISO 18000-7 fungiert nach

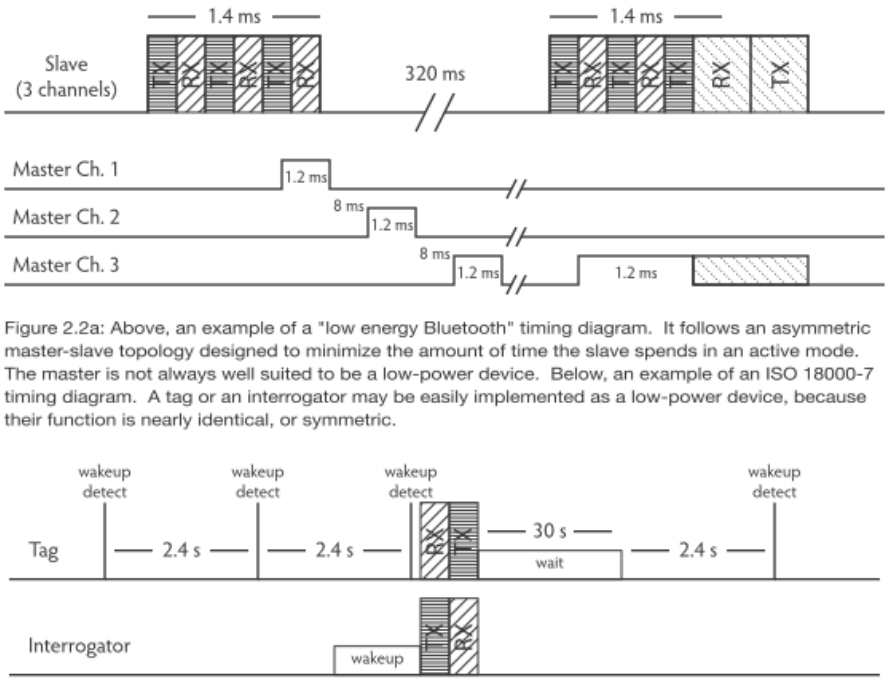

Figure 2.2a: Above, an example of a "low energy Bluetooth" timing diagram. It follows an asymmetric master-slave topology designed to minimize the amount of time the slave spends in an active mode. The master is not always well suited to be a low-power device. Below, an example of an ISO 18000-7 timing diagram. A tag or an interrogator may be easily implemented as a low-power device, because their function is nearly identical, or symmetric.

Abbildung 3.4: Vergleich Bluetooth Timing Diagramm und ISO Timing Diagramm [4]

dem Prinzip des command-response. Bei ihm initiiert der Reader einen Datentransfer mit einem Tag. Der Tag kann dabei niemals mit dem Reader kommunizieren ohne das der Reader ihn dazu aufgefordert hat. Falls also nun der durch den Reader angesprochene Tag eine korrekte Aufforderung erhält, sendet dieser die benötigten Daten zurück an den Reader. Ziel des ISO 18000-7 Standards ist es die Interoperabilität zu stärken. Soll heißen, dass alle Geräte die diesen Standard nutzen untereinander kommunizieren können. Somit muss ein Reader von Anbieter A mit Tags aller anderen Anbieter kommunizieren können.[3]
Damit Reader und Tag miteinander kommunizieren können wird vom Reader eine Wakeup-Sequenz verschickt (Abb. 3.5). Diese wird in die zwei Teile zerlegt. Man bezeichnet sie als Wakeup-Header und als Co-Header. Wobei der Wakeup-Header zwischen 2.4 und 4.8 Sekunden lang sein darf. Ihm folgt der Co-Header der 100 ms lang ist. Insgesamt dürfen beide Header dabei eine Dauer von 4.9 Sekunden nicht überschreiten.[3] Ein Problem für die Interoperabilität entsteht hierbei dadurch, dass zwischen wakeup-Header und Co-Header kein Delay sein darf. Denn sonst kann der Tag von Anbieter nicht das wakeup-Signal vom Reader des Anbieter A. Für die Übertragung der Signale wird als Modulation für alle active RFID-Systeme das Frequency Shift Keying (FSK) verwendet.

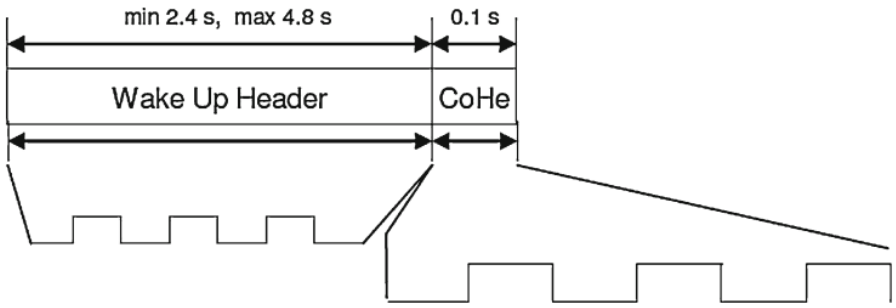

Abbildung 3.5: Wakeup-Sequenz [3]

3.4.2 Arbeitsweise DASH7

Wie bereits erwähnt verwendet DASH7 ISO 18000-7. Es wurde dabei so gestaltet, dass es sich das Bursty, Light-data, Asynchronous, Transitive (BLAST)-Konzept zu Nutze macht. Dabei steht jeder Buchstabe für eine Abkürzung eines bestimmten Prinzips.

Bursty:
Der Datenaustausch findet abrupt statt und enthält keine Inhalte wie Video, Audio oder andere asynchrone Datenformen.[4]

Light-data:
In den meisten konventionellen Anwendungen ist die Größe eines Paketes auf 256 bytes begrenzt. Die Übertragung von mehreren zusammenhängenden Paketen ist dabei möglich, sollte aber weitestgehend vermieden werden.[4]

Asynchronous:
DASH7 verwendet als Methode zur Kommunikation das bereits beschriebene command-response-Verfahren. Durch dieses wird eine Kommunikation ohne ein vorherigen „Handshake “ oder eine Synchronisation ermöglicht.[4]

Transitive:
Ein System von DASH7-Geräten ist von Haus aus mobil. Anders als andere Technologien für WSN steht bei DASH7 der Upload im Zentrum. Dies bringt den Vorteil, dass Geräte nicht weitgehend zentral über feste Infrastruktur gemanagt werden müssen.[4]

Im Gegensatz zur ISO 18000-7 Norm ermöglicht DASH7 eine Tag-to-Tag Kommunikation. Hier können die einzelnen Tags auch untereinander kommunizieren, was eher untypisch für die meisten aktiven RFID- Systeme ist. Durch die Nutzung von UHF sind derzeit bei der Übertragung Reichweiten von einem bis zu zwei Kilometern möglich. Potenziell kann dies noch bis auf 10 Kilometer (in Europa) erweitert werden. Dies wurde auch bereits erfolgreich getestet. Jedoch ist dabei auch zu beachten, dass eine weitere Übertragung immer auch eine höhere Übertragungsleistung und eine größere Antenne zur Folge hat.[4, 14, 16] Eine weitere positive Eigenschaft von DASH7 ist der besonders niedrige Energieverbrauch. Dieser ist dadurch zu erklären, dass aufgrund der eher strukturlosen Kommunikation der einzelnen Geräte keine Sessions aufgebaut werden müssen und somit die Dauer bis Daten übertragen werden können optimiert wird. Bei der Übertragung der Daten können dabei

Raten von bis zu 200 kbit/s erreicht werden. DASH7 findet heute neben dem Militär auch in vielen kommerziellen Anwendungen, wie der Automobilindustrie, der Logistik oder der mobilen Werbung, seinen Einsatz.[14, 16]

3.5 Vergleich der Protokolle

Nachdem die beiden Protokolle ZigBee und DASH7 vorgestellt wurden, werden sie in diesem Abschnitt miteinander verglichen. Dazu werden zunächst Kriterien für den Vergleich herausgestellt und danach die Protokolle anhand dieser gegenüber gestellt.

3.5.1 Vergleichskriterien

Um einen Vergleich ordentlich durchführen zu können, ist es nötig Kriterien zu finden, nach welchen verglichen werden kann. Für diese Arbeit sind die folgenden Begriffe herausgearbeitet worden, da sie besonders für militärische Anwendungen von hohem Interesse sind. Sie werden nachstehend mit einer kurzen Begründung benannt. Es sollte klar sein, dass sich diese Kriterien alle samt an den Anforderungen für ein WSN orientieren.

Energieverbrauch:
Der Energieverbrauch spielt eine herausgehobene Rolle in militärischen Anwendungen. Je länger ein WSN in einem Einsatzgebiet eingesetzt werden kann, desto mehr Informationen können über dieses Gebiet gesammelt werden. Dies wiederum kann zu einem Informationsvorteil und später auch zu einem Wirkungsvorteil führen.

Übertragung:
Auch die Übertragung ist in militärischen Anwendungen von Interesse. Sie ist abhängig von der Menge der Daten, die versendet werden sollen. Für die meisten Informationen die über ein WSN übertragen werden sollen ist eine hohe Übertragungsrate interessant. Gleichzeitig ist aber auch die Reichweite einer solchen Übertragung eine Rolle. Hier ist festzuhalten, dass eine Erreichbarkeit in größeren Entfernungen anstrebenswert ist.

Störanfälligkeit:
Im Zusammenhang mit der Übertragung spielt auch die Störanfälligkeit eine besondere Rolle. Hierbei sind sowohl die klassischen „low-level“ QoS-Parameter gemeint, als auch die „high-level“ Parameter derWSN. Hier ist grundsätzlich zu sagen, dass je robuster ein System gegen Störungen ist, es umso besser für den Einsatz im Militär geeignet ist.

Protokollkomplexität:
Je komplexer ein Protokoll ist, desto mehr Daten müssen später über den Kommunikationskanal übertragen werden. In militärischen Anwendungen, sollte also diese Komplexität so gering wie möglich sein, da so auch bei geringen Übertragungsraten mehr relevante Daten versendet werden können. Eine höhere Komplexität ist nur durch eine höher Übertragungsrate zu kompensieren.

Sicherheit:
Die Sicherheit ist das wohl wichtigste Thema für WSN in militärischen Anwendungen. Durch sie soll verhindert werden, dass der Gegner an die eigenen Informationen gelangt und dadurch seinerseits einen Informationsvorsprung erzielen kann. Die Art der Verschlüsselung ist hierbei von besonderer Bedeutung.

Kosten:
Auch die Kosten spielen eine Rolle. Bei Sensornetzen, die mehrere tausend Knoten umfassen können hier, vor allem über die Zeit, enorme Beträge entstehen die es zu betrachten gilt.

3.5.2 Vergleich

Nachdem die Kriterien für einen Vergleich zwischen ZigBee und DASH7 festgelegt wurden können die beiden Protokolle jetzt gegenübergestellt werden.

Energieverbrauch:
DASH7 schafft es durch die Nutzung des BLAST-Prinzips seinen Kommunikationsaufwand auf ein Minimum zu reduzieren, dadurch kann eine hohe Energieeffizienz erzielt werden. So werden im Sleep Modus nur vier Mikrowatt benötigt und auch beim Senden und Empfangen kann viel Energie gespart werden. Es werden für das Empfangen nur 7.5 mW und für das Senden 31 mW gebraucht. Der Durchschnittliche Verbrauch liegt, für zehn 256-Byte-Nachrichten pro Tag, bei 42 μW.
ZigBee benötigt im Ruhezustand ebenfalls vier Mikrowatt. Für das Senden und Empfangen werden aber 72 mW beziehungsweise 84 mW beansprucht. Im Durchschnitt werden für zehn 256 byte-Nachrichten am Tag 414 μW benötigt.[4]

Übertragung:
Durch die Nutzung des UHF-Bereichs bei DASH7 gelingt es hohe Reichweiten zu erzielen. Diese beträgt ungefähr zwei Kilometer und ist runter bis auf 10 Meter skalierbar. Unter optimalen Bedingungen sind aber bereits Reichweiten von bis zu zehn Kilometern erreicht worden. Durch diese großen Reichweiten kann die Anzahl der Hops, die zur Übertragung benötigt werden, minimiert werden. Die Datenrate kann frei geregelt werden und liegt zwischen 27.8 Kbps und 200 Kbps.
Mit ZigBee können Reichweiten zwischen 30 und 500 Metern bei einer Datenrate von 250 Kbps erreicht werden.[14]

Störanfälligkeit:
Durch die Nutzung des 433 MHz-Bandes braucht DASH7 keine Line-of-sight. Hindernisse wie Mauern, Bäume oder Wasser stellen für die Übertragung keine besonderen Probleme dar. Somit wird auch in stark bebauten Gegenden eine Kommunikation ermöglicht. Leider ist der UHF-Bereich aber ziemlich Anfällig gegen rauschen.
Die Nutzung des 2.4 GHz-Frequenzbereichs und somit ZigBee erfordert eine quasi-optische Verbindung zum Empfänger. Durch Wasser dringt diese Frequenz nicht hindurch und Mauern, gerade wenn sie aus Stahlbeton sind schwächen das Signal stark ab. Durch Quadrature Phase Shift Keying (QPSK) ist ZigBee wenig Störungsanfällig gegenüber Rau-

schen. Die gleichzeitige Nutzung dieses Frequenzbereiches durch Bluetooth und Wi-Fi erhöht aber wiederum die Anzahl der möglichen Störquellen.[4]

Protokollkomplexität:
DASH7 stellt ein sehr einfaches Protokoll dar, welches auf dem ISO 18000-7 Standard aufsetzt. Es werden keine extra Features durch das Protokoll definiert, so dass es auch einen sehr kleinen Overhead hat. Da bei DASH7 keine Sessions zur Kommunikation aufgebaut werden müssen führt das ebenfalls zu einer Vereinfachung des Protokolls. Durch das OpenSource-Projekt Opentag kann das Protokoll mit fast allen Microcontrollern verwendet werden.
ZigBee baut Sessions zur Kommunikation auf und definiert gleichzeitig noch andere Features. Dadurch benötigt es einen größeren Overhead.[4]

Sicherheit:
Beide Protokolle bieten eine Verschlüsselung über eine 128 Bit Blockchiffre an.[8, 14]

Kosten:
Die Preise eines Gerätes in der Anschaffung sind bei beiden Anwendungen etwa gleich hoch. Durch die hohe Energieeffizienz bei DASH7 können die Kosten für die Wartung dieser Geräte über zehn Jahre gerechnet auf knapp 100 Dollar geschätzt werden.
Die Wartung der Geräte von ZigBee kostet ungefähr 985 Dollar gerechnet auf zehn Jahre.[14]

3.6 Schluss

Nachdem der Vergleich nun anhand einiger wenigen Kriterien durchgeführt wurde kann nun eine Bewertung des DASH7 stattfinden. Im Anschluss daran wird der Inhalt dieser Arbeit nochmals grob zusammengefasst und ein Ausblick für weitere mögliche Anwendungsgebiete gegeben.

3.6.1 Bewertung

Für die Anwendung im militärischen Bereich sind die folgenden Kriterien von besonderer Bedeutung: Energieeffizienz, Reichweite, Störanfälligkeit, Sicherheit, Kosten.
In der Energieeffizienz hat DASH7 die Nase vorn. Denn es verbraucht nur ungefähr ein Zehntel der Energie die ZigBee bei vergleichbaren Lasten verbrauchen würde. Dadurch können Einsatzgebiete länger überwacht und somit auch mehr Informationen über diese gesammelt werden.
Auch bei der Reichweite kann DASH7 gegenüber ZigBee punkten. Hier können durch die Nutzung des UHF-Frequenzbereichs Weiten bis zu zwei Kilometer erreicht werden. ZigBee hingegen kann maximal im Umkreis von 500 Metern kommunizieren. Grundsätzlich ist die Frage der Reichweite abhängig von der Anwendung. Soll ein möglichst großes Gebiet mit so wenigen Sensoren wie möglich überwacht werden bietet sich DASH7 an. Im umgekehrten

Fall aber eher ZigBee.
Die Störanfälligkeit der Protokolle ist ebenfalls unterschiedlich. Während ZigBee auf dem gleichen Frequenzbereich wie Bluetooth oder Wi-Fi sendet arbeitet DASH7 im 433 MHz-Bereich. DASH7 braucht dadurch keine Line-of-sight und wird auch nicht durch andere Anwendungen gestört. Es ist aber anfälliger gegenüber Hintergrundrauschen.
Unter Sicherheit versteht man, wie gut Daten geschützt sind. Man versteht aber auch darunter, wie leicht ein Netzwerk aufzuklären ist. Was die Verschlüsselung der Daten angeht so bringen beide Protokolle den gleichen Mechanismus mit. Sie verschlüsseln ihre Daten mit 128 Bit Blockchiffren. DASH7 hat aber dennoch einen kleinen Vorteil, da es hier kein erkennbares Kommunikationsmuster gibt. ZigBee hingegen baut zuerst eine Session für die Übertragung auf.
Auch in Anbetracht der Kosten ist DASH7 die günstigere Variante. So sind die Kosten für ein Gerät über zehn Jahre gesehen zehn Mal günstiger als die des Konkurrenten.

3.6.2 Zusammenfassung und Ausblick

Inhalt dieser Arbeit war es die Datenkommunikation über das Protokoll DASH7 zu betrachten und mit bisher verwendeten Protokollen wie ZigBee zu vergleichen. Um diesen Vergleich durchführen zu können wurden die drahtlosen Sensornetzwerke vorgestellt und deren Anwendungsmöglichkeiten betrachtet. Anschließend wurden die Arbeitsweisen der einzelnen Protokolle beleuchtet. Zuerst ZigBee, dann DASH7. Diese beiden Protokolle sind dann anhand einiger Kriterien gegenübergestellt und ihre Stärken und Schwächen herausgearbeitet worden. DASH7 besticht vor allem durch seine große Reichweite und seine ausgesprochen gute Energieeffizienz. Durch diese ist es möglich große Einsatzgebiete mit wenigen Knoten, dafür aber über einen sehr viel längeren Zeitraum, als das durch ZigBee möglich ist, zu überwachen. Es kann durch das OpenSource Projekt Opentag auf fast jedem Microcontroller eingesetzt und auch um einige Funtkionen erweitert werden. DASH7 selbst kommt nur mit den nötigsten Features. Der Rest muss durch den Entwickler selbst bearbeitet werden. Die Energieersparnis ist durch die Nutzung des BLAST-Prinzips zu erklären. Hier wird der Kommunikationsaufwand auf das Nötigste reduziert.

Alles in Allem ist festzuhalten, dass mit DASH7 unter der Schirmherrschaft des Department of Defense ein Protokoll entstanden ist, welches für die Bedürfnisse des Militärs sehr gut geeignet ist. Es schlägt in dieser Hinsicht ZigBee um Längen. Es steckt aber auch sehr viel Potential für Anwendungen im kommerziellen Bereich. So kann und wird DASH7 in Zukunft noch stark weiterentwickelt werden. In Bereichen der Werbung, der Automobilindustrie oder aber der Logistik wird es bereits heute eingesetzt. Für die zukünftige Entwicklung kann davon ausgegangen werden, dass das noch mehr zunehmen wird.

Literaturverzeichnis

[1] Holger Karl, Andreas Willig. *Protocols and Architecture for Wireless Sensor Networks*, John Wiley and Sons, Ltd Paperback edition, Juli 2007

[2] Michael Winkler, Klaus-Dieter Tuchs, Kester Hughes und Graeme Barclay. *Theoretical and practical aspects of military wireless sensor networks*, Paper erschienen in Journal of Telecommunications and Information Technology, Februar 2008

[3] Ajay Ogirala, Peter J. Hawrylak und Marlin H. Mickle. *Interoperability Test Methodology for ISO 18000-7 Active RFID*, Paper erschienen in Journal Wireless Personal Communications, Springer Netherlands, Februar 2011

[4] JP Norair. *Introduction to DASH7 Technologies*, White-Paper, First Edition, März 2009

[5] Dr. Thomas Kretschmer. *Wehrtechnische Vorausschau 2005/2006*, Frauenhofer-Institut für naturwissenschaftlich-technische Trendanalysen, Euskirchen, 2006

[6] Lars Grebe. *Sicherheit und Interoperabilität von militärischen Kommunikationssystemen - Einführung in drahtlose Sensornetze*,Seminarband Militärische Funkkommunikation - Universität der Bundeswehr, München, März 2010

[7] Sebastian Seidel. *Anwendungsszenarien für Sensornetze im militärischen Umfeld*, Seminarband Militärische Funkkommunikation - Universität der Bundeswehr, München, März 2010

[8] Thomas Bühring. *Neighbor Discovery in Wireless Sensor Networks*,Seminarband Militärische Funkkommunikation - Universität der Bundeswehr, München, März 2010

[9] Olinka Koster, Nigel Blundell. *Smile you're on ele-vision: How a camera attached to an elephant's trunk captured amazing jungle views*,Artikel erschienen auf http://www.dailymail.co.uk/, 25.März 2008.

[10] ZigBee Specification. Document 053474r17. Januar 2008

[11] IEEE 802.15.4. http://www.ieee.org

[12] ISO/IEC 18000-7 International Standard, Third Edition, 2009

[13] ZigBee - Alliance. http://www.zigbee.org

[14] Dash7 - Alliance. http://www.dash7.org

[15] Wikipedia - ZigBee. http://de.wikipedia.org/wiki/ZigBee

[16] Wikipedia - DASH7. http://en.wikipedia.org/wiki/DASH7

[17] Wikipedia - Freie Enzyklopädie. http://www.wikipedia.de/ 10.02.2011

[18] Crossbow Technology Homepage. http://www.xbow.com/ 10.02.2011

Kapitel 4

Funkkommunikation zwischen Drohnen und Bodenstation

Raik Kiepert

In diesem Kapitel geht es um die Datenkommunikation zwischen Drohen und ihrer Bodenstation. Als Beispiel wird ein sogenannter Mikrokopter (MK) herangezogen, die Einschätzungen lassen sich aber auf fast alle kleineren Drohnen verallgemeinern. Es wird sowohl die Kommunikation in Richtung Drohne als auch in Richtung Bodenstation betrachtet. Vor- und Nachteile einzelner Sendeverfahren werden aufgezeigt und verglichen. Abschließend werden Empfehlungen für die Anwendung im militärischen Bereich getroffen und kommerzielle Systeme vorgestellt.

Inhaltsverzeichnis

4.1 Einleitung 79
4.2 Drohnen 79
4.2.1 Anforderungen für den militärischen Einsatz 80
4.3 allg. Funkkommunikation 83
4.3.1 Funk 84
4.3.2 rechtliche Aspekte 91
4.3.3 Übertragungsmethoden 93
4.4 Datenübertragung 94
4.5 Videoübertragung 95
4.5.1 Videokompression 95
4.5.2 FPV-Flug 96
4.6 Sicherheit 96
4.7 fertige Systeme 98
4.7.1 Bluetooth 98
4.7.2 ZigBee 99
4.7.3 Wi232 99
4.7.4 WLAN 99
4.7.5 UMTS/GPRS 100
4.7.6 analoge Videotransmitter 100
4.7.7 Komplettsysteme 100
4.8 Zusammenfassung 102

4.1 Einleitung

Für die militärische Anwendung ist Informationsüberlegenheit von entscheidender Bedeutung. Somit wundert es nicht, dass sehr große Anstrengungen getätigt werden, um qualitativ hochwertige Informationen möglichst schnell zu gewinnen und dann auch zu verteilen. Welches Medium eignet sich hier besser als Drohnen? Daten gelangen mittels Funkkommunikation in kürzester Zeit über großer Distanzen an ihr Ziel. Doch um welche Daten geht es hier eigentlich und wie werden sie beschafft? Welche Probleme bringt die Funkkommunikation mit sich und welche Beschränkungen gibt es? Diese und weitere interessante Fragen rund um das Thema Drohnen und Funkkommunikation soll die vorliegende Arbeit beantworten. Drohnen erlangen aufgrund günstiger Anschaffungskosten, einfacher Bedienung und hoher Flexibilität immer mehr an Bedeutung. Sie stellen nicht nur für das Militär eine sehr einfache Möglichkeit dar, sich ein schnelles Bild der Lage zu verschaffen. Hierbei geht es keinesfalls nur um Bilder, denn moderne Drohnen können auch mit verschiedensten Sensoren bestückt werden. Um sie gezielt auf ihr Einsatzgebiet zu lenken und um Zeiten zwischen Bildaufnahme oder Sensoranalyse und Auswertung der Daten im Gefechtsstand so kurz wie möglich zu halten, ist es notwendig eine direkte Übertragung von der Drohne zur Bodenstation und andersherum zu gewährleisten und genau darum soll es in diesem Kapitel gehen.

4.2 Drohnen

Die Definition des Wortes "Drohne" gestaltet sich zunächst schwierig, da einige Quellen nur von Luftfahrzeugen, andere wiederum von jeglichen ferngesteuerten Fahrzeugen zu Land, zu Wasser und in der Luft ausgehen. Für diese Arbeit wird folgende Definiton angenommen:

Eine Drohne ist ein unbemanntes Luftfahrtzeug, welches zur Überwachung, Erkundung, Aufklärung, als Zieldarstellungsdrohne und mit Waffen bestückt in Kampfeinsätzen verwendet werden kann[1].
Die Steuerung einer Drohne erfolgt entweder automatisiert über einen Mikrocontroller gesteuerten Autopilot oder über eine Funkverbindung von einer Bodenstation aus. Die Form von Drohnen ist sehr unterschiedlich. Während vor ein paar Jahren fast ausschließlich Flächenmodelle auf dem Markt waren, setzen sich nunmehr sogenannte MK durch. Diese haben den Vorteil sehr wendig, unanfällig gegen Wind und kostengünstig zu sein. Natürlich haben sie auch Nachteile. So ist die Einsatzzeit für Drohnen aufgrund von Akkukapazitäten stark begrenzt. Weiterhin ist die Nutzlast gegenüber Flächenmodellen recht gering. Das Flugprinzip von Mikrokoptern ist stark an das von Helikoptern angelehnt. Es gibt mehrere Propeller die gegeneinander drehen, um so das entstehende Drehmoment auszugleichen. Zur Richtungsänderung wird die Drehzahl einzelner Propeller herauf oder herunter gesetzt. Ausgelöst wird die Drehzahländerung durch die zentrale Steuerungseinheit, die entweder die derzeitige GPS Daten mit den gewünschten Position vergleicht und

[1] Quelle: Meyers Lexikon

Abbildung 4.1: deutsche Aufklärungsdrohne KZO [Quelle: www.rheinmetall-defence.com]

daraus einen Kurs oder eine Richtungsänderung berechnet oder durch die Entgegennahme von Steuerbefehlen von der Bodenstation. Die Vielfalt von kommerziell entwickelten Systemen sowie privaten Eigenentwicklungen ist sehr groß, nicht alle sind jedoch für die militärische Nutzung geeignet. Die Bilder 4.1, 4.2 und 4.3 zeigen sowohl ältere als auch aktuelle Aufklärungsdrohnen die bereits von der Bundeswehr bzw. anderen Streitkräften genutzt werden.

4.2.1 Anforderungen für den militärischen Einsatz

Um eine Drohne militärisch nutzen zu können, muss sie einige Voraussetzungen erfüllen, die sehr stark vom Einsatzszenario abhängen, daher sollen an dieser Stelle einige Szenarien geschaffen werden, welche Einsatzsituationen ähneln. Im Anschluss werden die Voraussetzungen den Szenarien zugeordnet.

Einsatzszenarien

1. Beim ersten Szenario geht es darum eine Fernaufklärung durchzuführen. Die Bodenkontrollstation befindet sich hierzu 150km vom Aufklärungsobjekt entfernt in einem

Abbildung 4.2: getarnte amerikanische Aufklärungsdrohne x-47B [Quelle: darpa- T- Online News]

Abbildung 4.3: deutsche Aufklärungsdrohne MIKADO [Quelle: www.Luftwaffe.de]

Container, der auf einem LKW verlastbar ist. Bei der Aufklärung geht es darum, zu erschließen wie viele militärische Fahrzeuge sich in einem Gebiet von 2qkm befinden.

2. Beim zweiten Szenario befindet sich ein Fahrzeugkonvoi vor einem verlassenen Dorf, welches teilweise mit Stacheldraht gesichert ist. Die Entfernung zur Stadt beträgt 500m. Ein Fahrer hat Bewegungen vor einem Fenster wahrgenommen, es ist aber niemand zu sehen. Die Erde der Straße im Dorf scheint an einigen Stellen aufgeworfen zu sein. Näheres ist im Fernglas nicht zu erkennen.

3. Beim dritten Szenario ist ein Rettungstrupp auf dem Weg zu einem abgestürzten Piloten. Anhand von Karten ist bereits zu erkennen, dass sich das Absturzgebiet in bewaldetem, bergigen Gelände befindet. Die Ausdehnung beträgt ca. 3km x 2 km. Der Weg zum Piloten wird zu Fuß geschehen müssen, da Wege für Fahrzeuge zu schmal sind oder gar nicht existieren. Helikopter können nicht eingesetzt werden, da es stark neblig ist und die Sichtweiten unter 100m liegen.

Bei allen Einsätzen ist erkennbar, dass die Aufklärung ohne eine Gefährdung von Mensch und Material schwierig erscheint. Es liegt also nahe, an dieser Stelle Drohnen einzusetzen.

Anforderungen an die Funkkommunikation

1. Fernaufklärung
   - Flugbereich: ca. 160km
   - Reichweite: min. 350km
   - zu übertragene Daten - mindestens: Steuerungsbefehle
   - zu übertragene Daten - wünschenswert: Steuerungsbefehle, Telemetriedaten, Bilder im sichtbaren Spektralbereich
   - zu übertragene Daten - optimal: Steuerungsbefehle, live Videostream, Telemetriedaten, hochaufgelöste Bilder in mehreren Spektralbereichen
   - Datenrate: kBit/s - 5 MBit/s (bei ausschließlich digitaler Datenübertragung komprimiert)
   - Sicherheitsanforderungen: sichere Übertragung
   - geschätzte Einsatzdauer: ca. 1h

2. Konvoibegleitung
   - Flugbereich: ca. 1000m
   - Reichweite: min. 1500 m
   - zu übertragene Daten - mindestens: Steuerungsbefehle
   - zu übertragene Daten - wünschenswert: Steuerungsbefehle, Telemetriedaten, Bilder im sichtbaren und infrarot Bereich, Sensordaten
   - zu übertragene Daten - optimal: Steuerungsbefehle, live Videostream, Telemetriedaten, hochaufgelöste Bilder, Sensordaten

- Datenrate: kBit/s - 50 MBit/s (bei ausschließlich digitaler Datenübertragung einfach komprimiert)
- Sicherheitsanforderungen: sichere Steuerbefehle, Rest unsicher
- geschätzte Einsatzdauer: 15 min

3. Rettungsmission

   - Flugbereich: ca. 10km
   - Reichweite: min. 3,5 km
   - zu übertragene Daten - mindestens: Steuerungsbefehle, live Videostream, Telemetriedaten
   - zu übertragene Daten - wünschenswert: Steuerungsbefehle, live Videostream, Telemetriedaten, Bilder im infrarot Bereich
   - zu übertragene Daten - optimal: Steuerungsbefehle, live Videostream auch im Infrarotbereich, Telemetriedaten
   - Datenrate: 50 MBit/s (bei ausschließlich digitaler Datenübertragung einfach komprimiert)
   - Sicherheitsanforderungen: sichere Steuerbefehle, zuverlässige Video- und Telemetriedatenübertragung
   - geschätzte Einsatzdauer: 45 min

Es ist an dieser Stelle recht einfach zu erkennen, dass sich die eingesetzten Drohnen grundlegend unterscheiden müssen, um dem Einsatzanforderungen gerecht zu werden. Während die Drohne im Szenario 1 sehr groß sein wird, um die große Reichweite abdecken zu können und die Nutzlast tragen zu können, werden die Drohnen im zweiten und dritten Szenario klein bis sehr klein sein, um möglichst mobil, schnell einzusetzbar und wendig zu sein. Somit wird im ersten Fall vermutlich eine Drohne in Form eines Flächenflugzeugs, wie die von der Bundeswehr genutzte KZO, zum Einsatz kommen. Im zweiten und dritten Fall ist eine Drohne in Form eines MK angebrachter, da sie ohne große Basisstation auskommt, und im Falle des Verlustes durch Beschuss oder Kollision eine überschaubare Geldmenge darstellt. Weiterhin kann man mit einem MK noch flexibler auf Lageänderungen reagieren, als dies mit größeren Drohnen möglich ist. Wie die von den Szenarien gestellten Anforderungen bestmöglich erfüllt werden können, zeigen die nun folgenden Abschnitte. Das Szenario eins bleibt hier außen vor, da der Fokus dieser Arbeit auf kleineren Drohnen, wie dem MK liegt.

4.3 allg. Funkkommunikation

Wie im Kapitel 4.2 schon angedeutet, ist zur Steuerung eines Mikrokopters eine Funkkommunikation nötig. Einerseits ist es dadurch möglich, direkte Steuersignale an den MK zu übertragen, andererseits aber auch Flugroutendaten an die Navigationseinheit zu übergeben. Es ist aber auch die Gegenrichtung interessant, beispielsweise ist es wünschenswert

Telemetriedaten vom MK zur Bodenstation zu übertragen. Aber auch Sensoren oder Videodaten haben einen höheren Einsatzwert, wenn sie aktueller sind, also im Optimalfall in Echtzeit übertragen werden. Die hierzu nötigen Voraussetzungen werden im Folgenden erläutert.

4.3.1 Funk

Der Name "Funk" geht auf den Begriff Funke zurück. Denn jeder entstehende Funke führt zu einem elektromagnetischen Feld und ist somit auch in der Lage, primitive Daten zu übertragen. Für die hier betrachteten Umstände reichen so primitive Übertragungen jedoch nicht aus.

Um Daten zum und vom MK zu übertragen benötigt man Funkfrequenzen bzw. Frequenzbänder, also elektromagnetische Wellen, die mit einer definierten Frequenz schwingen. Die hierfür gestellten Anforderungen sind von sehr unterschiedlicher Natur. Zum einen gibt es rechtliche Einschränkungen, da die Nutzung einzelner Frequenzen reglementiert ist, um so das "wilde" Aussenden von elektromagnetischer Strahlung zu begrenzen und somit natürlich auch gegenseitige Störungen zu vermeiden. Zum Anderen sind bestimmte Frequenzen, aufgrund physikalischer Effekte, besser oder schlechter geeignet. Die Gründe hierfür erklären die folgenden Abschnitte.

Funkausbreitung

Die Qualität eines an einem Empfänger ankommenden Signals hängt von sehr vielen verschieden Komponenten ab. Unter anderem auch davon, wie gut sich die Welle ausbreiten kann. Im folgenden werden hierzu die wesentlichen Einflussfaktoren [2] genannt.

- Entfernung zum Sender
- Geländegegebenheiten
- Abschattungs- Beugungserscheinungen durch Objekte
- Mehrwege- und Streuausbreitung an vielen Reflexionsstellen
- Rauschen des Empfängers
- Interferenzstörungen
- Impulsartige Störungen

Nicht alle diese Einflussfaktoren sind negativ einzustufen, so führt die Mehrwegeausbreitung zwar dazu, dass das Funksignal mehrfach beim Empfänger eintrifft und eventuelle sehr aufwändig herausgerechnet werden muss. Andererseits kann es aber auch der Grund

[2] nach Prof. Bertold Lankl - Digitale Funkkommunikation, 2010

dafür sein, dass überhaupt eine Funkverbindung zustande kommt, sofern der direkte Verbindungsweg, also die Sichtverbindung oder Line of Sight (LOS) versperrt ist. Alles in allem ist aber erkennbar, dass an den meisten der oben genannten Einflussfaktoren sehr wenig zu ändern ist oder eine Änderung zwar möglich, aber unerwünscht ist, denn ein Aufklärungsgerät, was beispielsweise nur in einer flachen hindernislosen Landschaft funktioniert, hat einen sehr geringen Einsatzwert. Trotzdem haben wir natürlich Möglichkeiten eine Funkverbindung positiv zu beeinflussen. Um zu verstehen wie dies möglich ist, müssen wir uns aber zumindest grundlegende physikalische Effekte ansehen, die zu den oben genannten Einflüssen führen.

physikalische Effekte Funkwellen breiten sich ähnlich wie Lichtwellen aus. Genauso wie Licht werden sie durch Hindernisse (z.B. Bebauungen) oder geografische Gegebenheiten (z.B. Berge oder Häuser) beeinflusst. Wie stark sie sich dem Verhalten von Licht ähneln, hängt von der Frequenz ab. Grundsätzlich sind fünf wesentliche Effekte zu beobachten.

1. Dämpfung: Elektromagnetische Wellen sind in der Lage, Hindernisse zu durchdringen (z.B. Mauern von Gebäuden). Dabei wird jedoch ein Teil des Signals absorbiert, so dass dem Empfänger nur ein abgeschwächtes Signal zur Verfügung steht.

2. Reflexion: Funkwellen werden beispielsweise an Gebäuden reflektiert.

3. Beugung: Die geradlinige Ausbreitung der Funkwelle trifft auf eine Kante und ändert so ihren Verlauf.

4. Abschattung: Elektromagnetische Felder können durch Berge, große Gebäude oder Bäume abgeschattet werden. Die Folge kann eine eingeschränkte oder abreißende Funkverbindung sein.

5. Absorption: Der Teil des Signals, der vom Material nicht reflektiert wird, wird absorbiert. Das Signal wird hierbei auch abgeschwächt.

Wie stark ein Signal gedämpft, reflektiert oder absorbiert wird, hängt neben der Frequenz auch stark von dem betrachteten Material ab. Pauschal kann man jedoch sagen, je höher die Frequenz, desto stärker treten Effekte wie Abschattung und Absorption auf. Mit anderen Worten ist die Wellenausbreitung immer lichtähnlicher, desto näher man dem Frequenzbereich des Lichtes kommt. Bei Frequenzen im Gigaherzbereich kann die Drohne selbst ausreichen, um das Funksignal vollkommen abzuschatten. Aus diesem Grund versucht man solche Übertragungssysteme in der LOS zu betreiben. Es soll also ständig eine Sichtverbindung bestehen. Dies bedeutet nicht, dass die Drohne in einer mit dem Auge sichtbaren Entfernung bleibt, sondern nur, dass sich keine Gegenstände im "Funkstrahl" befinden.

Ein weiterer Effekt von Beugung und Reflexion ist, die oben beschriebene Mehrfachausbreitung eines Signals. Hierdurch trifft das Signal am Empfänger mehrfach ein, da es unterschiedliche Wege zum Empfänger zurückgelegt hat. Verdeutlicht wird dies im Bild 4.4.

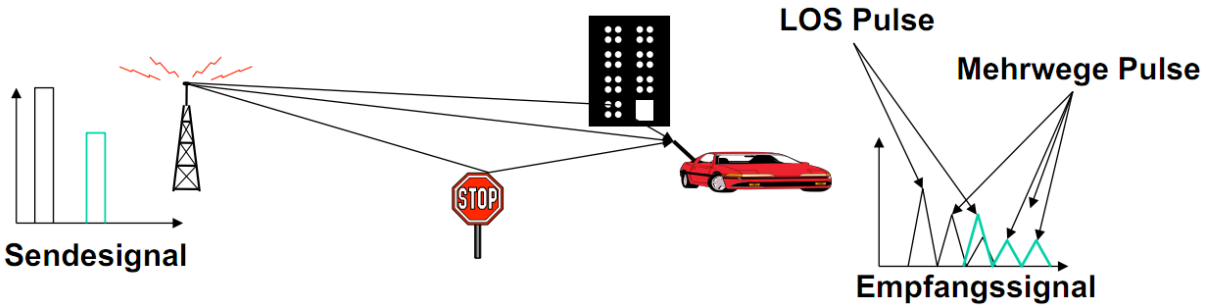

Abbildung 4.4: Mehrfachausbreitung von Funkwellen [Quelle: Prof. Dr. Gabi Dreo - Skript mobile Kommunikationssysteme 2010]

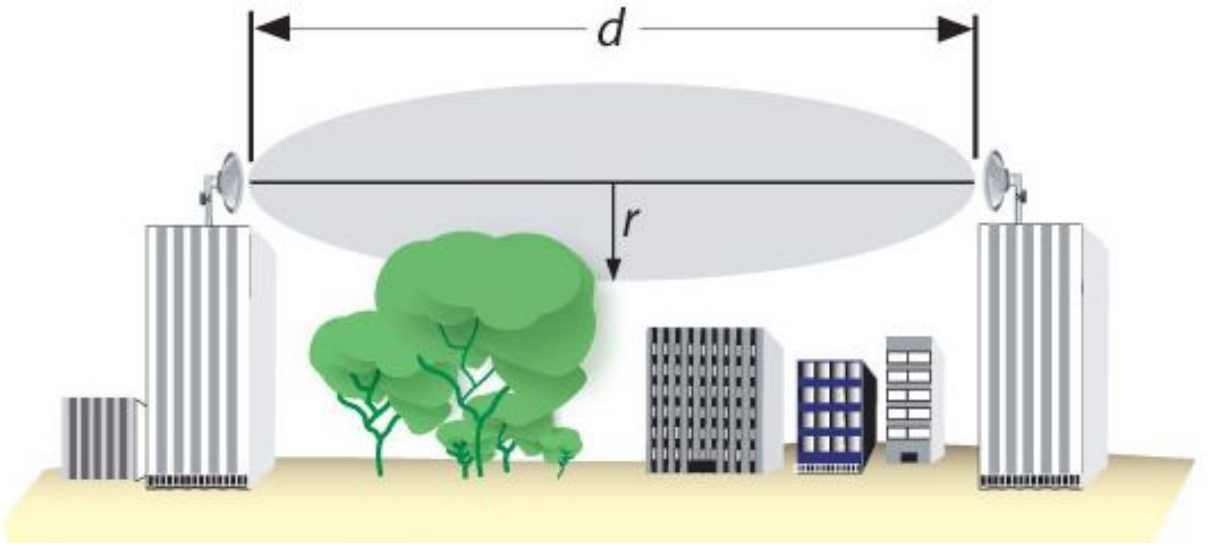

Abbildung 4.5: Die Fresnelzone [Quelle: www.itzgrund.net]

Doch wenn man nun davon ausgeht, dass eine direkte Sichtverbundung zwischen Sender und Emfänger besteht, also kein Hindernis im direkten Weg steht, so müsste doch der Empfang optimal sein, oder?

Fresnelzone Dies trifft so leider nicht immer zu, denn eine Funkverbindung ist kein linearer Strahl. Der Grund hierfür, liegt im sogenannten Fresnel-Effekt. Dies ist eine Zone, welche man sich als einen Rotationselipsoid um die Sichtlinie zwischen Sender und Empfänger vorstellen kann. Der Durchmesser der Zone hängt von der Distanz zwischen Sender und Empfänger, sowie von der Frequenz ab. Es gilt: Je größer die Entfernung, desto größer der Durchmesser und je größer die Frequenz, desto kleiner der Durchmesser. Um die Feldstärke am Empfänger zu verringern, recht es bereits aus, wenn sich ein Hindernis innerhalb dieser Fresnelzone befindet. Somit sinkt beispielsweise bei fünfzigprozentiger Verdeckung der Fresnelzone die el. Feldstärke auf die Hälfte ab. An dieser Stelle spricht man auch von Dämpfung, obwohl kein Körper direkt durchdrungen wird. Das Bild 4.5 veranschaulicht den Effekt.

Weitere Effekte, wie beispielsweise die Freiraumdämpfung etc., treten an dieser Stelle in den Hintergrund, da sie in unserem Anwendungsfall nur geringe Einflüsse auf die Funkverbindung haben.

Sendeleistung

Eine wesentliche Komponente der Funkübertragung ist die Sendeleistung. Sie entscheidet maßgebend in welcher Entfernung ein Sender noch empfangen werden kann. Je größer die Leistung mit der ein Sender abstrahlt ist, desto größer ist, bei sonst gleichen Bedingungen, auch die Empfangsleistung und desto besser kann das Signal natürlich auch ausgewertet werden. Da aber, wie im Kapitel 4.3.2 noch erläutert wird, genaue Regelungen die Sendeleistung bestimmen, kann die Übertragungsqualität über die Sendeleistung nur bedingt verbessert werden, denn diese darf nur bis zur rechtlich festgesetzten Grenze erhöht werden. Der Grund für die genaue Reglementierung ist, dass bei hohen Sendeleistungen unerwünschte Wechselwirkungen stattfinden. Die einzelne Wirkung hängt hierbei stark von der Frequenz ab. So kann zum Beispiel ein Funkgerät im 2,4 GHz Band wie ein Mikrowellenofen wirken, was für den Menschen sehr gefährlich wäre. Ein weiterer Nachteil ist, dass bei höheren Sendeleistungen der Kanalabstand [3] größer werden muss, da sonst weitere Kanäle gestört werden, es treten also Interferenzen auf.

Antennensysteme

Antennen sind eines der wesentlichsten Bestandteile einer Funkkommunikation. Sender und Empfänger können noch so gut sein, wenn die Antenne nicht abgestimmt ist, wird nie eine gute Funkkommunikation zustande kommen. Gerade Drohnen stellen hohe Anforderungen an Antennen, da sie sich dreidimensional bewegen und somit die Antenne in vielen Lagen im Raum senden und empfangen muss. Das Ziel ist natürlich das Signal zuverlässig zum MK bzw. zum Boden zu bringen. Während die Größe der Antenne am Boden eher zweitrangig ist, so muss sie in der Luft leicht sein, nicht allzu groß und möglichst unempfindlich gegen physikalische Einwirkungen. Sie sollte die Strahlung möglichst gleichmäßig abstrahlen und empfangen können und dabei andere Systeme nicht beeinträchtigen (wobei dies eher von der Frequenz abhängt). In der Luft verwendet man daher fast ausschließlich Langdrahtantennen, allgemein auch "Rundstrahler" genannt. Diese besitzen zwar die eben beschriebenen Vorteile, haben aber auch Nachteile, welche sich im Gegensatz zur nächst genannten Antennenart zeigen.

Auch am Boden kommen Langdrahtantennen zum Einsatz. Wenn es jedoch auf große Reichweiten ankommt, dann weicht man auf sogenannte Patchantennen aus. Diese meist rechteckigen, flachen Antennen wirken ähnlich einer Dipolantenne, haben aber eine auf der ebenen Fläche aufgebrachte Metallschicht welche die Strahlung reflektiert. Hierdurch haben sie zwar eine Richtcharakteristik, aber auch wesentlich bessere Sende- und Empfangseigenschaften. Um die Richtcharakteristik auszugleichen gibt es die Möglichkeit Antennenfolger oder Diversitysysteme einzusetzen. Warum nun Patchantennen gegenüber

[3] Abstand zwischen zwei Frequenzen eines Funkgerätes

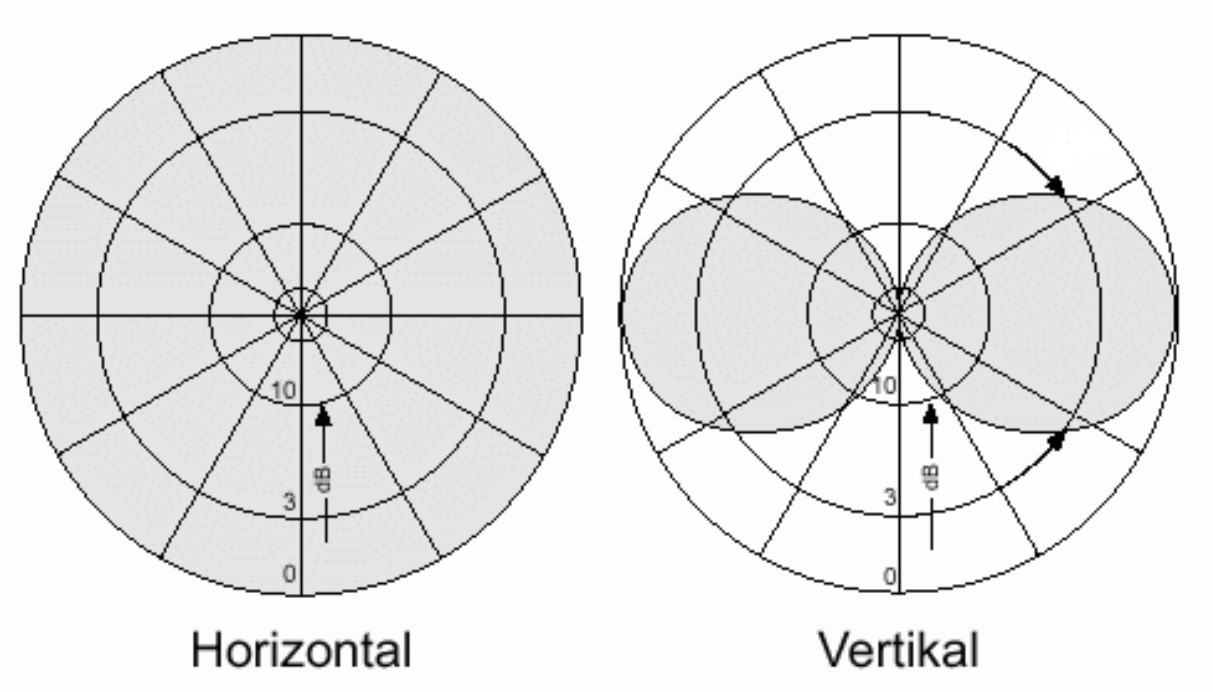

Abbildung 4.6: Antennendiagramm Langdrahtantenne / Rundstrahlantenne [Quelle: www.schiffertec.de]

den "Rundstrahlern" einen Reichweitenvorteil haben wird klar, wenn man die zugehörigen Antennendiagramme (Bild: 4.6 und 4.7) betrachtet.

Es ist hier recht deutlich die Richtcharakteristik zu erkennen. Wenn man nun annimmt, dass eine Antenne kugelförmig abgestrahlt, dass heißt die Leistungsdichte auf jedem Punkt der Kugeloberfläche gleich ist, so erscheint es logisch, dass, wenn bei einer Patchantenne die gleiche Sendeleistung nur auf einen Teil der Kugeloberfläche verteilt wird, die erreichte Leistungsdichte höher ist. Somit ergibt sich ein stärkeres elektromagnetisches Feld und damit eine Reichweitenerhöhung. Ähnlich verhält es sich beim Empfang von Signalen, da die effektive Fläche der Patchantenne um ein Vielfaches größer ist. Die Bilder 4.8 und 4.9 zeigen eine Rundstrahl- und eine Patchantenne.

Antennenfolger Antennenfolger sind Systeme, die über Motoren die Antenne dynamisch dem Flugobjekt nachführen, sodass ständig eine LOS gewährleistet wird. Hierzu ist es natürlich nötig die Position der Drohne zu kennen. Dies wird bei kommerziellen Systemen durch die Auswertung des On Screen Display (OSD) erreicht. Die, in das zum Boden übertragene Kamerabild, eingefügten Global Positioning System (GPS) Informationen werden extrahiert, mit den eigenen Positionsdaten verglichen und daraus die Richtung berechnet. Die Gefahr hierbei ist allerdings, dass sofern die Videokommunikation abreißt, die Antennennachführung auch nicht mehr funktioniert. Die Alternative hierzu besteht in einem weiteren Downlink, welcher die GPS Daten zusammen mit den Telemetriedaten überträgt und eine größere Reichweite hat als das Videosystem. Das Bild 4.10 zeigt ein Gestell eines solchen Antennenfolgers.

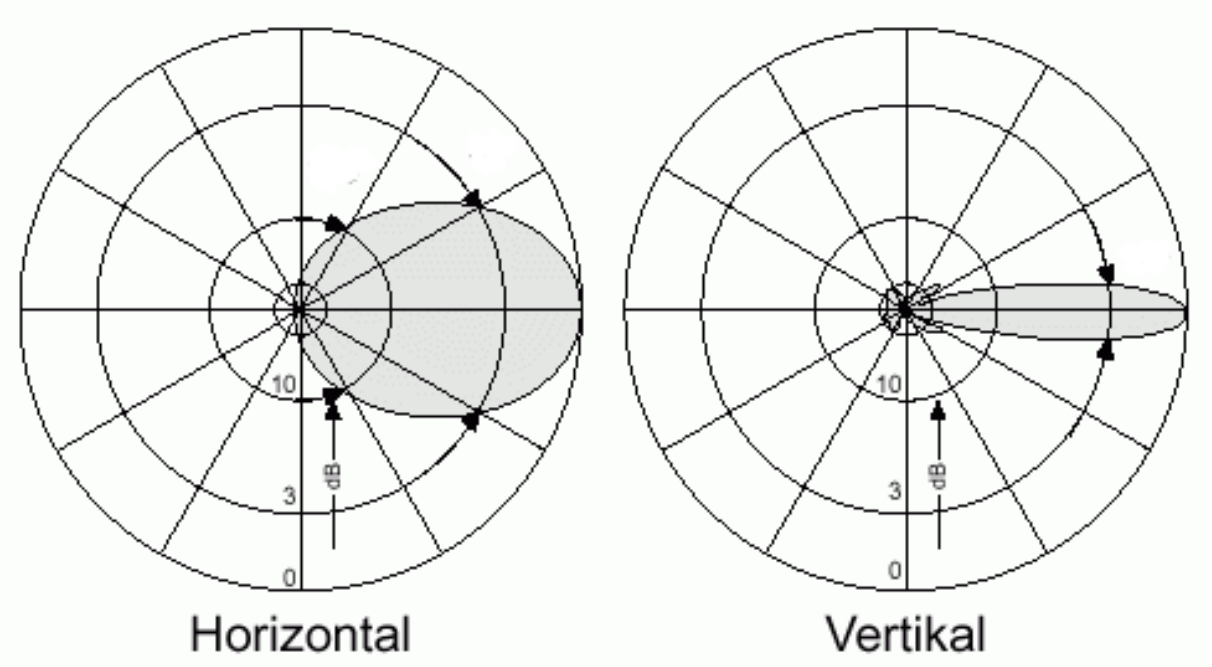

Abbildung 4.7: Antennendiagramm Patchantenne [Quelle: www.schiffertec.de]

Abbildung 4.8: WLAN Rundstrahlantenne [Quelle: www.batlink.de]

Abbildung 4.9: Patchantenne [Quelle: Globe Flight]

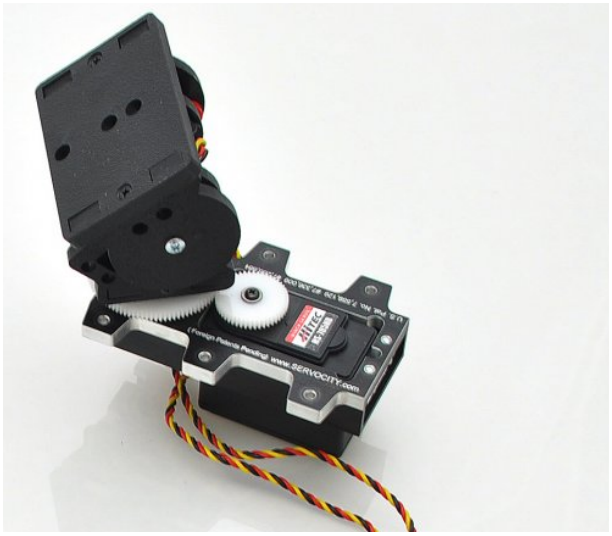

Abbildung 4.10: Antennenfolger [Quelle: Globe Flight]

Diversitysysteme Diversitysysteme (wie im Bild 4.11 gezeigt)können als zwei einzelne Empfänger betrachtet werden, die das jeweils bessere Empfangssignal an ihren Ausgang weiterleiten. Solche Systeme kommen sowohl am Boden, als auch in der Luft zum Einsatz. Sie ermöglichen es entweder mehrere gleichartige Antennen mit Richtcharakteristik so auszurichten, dass eine größere Ausleuchtung entsteht, oder die Kombination von Patchantenne für größere Distanzen mit "Rundstrahlern" für den umgebenen Nahbereich.In der Luft verhindern sie, dass der Empfang aufgrund dessen, dass das Modell selbst sich zwischen Sender und Empfänger befindet, zusammenbricht.

Abbildung 4.11: Diversityempfänger [Quelle: Globe Flight]

4.3.2 rechtliche Aspekte

Die Nutzung von bestimmten Frequenzen von elektromagnetischer Strahlung ist weltweit durch die International Telecommunication Union (ITU) festgelegt. Die in Deutschland für die Einhaltung dieser Gesetze zuständige Behörde ist die Bundesnetzagentur. Hier wird im sogenannten Frequenznutzungsplan jede Frequenz bzw. Frequenzbereiche auch einzelnen Nutzern zugeordnet. Es gibt aber auch das sogenannte ISM-Band. Dies ist eigentlich kein zusammenhängendes Band, sondern mehrere Frequenzbereiche, welche durch die Industrie, Wissenschaft und Medizin in häuslichen und ähnlichen Bereichen genutzt werden können. Festgehalten sind diese in den sogenannten Allgemeinzuteilungen. In diesen Frequenzbereich fallen bekannte Anwendungen, wie WLAN oder Bluetooth (wobei hierfür noch weitere Bestimmungen für Funkanwendungen gelten)aber auch Geräte, welche die elektromagnetische Strahlung zu ganz anderen Zwecken verwenden. Hier sind zum Beispiel Mikrowellen oder div. medizinische Geräte zu nennen. All diese Geräte benötigen nur eine allgemeine Zulassung. Das Problem welches sich hier schon zeigt ist, dass bei unzureichender Abschirmung und gleichzeitiger Nutzung verschiedener Systeme gegenseitige Störungen auftreten können. Da dies auch unmittelbar mit den Sendeleistungen einhergeht, werden diese zusätzlich zu den Frequenzen auch geregelt.

Die Frequenzen des ISM-Bandes sind in Tabelle 4.1 aufgelistet. Folgende Anwendungstypen werden hierbei noch unterschieden:

Von	Bis	Typ	Sendeleistung
6,765 MHz	6,795 MHz	A	42 dB$\mu A/m$
13,553 MHz	13,567 MHz	B	42 dB$\mu A/m$
26,957 MHz	27,283 MHz	B	10 dB/m
40,66 MHz	40,70 MHz	B	10 dB/m
149,995 MHz	150,005 MHz	B	41 dB$\mu A/m$
433,05 MHz	434,79 MHz	A	10 dB/m
2,400 GHz	2,500 GHz	B	20 dB/m
5,725 GHz	5,875 GHz	B	23 dB/m (30 dB/m)
24 GHz	24,25 GHz	B	20 dB/m
61 GHz	61,5 GHz	A	20 dB/m
122 GHz	123 GHz	A	20 dB/m
244 GHz	246 GHz	A	20 dB/m

Tabelle 4.1: ISM-Band Frequenzberieche mit Sendeleistung gültig für Deutschland [Quelle: Allgemeinzuteilungen - Bundesnetzagentur]

Frequenzen	Einschränkungen
26,995 bis 27,1	
27,195	
27,255	
35,010 bis 35,200	Darf nur für Fernsteuerung von Flugmodellen genutzt werden!
35,820 bis 35,910	Darf nur für Fernsteuerung von Flugmodellen genutzt werden!
40,665 bis 40,695	
40,715 bis 40,735	Darf nicht für Fernsteuerung von Flugmodellen genutzt werden!
40,765 bis 40,785	Darf nicht für Fernsteuerung von Flugmodellen genutzt werden!
40,815 bis 40,835	Darf nicht für Fernsteuerung von Flugmodellen genutzt werden!
40,865 bis 40,885	Darf nicht für Fernsteuerung von Flugmodellen genutzt werden!
40,915 bis 40,935	Darf nicht für Fernsteuerung von Flugmodellen genutzt werden!
40,965 bis 40,985	Darf nicht für Fernsteuerung von Flugmodellen genutzt werden!

Tabelle 4.2: Modellfunkfrequenzen [Quelle: Allgemeinzuteilungen - Bundesnetzagentur]

- Typ A: Anwendungen in diesen ISM Bändern bedürfen einer Genehmigung der jeweils regionalen Autoritäten. Diese können Einschränkungen z. B. im Bezug auf kooperative Funkprotokolle enthalten. Die Genehmigung kann auch pauschal erteilt werden.

- Typ B: Anwendungen in diesen Bändern benötigen keine Genehmigung, müssen jedoch mit Störungen jeder Art zurechtkommen.[4]

Speziell für den Modellfunk sind weiterhin die in Tabelle 4.2 angegebenen Mitten-Frequenzen freigegeben.

[4]Quelle: Bundesnetzagentur

Es gilt für alle Modellfunkfrequenzen die Beschränkung auf maximal 100mW Strahlungsleistung.

Es gibt natürlich auch spezielle militärische Frequenzen, dessen Nutzung muss jedoch auch einzeln mit der Bundesnetzagentur abgestimmt werden. Weiterhin ist es auch möglich, sich spezielle Frequenzen für die eigene Nutzung zu reservieren. Hierfür ist allerdings eine sehr aufwändiges Genehmigungsverfahren nötig.
Zusätzlich zu den Bestimmungen über Frequenz und Sendeleistung gibt es zumindest für Modellflugzeuge die Bestimmung, dass sie nicht komplett autonom fliegen dürfen. Der Pilot muss also jederzeit in der Lage sein Einfluss auf die Drohne zu nehmen, die Verbindung zur Fernbedienung darf also nicht abreißen. Diese Bestimmung zu umgehen sollte jedoch für militärische Zwecke keine große Hürde darstellen, denn bereits existierende Drohen wie KZO (Bild:4.1) fliegen vollständig autonom. Andere für Modellflugzeuge geltende Bestimmungen sollen an dieser Stelle nicht weiter ausgeführt werden, da sie, ähnlich wie die Bestimmung zum autonomen Fliegen, für militärische Drohnen keine Anwendung finden sollten.

4.3.3 Übertragungsmethoden

analoge Übertragung

Für den sog. Uplink, also für die Kommunikation zum MK über eine Fernsteuerung im Bereich der Fluglagesteuerung, kommen sowohl analoge, als auch digitale Systeme zum Einsatz. Für militärische Anwendungen sind ältere, analoge Sendeanlagen sehr ungünstig, da um die Kommunikation zur Drohne zu stören, lediglich eine Frequenz gestört werden muss. Dies kann sogar unabsichtlich geschehene, führt aber fast unweigerlich zur Gefährdung und meist auch zum Absturz der, dann unkontrollierbaren, Drohne. In neueren analogen Radio Controlled (RC) Systemen wirkt man dem durch Frequenzsprungverfahren entgegen. Hier verteilt man die Steuerungsdaten auf ein größeres Frequenzspektrum und verhindert durch das ständige Wechseln der Frequenz eine längere Störung.

Auch beim Downlink kommt sowohl digitale, als auch analoge Übertragung zum Einsatz. Wird ein Videosignal live zur Bodenstation gesendet, so nutzt man bisher ausschließlich analoge Systeme. Der Grund hierfür liegt in der Anwendung. Wenn man das Videosignal für den sogenannten First Person View (FPV)-Flug (siehe Kapitel 4.5.2) nutzen möchte, sind große Latenzzeiten sehr bedeutsam. Da mit derzeitiger Technik Videos nicht digital, unkomprimiert und in Echtzeit übertragen werden können, ist die Verwendung von Komprimierungsmethoden ein Muss. Hierdurch entsteht aber ein erheblicher Rechenaufwand, sowohl in der Luft, als auch am Boden, der zur Verzögerung des Videos führt. Somit bleibt hier kein großer Spielraum. Ein weiterer Nachteil digitaler Systeme in diesem Anwendungsbereich zeigt sich beim kurzzeitigen Kommunikationsabriss. Während ein analoges System nach kürzester Zeit wieder ein Bild zeigt oder gar nur Störungen im Bild zeigt, reißt der Videostream digitaler Systeme ab und braucht meist sehr lange um wieder aufgebaut zu werden. Wie stark die Verzögerung ist, hängt sowohl vom verwendeten Kommunikations-

protokoll, als auch vom CODEC[5] ab. Das Problem liegt hier also eher in der großen zu übertragenden Datenmenge, als im Übertragungsverfahren. Bei allen Vorteilen gibt es an dieser Stelle jedoch auch Nachteile. Wie oben schon genannt, muss um die Videokommunikation zu stören lediglich eine Frequenz gestört werden. Derzeit sind keine kommerziellen Systeme verfügbar, die Bandspreizungen oder ähnliche Verfahren verwenden.

digitale Übertragung

Im kommerziellen Bereich spielen digitale Übertragungssysteme für MK oder andere RC-Flugmodelle eine immer größer werdende Rolle. Fast alle namenhaften Hersteller haben ein System im Angebot, einige bieten sogar eine bidirektionale Übertragung an, um so Telemetriedaten zum Boden zu schicken. Der Vorteil von digitalen Systemen liegt auf der Hand. Dank Bandspreizverfahren und Chippingsequenzen können viele gleichartige Systeme gleichzeitig genutzt werden, ohne einander zu stören oder von außen gestört zu werden. Einzelne Systeme verteilen ihre Signale so im Frequenzband, dass sie ohne Kenntnis der Chippingseqeunz im Hintergrundrauschen untergehen. Im Abschnitt 4.3.3 wurde bereits detailliert auf die Probleme der Videoübertragung eingegangen, daher soll das an dieser Stelle nicht noch einmal geschehen. Es scheint, als wäre die digitale Bildübertragung für den Drohnenbereich grundsätzlich ungeeignet.

Dem ist allerdings nicht ganz so. Aufgrund der sehr ausgeklügelten und komplexen Elektronik von Mikrokoptern, sind diese durchaus in der Lage autonom zu fliegen. Für den Nutzer bleibt lediglich die Aufgabe dem MK eine Position und eine Höhe vorzugeben, welche der MK dann selbständig anfliegt. Da es hierbei nicht mehr auf Millisekunden, ggf. nicht mal auf Sekunden ankommt, ist es durchaus möglich die Kommunikation zum MK digital zu realisieren. Weiterhin können auch hoch aufgelöste Bilder oder Sensordaten zur Bodenstation gesendet werden. Im militärischen Bereich ist die digitale Kommunikation zu favorisieren, da die Daten so auch sehr einfach und zuverlässig verschlüsselt werden können, um sie vor unbefugter Nutzung zu schützen. Weiterhin ist die Sicherstellung der QoS wesentlich einfacher, da beispielsweise verlorene Datenpakete einfach noch einmal gesendet werden können, da ihr Verlust erkannt werden kann.

4.4 Datenübertragung

Für die militärische Anwendung ist die Datenkommunikation nach der Bildübertragung wohl die wichtigste. Gemeint sind hier sowohl Telemetrie, als auch Sensordaten, welche überwiegend zeitunkritisch sind, da sie auf den direkten Weiterflug nur bedingte Auswirkungen haben. Denkbar wären Sensoren für chemische oder biologische Kampfstoffe, elektrische Felder, aber auch Wetterdaten, wie Temperatur oder Windgeschwindigkeiten und Richtungen. Weiterhin sind hoch aufgelöste Bilder sowohl im sichtbaren, als auch im Infrarotbereich sehr aussagekräftig um Objekte zu identifizieren oder etwas über ihren Zustand auszusagen. Auch die Telemetriedaten der Drohne sind für die Aufklärung sehr

[5]CODEC - Kunstwort für coder und decoder, Verfahren zur Kodierung und Dekodierung digitaler Signale

nützlich, da beispielsweise die Temperatur große Auswirkungen auf Akkukapazitäten und damit der Flugdauer haben kann. Bei der Übertragung zum Boden fallen aber lediglich die Bilddaten wirklich ins Gewicht, da sie vom Volumen circa um den Faktor 10.000 größer sind. Da sämtliche Sensordaten meist digital erfasst werden, bietet es sich auch an, diese digital zu übertragen.

4.5 Videoübertragung

Sowie ein Bild mehr sagt, als 1000 Worte, so sagt ein Video mehr als 1.000 Messdaten. Auch wenn der Vergleich vielleicht an einigen Stellen etwas übertrieben scheint, so steht es doch außer Frage, dass Videos für die militärische Aufklärung von unschätzbarem Wert sind. Wenn der Teileinheitsführer in eine Stadt schauen kann, ohne auch nur ein einziges Menschenleben dabei zu gefährden, so ist dies ein größtmöglicher Erfolg. Gerade diese Anwendung führt aber auch zu großen Problemen. Ein Grund hierfür ist, dass bei der Videokommunikation im Gegensatz zur Datenkommunikation in sehr kurzer Zeit sehr viel Daten zustande kommen und somit auch übertragen werden müssen. Erst vor einigen Jahren wurden die hierfür notwendigen Technologien entwickelt. Eine recht kurzes 20 minütiges Video, welches unkomprimiert zur Verfügung steht, kann bei hoher Auflösung durchaus Größen von einem Terabyte und mehr erreichen. Daten dieser Größe können, wie im Abschnitt 4.3.3 und 4.3.3 bereits beschrieben, unmöglich in Echtzeit digital übertragen werden. Eine Möglichkeit besteht in der Kompression mit sogenannten CODECs. Das Datenvolumen wird hierdurch immens kleiner, sodass bereits Datenraten von wenigen MBit/s (circa 3 MBit/s) ausreichen um Videos live zu streamen. Da man hier jedoch durch die benötigte Rechenleistung (wie in 4.3.3 bereits beschrieben) sehr einschränkt ist, werden solche Daten in der Regel gespeichert und anschließend am Boden ausgewertet. Weiterhin wurde auch das Problem angesprochen, das falls der Stream abreißt, es sehr lange dauert bis wieder ein Bild zustande kommt. Der Grund hierfür liegt in der Funktionsweise der Komprimierungsmethode.

4.5.1 Videokompression

Der Ziel einer Komprimierung mittels CODEC ist, die Datenmenge eines Videos zu reduzieren. Einfache Verfahren ändern hier nur die Größe der einzelnen Bilder. Komplexere Verfahren erkennen Gemeinsamkeiten zwischen einzelnen Bildern und reduzieren die Daten dann auf die sich tatsächlich unterscheidenden Regionen. Hinzu kommt, dass über Bewegungsvektoren gleiche Bildteile an anderer Stelle wiedererkannt werden und somit auch redundante Daten darstellen, welche eingespart werden können. Zusätzlich werden Informationen, welche für den Menschen nicht sichtbar sind, verworfen. Auch Farbinformationen können aufgrund der Anatomie des Auges reduziert werden, da sie nur begrenzt wahrnehmbar sind. Es ist an dieser Stelle jedoch bereits leicht erkennbar, dass komplexe Berechnungen nötig sind, um Videos zu komprimieren und das, wenn ein Video Stream abreißt, erst wieder ein komplettes Bild übertragen werden muss, um im Anschluss die Änderungen darauf anwenden zu können. Derzeit erzielbare Kompressionsraten liegen

zwischen 1:5 und 1:200. Die Standardisierung von Videokodierungsverfahren wird beispielsweise duch die Moving Picture Experts Group (MPEG) vorangetrieben.

4.5.2 FPV-Flug

FPV-Flug oder auch Immersionsflug bedeutet First Person View-Flug und meint damit, dass dem Nutzer das Gefühl gegeben wird, er würde im Cockpit sitzen und hinaus schauen. Dies wird ermöglicht durch einen Livestream vom MK oder einem anderen Flugmodell zur Bodenstation. Der Pilot reagiert auf die Bilder, die er sieht und steuert dann, mit Hilfe seiner Fernbedienung, das Flugmodell. Spätestens an dieser Stelle wird klar, warum die in den Kapiteln 4.3.3 und 4.3.3 angesprochenen Latenzzeiten katastrophale Auswirkungen haben. Wer schon einmal ein Modellflugzeug oder einen MK geflogen hat, der weiß, welche Auswirkungen sehr kleine Ausschläge an der Fernbedienung auf das Flugmodell haben und wie oft es nötig ist, eine ungewollte Bewegung auszugleichen. Wenn der Pilot kein unmittelbares Bild seiner Fluglage hat, ist das Modell schon fast verloren. Um unabhängig von sonstigen Einflüssen zu sein und sich voll auf das Bild des MK zu konzentrieren, nutzen die meisten FPV-Piloten sogenannte Videobrillen. Diese werden wie normale Brillen aufgesetzt und projizieren das Bild dann auch direkt vor die Augen. Eine solche Brille trägt auch der Soldat auf dem Bild 4.12.

OSD Um dem Piloten mit allen wichtigen Informationen zu versorgen, nutzt man zusätzlich sogenannte OSD. Diese blenden dem Piloten wichtige Informationen direkt in das Videobild ein. Den Zusammenhang zum Thema Funk bilden die OSDs dadurch, dass sie zum Teil für die Ausrichtung einer beweglichen Antenne genutzt werden (siehe auch 4.3.1).

4.6 Sicherheit

Wie bereits bei anderen Abschnitten erwähnt wurde, sind militärische Daten einerseits meist immer sicherheitsrelevant, andererseits riskiert man im Falle einer Störung den Absturz der Drohne. Aus diesem Grund empfiehlt es sich, Daten immer sicher zu übertragen. Dies bedeutet, dass sie entweder von vornherein verschlüsselt übertragen werden und das man Methoden nutzt, die verlorene Daten erkennen und dementsprechend noch einmal senden oder, dass man versucht Daten so schnell wie möglich zu senden und die Sendeleistung so gering hält, dass der Bereich in dem das Signal abgehört werden kann, klein bleibt. Das wiederholte Senden von Datenpaketen ist jedoch nicht immer nötig, da beispielsweise bei RC Anlagen die Datendichte so hoch ist, dass es schneller geht, wenn man die nächsten Daten sendet, anstatt die vorherigen zu wiederholen. Mit anderen Worten ist das Steuersignal bei einer Wiederholung schon so alt, dass es nicht mehr benötigt wird. Gleiches gilt meist für Telemetriedaten. Der bereits angesprochene Geschwindigkeitsnachteil bei der Verschlüsselung ist ebenfalls abzuwägen. Gerade die Übertragung von Aufklärungsdaten im Videobereich ist sehr riskant, da sie aufgrund der Verzögerung

Abbildung 4.12: Drohne MIKADO und Bediener mit FPV Ausstattung [Quelle: m136.de]

meist unverschlüsselt und zu dem analog geschieht. Hier gab es bereits Ende 2009 Probleme, als Aufklärungsdaten einer Predator Drohne abgefangen wurden[6]. Feindliche Kräfte könnten so Schwerpunkte der eigenen Kräfte erkennen und dementsprechend handeln.

4.7 fertige Systeme

Wenn man ein Produkt auf den Markt oder in die Truppe bringen will, hat man die Möglichkeiten alles neu und selbst zu entwickeln oder man bedient sich vorhandener Systeme. Die komplette Eigenentwicklung hat, gerade im militärischen Bereich den Vorteil, das Informationen geheim gehalten werden können. Im speziellen Fall der Drohne wäre dies zum Beispiel die Übertragungsfrequenzen oder überhaupt die Kommunikation zwischen Drohne und Bodenstation. Weiterhin sind auch Einsatzdaten wie Flugdauer, Geschwindigkeit und maximale Höhe schützenswert. Eigenentwicklungen haben aber meist den entscheidenden Nachteil, dass sie zum Einen viel mehr Zeit für die Entwicklung benötigen und dadurch auch sehr teuer werden, zum Anderen kommt es nicht selten vor, dass man bei der Entwicklung wiederholt Fehler macht, mit denen auch bereits fertige Systeme zu kämpfen hatten. Es ist also sehr schwierig hier einen Standpunkt zu beziehen, meist wird der Mittelweg der Beste sein. Aus diesem Grund sollen an dieser Stelle auch einige Systeme, angefangen von der einfachen Datenkommunikation bis hin zur fertigen Drohne, betrachtet werden.

4.7.1 Bluetooth

Bluetooth ist die wohl einfachste Kommunikation zwischen Drohne und Bodenstationen. Fertige Bluetoothmodule werden hierzu einfach auf eine Adapterplatine gelötet, konfiguriert und schon besteht eine Serielle Datenkommunikation innerhalb eines PAN. Der Nachteil entsteht durch die doch sehr geringe Reichweite von Bluetooth. Selbst mit guten Modulen sind nicht mehr als 150m bei direkter Sichtverbindung zu erreichen. Ein weiterer Nachteil ist die Frequenz. Bluetooth arbeitet wie modernere RC Steueranlagen im 2,4 GHz Band und kann somit zum einen durch die RC Anlage beeinflusst werden, zum anderen aber auch selbst eine Beeinflussung darstellen. Daher ist Bluetooth, wenn überhaupt nur für die Kommunikation im Nahbereich geeignet. Ein weiterer Nachteil ist die sehr begrenzte Bandbreite, welche bei einer asymmetrische Verbindung theoretisch 706,25 kbit/s beim Empfang und 57,6 kbit/s beim Senden beträgt. Weiterhin ist eine symmetrische Verbindung mit bis zu 433,9 kbit/s möglich. Bei Bluetooth 2.1 können unter guten Bedingungen sogar bis zu 2,1 MBit/s übertragen werden. Alle drei Varianten reichen aber nicht aus, um hierüber live Videodaten zu übertragen, somit ist diese Verbindung nur für Datenverbindungen nutzbar. Denkbar wären hier Anwendungen um Missionsdaten auf den MK zu übertragen, ohne eine Kabelverbindung herstellen zu müssen.

[6]Quelle: Artikel am 17.12.2009, www.heise.de

4.7.2 ZigBee

Ähnlich wie Bluetooth ist auch ZigBee ein für PAN gedachtes Netzwerk. ZigBee ist ebenfalls nur für die Kommunikation zwischen Geräten auf Kurzstrecken geeignet, da die Reichweite ebenfalls lediglich zwischen 10 und 100 Metern. Die Übertragungsfrequenz liegt im 2,4 GHz Band, kann aber auch auf das 868 MHz Band umgestellt werden. Ein großer Vorteil der ZigBee-Komponenten liegt in dem sehr geringen Stromverbrauch. Dieser Vorteil wird aber durch die gegenüber Bluetooth noch geringere Datenübertragungsrate (20kbit/s bei 868 MHz und 250kbit/s bei 2,4 GHz) überschattet. Somit ist ZigBee nicht einmal für die Datenübertragung sinnvoll einzusetzen.

4.7.3 Wi232

Das Wi232 stellt, wie der Name schon andeutet, ebenfalls eine Serielle Schnittstelle her. Der Vorteil liegt hierbei in der Reichweite. Da das Wi232 Modul im 868 MHz Band arbeitet, werden hier mit einer einfachen Drahtantenne bereits Reichweiten bis 1000m erreicht. Es treten somit auch keine Störungen der RC Anlage auf. Der Nachteil besteht jedoch wieder in der Bandbreite. Lediglich 76,8 kbp/s stehen für die Übertragung zur Verfügung. Somit ist hier wie bei Bluetooth nur an eine Datenkommunikation zu denken. Da die Reichweite jedoch wesentlich höher ist, scheint das Wi232 Modul besser geeignet. Mit Hilfe größerer Antennen ist es sogar möglich die Reichweite bist auf 10km zu erhöhen. Somit sind diese Module im Bereich der Telemetriedatenübertragung sehr gut einsetzbar.

4.7.4 WLAN

Wireles Local Area Network (WLAN) scheint auf den ersten Blick wie geschaffen für die Kommunikation zwischen MK und Bodenstation. USB-Empfänger sind sehr leicht und die Bandbreite scheint endlich auszureichen, um auch Videodaten zu übertragen. Übertragungsraten von 54 MBit/s oder sogar 600 MBit/s beim 802.11n Standard klingen so vielversprechend, dass man parallel ohne weiteres noch Telemetriedaten übertragen können sollte. Doch so positiv wie es aussieht ist es dann letztendlich doch nicht. Erst einmal benötigt die Kommunikation zwischen WLAN Endgeräten einen großen Koordinierungsaufwand. Dies bedeutet das zwar USB-Empfänger recht klein sind, die eigentliche Arbeit hier aber auf das Betriebssystem und die dahinter stehenden Hardware übertragen wird. Weiterhin dauert es recht lange, bis eine WLAN Verbindung aufgebaut ist. Dies wäre nach einem kurzzeitigen Kommunikationsabriss sehr problematisch. Hinzu kommt das Daten normalerweise mittels TCP/IP Protokoll übertragen werden, welches durch die Header zusätzliche Datenrate benötigt. So kommt es, dass der Unterschied zwischen Brutto und Nettodatenrate immens ist. Nicht zu vergessen ist auch, dass mit wachsender Entfernung der Entgeräte nicht nur die Empfangsqualität sinkt, sondern daraus resultierend auch die Datenrate. Abhängig vom Protokoll werden Datenpakete bei Verlust in der Regel noch einmal gesendet, was die nutzbare Datenrate abermals schmälert. Weiterhin ist nicht zu vergessen, dass WLAN auch im 2,4 GHz Band arbeitet und somit RC Empfangsanlagen stören kann. Maximal erlaubte Sendeleistungen von 100mW führen, bei ausreichender Datenrate, zu recht kleinen Reichweiten. Alles in allem ist WLAN also auch keine Lösung.

4.7.5 UMTS/GPRS

Auch Mobilfunkstandards wie GPRS, UMTS oder auch LTE bieten ein Potential Daten zwischen MK und Bodenstation auszutauschen. Je nach Datenrate wäre die Übertragung von Telemetriedaten oder sogar Bildern denkbar. Die benötigte Hardware ist ausreichend klein und stromsparend. Das sich hierbei stellende Problem ist allerdings, dass in militärischen Einsatzgebieten selten gut ausgebaute Mobilfunknetze vorhanden sind und sollte dies sogar der Fall sein, dass man hier von externen Systemen abhängig ist, dessen Betrieb und Verfügbarkeit man nur sehr begrenzt beeinflussen kann. Weiterhin müssten auch hier die Daten verschlüsselt übertragen werden, da sie nun nicht mehr nur im unmittelbaren Umkreis der Drohne verfügbar sind, sondern theoretisch weltweit abgerufen werden können. Daher wird von dieser Möglichkeit Abstand genommen.

4.7.6 analoge Videotransmitter

Für die Videoübertragung zum Boden sind derzeit die analogen Videotransmitter sehr zu empfehlen. Es gibt sie für fast jedes Frequenzband und die Kosten halten sich in Grenzen. Die Reichweite beträgt ohne besondere Antenne ca. 500m. Die Hardware ist sehr leicht und kompakt. Im Gegensatz zur digitalen Übertragung gibt es unterschiedlich gute Bilder, dafür gibt es aber keinen aufwändigen Kommunikationsaufbau und leichte Störungen zeigen sich nur durch Verzerrungen im Bild. Nachteilig zu bewerten ist allerdings die fehlende Datenkommunikation. Es ist also für die Übertragung von Telemetriedaten ein weiterer Datenlink nötig.

4.7.7 Komplettsysteme

Im folgenden sollen Komplettsysteme beschrieben werden, die als solches ”off the Shelf” beschafft und eingesetzt werden können. Aber auch Systeme, deren Entwicklung ein sehr großes Potential bietet, um sie für den Einsatz in Streitkräften anzupassen.

AR.Drone

Die von der Firma Parrot entwickelte Drohne ”AR.Drone” ist für den militärischen Einsatz nicht brauchbar, allerdings hat sie mehrere Eigenschaften, die auch bei militärischen Drohnen wünschenswert wären. Die Drohne baut selbständig ein WLAN Netzwerk auf, über das sich die Steuereinheiten IPhone oder IPad dann mit der Drohne verbinden können. Wie im Abschnitt 4.7.4 beschrieben, ist zwar WLAN nicht das Mittel der Wahl, aber immerhin wird hier eine breitbandige Verbindung automatisch aufgebaut. Über eine Application, welche von der Herstellerwebside herunter geladen werden kann, ist es dann möglich die Drohne zu steuern. Den Flug übernimmt sie hier jedoch autonom, dass heißt, sie verharrt so lange in einem stabilen Schwebezustand, bis sie wieder einen Bewegungsbefehl erhält. Sogar der Start und die Landung erfolgt automatisch. Auch dies wäre für die

militärische Anwendung sehr brauchbar. Die Höhenmessung erfolgt über Ultraschallsensoren und die Beschleunigung über dem Boden wird über eine Kamera berechnet. Beide Methoden sind jedoch sehr ungenau, gerade wenn es in größere Höhen geht. Es sind insgesamt zwei Kameras an Board, welche über die WLAN Verbindung einen live MPEG Video Stream zur Verfügung stellen. Die AR.Drone versteht sich selbst als Spielzeug und ist daher sehr einfach über die Bewegungssensoren des IPhone oder IPad zu steuern. Mit weiteren Anwendungen ist es sogar möglich eine augmented Reality[7] aufzubauen. Hier kann man dann virtuell auf Gegner schießen, hat aber im Hintergrund weiterhin das Umgebungsbild der Frontkamera. Ein weiteres Plus des Systems ist, dass es als Spielzeug auch sehr robust gebaut ist und einen Absturz in der Regel auch ohne Schäden übersteht. Um weitere Entwicklungen voran zu treiben, ist das Software Devellopment Kit (SDK) frei auf der Webside verfügbar. Erste Entwicklungen zeigen, dass mit der richtigen Bodenstation hier sogar eine Bilderkennung möglich ist. Die Drohne ist also theoretisch in der Lage sich ihren Weg allein zu suchen.

Mikrokopter

Der in der Einleitung bereits erwähnte Mikrokopter ist als reine Flugplattform sehr gut für den militärischen Einsatz geeignet. Selbst mit aufwendiger Videoaufnahme und Übertragungstechnik an Bord, kommt er auf Flugzeiten um die 20 Minuten und erreicht dabei Modellflugähnliche Wendigkeit. Mittels optionaler Navigationsplatine ausgerüstet, ist er auch in der Lage eine vorher festgelegte Strecke abzufliegen. Seine Höchstgeschwindigkeit liegt bei ca. 25km/h, die Reichweite ist allerdings Softwareseitig auf den Sichtbereich beschränkt (aufgrund rechtlicher Bestimmungen). Es gibt für den MK fertige Telemetrieübertragungssysteme, wie auch Platinen welche ein OSD erzeugen. Die Ausrüstung mit Videoübertragungstechnik, wie sie aus dem Modellbau bekannt ist, stellt keine große Hürde dar. Selbst große Spiegelreflexkameras für hochaufgelöste Fotos sind machbar. Die Plattform ist sehr Windstabil und fliegt ähnlich wie die AR.Drone vollständig autonom. Erfolgt kein Steuerbefehl nimmt der MK eine stabile Gleichgewichtslage ein und korrigiert, GPS Modul vorausgesetzt, sogar seine Position, sofern er von Wind oder anderen Einflüssen abgetrieben wird. Hierbei muss jedoch ständig eine Verbindung zur Fernbedienung existieren (ebenfalls rechtliche Bedingungen). Lediglich Feuchtigkeit stört die komplexe Elektronik, was aber ein lösbares Problem darstellen sollte. Es scheint also, als wäre die perfekte Drohne gefunden, doch leider gibt es auch hier eine Einschränkung. Mikrokopter sind ein Selbstbau-Projekt von zwei Hobbybastlern (Ingo Busker und Holger Buss). Daher gibt es keinen komplett fertig zusammengebauten Mikrokopter zu kaufen.

MIKADO

Auch die Bundeswehr hat das Potential von Drohnen erkannt, und sich für eine zivile, kommerzielle Lösung entschieden, die scheinbar alle Anforderungen erfüllte. Der Name MIKADO leitet sich ab von: Mikro-Aufklärungsdrohne im Ortsbereich. Die Firma AirRobot GmbH entwickelte die dem MK sehr ähnliche Aufklärungsdrohne. MIKADO hat 4

[7] computergestützte Erweiterung der Realitätswahrnehmung

Propeller die jeweils über wartungsarme Elektromotoren angetrieben werden. Die Reichweite der Drohne beträgt ca. 500m und sie hat eine Flugzeit von 20 Minuten. Die Nutzlast der Drohne ist auf 200g beschränkt. Dies reicht allerdings aus um eine Tageslichtkamera, einen Dämmerungssensor oder eine Infrarotkamera zu installieren. Gesteuert wird MIKADO über eine 35 MHz Fernsteuerungsanlage. Dabei gelangt über einen 2,4 GHz Downlink ein Bild in Echtzeit zur Bodenstation und ermöglicht so die Steuerung über Display oder Videobrille. Beide Systeme arbeiten mit einer analogen Übertragung. Die Steuerung scheint sich jedoch etwas vom MK zu unterscheiden. Der Pilot steuert nicht die Fluglage, sondern bestimmt nur Geschwindigkeit und Richtung. Wenn keine weitere Steuerung erfolgt, fliegt die Drohne mit der vorgewählten Richtung und Geschwindigkeit weiter.

Eigene Einschätzung zu MIKADO Das System scheint für die Aufklärung aufgrund der verschiedenen Anbauteile sehr gut geeignet zu sein. Meiner Meinung nach ist aber die Reichweite unakzeptabel, da mindestens der Gefahrenbereich von Handwaffen überbrückt werden sollte. Weiterhin ist bei der Reichweite auch eine direkte Sichtverbindung notwendig, was im urbanen Gelände sehr unpraktisch ist. Auch die 35 MHz Anlage scheint sehr störungsanfällig zu sein, da wie im Abschnitt 4.3.3 beschrieben, nur eine Frequenz gestört werden muss, um die Drohne zum Absturz zu bringen. Trotzdem ist die Drohne durchaus positiv zu bewerten, da eine Eigenentwicklung zu teuer und zu langwierig gewesen wäre.

4.8 Zusammenfassung

Wenn man an dieser Stelle alle aus der Betrachtung gewonnenen Erkenntnisse bewertet, so erkennt man, dass es zumindest im Moment noch kein perfektes System auf dem Markt gibt, welches alle Probleme löst. Trotzdem zeichnen sich verschiedene Möglichkeiten mit ebenso verschiedenen Vor- und Nachteilen ab. Derzeit ist es meiner Meinung nach am erfolgreichsten, zur Steuerung ein 2,4 GHz System zu verwenden, welches die Daten auf digitalem Weg und mit verschiedenen Sicherungsverfahren zur Drohne sendet. Eine Datenverbindung sollte, aufgrund der Reichweitenvorteile, durch ein Wi232 System hergestellt werden. Dieses lässt sich bei Bedarf auch sehr einfach mit anderen Systemen wie Bluetooth verbinden. Für die Videoübertragung scheint im Moment nur eine analoge Übertragung praktikabel, da diverse Systeme ausreichend getestet und digitale Systeme zu groß und zu schwer sind. Weiterhin sind im Kapitel 4.3.3 angesprochene Nachteile digitaler Systeme unakzeptabel für den FPV-Flug. Der Einsatz der Drohne MIKADO wird es den Streitkräften ermöglichen Erfahrungen mit solchen Geräten zu bekommen und so in Zukunft auch Verbesserungen vorzunehmen. Insgesamt sollten Drohnen aus dem militärisch Einsatzszenario aber nicht mehr wegzudenken sein.

Kapitel 5

Drahtlose Sensornetze in der Lehre – Sicherheitsbetrachtung von ZigBee-Netzen

Björn Stelte

Gerade in den letzten Jahren kommen mehr und mehr Anwendungen auf Basis von drahtlosen Sensornetze auf dem Markt. So gibt es in den USA die Bestrebungen drahtlose Sensornetze für die Energieüberwachung (smart monitoring) einzusetzen, aber auch in der Hausautomatisierung, dem Gesundheitswesen, u.a. sind die Netze bestehend aus vielen kleinen Sensorknoten im Gespräch. Der de-facto Standard bzgl. der Kommunikation dieser Sensornetze ist derzeit ZigBee. Dieses Protokoll wird in nahezu allen gängigen Sensornetzen verwendet. Jedoch sind bereits seit einiger Zeit Schwächen dieses Protokolls bekannt. Wie Joshua Wright mit seinem KillerBee Framework gezeigt hat, ist ein praktischer Angriff auf eine ZigBee Infrastruktur mit wenigen Hilfsmitteln kostengünstig und schnell realisierbar. Dieser Beitrag gibt einen Überblick über das ZigBee Protokoll und einige seiner Schwachstellen, sowie über Werkzeuge, um die Problematik im Unterricht darzustellen.

Inhaltsverzeichnis

5.1 Einleitung und Motivation 105
5.2 ZigBee Standart 105
5.3 Simulation von drahtlosen Sensornetzen 107
5.4 ZigBee Monitoring mittels Wireshark 109
5.5 KillerBee Framework 111
5.6 Byzantinische Fehlertoleranz 113
5.7 Schlussbetrachtung 114

5.1 Einleitung und Motivation

Die drahtlosen Sensornetze sind in der Forschung schon seit längerem ein immer wichtiger werdendes Forschungsthema. So hat beispielsweise die EU in ihrem Forschungsprogramm FP7 die Schlagwörter 'Internet of Things' und 'Ubiquitous Computing' aufgenommen. Ebenfalls ist bereits heute ein Trend hinsichtlich der Nutzung drahtloser Sensornetze in Anwendung der Automatisierung (sensor-actor network) oder der Überwachung von bspw. der Energieaufnahme von Haushaltsgeräten (smart meter) erkennbar. So hat erst kürzlich in den USA die Ausrüstung von 'smart meters' im größeren Umfang stattgefunden. Diese 'smart meters' nutzen, wie auch mittlerweile nahezu alle Sensornetze, die ZigBee Technologie zur Übertragung ihrer Daten. Doch eben diese ZigBee Technologie hat hinsichtlich Authentifizierung und Verfügbarkeit einige Schwächen aufzuweisen. Diese wurden erstmals durch Joshua Wright's KillerBee Framework praktisch bewiesen. Mittels KillerBee sind Angriffe auf bestehende ZigBee Netze durchführbar. Lediglich ein Laptop und zwei kleine AVR Raven USB-Sticks werden benötigt um Daten-Übertragungen mitzuhören, Replay-Angriffe zu unternehmen, oder den 'Association'-Prozess derart zu stören, dass ein ZigBee Controller letztendlich ausfällt. Die in ZigBee definierten Sicherheitsmaßnahmen sind daher als nicht ausreichend zu bewerten. Auf der anderen Seite ist jedoch eine Detektion der durch das KillerBee hervorgerufenen Angriffe durchaus möglich. Jedoch aufgrund der Tatsache, dass Sensorknoten sehr ressourenschwache Geräte sind, ist selbst ein einfaches Host-Intrusion Detection System (HIDS) eine Herausforderung. Um in der Lehre das Verständnis für IT-Sicherheit zu schärfen kann eine Demonstration von Sicherheitsvorfällen dienlich sein. In diesem Beitrag stellen wir hierzu drei aufbauende Simulationen vor. Im nächsten Kapitel wird zunächst die Grundlage des Angriffs, das ZigBee Protokoll kurz erklärt. Die eigentliche Simulation des Angriff wird in Kapitel 5.5 beschrieben.

5.2 ZigBee Standart

Der ZigBee Industriestandard basiert auf dem IEEE 802.15.4 Standard und wurde von der ZigBee Allianz entwickelt. Vom IEEE 802.15.4 Standard wurden physikalische Übertragung und Kanalzugriff übernommen. Höhere Schichten werden dagegen vom ZigBee Standard spezifiziert. ZigBee ist technisch dem Wireless Personal Area Networks (WPAN) zuzuordnen. Im Vergleich zu Bluetooth und WLAN jedoch zeichnet sich ZigBee durch extrem geringen Stromverbrauch und niedrige Datenraten aus. Die Kommunikation erfolgt bei ZigBee Geräten über Funk. Hierbei besteht grundsätzlich die Problematik, dass die Kommunikation leicht gestört oder abgehört werden kann. Da ZigBee, insbesondere bei Verwendung in drahtlosen Sensornetzen, zur Sensorabfrage und/oder Steuerung eingesetzt wird, ist die Integrität der übermittelten Daten von besonderem Interesse. Der ZigBee Standard ist mittlerweile recht umfassend und wird daher hier aus Platzgründen nur vereinfacht dargestellt. Für tiefer-gehende Analysen sei auf den Standard der ZigBee Allianz zu finden in [1] verwiesen.

Die Architektur eines ZigBee-basierenden Systems ist in die folgenden Schichten untergliedert:

- Physikalische Übertragungsschicht (PHY Layer) und Medienzugangssteuerung (MAC Layer), basierend auf dem IEEE 802.15.4 Standard.
- ZigBee Network Layer (NWK) zur Bereitstellung einer Ende-zu-Ende Kommunikation.
- ZigBee Application Layer (APL) der einen Satz von Applikationselementen bereitstellt. Technisch besteht diese Schicht aus dem ZigBee Application Sub-Layer (APS) und den ZigBee Device Objects (ZDO), sowie aus herstellerspezifischen Application Objects.

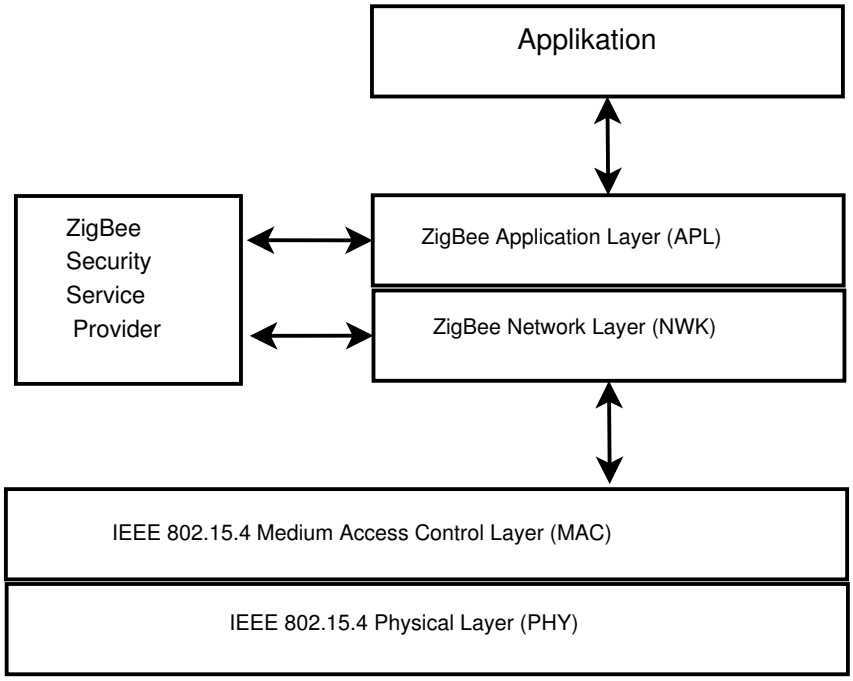

Abbildung 5.1: Architektur eines ZigBee-basierten Systems

Der in der physikalische Übertragungsschicht verwendete IEEE 802.15.4 Standard unterscheidet zwei Gerätetypen: Full Function Device (FFD) und Reduced Functional Device (RFD)

Der Unterschied zwischen einem FFD und RFD Gerät liegt im Umfang der implementierten Funktionalität. So kann ist ein FFD mit allen Betriebsfunktionen für ein WPAN ausgestattet. Die FFDs können untereinander und mit den RFD kommunizieren, hingegen kann ein RFD nur mit einem FFD Gerät Daten austauschen.

Hierauf aufbauend wird bei ZigBee (genauer im Network Layer) zwischen drei Geräteklassen unterschieden: Coordinator, Router und End-Device. ZigBee Coordinator und Router müssen zwingend vom IEEE 802.15.4 Typ FFD sein, End-Devices können sowohl RFD oder FFD Geräte sein. Ein ZigBee Coordinator kann gleichzeitig auch die Aufgabe eines Trust-Centers übernehmen. Dieses Trust-Center hat die Aufgabe der Authentifizierung neuer Knoten bei Aufnahme in das bestehende Netz. Üblicherweise wird in einem drahtlosen Sensornetz auf dem Coordinator Knoten auch die Trust-Center Funktionalität implementiert, wird gehen hier im weiteren davon aus.

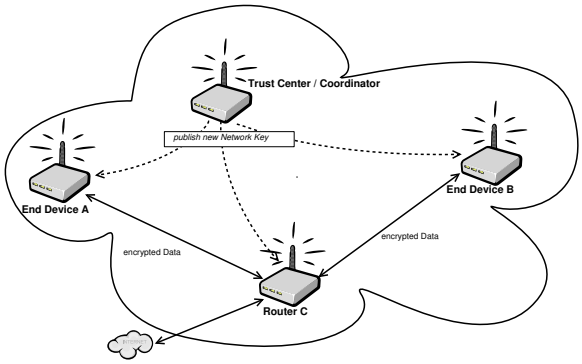

Abbildung 5.2: Ein typisches ZigBee Netz bestehend aus Coordinator, End-Geräten und einem optional Gateway-Knoten

Da die ZigBee Alliance den Industriestandard ZigBee in Hinblick auf den Einsatz als Kommunikationssystem für Sensor- und Steuerungsaufgaben optimiert hat, sind auch Maßnahmen zur Integritätssicherung berücksichtigt worden. Integritätssicherung und Verschlüsselung kann auf den Schichten APL, NWK und MAC optional aktiviert werden. Hierbei wird das etablierte AES-128 Verfahren verwendet. Der Knackpunkt dieses Sicherheitssystems ist wie nahezu in allen mobilen Geräten die Schlüsselverteilung. Entweder werden Schlüssel vorkonfiguriert oder über das Netz übertragen. Hierbei besteht das konzeptionelle Problem, dass das Schlüsselmanagement in der Schlüsselvereinbarung keine Authentisierung benutzt. Neben dieser Lücke ist auch ein einfacher Replay-Angriff in ZigBee Netzen möglich. Diese und weitere Angriffe können im Rahmen einer Demonstration in der Lehre verwendet werden, um das Bewusstsein für Aspekte der IT-Sicherheit zu schärfen. Wir werden im nächsten Abschnitt einen zur Demonstration der Sicherheitslücken brauchbaren Simulator beschrieben. Anschließend wird im Kapitel 5.5 beschrieben wie Angriffe auf das Protokoll im Rahmen der Simulation erfolgen können.

5.3 Simulation von drahtlosen Sensornetzen

Zur Veranschaulichung der Datenkommunikation eines ZigBee-basierten drahtlosen Sensornetzes gibt es prinzipiell zwei Möglichkeiten, der Aufbau eines physikalischen Testbeds oder die Simulation eines Netzes am Rechner. Gerade wenn Studenten den Umgang mit Sensornetzen kennenlernen sollen ist das physikalisch Vorhanden Testbed (mehrere Sensorknoten plus JTAG/Programmer) sicherlich reizvoll, jedoch sind die Kosten für eine benötige größere Laborausstattung sehr hoch. Daher wird man in den meisten Fällen auf eine Simulation zurückgreifen müssen. Hierbei ist zu beachten, dass es viele unterschiedliche Simulationsumgebungen gibt, mit unterschiedlichen Abstraktionsebenen. So gibt es Werkzeuge, um rein ZigBee Netze oder auch nur einzelne Schichten des Protokolls zu simulieren, jedoch gibt es auch Werkzeuge zur Simulation eines gesamten Sensornetzes samt den Sensorknoten. Eines dieser Umgebungen zur vollständigen Simulation ist Avrora [5]. Dieses Programm simuliert einen vollständigen Sensorknoten der verbreiteten Mica Familie (Mica, Mica2, MicaZ) basierend auf den AVR Microcontrollern [4].

Avrora ist ein Zyklus-genaue Instruction-Level-Simulator für die AVR-Mikrocontroller und für Sensor-Netzwerke mit AVR Mikrocontrollern. Avrora ist in Java implementiert, somit verwendet es ein objektorientierte Design und verfolgt somit die wichtigsten Konzepte in der Simulation wie Anweisungen, Geräte und Status in einer intuitiven Weise.

Die Avrora Architektur erlaubt die Implementierung eines Modells zu jedem Gerät, welche das Gerät emuliert und erlaubt die Kommunikation unter den Geräten. Jedes Geräte Modell ist in Java geschrieben und ist über die Kern-Simulation miteinander verbunden. Das Herzstück von Avrora ist die Simulator-Klasse, die aus Interpreter und Ereignis-Queue besteht. Der Interpreter führt jede Assembler Instruktion des geladenen Sensor-Programms aus. Durch eine Zyklus-genaue Instruktions-Level-Simulation können auch Schlafenphasen, wenn der Mikrocontroller im Ruhezustand ist, simuliert werden. On-Chip-Geräte (auf dem Microcontroller) kommunizieren mit dem Simulator über I/O-Register- und Ereignis-Queue-Schnittstelle. Die Mikrocontroller-Schnittstelle kapselt eine Instanz der Klasse Simulator und stellt On-Chip-Geräte, wie den Timer und den Analog-Digital-Wandler, zur Verfügung. Schließlich wird der Zugriff auf Off-Chip-Geräten wie Radio-Transmitter und LEDs durch die Plattform-Schnittstelle ermöglicht. Darstellung 5.3 gibt einen Überblick über die Struktur.

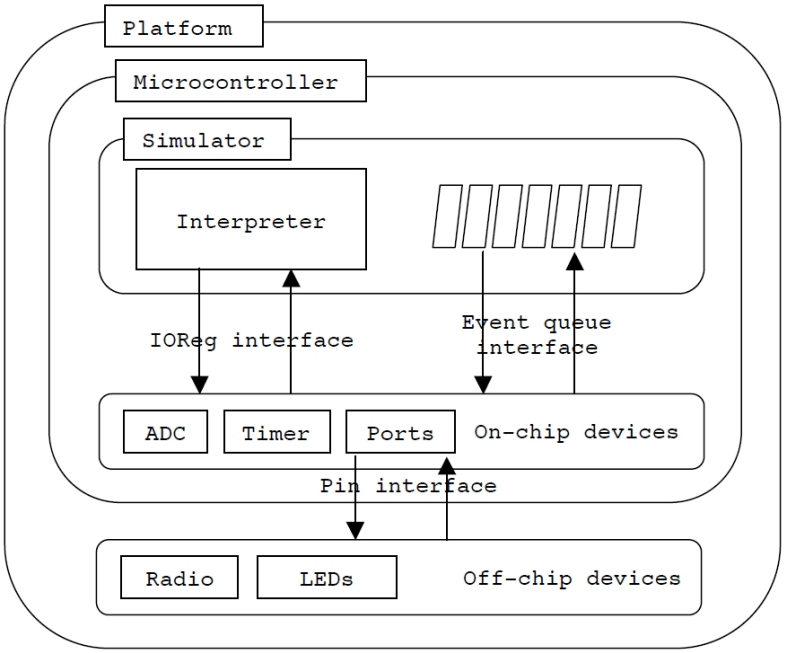

Abbildung 5.3: Struktur der Avrora Simulationsumgebung

Da bei Avrora ein Thread pro Knoten gestartet wird, ist im Hinblick auf die Skalierbarkeit die Anzahl der Knoten die simuliert werden kann nur durch das Host-Betriebssystem limitierend durch die maximale Anzahl der Threads pro Prozess. Threads werden nur synchronisiert, wenn erforderlich, um sicherzustellen, dass das globale Timing und die Reihenfolge im Funkverkehr während der Simulation erhalten bleibt. Die Autoren von Avrora haben in ihren Experimenten zeigen können, dass Avrora bis zu 1750 Knoten auf einem Dual-Prozessor Rechner simulieren kann. Allerdings wird echte Hardware-System-Performance (Vergleich zum physikalischen Testbed) nur für Netzwerke von weniger als 25 Knoten erreicht.

Bezüglich des simulierten Radio-Transmitter Moduls wird der IEEE 802.15.4-konforme Funk-Chip CC2420 von TI unterstützt. Die Unterstützung beinhaltet auch ein einfaches Indoor-Radio Modell bzgl. der Funkausbreitung um Received Signal Strength Indicator (RSSI) Werte in der Simulation zur Verfügung zu stellen. Des weiteren wird dem CC2420 Model alle nötigen Parameter zur Verfügung gestellt, um das im IEEE 802.15.4 MAC Layer verwendete CSMA-CA Verfahren anbieten zu können. Die Implementierung wurde ausgiebig mit TinyOS-1.x, TinyOS-2.x, SOS Beispiel-Applikationen getestet, sowie mit der Open-ZB (IEEE 802.15.4-Protokoll-Stack) Referenzimplementierung [2].

Um Avrora zu nutzen, wird ein Rechner mit einer installierten Java Virtual Machine benötigt. Die Software kann samt Quellcode und fertigen JAR-files von den Sourceforge Projektseiten kostenlos heruntergeladen werden. Die Ausführung des Programms erfolgt über die Kommandozeile, wie etwa JAVA -JAR AVRORA.JAR -HELP zur Anzeige der Informationsseite des Programms.

Da wir in dieser Arbeit eine Simulation von drahtlosen Sensornetzen und hier genauer die Funkkommunikation uns näher betrachten wollen, benötigen wir nun noch die auf den Knoten auszuführende Software. Der de-facto Standard für Betriebssysteme auf drahtlosen Sensornetzen ist das TinyOS Betriebssystem. Wir werden im Folgenden davon ausgehen, dass TinyOS Applikationen bereits zur Verfügung stehen. Je nach Umfang und Tiefe der Lehrveranstaltung kann natürlich vor dem Einsatz des Simulators noch eine Einführung in TinyOS gegeben werden, so dass die Studenten zunächst kleinere Applikation (LED an/aus) erlernen und in dem simplen von TinyOS zur Verfügung gestellten Simulator ausführen. Da wir hier jedoch vorrangig die Funkkommunikation eines ZigBee Netzes untersuchen wollen, gehen wir hier davon aus, dass bereits die TinyOS Applikationen den Studenten zur Verfügung gestellt werden. Wir verwenden als Applikation die Standard Beispiele von TinyOS 2.1.1 und der Open-ZB Erweiterung von TinyOS [2]. Hier ist im besonderen die Applikation ASSOCIATIONEXAMPLE zu nennen. Diese Applikation kann genutzt werden, um den typischen Aufbau eines kleinen ZigBee Netzes mit Coordinator und End-Device darzustellen. Der nächste Abschnitt gibt einen Einblick über die Möglichkeiten des Simulators bzgl. der Auswertung der Simulation und der Datenkommunikation.

5.4 ZigBee Monitoring mittels Wireshark

Eines der durch den im MAC Layer des IEEE 802.15.4 Standard unterstützten Merkmale ist die ASSOCIATION PROCEDURE zwischen PAN Coordinator und End-Devices. Ein Überblick über den nötigen Datentransfer laut ZigBee Standard gibt Abbildung 5.4.

Dieses Verfahren ist insofern als einführendes Beispiel hilfreich, dass es einen Angriff auf genau diese ASSOCIATION PROCEDURE gibt. Zuvor ist jedoch dem Studenten die reguläre Funktionsweise des Verfahrens zu erklären. Dies kann am besten anhand einer Avrora Simulation erfolgen.

Die Avrora Simulationsumgebung kennt mehrere Monitor Klassen, um Ergebnisse und Ereignisse der Simulation auszugeben. So gibt es Monitor Klassen für die Ausgabe der LED-Steuerung, des Energieverbrauchs, der Datenübertragung usw., sowie den Monitor

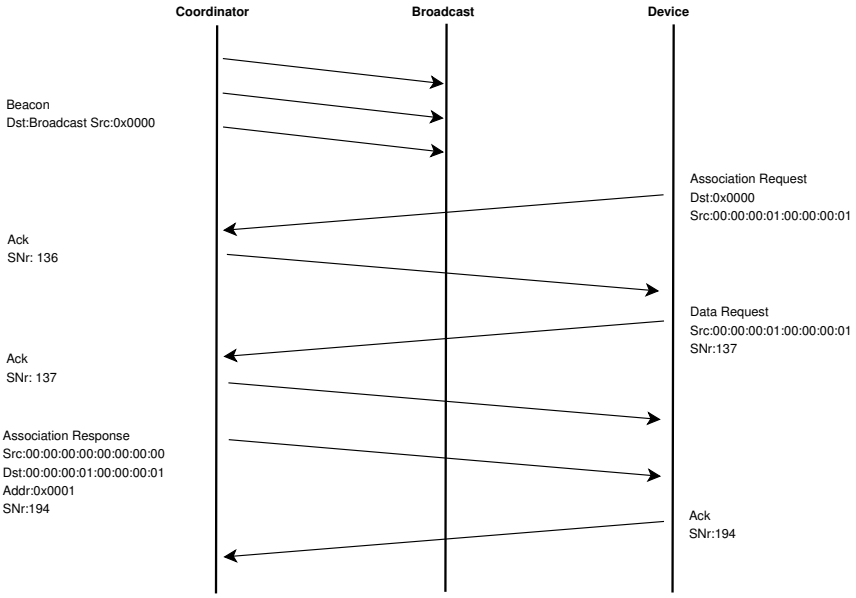

Abbildung 5.4: Flussdiagramm: Datenübertragung bei einer Association Procedure

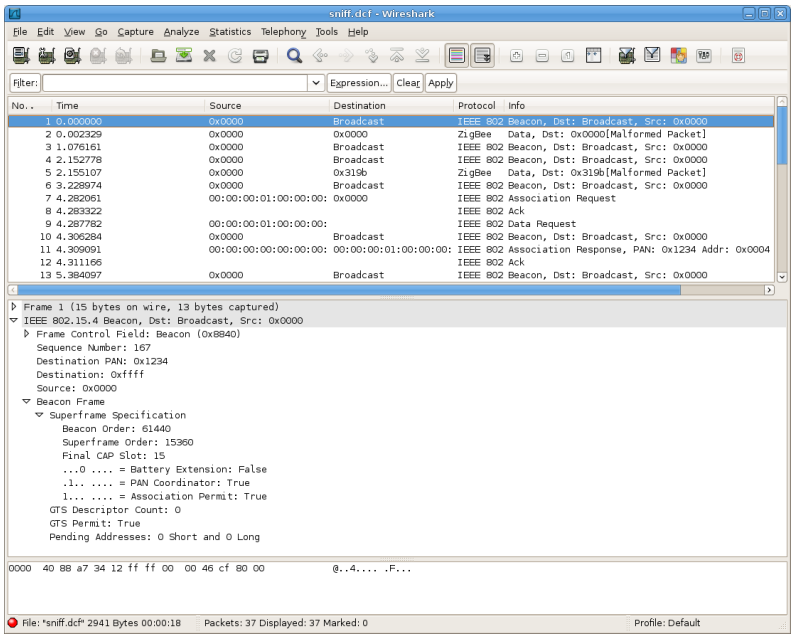

Abbildung 5.5: Protokoll-Analysator Wireshark: Datenübertragung bei einer Association Procedure

SNIFFER. Dieser Monitor erzeugt einen Mitschnitt der Datenkommunikation im Daintree Sensor Network Analyzer Format. Genau dieses Format kann mit dem bekannten Wireshark Protokoll Analysator Programm ausgelesen werden. Wireshark ermöglicht es somit den in der Simulation erzeugten Datenverkehr in Form einzelner Pakete darzustellen. Somit wird dem Student ermöglicht die zur ASSOCIATION PROCEDURE eines ZigBee Netzes benötigte Kommunikation zu sehen. Abbildung 5.5 gibt einen Einblick über die Ansicht der aufgezeichneten Kommunikation. Wireshark kann neben der einfachen Darstellung des Netzverkehrs ebenfalls beim Extrahieren von einzelnen Paketinformationen helfen. Die Informationen des Wireshark Werkzeugs sind hierbei bzgl. ZigBee vollständig, das Protokoll wird von Wireshark offiziell unterstützt.

Die Lernziele dieser ersten Simulation sind die Folgenden:

- Visualisieren und Verstehen von Netz- und Geräte-Verhalten durch eine System-Level-Netz-Analyse.
- Analysieren und Debuggen der zugehörigen Protokolle mit detaillierten Paket-Analyse.
- Verwendung der Werkzeuge für die Entwicklung, Inbetriebnahme und Verwaltung eingesetzter drahtloser Sensornetze.
- Kennenlernen von leistungsstarken und intuitiven Datenübertragungs-Standards, hier ZigBee.

5.5 KillerBee Framework

Das KillerBee Framework wurde von Joschua Wright auf der Toorcoon11 Konferenz vorgestellt und zeigt auf, dass es relativ einfach ist ein ZigBee Netz zu stören oder gar zu manipulieren. KillerBee ist als Open-Source Sammlung von Linux-Tools veröffentlicht und somit frei verfügbar. Es gedacht, um die Sicherheit von Zigbee-Netzen zu Testen. Hierzu sind mehrere Tools in der Sammlung enthalten, die allesamt bekannten Angriffsprogrammen aus dem Bereich WLAN ähneln. Den Grund hierzu ist der Tatsache geschuldet, dass einige Sicherheitsprobleme und deren zugrunde-liegenden Fehler denen von frühen WLAN Protokollen ähneln. So bietet bspw. Zigbee keinen hinreichenden Schutz gegen Replay-Attacken, bei denen mitgeschnittene Pakete wiederholt im Netz versendet werden. Die für uns am bedeutensten Programme der Sammlung sind 'zbgoodfind', 'zbassocflood' und 'zbreplay'. Das Programm 'zbgoodfind' ermöglicht es in abgefangene Übertragungen nach einem Netz-Schlüssel (encryption key) zu suchen. zbreplay ist ein Programm mittels dem abgefangene ZigBee Pakete wiederholt gesendet werden können, bzw. ein 'blackhole' Angriff eingeleitet werden kann. 'zbassocflood' täuscht Knoten vor, um mittels einer Überflutung von 'association-requests' den Controller zu überlasten. Darstellung 5.6 zeigt diesen Angriff schematisch. Hierbei sind die vorgetäuschten Konten durch den Angreifer ('malicious node') derart gewählt, dass der Coordinator diese als legitime neue Knoten ansieht.

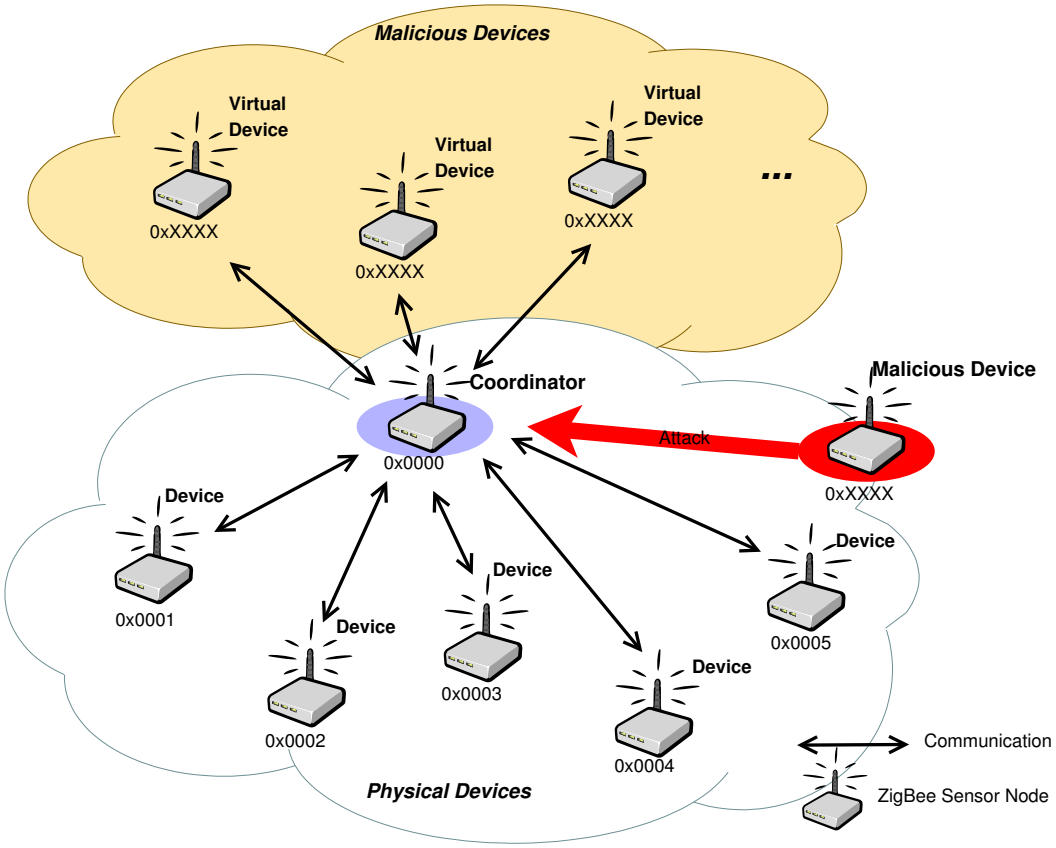

Abbildung 5.6: Struktur des ZigBee 'association-requests' Angriffs.

Zur Nutzung des KillerBee Framework wird Hardware-seitig einen modifizierten AVR RZ Raven USB-Stick benutzt, um eine Verbindung zwischen Rechner und ZigBee-Netz herzustellen. Da wir in unserer Lernumgebung aus Gründen der Wirtschaftlichkeit und der Verringerung der Komplexität des Versuchs eine Simulation nutzen, benötigen wir diese USB-Sticks nicht. In unserem Fall können wir anstelle eines externen Angriffs einen Angriff von Innen nutzen mittels Simulation eine KillerBee Knotens. Bei der Analyse der recht simplen KillerBee Python-Skripte fällt schnell auf, dass die Reimplementierung dieser Art von Angriffen – replay und association-request – mittels eines kleinen TinyOS Programm re-implementiert werden kann. Hierdurch sparen wir uns eine Schnittstelle zwischen Avrora Umgebung und KillerBee Host, ohne auf die Methode der verwendeten Angriffe verzichten zu müssen. Wir haben daher die bereits zuvor verwendetet AssociationExample Applikation um zwei Ausprägungen erweitert.

Um einen replay Angriff zu simulieren, haben wir die besagte Applikation als Basis genutzt. Nach einer erfolgreichen Association mit dem Netz wird im normalen Beispiel-Code ein Datenpaket gesendet und anschließen eine Disassociation vorgenommen. Anstelle ein Datenpaket direkt zu senden wird in der abgewandelten Version zunächst der Empfang eines beliebigen Datenpaketes abgewartet. Da der Sensorknoten als assoziierter Knoten des Netzes jedes Paket vollständig lesen kann, können wir nun dieses Paket direkt erneut versenden. Dies entspricht zwar keinem zielgerichteten Angriff, jedoch ist die Methode dieselbe. In dem durch den Sniffer Monitor erzeugten Datenmitschnitt kann der erfolgreiche Replay-Versuch nun mittels Wireshark analysiert werden. Es ist anzumerken, dass die Si-

mulation des CC2420 ZigBee Controllers in Avrora hier von der Wirklichkeit abweicht, da ein realer ZigBee Transceiver Chip ein Datenpaket mit einer fremden Empfängeradresse direkt verwerfen würde und nicht an den Microcontroller und somit die TinyOS Applikation weiterleiten würde.

Bei dem association-request Angriff des KillerBee Angriffs wird versucht den ZigBee Controller mit einer so hohen Anzahl von request Meldungen virtueller Knoten zu bombardieren, dass entweder der ZigBee Dienst unter der Last zusammenbricht oder aber die Anzahl von verfügbaren Adressen ausgeht und somit kein weiterer legitimer Knoten eine Association erfolgreich durchführen kann. Auch hier haben wir die Beispiel-Implementierung nutzen können, um die Funktionalität des KillerBee Angriffs zu simulieren. Hierzu wird beim Ausführen der TinyOS Implementierung die normalerweise statisch vergebene MAC-Adresse durch eine zufällig gewählte Zahl ersetzt. Wir führen dann die Avrora Simulation mit einem Controller, einem legitimen End-Geräten und einer höhere Anzahl (> 5) von End-Geräten mit modifizierter Applikation durch. Anstelle der im KillerBee simulierten Konten (virtuelle Knoten) können wir hier reelle Knoten der Simulation zuführen, der Effekt ist derselbe. Auch hier können wir wieder mittels Wireshark den Verlauf des Angriffs nachvollziehen. Der Controller sendet seine Beacon Paket aus und alle modifizierten Knoten senden associaten requests aus, die vom Controller bestätigt werden aber nicht entsprechend dem Protokoll von dem End-Gerät beantwortet werden. Durch die sehr hohe Anzahl von Datenpaketen wird zum einen die Wahrscheinlichkeit von Datenkollisonen steigen und zum anderen wird der legitime Knoten nie eine Association bestätigt bekommen. Dies liegt darin begründet, dass die Referenzimplementierung (AssociationExample Applikation) nur einen sehr kleinen Adressraum (4 Geräte in der AssociationExample Applikation) vorsieht. Da die modifizierten Knoten bereits zuvor alle Adressen verbraucht haben, bekommt der legitime Knoten keine ZigBee Adresse mehr zugeteilt.

Lernziele dieser erweiterten Simulation sind die Folgenden:

- Kennenlernen von zwei Angriffsmethoden und ihren Auswirkungen
- Erlernen der Fähigkeit Probleme mittels Paket-Analysator Werkzeug zu erkennen
- Verstehen der Schwächen im Sicherheitskonzept des ZigBee Protokolls

5.6 Byzantinische Fehlertoleranz

Im dritten und letzten Simulations-Versuch soll nun gezeigt werden, dass es möglich ist mit einfachen Mitteln einen Angriff (hier des Replay-Angriff) abzuschwächen. Hierzu wird das Konzept eines byzantinischen Protokolls benutzt, welches auf dem Byzantinischen Generäle Problem aufbaut. In dem von Lamport et al. beschriebenen Byzantinischen Generäle Problem wird die Problematik einer gemeinsamen Entscheidungsfindung beschrieben. Hierbei befehligt ein Kommandierender $n - 1$ Untergebene. Alle Beteiligten können untereinander kommunizieren und Kommunikation zwischen zwei Personen findet über einen synchronen und fehlerfreien Kanal statt. Der Kommandierende teilt allen seinen Untergebenen seine Entscheidung (Angriff oder Rückzug) zu einem Zeitpunkt mit. Die

Aktion wird nur dann als erfolgreich gewertet, wenn alle Untergebenen denselben Befehl (den des Kommandierenden) ausführen. In diesem Szenario ist es jedoch möglich, dass eine oder mehrere Personen versuchen die Aktion zu sabotieren und falsche Meldungen in den Umlauf bringen. Das Ziel des Byzantinischen Protokolls ist es, dass alle ehrlichen Untergebenen zu einer gemeinsamen Entscheidung kommen.

Zwei Beispiele verdeutlichen das Byzantinische Generäle Problem:

- Drei ehrliche Generäle und ein Betrüger
  - Kommandierender teilt seinen Generälen seine Entscheidung mit
  - Jeder General teilt den anderen Generälen die empfangene Nachricht mit
  - Jeder General wird den Angriff einleiten, wenn die Mehrheit der Generäle und der Kommandierende für den Angriff ist.
- Zwei ehrliche Generäle und ein Betrüger
  - Fall 1: Kommandierender ist unehrlich: ein General empfängt den Befehl zum Angriff und der andere General zum Rückzug.
  - Fall 2: Kommandierender ist ehrlich: ein General ist unehrlich und versucht zu betrügen
  - in beiden Fällen können die Generäle die empfangenen Nachrichten (Befehle) nicht verifizieren.

Lamport et al. haben die These formuliert, dass für n Personen mit k Betrügern ein Kommunikations-Protokoll existiert, welches zu einer gemeinsamen Entscheidung führt genau dann wenn $n \geq 3k + 1$. Der Beweis dieser These kann in [3] nachgelesen werden.

Die Applikation der Simulation wird umgebaut, so dass die Applikation nur auf Grundlage einer Mehrheitsentscheidung eine Aktion ausführt. Hierzu hat der Student bspw. die gegebene Applikation aus Kapitel 5.5 zu erweitern. Als Aktion kann z.B. die Aktivierung einer LED auf dem simulierten Sensorboard dienen. Diese Aktivierung soll nur dann stattfinden, wenn mindestens 4 End-Devices ein Datenpaket (per Broadcast) mit derselben Information senden. Ein einfacher replay-Angriff wird daher nicht zum Erfolg führen. Nur wenn 4 Datenpakete aus unterschiedlichen Quellen ankommen, wird erfolgreich die Aktion gemeinsam ausgeführt, die LED wird aktiviert. Der Student kann somit neben den Auswirkung des Angriffs hier die Möglichkeit einer Gegenmaßnahme erlernen.

5.7 Schlussbetrachtung

In der Lehre ist es häufig erforderlich zum einen aktuelle und spannende Themen aufzugreifen aber zum anderen auch diese den Studenten geeignet zu vermitteln. Eine Demonstration von Kommunikationsabläufen sicherheitskritischer Datenkommunikation und insbesondere die Erklärung der Funktionsweise von Angriffen auf selbige anhand einer Simulation erhöht den Lerneffekt. Die in diesem Beitrag aufgezeigte Sicherheits-Problematik

des ZigBee Protokolls ist ein aktuelles Thema. Die vorgeschlagenen Simulationen können bspw. im Unterricht oder bei Beteiligung der Studenten in einem Praktikum verwendet werden, um die Aspekte der IT-Sicherheit dem Studenten nahezubringen. Wir haben die Erfahrung gesammelt, dass der Drei-Satz Erkennen, Analysieren, Absichern den besten Lerneffekt erzielt. So sind die drei vorgestellten Simulationen in genau dieser Reihung zu sehen. Die erste Simulation schult das Erkennen der Problematik, die zweite Simulation vermittelt eine Analyse des Angriffs (hier KillerBee) und letztendlich wird in der dritten Simulation die Absicherung des Netzes anhand eines Beispiels erlernt. Weitere Angriffe auf ZigBee Netze sind möglich, so kann bei Interesse die Simulationsaufgabe nach belieben noch erweitert oder ausgebaut werden.

Literaturverzeichnis

[1] Paolo Barontib, Prashant Pillaia, Vince W. C. Chooka, Stefano Chessab, Alberto Gottab und Y. Fun Hu. *Wireless Sensor Networks: A Survey on the State of the Art and the 802.15.4 and ZigBee Standards.* Computer Communications, 30(7):1655–1695, 2007.

[2] Andre Cunha, Anis Koubaa, Ricardo Severino und Mario Alves. *OpenZB: an opensource implementation of the IEEE 802.15.4/ZigBee protocol stack on TinyOS.* IEEE International Conference on Mobile Adhoc and Sensor Systems Conference:1–12, 2007.

[3] Leslie Lamport, Robert Shostak und Marshall Pease. *The Byzantine Generals Problem.* ACM Transactions on Programming Languages and Systems, 4:382–401, 1982.

[4] *Crossbow Technology.* Homepage, 2011.

[5] Benjamin Lawrence Titzer, Todd Millstein und Rupak Majumdar. *Avrora – the AVR Simulation and Analysis Framework*, Master Thesis, 2004.

Abkürzungsverzeichnis

ACL	Access Control List.
AES	Advanced Encryption Standard.
APL	Application Layer.
APS	Application Support Sub-Layer.
BPSK	Binary Phase Shift Keying.
CBC	Cipher Block Chaining.
CSMA/CA	Carrier Sense Multiple Access with collision Avoidance.
CTR	Counter Mode.
DoS	Denial of Service.
DSSS	Direct-Sequence-Spread-Spectrum.
FFD	Full Functional Device.
IEEE	Institute of Electrical and Electronics Engineers.
MAC	Message Authentication Code.
MAC	Media Access Control.
nonce	number used once.
NWK	Network Layer.
QPSK	Quadrature Phase Shift Keying.
RFD	Reduced Functional Device.
SKKE	Symmetric Key Key Establishment.
SSP	Security Service Provider.
WPAN	Wireless Personal Area Networks.
ZDO	ZigBee Device Object.

ZED	ZigBee End Device.