Vergleich aktueller LPWAN-Technologien im Internet der Dinge unter Einbindung von Energy-Harvesting

Bachelor Thesis

im Studiengang Medien und Informationswesen

von

Tom Martin Jung

Sommersemester 2017

Hochschule Offenburg, Fakultät M+I

Erstbetreuer: Prof. Dr. Tom Rüdebusch

Zweitbetreuer: Prof. Dr. Volker Sänger

Abstract

Die vorliegende Bachelorthesis gibt einen Überblick über die Möglichkeiten zur drahtlosen Machine-to-Machine Kommunikation im Internet der Dinge. Sie bietet eine Einführung in die Low-Power-Wide-Area-Network-Technologie (LPWAN) und einen Vergleich deren Anbieter.

Zu Beginn der Arbeit wird die Funktionsweise der drahtlosen Datenübertragung erklärt und die wichtigsten Fachbegriffe werden erläutert. Anschließend werden die Technologien Short-Range Wireless Network, Mobilfunk und Low-Power-Wide-Area-Network voneinander differenziert und einige Standards jeder Kommunikationstechnik vorgestellt.

Anschließend wird konkreter auf die Funktionsweise der aussichtsreichsten LPWAN-Technologien eingegangen. Nach der Erläuterung der Funktionsweisen werden die Übertragungstechniken der Anbieter LoRa Alliance, SigFox, Ingenu und EnOcean anhand festgelegter Parameter untersucht und anhand eines Bewertungsschemas verglichen. Dabei zeigte sich, dass die Anbieter im Vergleich über verschiedene Ansätze zum Einsatz der LPWAN-Technologie verfügen und diese zudem von allen unterschiedlich umgesetzt wird. Aus dem Vergleich wurde jedoch deutlich, wo die Stärken und Schwächen der einzelnen Technologien liegen.

Ein kurzer Exkurs in das Thema des Energy-Harvesting – Der Technologie zur Stromerzeugung aus Umweltressourcen – zeigt die möglichen Umsetzungsarten der neuartigen Energiegewinnung und deren Einsatzgebiete für technische Geräte im Internet der Dinge.

Die Dokumentation eines Beispielprojekts beschreibt die Umsetzung einer solarbetriebenen LoRaWAN-Sendeeinheit, welche in der Lage ist die GPS-Daten ihrer Position über eine freie Funkfrequenz an ein LoRaWAN-Gateway in der Umgebung zu senden. Das Gateway interpretiert die Daten und stellt diese mithilfe eines Webdienstes auf einer interaktiven Karte dar.

Inhaltsverzeichnis

Darstellungsverzeichnis

Abkürzungsverzeichnis

LPWAN	Low-Power-Wide-Area-Network
3GPP	Third Generation Partnership Project
ABP	Activation-by-Personalization
AES	Advanced Encryption Standard
ARQ	Automatic Retransmission Requests
BBR	Bluetooth Basic Rate
BEDH	Bluetooth Enhanced Data Rate
BLE	Bluetooth with low energy funcionality
BNetzA	Bundesnetzagentur
CDMA	Code Division Multiple Access
CoAP	Constrained Application Protocol
CRC	Cyclic Redundancy Check
DBPSK	Differential Binary Phase Shift Keying
DDoS	Distributed Denial of Service
IDE	Integrated Development Environment
DSSS	Direct Sequence Spread Spectrum
EEP	EnOcean Equipment Profiles
FCC	Federal Communications Commission
FEC	Forward Error Correction
FTP	File Transfer Protocol
GFSKM	Gaussian Frequency Shifting Key Modulation
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
ISM	Industrial, Scientific and Medical
ISO	International Organisation for Standardization
ITU	International Telecommunication Union
LAN	Local Area Network
LBT	Liste-before-Talk
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Media Access Control
MHDR	Message Header
MIC	Message Integration Code
MISO	Master In Slave Out
MOSI	Master Out Slave In
MQTT	Message Queue Telemetry Transport Protocol
NB-IoT	Narrowband-Internet of Things
NFC	Near Field Communication

OSI	Open Systems Interconnection Model
OTAA	Over-the-Air-Activation
REST	Representational State Transfer
RFID	Radio Frequency Identification
RPMA	Random Phase Multiple Access
RSSI	Receive Signal Strength Indicator
SCK	Serial Clock
SF	Spreading Factor
SIG	Special Interest Group
SMTP	Simple Mail Transfer Protocol
SNR	Signal-Noise-Ratio
SPI	Serial Peripheral Interface
SRD	Short Range Device
TCP	Transmission Control Protocol
TKG	Telekommunikationsgesetz
TSG CT	Technical Specification Group Core Network & Terminals
TSG RAN	Technical Specification Group Radio Access Network
TSG SA	Technical Specification Group Service & System Aspects
UART	Universal Asynchronous Receiver Transmitter
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
WLAN	Wireless-Local-Area-Network

Einleitung

Diese Arbeit handelt von Low-Power-Wide-Area-Networks (LPWANs, deutsch: Niedrigenergie-Weitverkehr-Netzwerk) und deren mögliche Verwendung im Internet der Dinge. Neben Mobilfunk und den gängigen WiFi- und Bluetooth-Lösungen sind diese speziell für Sensoranwendungen im Internet der Dinge entwickelt worden und bieten viele Vorteile dafür. Solche Netzwerke sollen in der Lage sein, durch die Zufuhr von geringen Mengen an Energie sogar Jahrelang autark arbeiten zu können. Es soll gezeigt werden, wie ein solches Netzwerk aufgebaut werden kann, welche Technik und Grundkenntnisse dafür vorhanden sein sollten und was man zusätzlich dazu noch benötigt.

Da es sich in Kombination mit dem Internet der Dinge noch um ein recht neues Feld handelt, wird die Entwicklung der letzten Jahre sowie der derzeitige Verbreitungsstand aufgezeigt. Zusätzlich soll zusammengefasst werden, welche Möglichkeiten derzeit existieren, energiesparende Funknetzwerke mit hoher Reichweite für das Internet der Dinge zu nutzen und dazu einige Use-Cases von bereits möglichen Implementationen vorzustellen.

Weiterhin wird beleuchtet wer die derzeitig führenden Anbieter von LPWAN-Technologien sind, aus welchem wirtschaftlichen Hintergrund sie kommen und welche technischen sowie strukturellen Unterschiede zwischen ihnen existieren. Hierbei wird auf mehrere Faktoren eingegangen, welche sich als Vor- und Nachteile bei der Nutzung der verschiedenen Technologien ergeben. Im Zuge des Anbietervergleichs wird ein Anbieter ausgewählt und die Implementierung einer beispielhaften Anwendung durchgeführt und dokumentiert, um so einen Leitfaden zur Erstellung eines LPWAN-Netzwerkes zu erhalten. Bei der Anwendung handelt es sich um einen solarbetriebenen Notrufsender, welche mittels dieser Technologie in Notfällen ihre Position an einen Server weitergeben können.

Zusätzlich wird untersucht, wie weit der derzeitige Entwicklungsstand energiesammelnder Techniken im Internet der Dinge (Energy-Harvesting) ist und ob es möglich ist, LPWAN-Funknetzwerke mittels dieser Technologie mit Strom zu versorgen. Versucht wird hierbei ein funktionierendes Energy-Harvesting-System in die im Zuge der Arbeit dokumentierten Implementation einzusetzen um die Sensorstationen möglichst autark zu versorgen.

1. LPWAN – Low Power Wide Area Networks

1.1. Das Internet der Dinge

Mit der Vernetzung von Sensoren und dem Einbinden der Gerätesteuerung vielerlei Haushalts- und Industriemaschinen in das Internet war die Technologie des Internets der Dinge (Internet of Things, IoT) geboren. Physische Objekte werden so digitalisiert und in das mit dem Internet verbunden. Zahllose Geräte können mittlerweile miteinander kommunizieren und über standortunabhängige PCs und Mobilgeräte von überall auf der Welt gesteuert werden. Auch die autonome Gerätesteuerung durch Algorithmen, die ihre Parameter durch eingebundene Sensornetzwerke erhalten ist keine Neuheit mehr und ermöglicht beispielsweise einem Smart Home, wetterbedingt die Heizanlage sowie die Fenstersteuerung des Hauses anzupassen.

Der Begriff „Internet der Dinge“ wurde erstmalig Anfang der 90er Jahre von Forschern dies Massachusetts Institute of Technology (MIT) verwendet. Damals handelte es sich jedoch noch um eins der ersten RFID-Netze (Radio-Frequency-Identification), welches Computern ermöglichte durch ein programmiertes Verständnis der Umwelt selbst Daten zu sammeln. RFID wurde hier als intelligente Lokalisierungstechnik verwendet, sodass Sensoren und Geräte sich selbst identifizieren und Auskunft über ihren Status sowie ihren Standort geben konnten. [1]

1.1.1. Entwicklungen im Internet der Dinge

Das Internet der Dinge ist im Verlauf des letzten Jahrzehnts immer mehr in den Fokus der Wirtschaft und der Industrie gerückt. Sensordaten von Geräten und anderen physischen Objekten die über das Internet übertragen und ausgewertet werden, erlauben sowohl Firmen, als auch privaten Anwendern eine genaue und angepasste Steuerung von Prozessen und Geräten, ohne dass sie selbst anwesend sein müssen. Der nächste Schritt wäre nun, ganze Städte und Länder, oder Anwendungsgebiete ohne Heim- oder Firmennetzwerk mit Netzstrukturen auszustatten, welche das Internet der Dinge nutzen kann. Natürlich ist die Verbindung zum Internet dank moderner Mobilfunktechnik mittlerweile so gut wie überall möglich, jedoch würden für die Einbindung einer hohen Anzahl von Sensoren hohe Verbindungskosten entstehen. Zudem gibt es Bereiche, an denen auch Mobilfunk nicht zuverlässig oder überhaupt nicht senden kann, wie in unterirdischen Anlagen wie Kanalisationen oder großen Gebäudekomplexen. Zusätzlich zu den Vorteilen der Lokation solcher Sender und deren Anbindungskosten in bestehende Funknetze spielt immer die Stromversorgung der Sendeeinheiten eine große Rolle. Aus diesem Grund werden immer häufiger Sensoren mit aus der Umgebung generiertem Strom betrieben.

1.1.3. Kritik am Internet der Dinge

Neben allen Vorteilen die das Internet der Dinge bietet, werden im Verlauf der letzten Jahre die kritischen Stimmen zu der Technologieneuheit immer lauter. Besonders die häufig mangelnden Sicherheitsvorkehrungen von älteren IoT-Geräten wird hierbei kritisiert. Ein großflächig angelegter DDoS-Angriff im Jahr 2017 wurde auf die Ausnutzung von Schwachstellen in der Kommunikation älterer Smart Home- und Haushaltsgeräten zurückgeführt. Die Welle an Kritik die durch solche Angriffe aufkam, betitelte nun das Buzzword der IT-Branche als das „Internet der kaputten Dinge“ und sprach im Zuge der Hacker-Angriffe vom „Angriff der Toaster“.

1.1.4. Aussicht auf Entwicklungen von Funktechnologien im Internet der Dinge

In Zukunft werden drahtlose Technologien zur Informationssammlung und Steuerung von Prozessen immer weiter in den Vordergrund rücken. Statt Lichtschalter in das Stromnetz des Hauses einzubringen, können bereits heute kabellose Schalter angebracht werden, die durch die Generierung ihres eigenen Übertragungsstroms diverse Geräte und Lampen an- und ausschalten können. Zudem werden bereits von vielen Unternehmen intelligente Glühbirnen angeboten, die über WLAN mit Smart-Home-Anwendungen wie Assistenten (Siri, Alexa, Cortana) oder Apps in ihrer Helligkeit oder Farbe gesteuert werden können.

Passive WiFi

Einige interessante Entwicklungen führen auch darauf zurück, Spezifikationen eines drahtlosen Systems nicht nutzen zu können. So beispielsweise das sogenannte Passive WiFi. Dieses soll es Geräten ermöglichen, ohne die Konnektivität zu einem Accesspoint in der Nähe herstellen zu können, die WLAN-Signale in der Umgebung zu verarbeiten und auszuwerten. So soll es möglich sein, Geräte die WLAN-Signale ausstrahlen zu orten, indem die Quelle eines Funksignals gesucht oder dessen Signalstärke in Relation zum Ort gesetzt wird. Würde man es nun noch schaffen, die Signale einer bestimmten Quelle in ein Muster zu bringen und einer Person zuzuordnen, könnte diese Person allein durch ihre WLAN-Spur getracked werden. [2]

Vollduplex im IoT mit LoRa

Ein großes Problem von Single-Channel Funkstrecken ist die sogenannte self-interference, die ein Senden im Vollduplexmodus verhindert. Self-interference bedeutet, dass ein sendendes Gerät gleichzeitig immer ein wenig der Energie des gesendeten Funksignals im eigenen Receiver-Modul empfängt und durch dieses starke Störgeräusch nicht in der Lage ist, andere Signale während des Sendevorgangs zu empfangen. Man kann dieses mit dem Versuch gleichsetzen, ein Flüstern zu hören, während man selbst laut schreit.

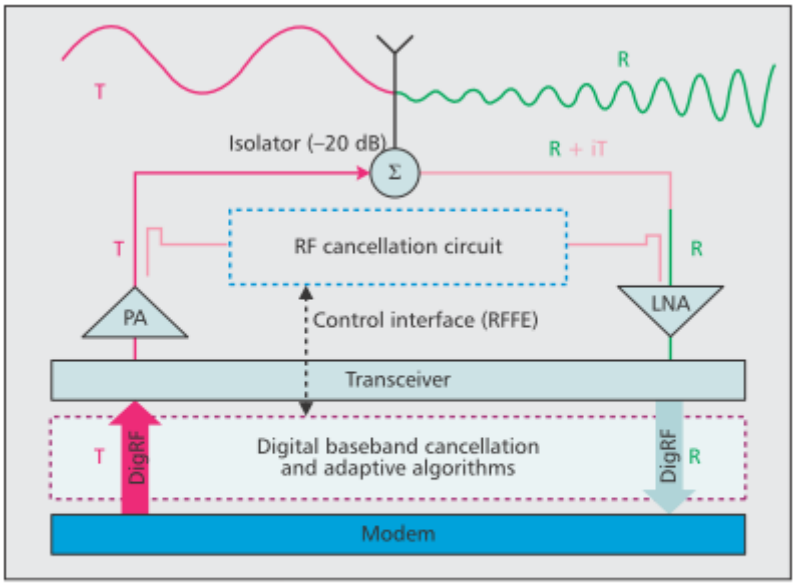


Figure 2. *Analog cancellation (shown in blue) is necessary to prevent receiver saturation (~50–80 dB). Once within the dynamic range of the receiver, digital cancellation (shown in purple) can handle the remaining distortions (~60 dB).*

Darstellung 1. Schaltskizze zur Aufhebung der Eigeninterferenz, Kumu Networks/Standford University [3]

Die Standford University hat in Zusammenarbeit mit der Firma Kumu Networks eine Möglichkeit gefunden, in Systemen die von einem Single-Channel-System profitieren würden, diese self-interference auszugleichen. Dazu wird das Sendesignal und das daraus resultierende Störsignal in der Transceiver-Einheit aufeinander moduliert und gegenseitig aufgehoben. Dies öffnet einen größtenteils rauschfreien Bereich für eingehende Signale, auch während des Sendevorgangs. Die skizzierte Funktionsweise der Technik wird in Darstellung 1 gezeigt.

Entwickelt wurde diese Technologie hauptsächlich für die Störfeldreduzierung im zukünftigen 5G-Mobilfunk, jedoch sind bereits Anwendungen für Kurzstreckenfunktechnologien wie WLAN oder Bluetooth und sogar für Mesh-Netzwerke sowie Low-Power-WANs im Anwendungsbereich dieser Technologie und werden derzeit erforscht. [2]

Besonders interessant ist diese Technologie für das Internet der Dinge, da sie es Single-Channel-Systemen das Senden im Vollduplexmodus ermöglicht, was sich wiederum auf den Preis pro Einheit in einem Smart-Home oder einer ähnlichen Anwendung auswirken dürfte.

1.2. Drahtlose Übertragung im Internet der Dinge

1.2.1. Grundlagen der Datenübertragung in Netzwerken

1.2.1.1. Protokolle und Protokollschichten

Wenn Geräte Teil eines Netzwerkes werden sollen, müssen sie durch das Ermöglichen der gegenseitigen Kommunikation zuerst netzwerkfähig gemacht werden. Die Herstellung einer Kommunikationsverbindung in Netzwerken ist die Aufgabe von Computernetzwerkprotokollen. Sobald mindestens zwei Geräte in die Aufgabenabwicklung in einem Netzwerk involviert sind, verwenden ihre Hardware- und Softwareschnittstellen Protokolle. Ein Protokoll umfasst den Ablauf und die Regeln der Netzwerkkommunikation, beschreibt in welcher Form die Daten weitergeleitet werden, die Reihenfolge sowie die Größe der zu sendenden Pakete. Kurose und Ross fassen diesen Vorgang wie folgt zusammen:

„Ein Protokoll definiert das Format und die Reihenfolge des Nachrichtenaustausches zwischen zwei oder mehr kommunizierenden Entitäten sowie die Handlungen, die bei Übertragung und/oder Empfang einer Nachricht oder anderer Ereignisse ausgeführt werden.“ – Kurose und Ross [4]

Um die Kommunikation zu strukturieren, werden Protokolle Netzwerkschichten zugeordnet. Jede Schicht sowie das dazugehörige Protokoll erfüllen eine spezielle Aufgabe. Während so zum Beispiel die unterste Schicht für die physikalische Übertragung der Bitströme über die Leitungen verantwortlich ist, werden andere Schichten für Aufgaben von der Ziel-Adressierung bis hin zur Darstellung des Paketinhalts in der Endanwendung benötigt. Jede Schicht verpackt bei dieser Vorgehensweise die tieferliegende Schicht und muss bearbeitet werden, bevor auf die so verpackten Schichten zugegriffen werden kann. Bei der Datenübertragung im Internet gibt es besonders drei Modelle dieser Schichtenarchitektur, auf die Kommunikation im Netz aufgebaut ist. Das TCP/IP-Referenzmodell, der fünfschichtige Internet-Protokollstapel, als auch das ISO/OSI-Referenzmodell. Um zu verstehen, an welcher Stelle die in dieser Arbeit vorgestellten Protokolltechniken ansetzen, werden im folgenden Teil zuerst diese Modelle erläutert und anschließend kurz existierende Protokolle zur drahtlosen Kommunikation vorgestellt. [4]

1.2.1.2. TCP/IP-Referenzmodell

Das für das Internet unabdingbare TCP/IP-Schichtenmodell wurde in den 70er Jahren vom Department of Defense der USA entwickelt. Es beschreibt den Aufbau des Protokollturms in vier Schichten: Netzzugang, Internet, Transport und Anwendung. Per Definition sind diese Schichten voneinander getrennt, was bedeutet, dass die für die Ausführung der Aufgaben genutzten Protokolle ausgetauscht und frei aus der großen Protokollvielfalt jeder Schicht gewählt werden können. Die zu sendenden Daten, Nachricht genannt, erhalten für jede Schicht einen Header, der die für die Schicht notwendigen Informationen enthält. Manche Protokolle, zumeist der Netzzugangsschicht zugehörig, hängen zusätzlich zum Header am

Beginn der Nachricht ein abschließendes Informationspaket an. Hier spricht man von einem sogenannten Trailer. [5]

1.2.1.3. Fünfschichtiger Internet-Protokollstapel / Hybrides Referenzmodell

Der fünfschichtige Internet-Protokollstapel, auch hybrides Referenzmodell genannt, baut auf dem TCP/IP-Referenzmodell auf, unterscheidet sich jedoch durch die Aufteilung der Netzzugangsschicht in zwei eigenständige Schichten sowie durch die Umbenennung der Internetschicht zur Vermittlungsschicht. Aus der Netzzugangsschicht des TCP/IP-Referenzmodells werden die Bitübertragungsschicht sowie die Sicherungsschicht des hybriden Referenzmodells. [5]

1.2.1.4. ISO/OSI-Schichtenmodell

In den späten 70er Jahren wurde von der internationalen Organisation für Standardisierung (ISO) vorgeschlagen, Computernetzwerke in sieben statt fünf Schichten aufzuteilen. Sie nannte dies die Open Systems Interconnection Norm (OSI). Gegenüber dem hybriden Referenzmodell, wurde das OSI-Schichtenmodell zwischen der Anwendungsschicht und der Transportschicht um zwei weitere Schichten ergänzt, die Darstellungs- und die Kommunikationssteuerungsschicht. Dieses Modell wurde bei seiner Einführung stark in Forschung und Lehre verwendet, verlor jedoch mit dem Aufkommen des Internets mehr und mehr an Bedeutung, da die ursprünglichen Aufgaben der zwei zusätzlichen Schichten ohne Weiteres in den Aufgabenbereich der Anwendungsschicht übertragen werden konnten. Die Darstellungsschicht enthielt Protokolle zur Datenkompression, -verschlüsselung und -beschreibung. Bei der Datenbeschreibung handelte es sich um die Beschreibung der Interpretation der im Datenpaket vorhandenen Dateiformate, die je nach Gerät oder Betriebssystem variieren kann. Die Kommunikationssteuerungsschicht beschreibt die Struktur und Synchronisation des Datenaustausches und umfasst Sicherungs- und Wiederherstellungsschemata.

Dass im fünfschichtigen Internetprotokollstapel diese zwei Schichten fehlen, lässt sich damit begründen, dass nicht jede Anwendung auf die Dienste der Schichten angewiesen ist. Es ist somit jedem Anwendungsentwickler überlassen, welche Funktionalität die Ebene der Anwendungsschicht umfassen soll. [4]

1.2.1.5. Schichten des Internetprotokollstapels und ihre Aufgaben

Im Folgenden werden die Schichten des Internetprotokollstapels und ihre Aufgaben im sogenannten Top-Down-Ansatz beschrieben und erläutert. Dies bedeutet, dass mit der Anwendungsschicht begonnen und mit der Bitübertragungsschicht abgeschlossen wird.

Anwendungsschicht

In der Anwendungsschicht finden sich die Protokolle die von Anwendungen im Netzwerk genutzt werden. Mit die bekanntesten Protokolle des Internets finden sich in dieser Schicht, sei es das HTTP-Protokoll (Hypertext Transfer Protocol), welches den Geräten ermöglicht Webdokumente anzufordern oder zu übertragen, das FTP-Protokoll (File Transfer Protocol) zum Versenden großer Dateien oder das SMTP-Protokoll (Simple Mail Transfer Protocol) zum Verschicken von Email-Nachrichten. [4]

Transportschicht

Die Transportschicht ist im Internet die erste Schicht deren Dienste auf die Nachricht der Anwendungsschicht gesetzt wird. Die Protokolle dieser Schicht trennen die Nachricht beim Sender in kleinere Teilstücke, in sogenannte Segmente auf und fügen einen Header mit den notwendigen Informationen an. Dieser Header enthält neben den Informationen zum korrekten Zusammensetzen der Nachricht zum Beispiel auch die Portnummer der Anwendung bei der die Nachricht beim Empfänger ankommen soll. Dort werden diese Segmente wiederum erkannt und können anhand des zugehörigen Headers korrekt zusammengesetzt werden. Die zwei hierbei genutzten Protokolle TCP (Transmission Control Protocol) und UDP (User Datagram Protocol) unterscheiden sich in der Art der Übertragung.

TCP ist ein verbindungsorientierter Dienst. Dies bedeutet, dass Client und Server vor dem Senden der Daten bereits Transportschicht-Steuerinformationen ausgetauscht haben, welche beide Parteien auf die Übertragung vorbereiten. Zudem bietet es neben der reinen Datenübertragung zusätzliche Funktionen wie Flusskontrolle, Überlastkontrollmechanismen und die Erkennung und Behebung von verlorengegangenen Paketen an. Die Flusskontrolle stimmt dabei die Sende- und Empfangsgeschwindigkeiten der Parteien während der Übertragung aufeinander ab. Ist das Netz aufgrund von erhöhtem Netzverkehr überlastet, kann dies der Kontrollmechanismus erkennen und die Übertragungsrate koordiniert zurückfahren. Aufgrund spezieller Felder im TCP-Header kann eine Prüfsumme gebildet werden, die sicherstellt, dass alle Segmente der Nachricht angekommen sind. Da zusätzlich die Ankunft der Segmente an den Sender quittiert werden, wird TCP als zuverlässig bezeichnet.

UDP hingegen gilt als verbindungsloser, unzuverlässiger und minimaler Dienst. Dieses Protokoll baut vor dem Übertragungsvorgang keine Verbindung zwischen den partizipierenden Parteien auf. Es verfügt im Gegensatz von TCP über keine Flusskontrolle oder Überlastkontrollmechanismen. Also ist es möglich, dass Pakete in beliebiger Geschwindigkeit beim Client ankommen können und keinerlei Rücksicht auf überlastete Verbindungen genommen wird. Außerdem können Pakete in einer anderen Reihenfolge ankommen, als sie vom Server gesendet wurden. Da das Protokoll über keinerlei Quittierungsmechanismus verfügt, kann die Übertragung eines Segments nie garantiert werden. UDP kann jedoch ebenfalls mittels einer mitgesendeten Prüfsumme bestimmen, ob alle Segmente einer Nachricht angekommen sind. Echtzeitanwendungen wie IP-Telefonie legen hohen Wert auf konstante Übertragungsraten und können einen gewissen Paketverlust tolerieren, bevor ein Qualitätsverlust spürbar wird. Gerade aus diesem Grund ziehen diese Anwendungen das leichtgewichtige UDP-Protokoll dem zuverlässigen TCP vor. [4]

Netzwerk- Vermittlungs- oder Internetschicht

Die nächste Schicht im Protokollstapel ist die Netzwerkschicht. Sie ist für die korrekte Weiterleitung der Pakete im Internet zuständig. Die Pakete der Vermittlungsschicht werden auch Datagramme genannt. Das zuständige Protokoll für die Adressierung und Weiterleitung der Datagramme ist das IP (Internet Protocol). So wie TCP und UDP das Paket

dem korrekten Zielprozess beim Empfänger zuordnen können, ist IP in der Lage den korrekten Empfänger durch die IP-Adresse zuzuordnen. Alle Geräte die im Internet kommunizieren benötigen eine IP-Adresse, um adressiert werden zu können.

Während es zur Adressierung und Weiterleitung im Internet nur das IP-Protokoll gibt, finden sich zahlreiche Routing-Protokolle, die ebenfalls auf der Netzwerkschicht arbeiten. Diese Protokolle verwenden verschiedene Ansätze, um den effizientesten oder sichersten Weg zu etablieren, den das Datagramm nehmen könnte. [4]

Sicherungsschicht

Die Sicherungsschicht, auch Media-Access-Control (MAC) genannt ist dafür zuständig, das eintreffende Paket von einem Netzknoten zum nächsten zu leiten, bis der Empfänger erreicht ist. Die Dienste, die im speziellen auf das Datagramm angewendet werden, unterscheiden sich je nach der Art des eingesetzten Protokolls. In dieser Schicht werden die Datagramme in Rahmen (Frames) verpackt und beispielsweise mittels der Protokolle Ethernet oder WLAN übertragen. Auf dem Weg vom Sender zum Empfänger ist es durchaus möglich, dass ein Rahmen mehrere verschiedene Leitungen und somit meist auch verschiedene Übertagungsprotokolle passiert, bevor er ankommt. Die Adressierung findet hierbei über die MAC-Adresse statt, welches die eindeutig identifizierbare, physische Adresse eines Netzwerkgerätes darstellt.[4]

Gerade für IoT-Anwendungen ist diese Schicht von besonderer Wichtigkeit, da ein Großteil der IoT-Protokolle diese Schicht nutzen.

Bitübertragungsschicht

Während die Sicherungsschicht ganze Rahmen an Daten von einem Host zum anderen transportiert, befasst sich die Bitübertragungsschicht mit der reinen Binär-Übertragung einzelner Bits. Die hier verwendeten Protokolle müssen auf das zu verwendende Übertragungsmedium, wie Kupferkabel, Glasfaser oder Koaxialkabel angepasst werden. So sieht Ethernet für jedes Übertragungsmedium beispielsweise ein anderes Protokoll zur Bitübertragung vor. [4]

Bei LPWAN-Anwendungen findet diese Übertragung natürlich nicht über Kabel statt, sondern über Funkverbindungen. Je nach Anbieter unterscheiden sich die genutzten Übertragungsarten in verschiedenen Parametern wie der Modulation oder dem genutzten Frequenzband. Was hinter den wichtigsten dieser Begrifflichkeiten steht, wird im folgenden Abschnitt erläutert.

1.3. Funknetz als LPWA-Netzwerk

1.3.1. Allgemein

Die Nutzung von Funk als Technologie zur Netzwerkerstellung ist keine neue Idee, viele Anwendungen nutzen bereits Funknetzwerke in Industrie- und Heimelektronik. Dennoch muss geklärt werden, wie ein Funknetz funktioniert und welche Regeln und Gesetze bei einem solchen Vorhaben Anwendung finden. Ob Funk zur Sprachkommunikation, Daten- oder Signalübertragung in Netzwerken genutzt wird, ist hierbei beispielsweise irrelevant. Per Gesetz ist es jedoch von Relevanz, welche Frequenzen im Speziellen von dem Anwender genutzt werden. Bevor ein LPWAN eingerichtet wird, sollte sich der zukünftige Betreiber darüber informieren, welche Rechte in seinem jeweiligen Land gelten und welche Funkfrequenzen ihm zur Verfügung stehen.

1.3.2. Funk in Deutschland

Funkfrequenzen werden in Deutschland von der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) reguliert und verwaltet. Als zuständige Behörde bestimmt sie, welche Frequenzbereiche für welchen Zweck eingesetzt werden dürfen. Zudem hat die Behörde die Entscheidungshoheit über die Zuteilung von Genehmigungen zur Funkübertragung auf den bestimmten Frequenzen. Bekommt jemand oder ein Verwendungszweck eine solche Berechtigung zugeteilt, spricht man von einer Frequenzzuteilung. Das besondere an LPWANs ist, dass diese ihre Übertragung über freie, der Allgemeinheit zugänglichen Frequenzbändern abwickeln. Anwender müssen also keine teure Funklizenz erwerben oder sich eine persönliche Frequenz reservieren lassen. Die Bundesnetzagentur hat auf ihrer Seite zum Thema Allgemeinzuteilungen ausgeschrieben:

„Frequenzen können der Allgemeinheit zugeteilt werden (sog. Allgemeinzuteilung). Damit wird einerseits eine größtmögliche Flexibilität für den Einsatz der Frequenzen geschaffen. Auf der anderen Seite müssen jedoch eventuelle Störungen bei der gemeinsamen Nutzung einer Frequenz durch andere Nutzer in Kauf genommen werden.“

In Deutschland werden Funkfrequenzen zwar von der BNetzA verwaltet, diese orientiert sich dabei jedoch an die Bestimmungen des deutschen Telekommunikationsgesetzes (TKG). Die entsprechende Passage zur Allgemeinzuteilung von Funkfrequenzen findet sich im §55 TKG.

Anmerkungen zum Gesetz umfassen neben der Regulierung von Frequenzzuteilungen zusätzlich Regularien zur zeitlichen Belegung dieser Frequenzen. So ist es in Deutschland lediglich gestattet 1% des 868MHz-Funkspektrums pro Stunde zu belegen, was einer Sendedauer von etwa 36 Sekunden auf eine Stunde gerechnet gleichkommt. Als Gegenmaßnahme ist jedoch erlaubt, mehr zu senden, wenn eine Listen-before-Talk-Funktionalität implementiert wurde. Dies bedeutet, dass ein Gerät überprüft ob der Kanal frei ist bevor es zu senden beginnt. [6]

1.3.3. Begrifflichkeiten des Funks

Da sich ein großer Teil dieser Arbeit mit der Funktionsweise von Funktechnologien beschäftigt, sollten zunächst einige Fachbegriffe erläutert werden, um im nachfolgenden Vergleich der Technologien auf diese Fachbegriffe zurückgreifen zu können.

Frequenzen und Frequenzbänder

Die Übertragung im Funk geschieht über den Transport der Informationen über elektromagnetische Wellen, die mit einer speziellen Frequenz schwingen und voneinander unterschieden werden können, da sie jeweils eine eigene Übertragungscharakteristik haben. Die Frequenz dieser Wellenschwingung wird hierbei in der SI-Maßeinheit Hertz angegeben. Schaut man sich nun einen Bereich von Frequenzen des gesamten Frequenzspektrums an, der nach internationalen Richtlinien Frequenzen zwischen 3Hz und 3THz (Terahertz) umfasst, spricht man von einem Frequenzbereich. Dieses Frequenzspektrum wurde von der internationalen Fernmeldeunion (ITU) und der Federal Communications Commission (FCC) in zwölf Bänder unterteilt wurden. [7]

Das für diese Arbeit interessante Frequenzband ist das Super-High-Frequency ITU-Band 9, welches von 300MHz bis 3GHz reicht und somit sowohl kleinere Short-Range-Devices mit 433MHz als auch WLAN-basierte Technologien mit 2,4GHz einschließt.

Modulation

Wie jedes elektrische Signal bestehen auch Funkwellen aus den Parametern Amplitude, Frequenz und Phase. Durch Anpassung der Werte ist es nun möglich, mehrere unterschiedliche Datenströme über dasselbe Trägersignal zu übertragen, ohne dass diese sich gegenseitig stören. Um möglichst viele Informationen verlustfrei per Funk übertragen zu können, werden die zu übertragenden Signale moduliert. Bei der Modulation werden das Informationssignal und das Trägersignal vom Sender moduliert und dann übertragen. Der Empfänger muss das eintreffende Signal nun demodulieren bevor er die ursprüngliche Nachricht erhalten kann. In modernen Funknetzen wird mittlerweile hauptsächlich digitale Modulation verwendet. Diese Modulationsart erleidet keinerlei Qualitätsverluste bis der S/N-Faktor zu hoch wird. Dies bedeutet, dass das Verhältnis zwischen dem übertragenen Signal und ungewolltem Rauschen zu hoch ist und die Verbindung vollständig abbricht. [8]

Leistungspegel

Die Kenngröße für den Leistungspegel einer Funkübertragungstechnik ist Dezibel-Milliwatt (dBm) und gibt den Leistungspegel der Funkübertragung in Dezibel, bezogen auf 1mW an. Neben der Sendestärke selbst kann auch der Dämpfungsgrad eines Systems mit dieser Kenngröße bestimmt werden. Der mathematische Zusammenhang zwischen der Leistung P in Milliwatt und dem dBm-Wert p ist wie folgt:

$$p = 10\log(\frac{P}{1mW})$$

0dBm zeigen also eine Leistung von 1mW an, 10dBm sind 10mW zugeordnet und schließlich lassen sich 20dBm in 100mW umrechnen. Je 10dBm potenziert sich die Leistung also um 10mW. [9]

Signal-Rausch-Verhältnis

Ein wichtiger Wert in der Betrachtung von Funkübertragungen ist das sogenannte Signal-Rausch-Verhältnis, auch Störabstand oder Signal-Noise-Ratio (SNR) genannt. Es gibt Auskunft darüber wie qualitativ das Signal ist, indem es die Leistung des Signals mit der Leistung des Rauschsignals vergleicht. Es wird aufgrund der potenziellen Angabe in mehrfachen Zehnerpotenzen logarithmisch angegeben. Das Signal-Rausch-Verhältnis berechnet sich wie folgt:

$$SNR\ (dB) = 10\log(\frac{Leistung\ Nutzsignal}{Leistung\ Rauschsignal})$$

Je näher dieser SNR-Wert an 1 liegt, desto ähnlicher sind sich Nutzsignal und Rauschsignal. Bei einem hohen SNR-Wert ist von einer schlechten Qualität des Signals und einer hohen Störanfälligkeit auszugehen. [10]

Spreadingfaktor/Spreizfaktor

Der Spreizfaktor bestimmt bei der Funkübertragung mit Bandspreizverfahren wie CDMA oder DSSS die Breite eines zu sendenden Signals. Dabei werden die Bits des Nachrichtensignals mit einer Folge von sogenannten Chips (pseudozufällige Bits zur Spreizung des Nachrichtensignals) multipliziert, um das Signal künstlich zu vergrößern. [11]

Welche Notwendigkeit eine solche Technologie bei der Funkübertragung spielt, lässt sich wie folgt erklären:

> *Mehrere Sender können gleichzeitig an einen Empfänger senden, indem sie Spreizcodes nutzen, die jeweils unterschiedlich und dem Empfänger bekannt sind. Mittels der ihm bekannten Spreizcodes kann der Empfänger die Signale dekodieren und ermitteln, von welchem Nutzer welches Signal gesendet wurde. Derartige Verfahren, die mehrere digitale Kanäle multiplexen, werden Codemultiplexverfahren genannt. [12]*

Der Spreizfaktor, in der Literatur meist Spreading Factor benannt, zeigt an wie stark ein Signal gespreizt wurde. Je weiter ein Signal gespreizt wird, desto geringer fällt zwar die Datenrate aus, da die zu sendenden Nachrichten-Bits multipliziert werden, jedoch ermöglicht es ein stabileres Signal zu senden, da durch die Multiplikation eine Kollision von Daten vermieden werden kann. Jede Nachricht verfügt über einen eigenen Satz an Chips und je höher der Spreadingfaktor, desto leichter lässt sich die Nachricht beim Empfänger

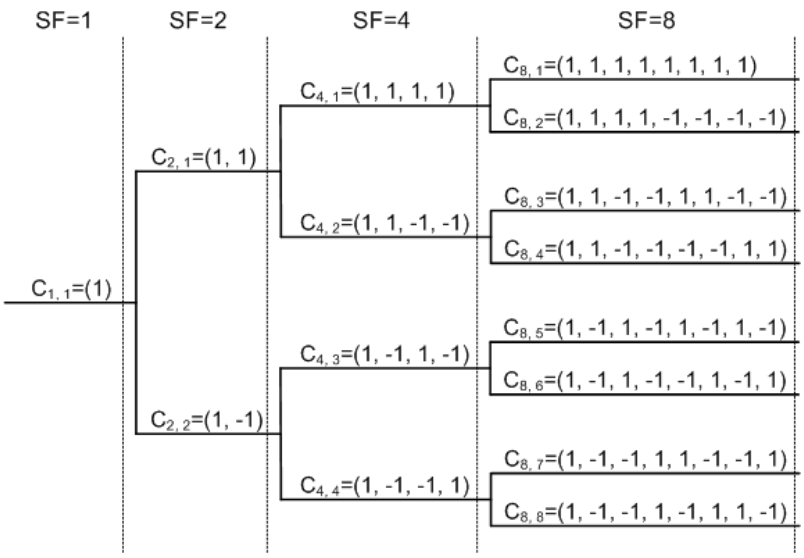
identifizieren. Bei geringen Spreadingfaktoren entstehen Komplikationen sobald zu viele Teilnehmer auf der selben Frequenz senden, da die mathematische Möglichkeit zur Multiplikation bei wenigen Chips verständlicherweise geringer ist, als bei vielen Chips. [11]

Berechnet wird der Spreadingfaktor wie folgt [11]:

$$SF = \frac{Chips\ pro\ Sekunde}{Nachrichtenbits\ pro\ Sekunde} \gg 1$$

Hierbei ist zu beachten, dass es immer mehr Chips als Nachrichtenbits geben muss. LPWAN-Technologien verfügen über niedrige Bitraten und nutzen im Regelfall kleinere Spreadingfaktoren von SF=4 bis hinauf zu einem SF=256, um ihre Übertragung über weite Strecken zu ermöglichen.

Darstellung 2 veranschaulicht, wie sich die Chiprate zum Spreadingfaktor verhält und wie man sich die Multiplikation vorstellen kann.



Darstellung 2. Beispiel der Chipraten bei Spreizfaktoren [13]

Link Budget – Leistungsübertragungsbilanz

Als Link Budget oder Leistungsübertragungsbilanz bezeichnet man den Kennwert der Übertragungstechnik, der die Verstärkungen und Dämpfungen aller Komponenten beschreibt, die ein Signal auf dem Sendeweg erfährt. Die Verstärkungen die das Signal durch Antennen erhält werden beispielsweise mit den Dämpfungen durch verschiedene Materialen bei der Übertragung bilanziert und schließlich in dBm angegeben. [14]

1.3.4. Störeinflüsse

Jedes Funksignal hat eine begrenzte Reichweite und kann von vielerlei Hindernissen gestört werden. Kreuzende Funksignale beeinträchtigen die Sendeleistung meist nur gering, da andere Modulationsarten oder Frequenzbänder genutzt werden und sich die Signale somit nicht überschneiden. Um die Signalstärke beim Empfänger eines Paketes anzeigen zu lassen, gibt es die Kenngröße des Received Signal Strength Indicator (RSSI). Der RSSI hat keine Maßeinheit, kann jedoch für jedes Gerät dessen Funksensibilität und Sendeleistung bekannt ist ins Verhältnis gesetzt werden. Viele Gerätehersteller geben einen Grenzwert für den minimalen RSSI eines Systems an (WLAN liegt bei beispielsweise einem RSSI von > -60). Setzt man so die Spezifikationen des Geräts mit dem RSSI in Verhältnis kann man die Signalstärke in dBm angeben. Grundsätzlich ist hierbei ein höherer dBm-Wert ein Kennzeichen für eine gute Verbindung. [2]

LTE

Elektronische Geräte in LPWANs nutzen in Europa vornehmlich die Frequenz 868MHz, was ihnen einen enormen Vorteil gegenüber Geräten verschafft, die in dem durch WLAN, Bluetooth oder ähnlichen Funksystemen überlasteten 2,4GHz-Frequenzbandbereiches senden. Da bislang vorrangig Garagensteuerungseinheiten oder ähnliche Kleingeräte auf dem lizenzfreien 868MHz Band sendeten, spricht man von dem SRD-Band (Short Range Devices). Da im Regelfall nur wenige dieser Geräte gleichzeitig auf dem Frequenzband aktiv sind, kann man die Störstrahlung dieser Geräte vernachlässigt behandeln. Diese SRDs und alle sendenden Geräte auf dem lizenzfreien Band sind, wie bereits unter 1.3.2. erwähnt, lediglich bis zu einer Sendeleistung von maximal 500mW zugelassen.

Hier entsteht nun ein anderes Problem innerhalb dieses Frequenzbereiches: Die Mobilfunkanwendung LTE. Durch die Abschaltung analoger Rundfunkstationen wurden immer mehr Frequenzen frei, die von den Behörden mitunter an Mobilfunkunternehmen versteigert wurden. Dazu gehörte auch ein Teil der 800MHz Frequenzen, die in Deutschland im Jahr 2010 unter den drei Telekommunikationsanbietern Telekom, Vodafone und O2 aufgeteilt wurden. Darstellung 3 zeigt, welcher Anbieter hierbei welchen Frequenzbereich erhielt.

Darstellung 3. Frequenzbelegung durch die drei LTE-Anbieter, (Eigene Darstellung nach Prof. Dr. Christian Plätz, Dipl.-Ing. (FH) André Volkmar) [15]

Anbieter	Uplink	Downlink
Deutsche Telekom	852-862 MHz	811-821 MHz
Vodafone	842-852 MHz	801-811 MHz
O2	832-842 MHz	791-801 MHz

Ersichtlich wird hierbei zwar, dass sich keine der versteigerten Frequenzen für den LTE-Betrieb mit dem SRD-Band von 868MHz überschneidet, aber andere Faktoren müssen hierbei bedacht werden. Während SRDs und LPWANs mit maximal 500mW senden dürfen, reicht die Sendeleistung von LTE-Basisstationen von 400W in städtischem bis hin zu 2500W in ländlichen Gebieten. Um ein LPWAN zu stören, ist die räumliche Entfernung zu den Sendestationen jedoch zu hoch. LTE-Endgeräte sind zwar dafür ausgelegt, mit niedriger Sendeleistung zu senden, können IoT-Geräten jedoch im Alltag räumlich sehr nah kommen. Das Problem stellt bei all dem vor allem die LTE-Modulation dar, denn durch die Auslegung auf möglichst hohe Datenraten kann es zu sogenannten Out-of-Band-Emissions kommen. Diese Emissionen verschlechtern in angrenzenden Bereichen deutlich das Signal-Rausch-Verhältnis und stören durch die Einstrahlung in benachbarte Frequenzen den dortigen Funkverkehr. In Deutschland liegt das Frequenzband der deutschen Telekom mit 862MHz fast direkt neben dem SRD-Band. Studien des Stiftungslehrstuhls für Systemzuverlässigkeit an der technischen Universität Chemnitz ergaben, dass die Störungen der SRDs bei Nichtbenutzung der LTE-Endgeräte nur geringe Störungen, wie beispielsweise Bitfehler, verursachten. Befand sich das Endgerät jedoch nicht nur im Netz des Funkbereichs, sondern sendete aktiv auf der LTE-Frequenz, kam es zu signifikanten Signaleinbrüchen auf den SRD-Frequenzen.

Abhilfe dazu schafft nur die räumliche Entfernung zwischen dem SRD und dem sendenden LTE-Gerät. Anwendungen - die unzuverlässige Protokolle im LPWAN nutzen - sollten keinen Wert auf garantierte Paketankunft legen. Dies ist aber auch oft nicht nötig, da es weniger schlimm ist, wenn vereinzelt Temperaturwerte einer Thermostat-Applikation nicht korrekt gesendet werden konnten. In jedem Fall ist LTE beim Aufbau eines LPWANs ein zu berechnender Störfaktor. [15]

Dämpfung durch Hindernisse

Funkwellen werden ohne regelmäßige Verstärkung mit steigender Entfernung immer schwächer. Dies muss man bedenken, wenn man ein Funknetzwerk einrichten möchte. Da in der natürlichen Umgebung in den seltensten Fällen Laborbedingungen gegeben sind, muss man zudem mit einer Vielzahl an physikalischen Hindernissen rechnen, die sich den Funkwellen in den Weg stellen. Die Materialien, aus denen diese Hindernisse bestehen, bestimmen hierbei den Grad der zur erwartenden Dämpfung.

Darstellung 4. Dämpfwirkung verschiedener Materialien (Eigene Darstellung, nach Grundlagen Funktechnik) [8]

Material	Dämpfung	Beispiele
Holz	gering	Möbel, Decken, Zwischenwände
Gips	gering	Zwischenwände ohne Metallgitter
Glas	gering	Fensterscheiben
Wasser	mittel	Mensch, feuchte Materialien, Aquarium
Mauersteine	mittel	Wände, Decken
Beton	hoch	Massive Wände, stahlarmierte Betonwände
Gips	hoch	Zwischenwände mit Metallgitter
Metall	sehr hoch	Aufzugsschacht, Brandschutztüren, Stahlbeton

Darstellung 4 stellt dar, wie stark sich die Dämpfung unterschiedlicher Materialien auf Funksignale auswirken. Während Materialien mit geringer Dichte wie Holz, Gips oder Fensterglas Funkwellen nur bedingt aufhalten, muss bei stahlarmierten Betonwänden, Mauersteinen oder mit Metallgittern versetzten Zwischenwänden mit deutlichen Leistungs- und Reichweiteneinbußen gerechnet werden. Reine Metallkonstruktionen sind fast undurchdringbar für Funkwellen und schirmen dahinterliegende Bereiche meist völlig von Funkeinstrahlung ab. [8]

1.4. Technologien zur drahtlosen Datenübertragung im Internet der Dinge

Im Internet der Dinge werden bereits viele Technologien genutzt, die seit dem Aufkommen der IoT-Technologie an die Anforderungen langer Batteriedauer und niedriger Bandbreite angepasst wurden. Besonders im Consumerbereich finden Protokolle wie WiFi und Bluetooth Anwendung, was für Heimanwendungen meist zwar völlig ausreicht. Für die Verwendung in der Industrie jedoch reichen diese Protokolle meist nicht aus, da sie in diversen Punkten nicht die nötigen Spezifikationen erfüllen können. Im folgenden Teil werden zuerst aktuelle Technologien zur drahtlosen Übertragung im Internet der Dinge aus den Bereichen Local-Area-Network/Short-Range Communication und Mobilfunk vorgestellt, bevor die speziellen LPWAN Technologien expliziter beleuchtet und von den alternativ nutzbaren Technologien abgegrenzt werden.

1.4.1. Local Area Network/Short Range Communication

Bluetooth

Die bekannte drahtlose Bluetooth-Technologie des Unternehmens SIG Bluetooth (Special Interest Group) kann über kurze Distanz hohe Datenraten erzielen, verbraucht dabei aber entsprechend viel Strom. Um jedoch die Anforderungen des Internets der Dinge zu erfüllen und den Stromverbrauch gering zu halten, wurden mit Version 4.0 die Kernfunktionalitäten in drei Bereiche aufgeteilt.

Die allgemein bekannte Bluetooth-Technologie wird als Bluetooth Basic Rate/Enhanced Data Rate (BR/EDH) bezeichnet und bietet eine kontinuierliche Übertragung hoher Qualität auf kurze Distanz, was ideal für Media-Streaming von Musik und Filmen ist. Sie arbeitet auf dem Frequenzband 2,4GHz wie viele andere drahtlosen Netzwerkverbindungen.

Neu seit Version 4.0 ist die Bluetooth with low energy funcionality (LE) Spezifikation, die es den Geräten ermöglicht, durch kurze Sendestöße, sogenannte Bursts, kleinere Datenmengen über eine größere Distanz zu senden. Anwendung findet dies besonders bei IoT-Geräten die nicht auf eine kontinuierliche Verbindung angewiesen sind und mit einer längeren Batterielaufzeit von dieser Vorgehensweise profitieren.

Letztlich bietet Bluetooth einen Dual-Mode für Geräte an, die als Schnittstelle zwischen BR/EDH- und LE-Geräten genutzt werden. Ein Beispiel dafür wären Smartphones, die einerseits Musik zu drahtlosen Kopfhörern über BR/EDH streamen, aber auch Smart-Home-Anwendungen steuern und mit Wearables wie Fitness-Tracking Armbändern kommunizieren müssen. [16]

IEEE 802.X

Das Institute of Electrical and Elektronics Engineers ist eine internationale Organisation aus Fachleuten der Elektrotechnik und der Informationstechnologie. Das IEEE ist die weltweit führende Organisation für Standardisierung in diesen Bereichen und ist besonders für die Standards LAN, WLAN und FireWire bekannt. Der Ethernet-Standard LAN ist Teil des Standardisierungsprojektes IEEE 802, an welchem stetig weitergeforscht wird. So umfasste die Version 802.11 zum Beispiel den meistgenutzten Standard für drahtlose Netze weltweit, das WLAN. IEEE 802.11 wird von fast allen Geräten verwendet, die sich mit Drahtlosnetzwerken auf dem Frequenzbad 2,4GHz verbinden möchten. [17]

Der auf Bluetooth aufbauende 802.15 Standard ist Grundlage von vielen der folgenden genannten Technologien, wie beispielsweise ZigBee und Thread.

Häufig wird für WLAN ebenfalls der Begriff WiFi genutzt, was jedoch nicht vollends korrekt ist. Als WiFi-Geräte werden nur Geräte bezeichnet, die von der Organisation WiFi-Alliance auf ihre Kompatibilität mit dem IEEE-Standard getestet und zertifiziert wurden. Um eine solche Zertifizierung zu erhalten, muss man neben dem Erfüllen der technischen Spezifikationen ein Mitglied dieser Allianz sein [18].

Das bedeutet: Auch wenn ein Gerät nicht WiFi-zertifiziert ist, kann es dennoch WLAN-fähig im Sinne des IEEE-Standards sein.

ZigBee

Einen weiteren Standard für Funkübertragung im Internet vertreibt und entwickelt die in 2002 gegründete ZigBee-Allianz. Die von ZigBee entwickelten Technologien bauen auf dem IEEE 802.15.4 Standard auf, unterteilen sich aber je nach Anwendungsfall in die Spezifikationen ZigBee IP/920IP, ZigBee RF4CE und ZigBee PRO.

ZigBee IP/920IP gilt als der erste offene Standard für IPv6-basierte full-wireless Meshnetzwerke. IP/920IP ist in der Lage, in das Netzwerk eingebundene Geräte sowohl über regions-spezifischen, lizenzfreien Funk unter 1GHz, als auch über die 2,4GHz Frequenz des IEEE 802.15.4 kommunizieren zu lassen. Mit IP/920IP gesendete Daten können durch die Nutzung von AES-128-CCM vor dem Zugriff dritter Parteien geschützt werden und bieten somit eine sichere Übertragung. Weiterhin verfügt dieses Protokoll über eine sehr gute Interoperabilität und kann über viele der Standard-Internetprotokolle kommunizieren, unter anderen zum Beispiel: 6LoWPAN, IPv6, RPL, TCP und UDP. Besonders durch die Nutzung von IPv6 ist es möglich, jede Node mit ihrer eigenen IP zu versehen und die Nutzbarkeit von TCP und UDP ermöglicht es, alle Internetanwendungen in Verbindung mit ZigBee IP zu nutzen (wie HTTP). [19]

ZigBee RF4CE wurde zur Steuerung der Multimedia-Elektronik innerhalb eines Hauses entwickelt, sowie für die Steuerung von Garagentoren und schlüssellosen Zugangssystemen. Hier sind zwei Technologien zugehörig: Zum einen ZigBee-Remote Control, zum anderen ZigBee-Input-Device. Während zu steuernde Geräte wie TV, DVD-/Blu-ray-Player oder Musikanlagen über die Funktionalität des Remote Control Standards

verfügen müssen, um angesteuert werden zu können, benötigen Steuereinheiten wie Funkmäuse und -Tastaturen, Touchpads oder ähnliche Fernbedienelemente die Input-Device-Technologie.

Die Übertragungen sind durch die automatische Auswahl des günstigsten 2,4GHz-Channels weniger anfällig für Störungen. Die Technologie kann vom Gerätehersteller jederzeit durch ein Softwareupdate eingespielt werden. [20]

ZigBee PRO wurde speziell für Anwendungen im Internet der Dinge geschaffen. Es bietet einen niedrigen Energieverbrauch im Drahtlosnetzwerk und unterstützt bis zu 64000 Geräte in einem Netzwerk. Es kann sowohl für die lizenzfreien Frequenzen als auch die übliche 2,4GHz-Frequenz senden. Zudem verfügt es über das optionale Green-Power-Feature, welches die Nutzung von Strom aus Energy-Harvesting-Quellen ermöglicht. [21]

Near Field Communication - NFC

NFC wurde konzipiert, um kontaktlose bidirektionale Interaktion zwischen elektrischen Geräten zu ermöglichen. Anders als die bereits vorgestellten Technologien, basiert NFC auf dem ISO/IEC 14443 contactless smart Card Standard. Von allen bereits vorgestellten Möglichkeiten zur drahtlosen Kommunikation hat NFC den kleinsten Wirkungskreis, denn Geräte mit dieser Technologie können lediglich bis zu 10cm weit Daten senden oder empfangen. [22]

Besonders aufgrund der geringen Reichweite ist NFC nur bedingt für die Kommunikation im Internet der Dinge brauchbar, kann aber beispielsweise in bestehenden IoT-Netzwerke eingebunden werden, um diese durch Anwendungen wie Zugangskontrollen zu erweitern.

Radio Frequency Identification – RFID

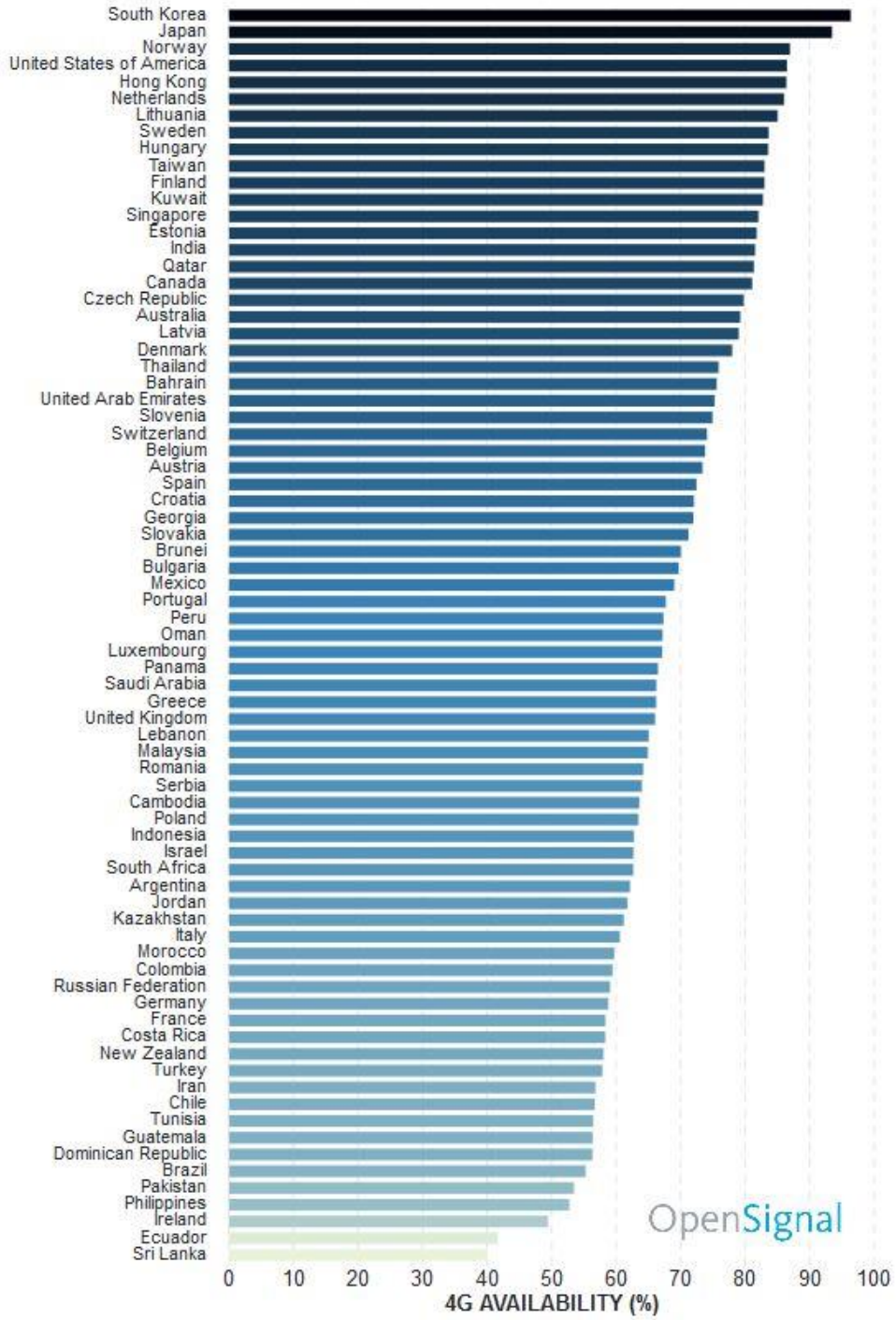
RFID ist eine der ältesten Funkübertragungstechnologien für Geräte und stammt ursprünglich aus der militärischen Radartechnologie des 2. Weltkrieges. Durch das Anbringen von Identifikationseinheiten an alliierte Flugzeuge konnte eventueller Freundbeschuss verhindert werden. Aus diesen Identifikationseinheiten, welche per Funk Informationen über ihren Träger senden konnten, entstand schließlich die uns bekannte Radio Frequency Identification (RFID) Technologie.

RFID ist ein automatisches Identifikationssystem und lässt sich sehr gut mit dem weltweit verbreiteten Barcode-System vergleichen. Diese zwei Technologien haben grundsätzlich den selben Anwendungsbereich, jedoch muss für die Nutzung von RFID keine direkte Sichtverbindung zwischen dem lesenden Gerät und dem zu lesenden Objekt (Transponder) bestehen, da RFID über Funk angesprochen wird. Zum Aufbau eines funktionierenden RFID-Systems benötigt man ein RFID-Lesegerät, ein daran angeschlossenes Informationssystem sowie auslesbare RFID-Transponder. Ein solcher Transponder besteht aus einem Mikrochip und einer Antenne. Nähert man das RFID-Lesegerät nun dem Transponder, überträgt dieser die zur Verbindung nötigen Daten sowie den Übertragungstakt.

Der Mikrochip des Transponders bearbeitet nun die Anfrage des Lesegeräts und sendet eine Antwort. Häufig verfügen RFID-Transponder über keine eigene Stromversorgung und eine Antennenspule ersetzt die Antenne. Diese ist in der Lage vom Transponder ausgesandte Energie zur Versorgung des Transponders aufzunehmen. Besonders die Energie- und Kosteneffizienz von RFID-Systemen machen diese in gewissem Maße interessant für das Internet der Dinge, jedoch ist die maximale Reichweite von 10m bei extrem hohen Frequenzen und 5m bei den gängigen freien Funkfrequenzen zu wenig, um eine gute Anwendung dafür zu finden. [23]

1.4.2. Mobilfunk/Traditional M2M

Mobilfunk ist heutzutage so gut wie allgegenwärtig und gerade in Industrienationen sind über 70-90% der Fläche bereits durch LTE-Mobilfunk abgedeckt. Deutschland liegt einer Studie der Plattform OpenSignal mit 58,80% auf dem 58. Platz der überprüften Länder. Darstellung 5 gibt einen Überblick über die Ergebnisse der Studie. (Stand Juni 2017) [24]



Darstellung 5. State of LTE, OpenSignal.com [24]

Auch wenn Abdeckungsraten von 50% auf den ersten Blick nicht viel erscheinen, so ist damit doch eine beträchtliche Menge an bewohntem Gebiet abgedeckt. Naheliegend ist hierbei schnell, diese vorhandene Abdeckung der Mobilfunknetze zu nutzen, um Sensoren und Geräte des Internets der Dinge darüber kommunizieren und steuern zu lassen. Jedoch sind Anschaffungs- und Verbindungskosten in Mobilfunknetzen meist zu hoch für langfristige Sensornetzwerkinstallationen.

Der weltweite Mobilfunk wird von einem großen Gremium, dem The 3rd Generations Partnership Project gesteuert, weiterentwickelt und kontrolliert.

The 3rd Generations Partnership Project – 3GPP

Das 3GPP ist eine globale Initiative zur Standardisierung von Mobilfunktechnologien. Sie steht unter anderem hinter den bekannten Mobilfunkstandards UMTS, GPRS&EDGE, sowie LTE und LTE-Advanced. Es handelt sich hierbei um eine Kooperation von sieben internationalen Normierungsgremien für Mobilfunk. Zu diesen Gremien zählen:

- ARIB (Association of Radio Industries and Businesses, Japan)
- ATIS (ehem. T1) (Alliance for Telecommunications Industry Solutions, USA)
- CCSA (China Communications Standards Association, China)
- ETSI (European Telecommunications Standards Institute)
- TSDSI (Telecommunications Standards Development Society, India)
- TTA (Telecommunications Technology Association, Korea)
- TTC (Telecommunications Technology Committee, Japan)

Das 3GPP treibt die Weiterentwicklung von funkbasierten Netzwerktechnologien, neuartigen Codecs, der Übertragungssicherheit sowie die Sicherung der Übertragungsqualität voran. Alle Spezifikationen und Studien der Initiative entstehen in Zusammenarbeit der Mitgliedsunternehmen, Arbeitsgemeinschaften und den Technical Specification Groups (TSG), folgenden drei spezialisierten Untergruppierungen:

- RAN (Radio Access Network)

  Das TSG RAN ist für die Entwicklung der Funkperformance, der physikalischen Layer sowie die Spezifikationen der Funktionen und Voraussetzungen der GSM EDGE Radio Access Networks (GERAN), der Universal Terrestrial Radio Access Networks (UTRAN) verantwortlich.

- SA (Service & System Aspects)

  Das TSG SA ist für die Architektur aller 3GPP Standards verantwortlich. Es Dokumentiert die Fortschritte der Projekte und betreut alle Belange die alle Projekte betreffen wie Sicherheit, Service Kapazitäten sowie den projektübergreifenden Wissensaustausch.

- CT (Core Network & Terminals)

Die Arbeitsgruppe TSG CT befasst sich mit der Kernkommunikation der 3GPP Technologien. Die Gruppierung sichert die übergreifende Kommunikation zwischen unterschiedlichen externen Netzwerken und die Kommunikation der Core Nodes des Netzwerks.

Derzeit arbeitet das 3GPP an der Weiterentwicklung des 4G-Standards (LTE Advanced) sowie an der Einführung der nächsten Generation, dem 5G-Standard, welche für die zweite Jahreshälfte 2018 geplant ist [25]. Die Entwicklungen der Initiative lassen sich gut anhand der „Releases“ die von 3GPP herausgegeben werden verfolgen. Sie stellen paperähnliche Meilensteindokumente dar in denen die neusten Änderungen erläutert werden. Interessant für die vorliegende Arbeit ist im speziellen Release 13, da sich mit diesem eine Erweiterung des LTE Standards zum „LTE-Advanced Pro“ um die sogenannten NarrowBand IoT (NB-IoT) oder auch Funktionalität ergeben hat. NB-IoT verfügt im Gegensatz zum allgemein bekannten LTE über eine weitaus geringere Datenrate und versucht somit den Energieverbrauch von mobilfunkgestützten IoT-Anwendungen drastisch zu reduzieren. [26]

NarrowBand Internet of Things

LTE ist allgemein als Mobilfunktechnologie mit schneller Datenübertagung und hoher Bandbreite bekannt und derzeit die schnellste Übertragungsart auf dem deutschen Verbrauchermarkt. Mobilfunkunternehmen werben mit hohen Bandbreiten und den damit verbundenen Streaming- und Kommunikationsmöglichkeiten. Für ein LPWAN sind solche Datenraten jedoch aufgrund der damit verbundenen Energiekosten suboptimal, da eine hohe Sendeleistung der Geräte einen hohen Stromverbrauch mit sich zieht.

NarrowBand-IoT, auch als LTE-Cat-NB1 bezeichnet, ist ein Feature des LTE Advanced Standards, welches im Zuge des Release 13 des 3GPP veröffentlicht wurde. Das Release 13 umfasst ca. 170 Studien und Features, wobei das klare Hauptaugenmerk der Entwicklung bei Verbesserungen des existierenden Standards in Hinblick auf Energieverbrauch bei der M2M-Kommunikation liegt. Die Entwicklung der Technologie wird in Darstellung 6 gezeigt. [27]

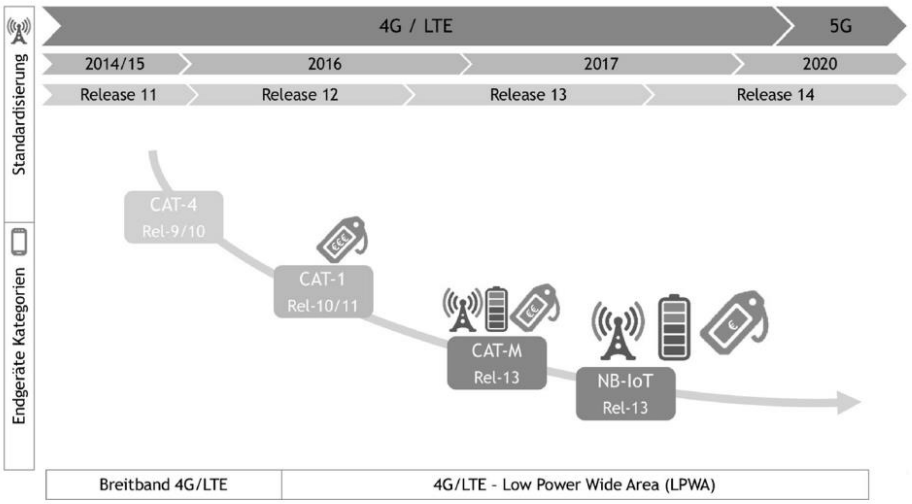


Abb. 2. Mobilfunkentwicklung auf Netz- und Endgeräteseite hin zu LPWAN

Darstellung 6. Mobilfunkentwicklung auf Netz- und Endgeräteseite hin zu LPWAN, Kainz, Bürger [28]

5G-Technologie

3GPP ist ebenfalls für die Entwicklung des offiziellen Nachfolgers der 4G- bzw. LTE-Technologie verantwortlich, welcher mit dem Release 15 veröffentlicht werden soll. Die 5G-Technologie befindet sich derzeit noch in einem relativ frühen Entwicklungsstadium, wird allerdings schon jetzt als Nachfolger der LTE-Technologie, besonders im Hinblick auf M2M Kommunikation, gehandelt.

Die finale 5G-Technologie soll sich zu ihrer Vorgängerversion LTE-Advanced vor allem in Energiesparoptionen, niedrigem Stromverbrauch sowie extrem hohen Datenraten abheben. Gerade niedriger Stromverbrauch und hohe Datenraten im Funk widersprechen sich hierbei. Deshalb wird davon ausgegangen, dass nicht beide Funktionalitäten gleichzeitig nutzbar sind und pro Anwendungsfall entschieden werden muss worauf der Fokus liegt. Zu technischen Details und Abdeckungszahlen wurden bisher noch keine feststehenden Daten genannt. Die Veröffentlichung des 5G-Standards ist derzeit für 2020-2025 geplant. [25]

2. Low Power Wide Area Network Technologien

2.1. Grundlagen

Low Power Wide Area Networks (LPWANs) wurden speziell für Funkstrecken des Internets der Dinge entwickelt, um Schwachstellen bestehender, weit verbreiteter Systeme wie WLANs oder des Mobilfunks entgegenzuwirken. Also unterscheiden sie sich in einigen grundlegenden Punkten von normalen Funknetzwerken wie Bluetooth oder WLAN sowie von Mobilfunknetzwerken.

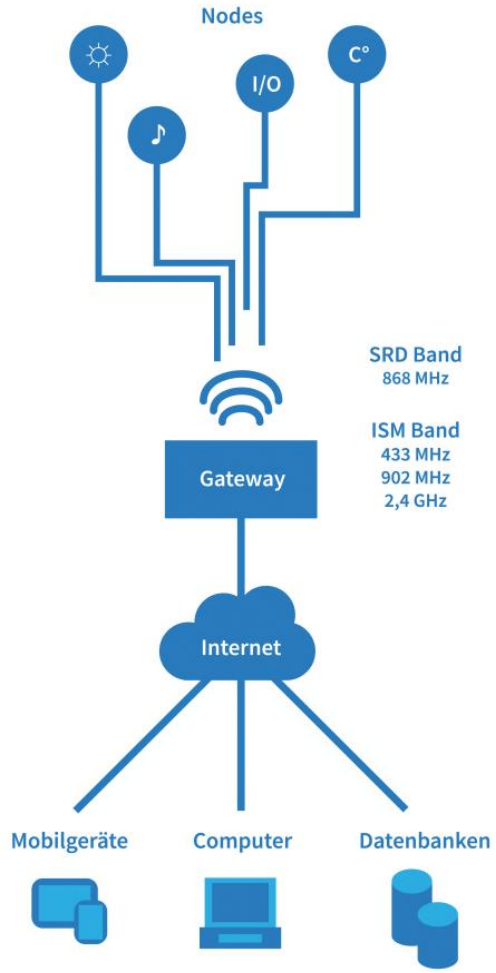
Short Range Wireless (Bluetooth, WiFi)	LPWAN	Mobilfunk
+	+	+
Weit verbreitet	Energieeffizient	Enorme Abdeckung
Ideal in Gebäuden	Geringe Kosten	Hohe Bandbreite
	Positionierungsmöglichkeiten	
-	-	-
Energieverbrauch	Niedrige Bandbreite	Keine Autonomie
Bereitstellungskosten	Konkurrierende Standards	Hohe Kosten
Reichweite		

Darstellung 7. Unterschiede zwischen Drahtlosnetzwerken (Eigene Darstellung in Anlehnung an LoRa) [29]

Darstellung 7 zeigt welche Vorteile oder Nachteile die jeweiligen Techniken in Hinblick auf eine Nutzung im Internet der Dinge mit sich bringen. WiFi und Bluetooth sind die verbreitetsten Technologien im Consumerbereich und können so gut wie überall gefunden werden. Aufgrund des möglichen Datendurchsatzes und dem stetigen Routing ist jedoch eine stetige Stromversorgung fast unabdingbar. LPWANs haben eine sehr geringe Datenübertragungsrate die für die Verwendung im Internet der Dinge jedoch völlig ausreicht, da solche Netzwerke nicht zur Übertragung großer Datenmengen gedacht sind. Im Gegensatz zur WiFi- oder Bluetooth-Technologie kann ein LPWAN jedoch weitaus höhere Entfernungen bei der Datenübertragung überbrücken. Diese Entfernungen können bei entsprechender Technik ohne Probleme die 10-km-Marke überschreiten. Auch die Energiekosteneffizienz-Vorteile der Benutzung liegen im deutlich niedrigeren Energieverbrauch der Sensoren, sowie der Anschaffungskosten.

Der Aufbau eines LPWANs beruht auf Protokollen der M2M-Kommunikation (Machine to Machine), welche auch oft Anwendung im Bereich des Internet der Dinge finden, wie MQTT oder CoAP. LPWANs sind so aufgebaut, dass eine sehr hohe Geräteanzahl am Netzwerk

teilhaben kann. Ein LPWAN besteht im Regelfall aus mehreren Sensoren oder Akteuren, welche per Funk mit einer Basisstation kommunizieren. Diese mit Antennen ausgestatteten Sensorsysteme werden Nodes genannt. Sie senden die zu übertragenden Daten über niederfrequente Funkwellen zu den Basisstationen, sogenannten Gateways, welche als Schnittstelle zwischen den Nodes und dem Internet agieren. Das Gateway leitet die Daten zu einem Webserver, weiter welcher als Cloud fungiert. Dort werden die Daten abgespeichert oder weiterverarbeitet. Da es sich bei LPWANs um bidirektionale Netzwerke handelt, können nun Anweisungen vom Server über das Gateway zu den Nodes weitergeleitet werden. Darstellung 8 skizziert den Aufbau eines LPWAN-Netzwerks. [29]



Darstellung 8. Aufbau eines funkbasierten LPWANs, Eigene Darstellung

Gegenüber den WiFi- oder Mobilfunklösungen versuchen sich LPWANs durch folgende Punkte besonders abzuheben [29]:

- Niedriger Energieverbrauch, um jahrelange Batterielaufzeiten zu gewährleisten

- geringe Kosten pro Sensor/Aktor-Einheit (Cost per Unit)

- geringe Baugröße der Nodes

- sehr hohe Funkreichweite durch Reduzierung der Datenübertragungsrate

- Ubiquitous Computing, Allgegenwärtigkeit des Netzwerks

Gateways in LPWANs nutzen meist eigene Protokolle zur Datenweitergabe an die verbundenen Nodes, sind aber meist in der Lage, übliche Protokolle des Internets der Dinge zu verarbeiten und zu übersetzen. Die meistgenutzten Protokolle im Internet der Dinge sind CoAP und MQTT, die nun kurz vorgestellt werden.

Constrained Application Protocol (CoAP)

Das Constrained Application Protocol ist ein spezielles Netzwerkprotokoll für die Nutzung von miteinander verbunden Knoten, sogenannten Nodes, in verlustbehafteten Niedrigenergienetzwerken. Diese Netzwerke zeichnen sich dadurch aus, dass die Nodes häufig mit Mikrocontrollern betrieben werden, welche nur auf geringe Ressourcen zurückgreifen können, speziell die Read-only-Memorys und Random-Access-Memory. Grundsätzlich ist hierbei der Aufbau des Protokolls nicht sehr verschieden und es wäre in der Lage HTTP in einer kompakteren Form abzubilden, jedoch ist seine Hauptaufgabe die energiearme Kommunikation zwischen Maschinen. CoAP arbeitet über UDP und unterstützt Uni- als auch Multicast. Der klein gehaltene Header-Overhead bewirkt, dass die Pakete des Protokolls kleiner und somit ressourcenärmer übertragen werden können. Es kann via HTTP gesteuert werden.

Teilnehmende Parteien des Datenaustausches werden Endpunkte genannt, wobei diese in Sender, Empfänger, Client und Server unterteilt werden. [12]

Um den Protokollaufbau der LPWAN-Anbieter besser verstehen zu können, werden nun zuerst die meistgenutzten Protokolle im Internet der Dinge - MQTT und CoAP - vorgestellt, da die LPWAN-Protokolle meist zu großen Teilen auf diesen aufbauen. Im Anschluss werden die Anbieter und die Funktionsweise von aktuellen LPWAN-Technologien vorgestellt und beleuchtet.

Message Queue Telemetry Transport Protocol (MQTT)

MQTT ist ein anderes Protokoll, welches speziell für Machine-to-Machine (M2M) Kommunikation sowie die Nutzung im Internet der Dinge entwickelt wurde. Es wurde darauf geachtet, dieses in der Implementation einfach zu halten und innerhalb des Protokolls einen gewissen Leichtbau zu erhalten um, wichtige Faktoren wie zum Beispiel die Bandbreite nicht zu stark zu beeinflussen. Im Gegensatz zum CoAP arbeitet es über TCP und hat somit die Möglichkeit per Fluss und Paketkontrolle auf aufkommende Paketverluste zu reagieren. MQTT bietet hierbei drei Qualities of Service an, dass bedeutet Pakete werden im Fehlerfall:

- "At most once", noch einmal verschickt - Duplikate werden jedoch herausgefiltert. Hierbei wird versucht, das bestmögliche Ergebnis der Datenübertragung zu erhalten. Pakete können verloren gehen.
- "At least once", ebenfalls noch einmal verschickt – Duplikate werden jedoch nicht herausgefiltert und somit können Duplikate nicht ausgeschlossen werden.
- "Exactly once", ebenfalls noch einmal verschickt, jedoch werden Duplikate herausgefiltert und durch zusätzliche Prozeduren wird zu verhindern versucht, dass Duplikate verarbeitet werden. Wird für alle Anwendungen verwendet bei denen es

wichtig ist, dass Pakete exakt einmal übertragen werden. In einem solchen Fall würden Duplikate oder verlorene Pakete zu Fehlbuchungen führen.

Zudem wurde im MQTT Protokoll ein publish/subscribe Nachrichtensystem implementiert, mit welchem einfache One-to-Many-Distribution ermöglicht wurde. Um den Netzwerkverkehr gering zu halten wurde versucht, den Transport-Overhead sowie den Protokollaustausch möglichst gering zu halten. [30]

2.2. Anbieter von Low Power Wide Area Network – Technologien

Im folgenden Abschnitt werden die führenden Anbieter und Entwickler von LPWAN Technologien vorgestellt, die für das Internet der Dinge interessant sind oder werden könnten. Nicht betrachtet werden hierbei Mobilfunkanbieter, da deren Lösungen über hohe Übertragungsraten verfügen, die einen hohen Stromverbrauch mit sich ziehen und die Kosten zur Anbindung von IoT-Geräten mit den aktuellen Datenpaketen einen solchen Ansatz uninteressant machen. Da neben den großen Organisationen und Allianzen viele kleinere Unternehmen an eigenen „Standards“ arbeiten, werden nur die derzeit größten, aussichtsreichsten Alternativen beleuchtet und im Zuge dieser Arbeit miteinander verglichen.

2.2.1. LoRa Alliance

Darstellung 9. Logo der LoRa Alliance, LoRa Alliance [31]

Die LoRa Alliance ist ein von Semtech gegründeter Zusammenschluss führender Unternehmen des Informationstechnologie-Sektors, die es sich zur Aufgabe gemacht haben, einen offenen Standard für die Verwendung von LPWANs im Internet der Dinge zu setzen. Die 428 Mitglieder der Allianz (Stand Januar 2017), zu denen unter anderen Firmen wie IBM und Cisco gehören, streben an durch offene Verbreitung des LoRa-Protokolls sowie der freien Wissensweitergabe eine Interoperabilität zwischen Anwendern des sogenannten LoRaWANs sicherzustellen. [31]

Während die LoRa-Modulation proprietär und nicht zugänglich für die Öffentlichkeit ist, ist die Anwendungs- sowie die Netzwerkschicht des LoRaWAN-Protokollstapels Open-Source.

Bitübertragungsschicht

Die physikalische Schicht des LoRa-Protokolls überträgt die Daten über die regional unterschiedlichen Frequenzbänder. LoRa unterstützt 868MHz und 433MHz für Europa, 904MHz in den USA, 915MHz in Australien und 430MHz in Asien. Die Funkübertragung arbeitet nach dem Listen-before-Talk-Prinzip (LBT) und sendet nur Daten, wenn das Trägermedium frei ist. [32]

Darstellung 10 zeigt, wie eine Uplink-Nachricht bei der Funkübertragung mit LoRa aufgebaut ist. Im Fall einer Downlink-Nachricht besteht die Funktion des Cyclic-Redundany-Checks (CRC) nicht. Einer Präambel folgt der Physical-Header, gefolgt eines Header-CRCs. Im Anschluss an diesen folgen die eigentlich zu übertragenden Daten im PHYPayload. [33]

Preamble	PHDR	PHDR_CRC	PHY_Payload	CRC*

Darstellung 10. Nachrichtenformat der LoRaWAN Bitübertragunsschicht [33]

Die zu übertragenden Daten im PHYPayload sind wiederrum unterteilt in einen MAC-Header (MHDR), den MAC-Payload oder einen Join-Request/Response und einen Message-Integrity-Code (MIC) wie in Darstellung 11 gezeigt. [33]

MHDR	MACPayload	MIC

or

MHDR	Join-Request	MIC

or

MHDR	Join-Response	MIC

Darstellung 11. Aufbau des PHYPayload [33]

Nach einem Upload-Vorgang öffnen LoRa Geräte nach einer gewissen Empfangs-Wartezeit zwei kurze Empfangsfenster die von den regionalen Übertragungsfrequenzen abhängig sind. Der in Darstellung 12 skizzierte Sendevorgang kann erst wieder ausgeführt werden, wenn in einem Empfangsfenster der vorherigen Übertragung eine Nachricht empfangen wurde, oder die Zeit des RX2-Fensters abgelaufen ist. [33]

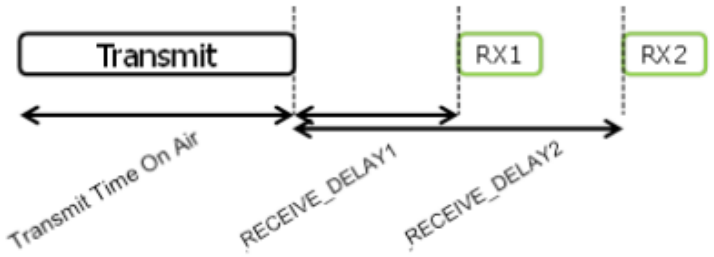


Figure 4: End-device receive slot timing.

Darstellung 12. Sendevorgang von LoRa-Geräten [29]

LoRaWAN Modulation

Die LoRa Modulation setzt auf der Bitübertragungsschicht des jeweiligen Frequenzbandes auf und verbindet den Datenstrom mit der entsprechend genutzten Frequenz, wie in der Darstellung 13 erkennbar ist. Die LoRa Modulation ist der einzige proprietäre Anteil eines LoRaWANs, während die Anwendungsschicht von LoRa frei zur Verfügung gestellt wurde. In manchen Regionen wie Europa, China und Indien kann auch die Gaussian-Frequency-

Shifting-Keying-Modulation Anwendung finden, die auch bei Bluetooth oder dem GSM-Standard eingesetzt wird.

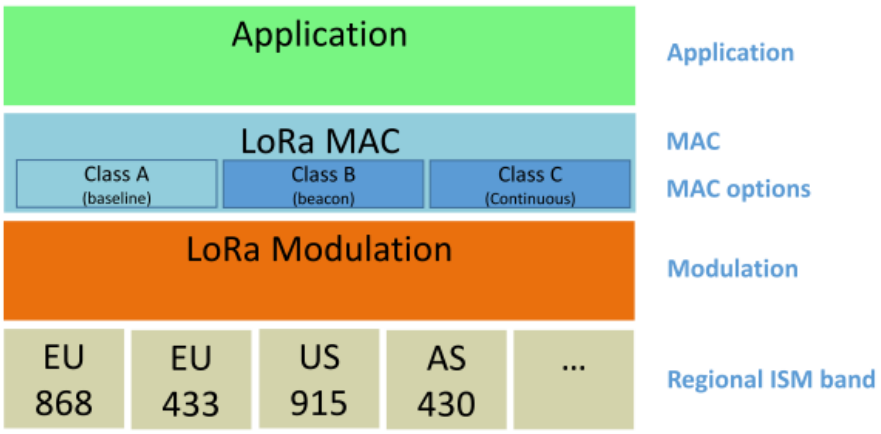


Figure 1: LoRaWAN Classes

Darstellung 13. LoRa Protocol Stack [29]

Netzwerkschicht/MAC-Layer

Die Netzwerkschicht eines LoRaWAN verarbeitet den von den unteren Schichten weitergereichten MAC Payload als sogenannten „data frame“. Der Aufbau des MAC Payloads und des Frameheaders sind in Darstellung 14 zu sehen. Dieser ist aus einem Frameheader, dem optionalen Frame Port und dem Frame Payload zusammengesetzt. Der Frameheader enthält die Adresse des Endgeräts, eine 8 Bit Framekontrolle, einen 16Bit-Framecounter und bis zu 124Bit an zusätzlichen Frame-Options, die Netzwerksteuerungsbefehle beinhalten können. [33]

MHDR	MACPayload	MIC

DevAddr	FCtrl	FCnt	FOpts

Darstellung 14. Aufbau des MACPayloads und FHDR [33]

Der Frame Header Payload ist der Datencontainer der Übertragung. Die darin übertragenen Daten werden mit einem AES-128Bit-Algorythmus verschlüsselt. Nach der Verschlüsselung wird zur Inhaltsprüfung ein Message-Integrity-Code generiert. [33]

Netzwerkklassen in einem LoRaWAN

Ein LoRaWAN kann in eine der Klassen A, B oder C unterteilt werden, wie Darstellung 13 zeigt. Klasse-A-LoRaWANs werden auch „basic“ oder „baseline“ LoRaWANs genannt, während Klasse-B und C-Netzwerke diese, um optionale Funktionen erweitern.

Die Klassen unterteilen sich in der Media-Access-Control (MAC) Ebene der zweiten Schicht des OSI-Modells und lassen sich wie folgt aufteilen:

Bidirectional End-Devices (Class A, baseline):

Bei Klasse-A-Geräten folgen bei der bidirektionalen Kommunikation zwei kurze Empfangsperioden auf die Sendeperiode.

Bidirectional End-Devices with scheduled receive slots (Class B, beacon):

Klasse-B-Geräte erweitern diese Funktionalität, indem sie der Kommunikation zusätzliche Empfangsfenster fester Länge hinzufügt, die zum Download von Servernachrichten genutzt werden. Diese Fenster werden vom zuständigen Gateway zeitlich mit allen Nodes abgestimmt, damit alle Geräte periodisch ein Empfangsfenster öffnen.

Bidirectional End-Devices with maximal receive slots (Class C, continuous):

Bei der letztmöglichen Klassifizierung, Klasse C sind die Empfangsfenster stetig offen, mit Ausnahme der Sendevorgänge. Diese Methode ist nur für spezielle Anwendungen gedacht, da sie einen viel höheren Energiebedarf wie Klasse A und B aufweist.[29]

LoRaWAN arbeitet zudem nach dem „Dumb Gateway“ – „Smart Cloud“-Prinzip. Dies bedeutet, dass eine Node nicht einem Gateway zugeordnet ist, sondern seine Daten an alle verfügbaren Gateways sendet. Diese leiten die Informationen dann an die jeweilige Webapplikation weiter, wo doppelte Pakete aussortiert werden können. [29]

2.2.2. SigFox

SigFox ist eine in 2009 gegründete französische Firma, welche ein eigenes Protokoll zur Verwendung in einem LPWAN entwickelt hat. SigFox ist die einzige Firma die neben eigener Protokolle ihr eigenes Netzwerk betreibt. Mit ihrem SigFox Protokoll ermöglichen sie eine kommerzielle Nutzung des Netzwerkes, welches seitens der Firma selbst aufgebaut wird. Die Unterstützung privater LPWANs ist durch das Unternehmen nicht geplant, SigFox-kompatible sowie zertifizierte Hardware kann sich ausschließlich mit dem vom SigFox verwalteten LPWAN verbinden und kommunizieren. Um Geräte mit SigFox kommunizieren zu lassen, muss man sich in einem Gebiet befinden, das von SigFox abgedeckt ist. Das vorrangige Unternehmensziel ist der Aufbau eines globalen funkgestützten LPWANs. SigFox erweitert stetig ihr bestehendes Netz, indem sie Gateways in bereits existierenden Funktürmen installieren. [34]

Ihre Lösung soll sich durch einen günstigen Preis in der Hardwareanschaffung und einen niedrigen Energieverbrauch auszeichnen. Um Teil des SigFox-Netzes zu werden muss neben einer Anmeldung eine monatliche Gebühr entrichtet werden. Im Regelfall kann die Technologie das erste Jahr kostenfrei genutzt werden. Die Firma bietet Unterstützung für Entwickler und Macher an, hat eigene Partnerprojekte mit Hardwareherstellern und bietet eigene Lösungen zum Kauf an.

SigFox hat keinerlei technische Spezifikationen der Übertragungstechnologie und ihrer Protokolle veröffentlicht. Auf Anfrage beim Support konnte in Erfahrung gebracht werden, dass nur Hersteller die für SigFox Anwendungen entwickeln einen Antrag auf Einsicht stellen können, dieser wird jedoch mit einem Non-Disclosure-Agreement gekoppelt, so dass keine tiefergehenden Informationen zur Technologie veröffentlicht werden können.

Die Firma stellt jedoch auf ihrer Homepage YouTube-Videos zur Verfügung, welche statt Texten einen kleinen Einblick in die Technologie ermöglichen. [35]

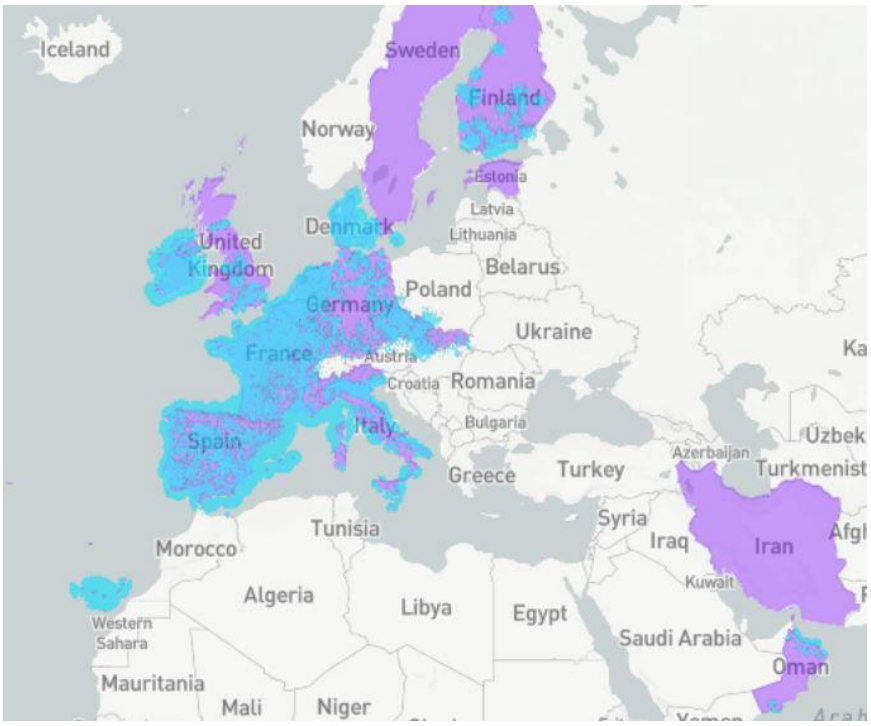
SigFox-Protokollturm

Der SigFox-Protokollturm deckt die Layer Bitübertragung, Sicherung und Netzwerk ab. In der Netzwerkschicht werden die aus der Anwendung stammenden Daten in einen Funkrahmen eingefügt, mit einer Sequenznummer versehen und mit Informationen zur Adressierung und einem Code zu Fehlerkorrektur versehen. Die physikalische Ebene wendet für Uplink-Nachrichten die Differential-Binary-Phase-Shift-Keying-Modulation (DBPSK) oder die GFSK-Modulation für Downlink-Nachrichten an. Schließlich sendet diese Ebene die Daten mit einer Datenrate von 100-600bp/s über eine der möglichen Funkfrequenzen. [36]

Mehr Informationen zur Übertragung können dem Video nicht entnommen werden.

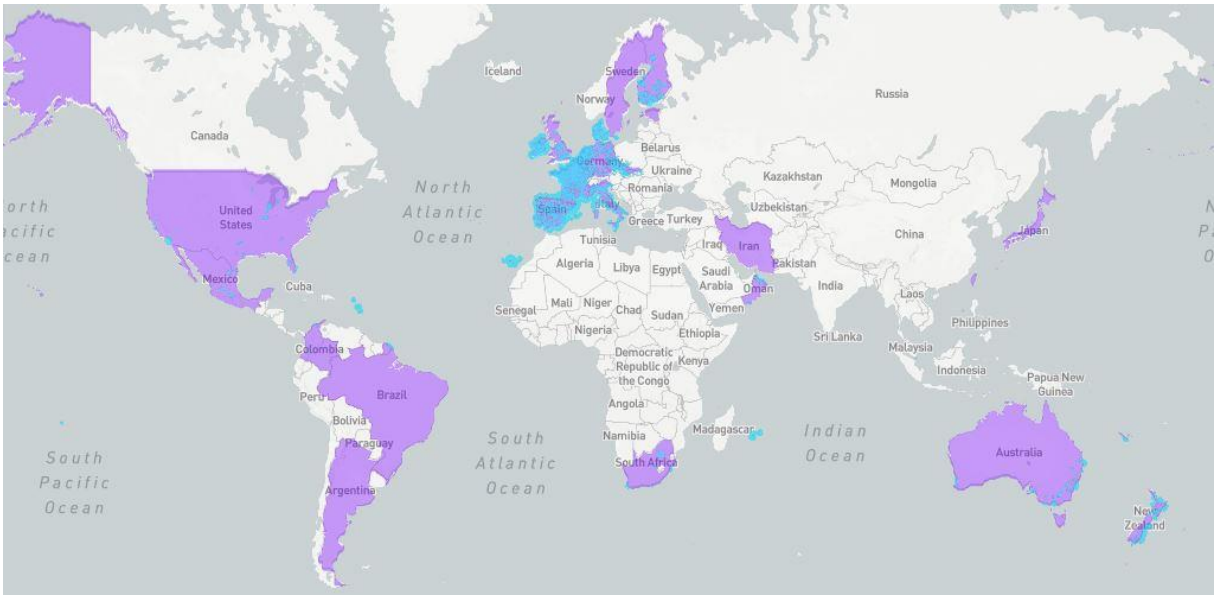
SigFox Abdeckung

Das erste Land, das seit Januar 2014 fast vollständig abgedeckt wurde, ist Frankreich. Überall in Europa sind vereinzelt Gebiete zu finden die bereits durch SigFox abgedeckt sind. Bemerkenswert hoch ist der Anteil jedoch in Irland, den Beneluxstaaten sowie auf den Kanarischen Inseln (Siehe Darstellung 15).



Darstellung 15. Abdeckung durch SigFox in Europa [37]

Darstellung 15 zeigt in blau die aktiven, abgedeckten Sendebereiche des SigFox-Netzwerkes, welche bereits vollständig benutzbar sind. Der violette Farbton markiert Länder in denen nur wenige Stationen vorhanden sind und eine großflächiger Aufbau des Netzwerkes geplant ist. Mittlerweile ist die Firma in 60 Ländern weltweit vertreten, doch die großflächige Abdeckung durch SigFox ist bislang auf die wenigen, genannten europäischen Gebiete beschränkt. Im Vergleich zu Darstellung 15 zeigt Darstellung 16 die derzeitige weltweite Abdeckung durch SigFox. [37]



Darstellung 16. Weltweite Abdeckung durch SigFox [37]

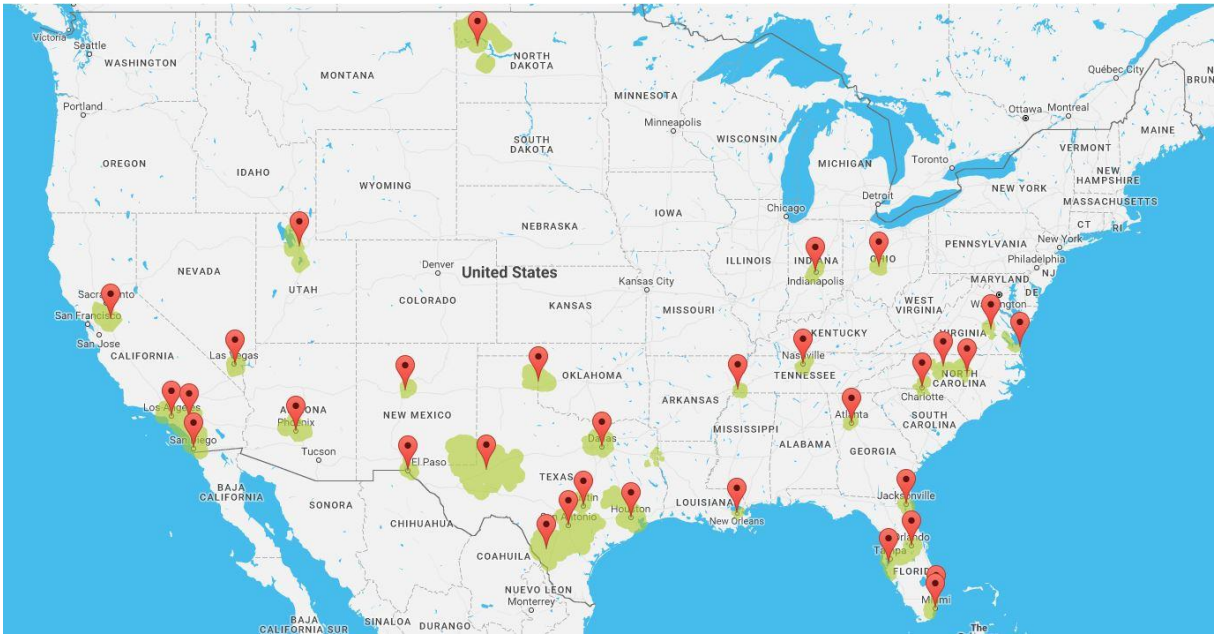
2.2.3. Ingenu

Ingenu ist ein mittelständisches amerikanisches Unternehmen mit Sitz in San Diego. Die Fachbereiche der in 2008 gegründeten Firma liegen im Bereich M2M-Kommunikation, drahtloser Übertragung und der Entwicklung von Technologien für das Internet der Dinge. Ingenu entwickelte das IoT-Protokoll RPMA (Random Phase Multiple Access), welches ausschließlich zur Kommunikation zwischen Maschinen gedacht ist. Auf RPMA basiert auch das öffentliches Drahtlosnetzwerk des Unternehmens - The Machine Network - welches von Ingenu gewartet und erweitert wird. Ingenu sieht sich selbst als Pionier der LPWAN-Technologien und gibt vor, vor seinen Mitbewerbern eine Lösung zur energieeffizienten, großflächigen Kommunikation von Geräten entwickelt zu haben. [38]

Random Phase Multiple Access – RPMA

Die RPMA-Technologie hebt sich in Sachen LPWAN leicht von ihren Mitbewerbern im LPWAN-Sektor ab und verwendet nicht die lizenzfreien Funkfrequenzen unter 1GHz, sondern die weltweit vertretene 2,4GHz-Frequenz. Die vom Unternehmen entwickelte Übertragungsschicht verwendet die Technologie Direct Sequence Spread Spectrum (DSSS), ein Frequenzspreizverfahren, das ursprünglich vom Militär genutzt wurde, um eine sichere Übertragung gewährleisten zu können. Diese Technologie moduliert mathematisch den zu sendenden Datenstrom mit einem String, ähnlich einem Schlüsselwort und verrauscht somit das Signal. Dadurch ist die Funkübertragung sehr störresistent und abhörsicher, da man die Nachricht nur mit dem aufmodulierten Schlüsselwort entschlüsseln kann. Ohne dieses Schlüsselwort kann die Übertragung nicht von dem Hintergrundrauschen einer Funkübertragung unterschieden werden. Die von Ingenu verwendete Variante des DSSS ist um einiges stärker als die in WLAN- und Mobilfunknetzen eingesetzten Varianten. Die extreme Spreizung der Nachricht führt zu einer längeren Übertragungsdauer, aber IoT-Devices benötigen keine schnelle Übertragungsraten wie beispielsweise Anwendungen zur Sprachübertragung. Dies ermöglicht die signifikante Verstärkung des processing gains, des Verarbeitungsgewinns der Übertragung. Dies bedeutet nichts anderes, als dass bei der Verwendung von RPMA ein extrem hohes Link-Budget gewährleistet werden kann – bis zu 177dB. Auf den Mobilfunk übertragen bedeutet dies eine 30-fach höhere Budgetleistung eines UMTS Netzes.

Ingenu unterscheidet sich von Technologien wie WLAN oder Bluetooth vor allem durch die Reichweite. Das Unternehmen gibt an, mit einem Funkturm 400 Quadratmeilen abdecken zu können. [39]



Darstellung 17. Abdeckung von Amerika durch das Ingenu Machine-Network [40]

Wie Darstellung 17 zeiugt beschränkt sich Ingenus Abdeckung derzeit auf Amerika, wo bereits viele Industrieanwendungen wie texanischen Ölfelder oder die Vernetzung ganzer Städte, durch das öffentliche Netzwerk „The Machine Network“, die mit der RPMA-Technologie arbeiten. Ingenu treibt die Implementation ihrer Technologie in großen amerikanischen Städten immer weiter voran und installiert nach und nach mehr Funktürme in urbanen Gebieten. [39]

Kommunikation über AMQP und REST

Zur Ansteuerung der Geräte verwendet Ingenu in der Regel kein Protokoll, unterstützt jedoch ein offenes Übertragungsprotokoll namens Advanced Messaging Queuing Protocol (AMQP). AMQP ist ein ISO-zertifiziertes Internetprotokoll zur Übertragung von Nachrichten. Standardmäßig wird zur Kommunikation der vernetzten Einheiten eine Methode namens Representational State Transfer (REST) genutzt. [41]

Diese REST-Technologie baut auf der Adressierung der Geräte durch URLs sowie ihrer Steuerung durch HTTP-Befehlen auf. Bei diesem Ansatz besitzt jedes Gerät eines Netzwerkes eine eigene ID und kann durch die Angabe einer spezifischen URL, in der die ID des Geräts eingebunden ist, angesprochen und durch HTTP-Methoden wie GET, POST, DELETE und PUT abgefragt und in unterschiedliche Zustände versetzt werden. REST ist in der Lage JSON- und XML-Daten zu interpretieren und kann so universell mit Netzwerkgeräten sowie Webservern und -diensten kommunizieren. [42]

2.2.4. EnOcean

Die EnOcean GmbH ist das größte deutsche Unternehmen mit Expertise im Bereich batterieloser Anwendungen und Funktechnologien für Gebäude- und Industrieautomation, Smart-Homes und dem Internet der Dinge. Das Unternehmen bietet wartungsfreie und batterielose Systeme an, welche durch Energy-Harvesting sowie effizientes Energiemanagement mit einem Minimum an Strom auskommen. Andreas Schneider, der CEO von EnOcean sagt über die Vision des Unternehmens:

"Batterielose Funksensoren werden in die verschiedenste Bereiche unseres Lebens Einzug halten. Ob zu Hause, im Büro oder in unserer kostbaren Freizeit - überall gibt es neue Möglichkeiten, Dinge zu schalten oder Zustände zu erfassen. Keine aufwendige Installation, hoch effizienter Umgang mit begrenzten Ressourcen - die Freude an innovativen Lösungen hält unser Team zusammen und wird auch Sie faszinieren!"- Andreas Schneider [43]

Die Firma hat einen batterielosen Funkstandard im Sub-1GHz-Frequenzbereichs entwickelt und patentieren lassen, der damit beworben wird interoperabel zwischen Systemen verschiedener Anbieter zu sein. Zudem soll es möglich sein, mit diesem Standard energieautarke Systeme kommunizieren zu lassen. [44]

EnOcean-Funktechnologie

Die EnOcean-Funktechnologie setzt sich aus zwei Teilen zusammen. Der patentierte Funkstandard mit der Normbezeichnung ISO/IEC 14543-3-1X - dessen Protokolle die Bitübertragungs-, Sicherungs- und Netzwerkschicht beschreiben - sowie die sogenannten EnOcean-Equipment-Profiles (EEP), welche den Geräten über die Anwendungsschicht standardisierte Kommunikationsprofile bereitstellt. Diese Kommunikationsprofile sollen der Interoperabilität zwischen verschiedenen Herstellern von EnOcean zertifizierten Hardwarelösungen gewährleisten. So können die Sensoren eines Herstellers mit dem Gateway eines anderen Herstellers kommunizieren. Die zugehörige Produktserie trägt den Namen „Dolphin – Self-powered IoT by EnOcean“. [44]

Das Übertragungsprotokoll des Unternehmens wird EnOcean Radio Protocol (ERP) genannt und setzt sich aus den untersten drei Schichten des Protokollstacks zusammen, wie in Darstellung 18 gezeigt wird.

Darstellung 18. Layer Architecture, (Eigene Darstellung nach EnOcean Radio Protocol 2) [45]

Layer	Container	Tasks
Network	Packet	Sub Telegram Timing, Media Access CSMA-CA (LBT)
Data Link	Frame	Sub-Telegram Structure, Hash Algorithms, Header Compression
Physical	Bit	Frequency, Modulation, Preamble, Sync, Coding, Length

EnOcean Bitübertragungsschicht

In der Bitübertragungsschicht wird die Nachricht über die verfügbaren Funkfrequenzen gesendet. Die Übertragung wird hier über Frames umgesetzt. Jeder dieser Frames setzt sich aus einer Präambel, einem Synchronisationswort, der Länge der zu übertragenden Nachricht sowie der Nachricht. [45]

Darstellung 19. Aufbau des EnOcean-Frames in der Bitübertragungsschicht [45]

Der Aufbau des Frames wird in Darstellung 19 ersichtlich. Die Nachricht wird in der Darstellung als Data_PL bezeichnet. Die Präambel und das Synchronization-Word bestehen jeweils aus 16bit, die Länge der Nachricht ist im ersten Byte nach dem Synchronization-Word gespeichert. Die Nachricht muss minimal eine Länge von einem Byte und kann maximal die Länge von 255 Bytes umfassen. [45]

EnOcean Sicherungsschicht

Die Länge sowie die Nachricht werden an die Sicherungsschicht weitergeleitet. Die Sicherungsschicht überträgt die Nachricht in sogenannten Subtelegrams, von denen jeweils drei gesendet werden. Um Kollisionen von Subtelegrams zu vermeiden wird die Listen-before-Talk-Technik eingesetzt. Dies bedeutet, dass der Sender die Leitung abhört und Nachrichten nur gesendet werden, wenn die Leitung frei ist. Die Subtelegrams - bestehend aus Länge und Nachrichteninhalt - können auf zwei verschiedene Weisen aufgebaut werden, je nachdem ob die Datenlänge über sechs Byte liegt. [45]

Darstellung 20. Aufbau des Subtelegrams bei einer Länge <= 6 Byte [45]

Wie in Darstellung 20 ersichtlich, bestehen Subtelegrams die kleiner als sechs Byte sind lediglich aus der Länge, der Sender-ID sowie den zu übertragenden Daten. Diese Subtelegrams sind reserviert für späteren Nutzen, bislang wird lediglich die fünf Byte lange Nachricht als Smart-Acknowledgement genutzt. [45]

Darstellung 21. Aufbau des Datagramms bei einer Länge > 6 Byte [45]

Darstellung 21 zeigt den Aufbau eines Subtelegrams mit einer Größe über sechs Byte. Der Header enthält Informationen darüber, welche Größe die IDs besitzen, ob es sich um einen Extended-Header handelt. Ein erweiterter Header enthält zusätzliche Informationen über die Anzahl von Wiederholungsversuchen und ob es sich um die Originalnachricht handelt, sowie mögliche Zusatzdaten, wie die Art des Subtelegrams. Diese Information wäre im Feld

Extended Telegramtype zu finden. Bei Energiespar-Anwendungen wird auf diesen Header verzichtet. Die ID des Senders sowie die des Empfängers sind in den Abschnitten Originator-ID und Destination-ID beinhaltet. Während die Empfänger-ID immer 32-Bit ist, kann die Sender-ID 24, 32 oder 48 Bit umfassen. In Data DL ist die zu übertragende Nachricht gespeichert. Der Inhalt der zusätzlichen Daten ist nicht festgelegt. In diesen 0-3 Bits können jedoch Anwendungsspezifische Informationen untergebracht werden, wenn nötig. Das Subtelegram schließt mit einem Cyclic-Redundancy-Check (CRC), der einen zuvor generierten HASH-Wert der Nachricht beinhaltet. Somit kann die Korrekte Übertragung im Nachhinein überprüft werden und Duplikate verworfen werden. [45]

EnOcean Netzwerkschicht

Wie bereits in Abschnitt 1.2.1.5. beschrieben befasst sich die Netzwerkschicht mit der Adressierung und Weiterleitung der Telegramme. Diese Telegramme enthalten Informationen darüber, wie oft sie bereits weiderholt wurden. Bei EnOcean gibt es zwei Level von Repeatern. Level-1-Repeater wiederholen nur Originalnachrichten, während Level-2-Repeater zusätzlich Nachrichten wiederholen die bereits einmal wiederholt wurden. Mehr Wiederholungen sind nicht möglich. Die Adressierung wird über einen Verkapselungsmechanismus im Telegramm abgewickelt. Dabei gibt ein Wert im Telegram-Typ-Feld Auskunft darüber, wo sich die Adressinformationen befinden, die daraufhin im Telegram gefunden und ausgelesen werden können. [46]

2.2.5. Weightless

Weightless ist ein auf dem GSM-Mobilfunk-Standard aufbauende Funktechnologie die speziell für LPWANs und das Internet der Dinge ausgelegt wurde, um die Schwächen von teuren Mobilfunk-Einheiten und Funk mit kurzer Reichweite wie Bluetooth oder WLAN zu kompensieren. Weightless bietet zwei unterschiedliche Varianten ihres Standards an: Weightless-N und Weightless-P.

Weightless-N arbeitet auf dem Ultra-Narrow-Band und basiert auf der Idee ihres Vorgängers Weightless-W, einer sternförmigen LPWAN-Topologie die über sogenannte White-Spaces kommuniziert. White-Spaces sind die durch Abschaffung terrestrischer Funkanwendungen im TV oder Radio freigewordene Frequenzen. In Deutschland wird dieser Bereich auch Digitale Dividende genannt und unterliegt der Verteilung der Landesrundfunkanstalten. Dies führte schließlich zur Entwicklung der N- und P-Standards, welche über die freien ISM-Bänder kommunizieren können. Übertragungen können bei Weightless-N nicht nur mit einem 128Bit-AES-Algorithmus verschlüsselt werden, sondern bieten auch Frequency-Hopping durch die Nutzung des Differential Binary Phase Shift Keying (DBPSK) an. Dies bietet dem Standard eine hohe Störsicherheit, da bei Interferenzen die Frequenz gewechselt wird und somit die sichere Übertragung gesichert ist.

Weightless-P ist die Weiterentwicklung dieser Idee, bei der versucht wurde, das System von Weightless-N aufzugreifen und performanter zu machen. Das P steht aus diesem Grund auch für Performance. Diese Technologie ist das selbsternannte Flaggschiff des Unternehmens und erweitert Weightless-N um verbesserte Netzwerkfunktionen wie beispielsweise die Forward Error Correction (FEC) oder Automatic Retransmission Requests (ARQ). [47]

2.2.6. IEEE 802.11ah/WiFi-HaLow

WiFi-HaLow ist der Versuch der unter 1.4.1. beschriebenen WiFi-Allianz, eine auf dem WLAN-Standard aufbauende Technologie zur Konnektivität von Geräten in einem LPWAN zu gestalten. Dabei erweitert es die Funktionalität des IEEE 802.11 WLAN dadurch, dass es über 900MHz im Sub-1GHz-Raum senden kann. Das Unternehmen beschreibt die Reichweite der Technologie als bereits doppelt so weit wie der WLAN-Standard. Geplant ist, diese Technologie allen Geräteherstellern der WiFi-Allianz zur Verfügung zu stellen, um den Geräten die Netzwerkfähigkeit über 2,4GHz, 5GHz sowie 900MHz zu ermöglichen.

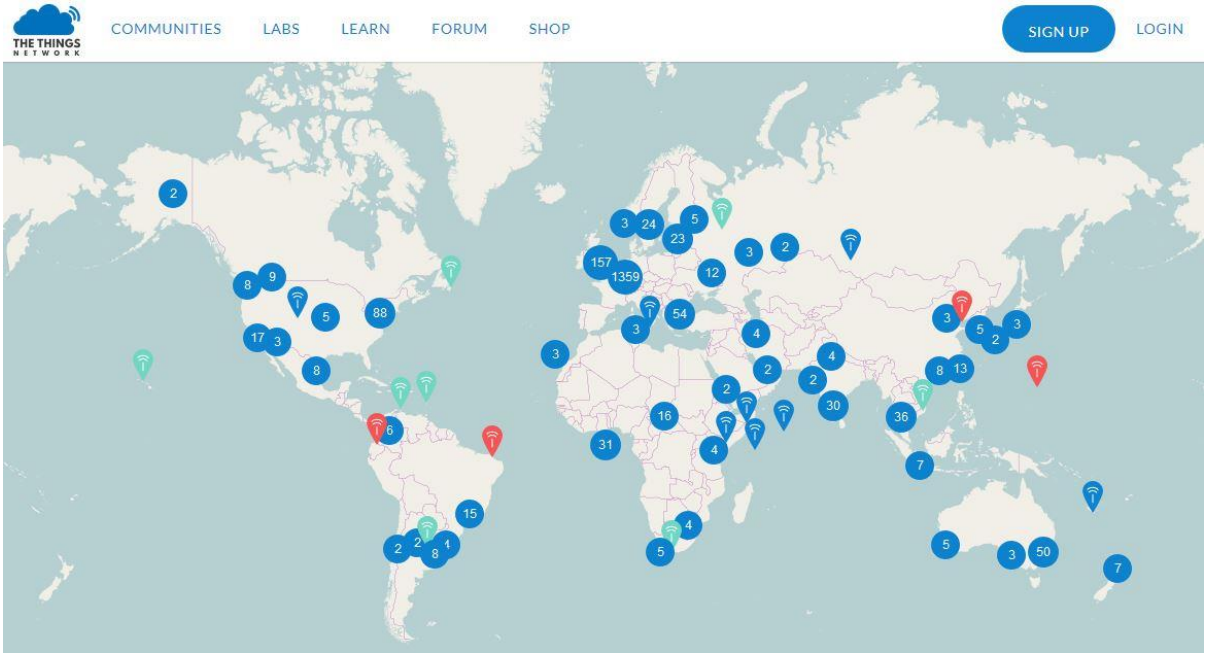
Da es viele der Protokolle und Features des Ursprungstandards beibehält, verfügt HaLow über eine IP-basierte Konnektivität und dessen Sicherheitsmöglichkeiten ermöglicht aber zusätzlich, dass Tausende von Geräten an einen WiFi-Knoten gekoppelt werden können. Zusätzlich zur Erweiterung des Frequenzspektrums verfügt WiFi-HaLow über niedrige Energieanforderungen, die einen Einsatz im Internet der Dinge überhaupt erst möglich machen sollten. [48]

2.3. Internationale Verbreitung von LPWAN für IoT

LPWANs sind derzeit weltweit eine Neuheit. Da sich LPWANs derzeit noch in vielen Bereichen in der Entwicklungsphase befinden und es keinerlei festgesetzte Standards zu Übertragung und Verarbeitung gibt, gibt es wenige Firmen oder Allianzen die sich mit der Verbreitung von LPWAN-fähigen Geräten und den dazugehörigen Protokollen beschäftigen. Anwendungsgebiete von Ingenu sind so meist große Industriestätten wie Ölfelder. Ferner wird die Technologie eingesetzt um ganze Städte zu vernetzen.[39] SigFox baut sein Netzwerk nach und nach in Europa aus, außerhalb von Europa sind die verfügbaren Accesspoints jedoch selten. [37]

EnOcean ist nicht auf eine großflächige Abdeckung ausgelegt und wird ausschließlich im Nahbereich verwendet.

Die Abdeckung durch private LoRaWAN-Netzwerke lässt sich nur schwer einschätzen, jedoch gibt es für LoRaWAN bereits öffentliche Netze, die ähnlich einer Community betrieben werden.



Darstellung 22. Übersicht aller LoRaWAN-Gateways im "The Things Network" [49]

Wie Darstellung 22 zeigt, verfügt The Things Network besonders in europäischen Städten über viele Möglichkeiten zur Anbindung, aber auch weltweit sind etliche Access-Points registriert. Da diese jedoch meist privat eingebunden werden, ist nicht davon auszugehen, dass eine ideale Infrastruktur vorhanden ist. [50]

3. Vergleich aktueller Anbieter von LPWAN-Systeme für das Internet der Dinge

3.1. Parameter zum Vergleich der LPWAN-Systeme

Im Folgenden werden einige Parameter erläutert, welche eine grundlegende Bewertung der vorhandenen Technologien zur LPWAN-Erstellung ermöglichen. Hierbei wird ausschließlich auf Literatur zurückgegriffen, da es im Rahmen der Arbeit aufgrund des Budgets und der Verfügbarkeit der teils noch experimentellen Hardware leider nicht möglich war, Benchmarking-Tests aller verfügbaren Technologien durchzuführen.

3.1.1. Anbindung von Geräten an das Netzwerk

Besonders wichtig zur Bewertung der LPWAN-Möglichkeiten ist die Anzahl der Geräte, die an ein Netzwerk gekoppelt werden können. Auch die das Einbindens neuer Geräte in ein bestehendes Netzwerk sollte keine Komplikationen darstellen.

3.1.2. Störanfälligkeit, Gegenmaßnahmen

Funknetzwerke sind stets anfällig für Störungen durch andere Funkanwendungen, überlappende Frequenzen und ähnliche Faktoren. Moderne Protokolle verfügen über Möglichkeiten, solchen Störungen entgegenzuwirken und auf andere Frequenzen oder Übertragungsmethoden umzuschalten, sollten Probleme auftreten. Unter diesem Punkt soll untersucht werden, wie störanfällig die Systeme sind und welche Störungen von den Anbietern erkannt, vorgebeugt und behoben werden können.

3.1.3. Stromverbrauch

Bereits im Namen der zu untersuchenden Netzwerkart vorkommend, werden bei LPWANs die Möglichkeiten zur low-power consumption großgeschrieben. Bei der Übertragung im Internet der Dinge ist weiterhin der Stromverbrauch ein großes Thema. Sensoren können bereits jahrelang mit einer einzelnen Knopfzelle mit Strom versorgt werden, wenn Sie über Ruhemodi verfügen. Datenübertragung via Funk über eine weitere Strecke fordert jedoch deutlich höhere elektronische Ressourcen ein – wie hoch diese bei den Anbietern sind und ob der Sendevorgang über Energiesparoptionen verfügt, soll verglichen werden.

3.1.4. Reichweite

Selbstverständlich kommt es bei der Reichweite nicht nur auf den programmiertechnischen Aufbau des Übertragungsprotokolls an, sondern auch auf eine Kombination aus selbiger, dem verfügbaren Energiepotenzial, der Sendeleistung sowie der Art der Antenne. Dennoch gibt es Unterschiede in der Reichweite der vorzustellenden Systeme welche hier beleuchtet werden sollen. Die Reichweite setzt sich unter anderem auch aus Sensitivität der Empfangseinheiten sowie dem Aufbau des Signals zusammen. Ein starkes Signal kann von empfindlichen Empfängern über größere Distanzen empfangen werden, als ein schwaches.

3.1.5. Frequenzbereiche

Weltweit werden verschiedene Frequenzbereiche verwendet, um das Internet der Dinge zu vernetzen. Während Kleingeräte in Europa häufig mit 868MHz oder 414MHz senden, sind in Amerika und Asien andere Frequenzbänder für eine derartige Kommunikation reserviert. Außerdem müssen die regional unterschiedlichen Gesetzgebungen zur freien Verwendung von Frequenzen beachtet werden, die einerseits von Land zu Land unterschiedlich sein können, andererseits aber auch durch international gültige Funkfrequenzverträge geregelt sind. Das Funken auf reservierten Frequenzen stellt nicht nur in Deutschland einen Straftatbestand dar. Internetdienste sollten international verwendbar sein und somit sollten die Anbieter berücksichtigt haben, weltweit lizenzfreie Frequenzen in ihren Protokollen nutzbar zu machen. Zum einen wird betrachtet, ob neben dem ISM-Band die freien Frequenzen anderer Länder unterstützt werden und zum anderen ob eine Einbindung über 2,4GHz in handelsübliche Drahtlosnetzwerke möglich ist.

3.1.6. Übertragungsrate

LPWANs benötigen grundsätzlich keine hohe Übertragungsrate, da dies der Idee des Systems widersprechen würde. Hierbei ist jedoch interessant welchen Bereich die überprüften Technologien abdecken und mit welcher Datenrate ein Sendevorgang möglich ist.

3.1.7. Mögliche Sicherheitsmaßnahmen

Die Nutzung von freien Funkfrequenzen haben den großen Nachteil, dass sie frei sind und somit von jedem benutzt werden können. Natürlich ist es von Vorteil für funkbasierte Internet-der-Dinge-Anwendungen, ohne Lizenzen Daten über gewisse Frequenzen zu senden. Dies bedeutet jedoch im Umkehrschluss, dass die auf den entsprechenden Frequenzen gesendeten Daten ebenfalls von jedem abgehört oder empfangen werden

können. Unter diesem Punkt soll untersucht werden, ob und wie die Anbieter die Möglichkeit zur Verschlüsselung der zu sendenden Daten geschaffen haben.

3.1.8. Kosten

Betrachtet man die Kosten der unterschiedlichen LPWAN-Systeme, schlüsseln diese sich in zwei unterschiedliche Teilkosten auf. Als wichtigster Punk werden Anschaffungskosten berücksichtigt, zu denen die Hardware (Sender, Empfänger, Antennen) gehört. Der zweite Faktor sind die Unterhaltungskosten. Dies könnten beispielsweise monatliche Gebühren für die Nutzung eines Firmennetzwerkes sein.

3.1.9. Stand der Entwicklung

Obwohl das Feld der LPWANs im Internet der Dinge noch relativ neu ist und derzeit noch kein wirklich festgesetzter Standard zur Datenübertragung existiert, rühmen sich die Anbieter der Systeme mit der weitesten Verbreitung oder damit, dass sie den einzig wahren Standard besitzen. Wie weit sind die angepriesenen Produkte jedoch wirklich entwickelt, welche Schritte fehlen noch zu einem vollständig marktreifen Produkt? Unter diesem Punkt werden die aktuellen Entwicklungen der Technologien kurz beschrieben und es wird überprüft ob und wie sie bereits eingesetzt werden.

3.3. Bewertungssystem

Um den Vergleich der Technologien übersichtlicher zu gestalten, werden folgende vier Bewertungsmöglichkeiten eingeführt:

[++] Die Technologie des Anbieters zeigt eindeutige Stärken in dieser Disziplin.

[+] Die Technologie setzt den Punkt gut um, könnte jedoch verbessert werden.

[-] Die Technologie zeigt Defizite bei der Umsetzung der festgelegten Punkte.

[--] Die Technologie hat große Schwächen oder Defizite in diesem Abschnitt.

Die Bewertung ist in jedem Abschnitt in der Zeile der Überschrift rechts zu sehen. Im Anschluss an die Einzelbetrachtung werden die Bewertungen der Anbieter tabellarisch zusammengefasst und dargestellt.

3.4. Vergleich der ausgewählten Anbieter

Im folgenden Textabschnitt werden mit den aufgeführten Parametern die Anbieter LoRa, SigFox, Ingenu und EnOcean verglichen und mit dem eingeführten Schema bewertet. Vom Vergleich weiterer Anbieter wird abgesehen, um einen Überblick über die aussichtsreichsten und am fortschrittlichsten Technologien abzubilden.

3.4.1. LoRaWAN

Anbindung von Geräten an das Netzwerk [++]

LoRaWAN nutzt zwei primäre Technologien zum Anbinden neuer Geräte: Die Over the Air Activation (OTAA) sowie die Activation by Personalisation (ABP). Für das OTAA-Verfahren wurde der jeweilige Sensor bereits beim Hersteller mit einem einzigartigen Device Identifier sowie einem Application Identifier versehen mit dem sich das Gerät selbstständig im Netzwerk anmelden kann. Das jeweilige Gateway erkennt, welches Gerät sich für welche Aufgabe in das Netz einwählen möchte und baut eine gesicherte Verbindung auf, über die nun Daten ausgetauscht werden können. Bei dem ABP-Verfahren ist ein Großteil dieses Vorgangs schon durch passende Parameter vorkonfiguriert und die sichere Verbindung kann sofort aufgebaut werden. Zudem können in ein korrekt angelegtes LoRaWAN-Netzwerk problemlos mehrere Hundert Nodes eingebunden werden. [51]

LoRaWAN Geräte können sich also selbst in bestehenden Netzwerken anmelden und ihre Daten an die Gateways senden. Hier kommt wieder die „Dumb-Gateway Smart-Cloud“-Funktionalität zum Tragen. Nachdem sich das Gerät angemeldet hat, sagt es den zuständigen Gateways, für welchen Dienst die Nachricht gedacht ist und dieses leitet die Nachricht weiter. [29]

Semtech stellt bereits viele verschiedene Chipsätze her, die es ermöglichen LoRa-Netzwerke aufzusetzen. Die benötigte Hardware ist günstig und wird von verschiedenen Anbietern der LoRa-Allianz sowie Drittanbietern vertrieben.

Störanfälligkeit, Gegenmaßnahmen [++]

LoRaWAN zeichnet sich durch eine besonders hohe Störsicherheit aus. Die implementierte Frequenzspreizung führt dazu, dass die Funksignale unabhängig von existierenden Störquellen vollständig übertragen werden. Außerdem können Sensibilitätswerte von bis zu -137dBm erreicht werden, was die Durchdringung von Wänden bis hin zu Kellerräumen ermöglicht. [51]

Stromverbrauch [++]

Der Stromverbrauch bei den von Semtech hergestellten Mikrochips liegt bei einer Sendeleistung von 20dBm bei ca. 120mA. Der nötige Empfangsstrom RX ist bei LoRaWAN beeindruckend niedrig, da er mit unter 3mA fast siebenfach unter dem Wert von Mitbewerbern liegt. Alle von Semtech hergestellten LoRa-Chips besitzen einen Sleep Mode der lediglich einen konstanten Strom von nur 100nA benötigt. [52]

Reichweite [+]

Bei herkömmlichen LoRaWAN-Geräten können je nach Umgebung und Bebauung Reichweiten zwischen 2 und 15km erreicht werden. Dabei ist davon auszugehen, dass in ländlichen Gebieten eine höhere Reichweite zu erwarten ist als in einer Stadt. Leistungsstarke Systeme können bei idealen Gegebenheiten sogar bis zu 50km in ländlichen Gebieten erreichen. [51]

Frequenzbereiche [+]

LoRaWAN ist darauf ausgelegt, alle freien Frequenzbänder zu nutzen. So werden in Deutschland die SRD/ISM-Bänder 433MHz und 868MHz genutzt. Aber LoRaWAN ist ebenfalls in der Lage auf 915MHz für Länder in Asien oder Amerika zu senden. Viele der Chips sind in der Lage von 137-1020MHz zu senden, jedoch ist eine voreingestellte Beschränkung sinnvoll, um rechtliche Probleme zu vermeiden. [53]

Übertragungsrate [-]

LoRaWAN steuert die Datenrate jedes Gerätes im Netzwerk je nach Anwendung selbst. Die Anwendungsfälle unterteilt LoRa hierbei in die Klassen A, B und C (Nachzulesen im Abschnitt 2.2.1.). Ziel dabei ist es, besonders niedrige Datenraten zu erzielen, um so eine energieeffiziente Datenübertragung über weite Strecken zu ermöglichen. Bei LoRaWAN liegen die Datenraten im Durchschnitt zwischen 0,3-50 kbits/s [53]

Mögliche Sicherheitsmaßnahmen [+]

Die sichere Funkübertragung bei LoRaWAN ist mithilfe drei verschiedener 128Bit-AES-Schlüssel gewährleistet: Ein Schlüssel, der nur der Anwendung und dem Gerät bekannt ist, ein Anwendungs-Sitzungsschlüssel sowie ein Netzwerk-Sitzungsschlüssel. Diese verhindern das Abhören des Datenstroms durch Dritte.

Außerdem setzt das Protokoll das sogenannte Frame Counting ein. Mit jeder Übertragung wird ein hochzählender Wert beim Sender mit dem erwarteten hochzählenden Wert des Pakets beim Empfänger verglichen. Liegt dieser Wert unter dem erwarteten Wert, wird das Paket abgelehnt. [53]

Geräte und Anwendungen verfügen über eindeutig zuordenbare 64bit-Device-IDs und Application-IDs. Tritt ein Gerät einem Netzwerk bei, bekommt es zusätzlich eine 32bit-Device-Adress zugeteilt, die sie im Netzwerk identifiziert.

Kosten [++]

Die Hardwarekosten variieren selbstverständlich nach Anbieter und Ausführung, jedoch können für LoRaWAN günstige Hardwarebestandteile erworben und selbst zusammengebaut werden. LoRaWAN legt Wert darauf, private Netzwerke zu ermöglichen, was die durchschnittlichen Kosten eines LoRa-Systems weit unter seinen Mitbewerbern hält, da der Anwender lediglich die Stromkosten entrichten muss, sobald die Infrastruktur aufgebaut wurde. [54]

Die Chipsätze die zur Nutzung von LoRaWAN benötigt werden, werden jedoch ausschließlich von Semtech produziert – In Zukunft will Semtech wohl andere Hersteller lizenzieren, bislang ist dies jedoch noch nicht geschehen. [55]

Stand der Entwicklung [+]

Die LoRaWAN Technologie ist derzeit noch in der Weiterentwicklung, wird jedoch bereits von vielen Hardwareherstellern implementiert. Hinter LoRa stehen neben der Muttergesellschaft Semtech viele namhafte große IT Firmen, welche die Entwicklung der Technologie forcieren. Dieser Zusammenschluss ergibt die LoRa-Alliance. LoRas großer Vorteil liegt außerdem in der Funktionalität zur Erstellung von privaten Netzwerken, was die Nutzung von LoRa in Industrie und Forschung gerade zu einem frühen Zeitpunkt interessant macht. [31]

Zusätzlich zu privaten Netzwerken stehen bereits zwei große öffentliche Netzwerke zur Verfügung, in die man sich einwählen kann: MachineQ und The Things Network. Diese Netzwerke ermöglichen es den Nutzern Basisstationen zur Verfügung zu stellen und gleichzeitig alle Basis-Stationen zu nutzen, die bereits im Netzwerk vorhanden sind. [56]

3.4.2. SigFox

Die Firma SigFox hat ihren Geschäftsbereich darauf spezialisiert, als Verwalter und Anbieter von IoT-Funklösungen zu sein. Dabei behält sie vor, den Einblick in sämtliche technische Dokumentation zur Übertragungstechnik unter Verschluss zu halten.

Anbindung von Geräten an das Netzwerk [--]

Das SigFox-Netzwerk ist ein rein kommerziell betriebenes Netzwerk, welches lediglich von Sendestationen des Unternehmens ausgesendet wird. Die Homepage der Firma gibt deutlich Auskunft darüber, dass SigFox kein Interesse an der Unterstützung von

Privatnetzwerken hat. Um Geräte in das SigFox-Netz einbinden zu können muss man Kunde der Firma werden und monatliche Gebühren entrichten. Dabei ist zu beachten, dass SigFox bislang keine großflächige Abdeckung außerhalb Frankreichs besitzt und somit uninteressant für jeden Nutzer ist, der außerhalb des möglichen Empfangsbereichs ist. [37]

Derzeit ist es Kunden des niedrigsten Leistungspakets nur möglich 140 Uplink- sowie vier Downlink-Nachrichten pro Tag zu versenden. Ein weiterer Kritikpunkt ist, dass ein Nutzer gezwungen ist, Geräte von SigFox oder deren Partnerfirmen zu erwerben, um dem Netzwerk überhaupt Geräte hinzufügen zu können. [57]

Störanfälligkeit, Gegenmaßnahmen [+]

SigFox sendet seine Daten im Ultra-Narrow-Band mit etwa 100Hz. Damit liegt SigFox weit unter allen Mitbewerbern. Die bedeutet jedoch gleichzeitig, dass es störanfällig für Interferenzen von Breitbandfunk ist. Außerdem wird die Übertragung von Uplink-Nachrichten durch die eingesetzte Differential-Binary-Phase-Shift-Keying-Modulation (DBPSK) und die Nutzung des dadurch ermöglichten Frequency-Hopping störsicherer. [58]

Stromverbrauch [++]

Im Gegensatz zu LoRa, deren Chips ausschließlich durch Semtech hergestellt werden, lässt SigFox diverse Firmen Chipsätze in Lizenz bauen. Zu den lizenzierten Chipherstellern gehören neben unbekannteren Firmen auch große Unternehmen wie Texas Instruments oder Atmel. Da unterschiedliche Hersteller Chipsätze produzieren, weichen die Werte zum Stromverbrauch je nach Gerät leicht ab, halten sich jedoch immer in einem Bereich von 50-70mA bei einer Übertragungsleistung von 14dBm und einem Empfangsstrom von etwa 30mA. Die meisten SigFox-fähigen Chipsätze verfügen über diese Sendeleistung. Im Ruhezustand verbrauchen SigFox Geräte der Firma Telit lediglich 1,5 µA.[59]

Reichweite [+]

SigFox gibt an, in ländlichen Gebieten zwischen 30 und 50 Kilometer abdecken zu können. In dicht besiedelten Gebieten oder Städten fällt die Reichweite auf 3-10 Kilometer. [60]

Frequenzbereiche [+]

SigFox ist in der Lage auf den Frequenzbändern 868MHz in Europa sowie 902MHz in Amerika zu senden. [60]

Übertragungsrate [-]

Die Übertragungsrate von SigFox liegt zwischen 100bps und 600bps, abhängig davon, in welcher Region das Gerät genutzt wird. In Europa sind nur 100bps möglich - um Überschreitungen der Frequenzbelegungsdauer zu vermeiden. [36]

Mögliche Sicherheitsmaßnahmen [-]

Über die implementierten Sicherheitstechniken der Übertragungstechnologie ist auf Grund der Informationszurückhaltung und der Proprietarität der Protokolle seitens SigFox keinerlei Aussage über die Qualität der Sicherheitsmaßnahmen zu machen. [60]

Kosten [+]

SigFox lässt seine Hardware in großen Mengen bei Firmen wie Atmel oder Texas Instruments herstellen. Chips und andere Einheiten können in großen Mengen unter 10$ pro Stück erworben werden. SigFox legt keinen Wert darauf, durch den Vertrieb der Hardware Gewinn zu machen. Das Konzept dieser Firma ist es, die Software und das Netzwerk selbst zu verkaufen. So sollten Datenpakete geschnürt werden die sich nach einer gewissen Menge an Nachrichten pro Tag richten. Über die Preise der Pakete konnten keine Informationen gesammelt werden [55]

Diese Datenpakete könnten wie folgt aussehen:

Darstellung 23. Datenoptionen des SigFox-Netzwerks,(Eigene Darstellungen nach One Day at SigFox) [59]

Datenpakete	*Uplinknachrichten*	*Downlinknachrichten*
Platinum	101 bis 140 Stk.	4 Stk.
Gold	51 bis 100 Stk.	2 Stk.
Silver	3 bis 50 Stk.	1 Stk.
One	1 bis 2 Stk.	keine

Stand der Entwicklung [+]

SigFox ist derzeit noch in einer frühen Phase - Zwar ist die technologische Entwicklung bereits gegeben, jedoch ist die Verfügbarkeit von Accesspoints für das SigFox-Netzwerk sehr klein. Bis auf große Teile Frankreichs und der Beneluxstaaten gibt es keine große Abdeckung durch SigFox-Basisstationen. Weiterhin ist unklar, wie sich das Bezahlmodell entwickeln wird, da darüber bislang noch kaum Informationen preisgegeben wurden. Durch den Zwang, das Netzwerk des Unternehmens nutzen zu müssen, verwenden viele Industrie- und Forschungseinrichtungen stattdessen LoRa oder ähnliche Technologien. [55]

3.4.3. Ingenu

Anbindung von Geräten an das Netzwerk [-]

Sofern man ein RPMA fähiges Gerät besitzt, sollte dieses ohne Probleme dem öffentlichen Netzwerk der Firma (The Machine Network) beitreten können, nachdem man sich im Netzwerk angemeldet und das Gerät hinzugefügt hat.[61]

Dazu muss sich das Endgerät jedoch in Reichweite einer Basisstation des Ingenu-Netzwerkes befinden, welche sich fast ausschließlich in Amerika befinden. Dies ist besonders für Europäer ein großer Nachteil dieser Technologie.

Störanfälligkeit, Gegenmaßnahmen [+]

Aufgrund der speziellen Wellenform des RPMA-Funks ist diese Technologie sehr unempfindlich gegen Störquellen. Die Verwendung des verbesserten Direct-Sequence-Spread-Spectrum (DSSS) gewährleistet eine sehr störresistente und abhörsichere Übertragung, die um einiges stärker als die in WLAN- und Mobilfunknetzen eingesetzten Varianten. Diese Spreizung der Übertragungen führt zu einem hohen Link Budget. [39]

Stromverbrauch [+]

Ingenu legt viel Wert auf die Anpassung ihrer Technologie zugunsten von Energiesparoptionen. Sie verwenden adaptive Spreizfaktoren um die Sendezeit der Nodes möglichst gering zu halten. RPMA sendet zudem nur in notwendigen Fällen und versetzt die Einheiten sonst in einen Sleep-Mode. [62]

Das von der Firma ublox angebotene NANO-S100-Modul verbraucht in diesem Sleep-Mode 10µA. Der zum Empfang benötigte Strom liegt zwischen 75 und 90mA, während die Übertragung bei einer Sendeleistung von 23,3dBm (entspricht ca. 214 mW) zwischen 200 und 300mA benötigt. [63]

Dies ist im Vergleich zu den Mitbewerbern zwar etwas mehr, jedoch senden diese auch mit niedrigerer Sendeleistung. Für die erbrachte höhere Sendeleistung ist der Energieverbrauch durchaus niedrig.

Reichweite [++]

Ingenu gibt an, in Amerika mit einer Basisstation ganze 70 Quadratmeilen (181.3 km^2) und 33 Quadratmeilen (77,7 km^2) in Europa abdecken zu können. [62]

Frequenzbereiche [-]

Ingenu arbeitet ausschließlich innerhalb des 2,4GHz Bandes und verfügt über keine Konnektivität zu den Frequenzen des Sub-GHz Raums.

Übertragungsrate [++]

Laut Ingenu verfügt die RPMA-Technologie von Datenübertragungsraten bis zu 19000bps in Europa [62].

Da auf der 2,4GHz Frequenz gesendet wird, gelten regionale Datendurchsatzbeschränkungen nicht für diese Technologie. Dies ist der größte Vorteil von Ingenu gegenüber seinen Mitbewerbern.

Mögliche Sicherheitsmaßnahmen [++]

Ingenu implementiert in der Übertragungstechnik aktuelle Sicherheitstechnologien wie Zwei-Wege-Authentifizierung, sicheren Multicast, Geräteanonymisierung, authentisierte Firmware-Updates, Nachrichtenintegrität und -vertraulichkeit sowie einen Schutz vor der Penetration durch wiederholte Nachrichten. [60]

Kosten [-]

Ingenu verfolgt bei der Verbreitung eine Mischung aus den Ansätzen von LoRaWAN und SigFox. Ingenu verfügt über ein öffentliches Netzwerk namens „The Machine Network“ in dem man sich mit RPMA-fähigen Geräten anmelden kann. Die Einrichtung von Sendestationen bleibt jedoch bei Ingenu. Die Konnektivität ist aus diesem Grund auf wenige Städte der USA beschränkt. [62]

RPMA-taugliche Hardware wird von unterschiedlichen Firmen angeboten, doch ist nicht in Webshops käuflich. Auf der Ingenu-Hompage sind beispielhaft kompatible Geräte sowie ihre Hersteller aufgelistet, jedoch sind weder auf der Ingenu-Internetseite noch auf vielen der Hersteller- und Vertriebseiten Preise zu finden. [64]

Die Firma ublox bietet ein von Ingenu zertifiziertes Starterkit an, welches eine kleine Programmiereinheit mit RPMA-Funktionalität beinhaltet. Dieses Kit kostet 245€. [65]

Stand der Entwicklung [+]

Ingenus RPMA ist eine einzigartige Technologie zur Funkübertragung im Internet der Dinge. Sie ist weltweit die einzige Langstreckenfunk-Technologie die das 2,4GHz Spektrum zur Datenübertragung nutzt. [62]

Das von Ingenu angebotene öffentliche Netzwerk ist derzeit noch im Aufbau und beschränkt sich größtenteils auf amerikanische Großstädte.[40]

Neben einigen industriellen Anwendungen die von Firmen in Auftrag gegeben wurden, ist die Erstellung eigener Gateways zum RPMA Netzwerk nicht möglich. Da die Endgeräte noch sehr teuer sind, keine großflächige Abdeckung existiert und die Sendeparameter für den amerikanischen Funkraum optimiert sind, was Übertragungsraten und Sendeleistung angeht, ist diese Technologie derzeit nicht für eine Anwendung in Europa geeignet. Dennoch ist die Technologie beeindruckend und zählt zu den besten LPWAN-Optionen.

3.4.4. EnOcean

Anbindung von Geräten an das Netzwerk [++]

EnOcean-Geräte können ohne Probleme an bestehende EnOcean-Anwendungen gekoppelt werden. Die von EnOcean entwickelte Middleware ermöglicht die Interoperabilität mit vielen verbreiteten Geräten zur Gebäudeautomation. Hersteller können zudem der EnOcean-Alliance beitreten, um Unterstützung bei der Entwicklung von EnOcean-fähigen Geräten zu bekommen. Einige Einheiten sind sogar bereit von Werk aus in der Lage, über Bluetooth oder WiFi mit anderen Geräten zu kommunizieren. [66]

Störanfälligkeit, Gegenmaßnahmen [+]

EnOcean zählt zu einer der störungsfreisten Funktechnologien derzeit, was hauptsächlich durch die kurzen Telegramme ermöglicht wird. Durch das Senden von etwa 1ms langen Telegrammen ist es möglich, die meisten Kollisionen im Netzwerk zu vermeiden.

Stromverbrauch [++]

Das Unternehmen ist Experte auf dem Gebiet des low-power-managements sowie des Energy-Harvesting. Durch Minimierung des Protokolloverheads sowie der nötigen Nachrichtenlänge können in kürzester Zeit die nötigen Sensordaten mittels Funk weitergeleitet werden. So können die Funksender von EnOcean ein Signal mit nur 50µW über 300m auf dem Freifeld gesendet werden. [67]

Reichweite [--]

EnOcean ist nicht zur Langstreckenübertragung gedacht, dennoch zählt es zu den gängigsten LPWANs derzeit. Die Firma gibt an, 30m in Gebäuden sicher überbrücken zu können und bis zu 300m im freien Feld. Die Reichweite kann durch das Einsetzen von Repeatern auf der Funkstrecke jedoch erweitert werden. Damit liegt EnOcean im Reichweitenvergleich dennoch weit hinter seinen Mitbewerbern. [67]

Frequenzbereiche [++]

EnOcean-Lösungen bieten folgende Frequenzbänder an, welche regionsspezifisch an die Hardware angepasst werden können.

- 868 MHz gemäß R&TTE-Spezifikation EN 300220, für Europa
- 902 MHz gemäß FCC/IC-Spezifikation, für Amerika
- 928 MHz gemäß ARIB-Spezifikation, für Japan
- 315 MHz gemäß FCC-Spezifikation, für Asien

Zudem sind ein Teil der Produkte von EnOcean in der Lage über die 2,4GHz-Frequenz zu kommunizieren, was die Einbindung vieler Alltagsgeräte ermöglicht die über keine

Funkempfänger verfügen. EnOcean bietet somit Lösungen für alle gängigen freien Funkfrequenzbänder an.[66]

Übertragungsrate [-]

EnOcean hat eine sehr niedrige Übertragungsrate von 125kbit/s, um so einen niedrigen Energieverbrauch gewährleisten zu können. Da die übertragenen Pakete ohnehin sehr klein sind, genügt diese Übertragungsrate völlig für die angedachten Verwendungen. [45]

Mögliche Sicherheitsmaßnahmen [+]

Die übertragenen Daten werden bei dem Funkstandard für Gebäudeautomation durch einen sogenannten Rolling Code gesichert. Dies bedeutet, dass Sender und Empfänger jeweils die Information über einen symmetrischen Schlüssel erhalten. Der Sender sendet zur Authentifizierung bei jedem Sendevorgang einen sogenannten Next-Code an den Empfänger. Dieser überprüft den eingetroffenen Next-Code mit einer algorithmisch definierten, zyklisch durchiterierten Liste und authentifiziert den Sender bei Übereinstimmung. Zusätzlich werden die Daten noch durch einen 128Bit-AES-Verschlüsselung vor dem ungewollten Zugriff Dritter geschützt. [66]

Kosten [+]

Der für Deutschland verantwortliche Distributor ist FutureElectronics. Der Online-Shop bietet alle verfügbaren EnOcean-Produkte wie Schalter, Sensoren, Energy-Harvesting Platinen oder Sendeeinheiten an. Die Produkte beginnen bei 6-10 €, wenn lediglich die nötige Platine gekauft wird. Komplette Schalter- oder Sensorsysteme liegen zwischen 20 und 80€. [68]

Stand der Entwicklung [++]

EnOcean-Sensoren und -Aktoren können bereits seit Jahren erworben und eingesetzt werden. Die Technologien werden stetig weiterentwickelt und Neuheiten in White Papers auf der Homepage präsentiert. Die energiearme Funktechnologie zur Steuerung von Smart-Home und Internet-der-Dinge-Anwendungen wurde bereits 2015 vorgestellt und vertrieben. EnOcean kann jedoch aufgrund der Ausrichtung auf Kurzstrecken kaum mit den Anbietern von Langstreckenfunk mithalten, da die Reichweite der meisten Produkte auf wenige Meter beschränkt ist.

EnOcean arbeitet derzeit weiterhin daran, ihre Technologie der batterielosen Gebäudeautomation für Schulen, Krankenhäuser und Industriegebäude zu verbessern und legt keinen sichtbaren Wert darauf Lösungen für Langstreckenfunk zu entwickeln. [67]

3.5. Auswertung und Zusammenfassung der Ergebnisse

In der folgenden Darstellung 24 sind die Bewertungen der einzelnen Disziplinen den jeweiligen Anbietern tabellarisch zugeordnet und gegenübergestellt.

Darstellung 24. Vergleich der Anbieter, Eigene Darstellung

	LoRa	sigfox	enocean	INGENU simply genius
Geräteanbindung	++	--	++	-
Störsicherheit	++	+	+	+
Stromverbrauch	++	++	++	+
Reichweite	+	+	--	++
Frequenzbereiche	+	+	++	-
Übertragungsraten	-	-	-	++
Sicherheit	+	-	+	++
Kosten	++	+	+	-
Entwicklungsstand	+	+	++	+

Betrachtet man die Funktionsweisen, Leistungsmerkmale und Anwendungsgebiete der vorgestellten und verglichenen Technologien wird schnell klar, dass bei dem direkten Vergleich die Benennung des besten LPWAN Anbieters schlecht möglich ist, da jeder Anbieter einen anderen Ansatz verfolgt energieeffiziente Funknetzwerke aufzubauen. Auch die Vor- und Nachteile der verschiedenen Anbieter sind auf unterschiedliche Ansätze des Vertriebs oder der technischen Umsetzung zurückzuführen.

Für die wissenschaftliche Anwendung und die Implementation kleinerer Projekte ist LoRaWAN wohl am besten geeignet, da es über günstige Hardware verfügt und die Erstellung von privaten Netzwerken unterstützt. Zudem kann es weltweit in freien Funkräumen eingesetzt werden solange der richtige Chipsatz gewählt wurde.

SigFox verfügt über beinahe identische technische Spezifikationen wie LoRaWAN, setzt jedoch voraus, dass Anwender dem vom Unternehmen kontrollierten Netzwerk gegen den Abschluss eines Abonnements beitreten. Zudem ist die Abdeckung durch dieses Netzwerk nur in einigen Regionen gewährleistet, was die Nutzung der Technologie regional abhängig macht.

EnOcean ist der am weitest entwickelte Standard unter den vorgestellten Anbietern. Nicht nur, dass die Funktechnologie einen minimalen Energiebedarf aufweist, sondern auch die

Möglichkeiten zur Nutzung und Erschließung von Umweltressourcen durch Energy Harvesting ist durch EnOcean Produkte gewährleistet. EnOcean hat von allen vorgestellten Anbietern zudem das am weitest verbreite Produktportfolio und ist bereits vollständig auf dem Markt etabliert, was sich unter anderem auch auf die Interoperabilitätsmöglichkeiten der Produkte zurückführen lässt. Der große Nachteil der Funktechnologie der Firma liegt in der begrenzten Reichweite, die auf freiem Feld mit etwa 300m weit unter den anderen Anbietern im Vergleich liegt.

Ingenu verfolgt einen völlig anderen Ansatz wie die anderen vorgestellten Anbieter. Es nutzt das durch WiFi und Bluetooth bekannte 2,4GHz-ISM-Band, doch auf eine völlig andere Art und Weise. Dies ermöglicht der Technologie sehr weite Strecken durch störungsresistenten Funk abzudecken. Dadurch, dass das 2,4GHz-Band weltweit weniger Auflagen über Sendeleistung und -dauer unterliegt, ist es möglich eine höhere Datenrate bei etwa gleichem Energieverbrauch zu den Mitbewerbern anbieten zu können. Dabei ist zu erwähnen, dass die Technologien von LoRa, SigFox und EnOcean nicht auf eine hohe Datenrate ausgelegt sind, sondern durch eine niedrige Datenrate den niedrigen Energieverbrauch gewährleisten. Technisch gesehen ist die RPMA-Technologie den anderen in vielen Punkten weit überlegen, jedoch fehlt es derzeit noch an einer großflächigen Abdeckung und günstiger Hardware.

Die Entwicklung von LPWAN-Technologien steckt immer noch in der Startphase und wird in den kommenden Jahren zu einer der wichtigsten Übertragungsarten des Internets der Dinge werden. Mit der weiteren Entwicklung der vorgestellten - sowie neuer Technologien - wird es schon in naher Zukunft möglich sein weite Strecken mit wartungsfreien energieautarken Sensorsystemen mit tausenden Endgeräten abzudecken.

4. Energy-Harvesting

4.1. Einführung

Das Internet der Dinge zeichnet sich durch die Vernetzung vieler kleiner Sensoren und Aktoren aus - alles elektrische Geräte, die als Messinstrumente oder Steuereinheiten eines intelligenten Systems fungieren. Die meist kleine Bauweise der Hardwarekomponenten, die im Internet der Dinge eingesetzt werden, lässt bereits darauf schließen, dass ein Großteil der Bauteile über einen niedrigen Energieverbrauch verfügt. Viele der aktuellen IoT-Systemkomponenten sind bereits durch Hochleistungsakkus sowie effiziente Sleep- und Energiesparoptionen jahrelang wartungsfrei einsetzbar, ohne Batterietausch oder einen festen Stromanschluss.

Bei dem sogenannten Energy-Harvesting geht man bereits einen Schritt weiter. Energy-Harvesting bezeichnet den Vorgang der Stromerzeugung durch Umweltressourcen wie Wind, Wasser, Hitze, Vibration oder andere natürliche Energiequellen. Energiesammelnde Komponenten wie Photovoltaik-Module versorgen die Geräte unabhängig von Batterien mit Strom oder laden die eingebauten Akkus immer wieder auf. Derzeit wird diese Technologie bei meist batterielosen Kleingeräten eingesetzt, welche für die Ausführung ihres Verwendungszweckes nur geringe Mengen an Strom benötigen. Einsatzorte einer solchen Technik sind beispielsweise intelligente Funkschaltersysteme die oft in Bereichen eingesetzt werden, an denen das Verlegen von Stromleitungen schwierig ist, wie beim Camping oder nachträglich angebrachten Schaltungen bei Industriegebäuden- oder Maschinen. Diese Arbeit soll zeigen, dass es möglich ist, durch Energy-Harvesting Sensordaten über weite Strecken zu senden, ohne dem System Netzstrom hinzuzufügen.

4.2. Funktionsweise

Um einen Überblick zu schaffen, welche Möglichkeiten des Energy-Harvesting bereits existieren und kommerziell einsetzbar sind, werden nun die Funktionsweisen der gängigsten Arten beleuchtet. Zu den meistgenutzten Technologien gehören thermoelektrische Generatoren, mikrobielle Brennstoffzellen, Photovoltaikzellen und Piezoelektrische Sammeleinheiten. Unterschieden werden diese in Continuous-Time und Discrete-Time Energy-Sources. Während Continuous-Time Energy-Sources einen spannungsarmen, aber kontinuierlichen Strom abgeben, sind Discrete-Time Energy-Sources in der Lage hohe Ströme zu produzieren. Dies passiert jedoch nicht kontinuierlich, sondern ist von Ressourcen wie Bewegung oder Sonneneinstrahlung abhängig, die entsprechend der Stärke der Umwelteinflüsse schwanken. [69]

4.2.1. Thermoelektrische Generatoren

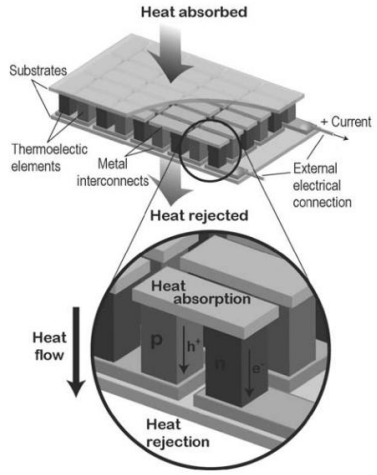


Fig. 11.2 Schematic of a thermoelectric generator. Many thermoelectric couples (inset *bottom*) of n- and p-type thermoelectric materials are connected electrically in series and thermally in parallel to make a thermoelectric module (*top*) or thermopile. The height of the thermoelectric elements and the area of the substrates are used to determine the thermal resistance of the module (see Eq. 11.14). Copyright Nature Publishing Group (Snyder and Toberer, 2008), reprinted with permission

Darstellung 25. Funktionsweise thermoelektrischer Generatoren [69]

Thermoelektrische Generatoren nutzen in der Umgebung vorkommende Temperaturgefälle zwischen zwei Bereichen, wie etwa einem Heißwasserrohr und der Umgebungsluft, um Strom zu generieren. Die Generatoren sind solid-state Halbleiter. Der Strom kann entstehen, da sich geladene Teilchen ähnlich frei in Metallen bewegen können, wie Gasteilchen in der Luft. Nimmt das Material des Generators nun Wärme auf, setzen sich die geladenen Teilchen in Richtung der kälteren Seite des Halbleiters in Bewegung. Durch diese Diffusion bildet sich ein elektrisches Potenzial und eine Netzspannung entsteht am kälteren Ende. [69]

4.2.2. Mikrobielle Brennstoffzellen

Eine weitere Art kontinuierlichen Strom aus Umweltressourcen zu generieren, ist die Nutzung sogenannter mikrobieller Brennstoffzellen. Eine solche Zelle kann beispielsweise Elektrizität durch die Photosynthese von Algen generieren. Der von den Algen produzierte Strom ist mehr ein Nebenprodukt des Photosynthese-Vorgangs, welcher unter anderem bei der mikrobiologische Abwasserreinigung Anwendung findet. Die bei solchen Vorgängen durch die von Algen und Mikroben ausgelösten chemischen Prozesse generieren Elektrizität, welche dann mithilfe von Anoden und Kathoden einem Stromkreislauf hinzugefügt werden können. [49]

4.2.3. Photovoltaik- und Solarzellen

Photovoltaik- bzw. Solarzellen wandeln einstrahlendes Sonnenlicht direkt in elektrische Energie um. Da die Sonne nur eine begrenzte Zeit am Tag zur Energieerzeugung genutzt werden kann, sollten Energy-Harvesting-Systeme die Photovoltaik oder Solar nutzen über einen Energiespeicher verfügen, der das System auch über Nacht mit Strom versorgen kann. Dabei können bis zu 15000 µW / cm^3 von Solarmodulen produziert werden. [69]

4.2.4. Piezoelektrische Sammeleinheiten

Bei Piezoelektrischen Sammeleinheiten wird Vibrationsenergie in Strom umgewandelt. Dabei werden dünne Flächen mit einer Schicht aus piezoelektrischen Polymerkristallen bedeckt und in Schwingung versetzt. Diese Schwingungen führen zu Veränderungen der Gitterstruktur der Kristallmoleküle wodurch Ladungsteilchen auftreten. [69]

4.2.5. Mechanische Energie

Mechanische Energie die auf ein mit Spulen versehenes System ausgeübt wird, kann Strom produzieren - Beispielsweise ein Fahrrad-Dynamo, ein Wasserrad oder die Lichtmaschine in einem PKW. So kann der ECO-200-Mechanical-Energy-Converter der Firma EnOcean mit einer Auslösung 120µWs generieren, was für 3 Funkübertragungen mit einem passenden Low-Power-Transmitter genügen würde. [70]

4.3. Einsatzgebiete, Arten und Beispiele Umsetzung

4.3.1. Batterielose Funktechnologie

Die Technologie des Energy-Harvesting wird hauptsächlich in der batterielosen Funktechnologie genutzt. Anwendungsfälle finden sich in der Heimautomation, bei Alarm- und Feuermelderanlagen für Hotels und Bürokomplexe, aber auch beim Camping zur Steuerung von elektrischen Geräten in Wohnmobilen wird diese Technologie eingesetzt.

Auch zur Versorgung von Sensoren und GPS-Empfängern auf Booten kann Energy-Harvesting eingesetzt werden. [71]

4.3.2. Anwendungsbeispiele

Im folgenden Abschnitt wird gezeigt, was mit Energy-Harvesting möglich ist oder sein könnte. Neben der Nutzung von Umweltressourcen für batterielose Funktechnik oder die Aufladung von Mobilgeräte in der Natur, entstehen immer neue innovative Ideen zur Nutzung von Energy-Harvesting.

Handyaufladung durch einen Schlafsack oder eine Hosentasche

Die Universität von Southhampton hat sich die thermoelektrische Energiegewinnung zunutze gemacht und Module entwickelt, die durch den Temperaturunterschied zwischen zwei Bereichen ein Handy mit Strom versorgen können. Verbaut wurde Dieses dann in einem Schlafsack. Wenn man davon ausgeht, dass in dem Schlafsack eine Temperatur von 37 Grad Celsius und eine Außentemperatur von zehn Grad Celsius herrscht, soll ein achtstündiger Schlaf genügend Strom liefern um 24 Minuten Sprechzeit oder elf Stunden Stand-By zu ermöglichen. Auch getestet wurden kleinere Module die in die Gesäßtasche einer Hose eingearbeitet wurden. Wer mit diesen Hosen einen ganzen Tag über läuft oder tanzt, soll genug Energie produzieren um ein Smartphone fünf Stunden lang betreiben zu können. [72]

Straßenbeleuchtung durch Fußgänger in der Londoner U-Bahn

Während den olympischen Spielen 2012 in London wurden in der Underground Station West Ham Platten ausgelegt, die durch die kinetische Energie der Schritte der Bahnfahrenden Strom für die umliegende Straßenbeleuchtung produzierten. Durch die Biegung des Materials um etwa fünf Millimeter wurden bis zu sechs Watt pro Schritt generiert. Im Verlauf der zweiwöchigen Olympischen Spiele wurden insgesamt 20 Kilowattstunden produziert. [73]

5. Umsetzung eines über LPWAN kommunizierendes Systems mit Versorgung durch Energy-Harvesting

5.1. Beispielprojekt „Emergency Beacon“ – Notsignalgeber für Veranstaltungen oder Katastrophenfälle

Ein großes Problem bei Naturkatastrophen, Anschlägen jeder Art, großen Unfällen bei Veranstaltungen oder in Gebieten mit vielen Menschen ist die Kommunikation. Oft führen Stromausfälle oder Beschädigung der Sendetechnik während solchen Ereignissen zu Ausfällen des Mobilfunks. Koppelt man nun jedoch ein LPWAN-Gateway an einen festen Internetanschluss, kann so in Gebieten ohne Möglichkeit zur Datenübertragung schnell ein Ersatznetz aufgebaut werden. Ein mobiles solarbetriebenes GPS-Signal könnte in einem durch ein LPWAN abgedeckten Bereich die GPS-Koordinaten einer verletzten Person senden und auf einen sicheren Standort oder eine Versorgungsstation hinweisen.

5.2. Umsetzungsidee

In diesem Beispielprojekt soll eine solarbetriebene Sendeeinheit zusammengestellt werden, die in der Lage ist die GPS-Daten ihrer Position mittels LoRaWAN über die freie Funkfrequenz 868MHz an ein LoRa-Gateway in der Umgebung zu senden.

Das Gateway soll die Daten interpretieren und mithilfe eines Webdienstes auf einer interaktiven Karte darstellen.

5.3. Benötigte Technik

Um die Umsetzung des Projektes gewährleisten zu können, mussten zuerst die erforderlichen Bauteile gefunden werden. Hierbei war besonders ein Augenmerk auf die mobile Funkeinheit zu legen, da diese im Idealfall durch Energy-Harvesting betrieben werden sollte. Da die LPWAN-Technologie noch nicht vollends entwickelt ist, galt es ein möglichst funktionales System zu kleinem Preis zusammenzustellen. Es sollte daher nicht nur in der Lage sein ein LPWAN ausstrahlen und darüber zu senden, sondern es sollte fähig sein durch die Energieversorgung eines kleinen Solarpanels genügend Strom zu erhalten. Nach einiger Recherche schien das LoRa-IoT-Starterkit der Firma Dragino Tech ideal für diese Zwecke zu sein, da es neben zwei unterschiedlichen Arten von Nodes ein vorprogrammiertes Gateway diversen Netzwerkanschlüssen enthielt.

Das finale Projekt besteht aus folgenden Bauteilen:

- Dragino LoRa Single-Channel Gateway LG01
- Arduino Uno
- Dragino LoRa/GPS Shield für den Arduino
- 200mA/6V Solarpanel mit der Größe 112mm x 80mm
- Ein SparkFun Energy-Harvesting Breakout-Board
- Optional zur Energiespeicherung: 2 Superkapazitatoren
- Zudem benötigt: Jumperkabel, Sperrdiode, Lötzinn, Werkzeug

Alle Hardwarekomponenten werden im Folgenden vorgestellt, um einen Überblick der Möglichkeiten solcher Systeme zu verschaffen und die Technik vorzustellen

5.3.1. Dragino Single-Channel Gateway LG01

Darstellung 26. Dragino LG01-Gateway [74]

Das Dragino Gateway LP01 ist ein Single-Channel LoRa-Gateway das als Basisstation des LPWANs und als Verbindungspunkt der Nodes zum Internet genutzt wird. Single-Channel bedeutet, dass es im Gegensatz zu Multi-Channel-Gateways lediglich in der Lage ist, auf einem Kanal mit nur einem Spreading-Faktor zu empfangen. Multi-Channel-Gateways sind in der Lage, acht bis zehn Channel abzuhören und jeweils einen von sechs Spreizfaktoren zu verarbeiten. Der große Vorteil eines Single-Channel-Gateways liegt besonders im geringen Preis, was es attraktiv für LoRa-Anfänger macht. [74]

Darstellung 27. Anschlüsse und Platine des Dragino LG01-Gateways [75]

Das Gateway verfügt über zwei RJ45-Ports und eine USB-2.0-Schnittstelle. Die Funktionalität des Gerätes umfasst 802.11 b/g/n WiFi, Ethernet sowie optionale 3G/4G-Konnektivität, die durch das zusätzliche Anbringen einer Mobilfunkplatine bereitgestellt wird. Im Inneren besteht das LG01 zum einen aus einer Mikrocontrollerunit (MCU) die mit der LoRa-Sendeeinheit verbunden ist sowie einem separaten Linux-System. Vergleichsweise wie ein Arduino Yún verfügt das LG01 für jeden dieser Bereiche über einen eigenen Prozessor: Einen ATMega328P mit 32KB Flashspeicher und 2KB RAM als MCU-Prozessor, sowie einen 400MHz AR9331-Prozessor mit 16MB Flashspeicher und 64MB RAM. Die werksseitig aufgespielte Linux-Distribution OpenWrt ist Open-Source und kann vom Anwender je nach Anwendungszweck ohne Weiteres angepasst und verändert werden. [74]

Das Gateway ist in der Lage mit einem Leistungspegel von konstanten 20dBm zu senden, bei einer Bitrate von bis zu 300kbps. Die Einheit verfügt über eine hohe Sensitivität die bis -148dBm hinunterreicht. Zudem ist der Verbrauchsstrom zum Empfang von Daten bei niedrigen 13,3mA. [74]

5.3.2. Arduino Uno

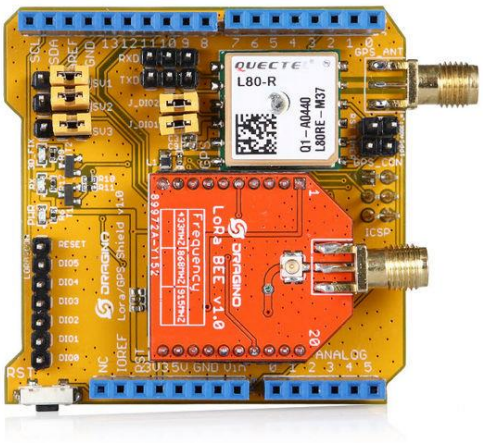
Darstellung 28. Arduino Uno [76]

Der Arduino Uno ist der derzeit wohl am weitest verbreitete Mikrocontroller für Heimanwendungen. Er basiert auf dem ATmega328 Prozessor und verfügt über 16 digitale sowie sechs analoge Schnittstellen die Verbindungen zu diversen Peripheriegeräten ermöglichen. Auf ihn können per USB-Anschluss schnell und einfach C-Programme

übertragen werden. Er kann sowohl über einen 9V-Netzanschluss sowie über einen USB-B-Steckanschluss mit Strom versorgt werden, wobei die Versorgung über USB nicht den gleiche Strom bieten kann wie der Netzanschluss. [76]

Um die Funktionalität des Mikrocontrollers beispielsweise um die Nutzung von drahtlosen Netzwerken zu erweitern, können Platinen mit entsprechender Funktionalität einfach auf ihn aufgesteckt werden. Bei diesen Platinen spricht man von sogenannten Shields.

5.3.3. Dragino LoRa/GPS Shield



Darstellung 29. Dragino LoRa/GPS-Shield für Arduino mit aufgesetztem LoRa-Bee Modul [77]

Das Dragino LoRa/GPS Shield ist ein Erweiterungsboard für den Arduino UNO und kann mittels der Steckverbindung auf die Pins eines handelsüblichen Arduino aufgesetzt werden.

Es besteht aus drei Bauteilen die in Darstellung 29 deutlich erkennbar sind. Die gelbe Grundplatine ist das LoRa/GPS-Shield-Motherboard, welches die Konnektivität zum Arduino herstellt und dessen Anschlüsse erweitert. Auf ihr befindet sich das GPS Modul der Firma QUECTEC, in der Darstellung weiß und rechts oben im Bild. Das dritte Bauteil ist das rote Dragino LoRa-Bee-Modul welches die Funkverbindung zu LoRa Systemen herstellen kann. [78]

Das LoRa-Bee Modul verfügt über folgende Spezifikationen:

- 168 dB maximales Link Budget.
- Bis zu +20 dBm konstante Sendeleistung
- Programmierbare Bitrate von bis zu 300 kbps
- Hohe Sensivität bis zu -148 dBm.
- Niedrigen Empfangsstrom von 10.3 mA, nur 200 nA im Energiesparbetrieb
- FSK, GFSK, MSK, GMSK, LoRaTM und OOK Modulation
- 127 dB Dynamic Range RSSI
- Eingebauter Temperatursensor und Batteriewarnleuchte [78]

Das LoRa/GPS-Shield ist in der Lage auf den Frequenzen 868MHz, 433Mhz und 915MHz zu senden, jedoch wird die Frequenz des Moduls bereits im Werk voreingestellt. Zudem ist es

möglich, neben der Antenne für die Funkverbindung eine externe GPS-Antenne anzubringen. Das GPS-Modul selbst verfügt aber über eine eingebaute 15x15x4 Patch-Antenne, die zur optimalen Funktion in Richtung Himmel zeigen sollte. Das GPS-Modul ist hitzempfindlich und sollte von großer Hitze ferngehalten werden. [78]

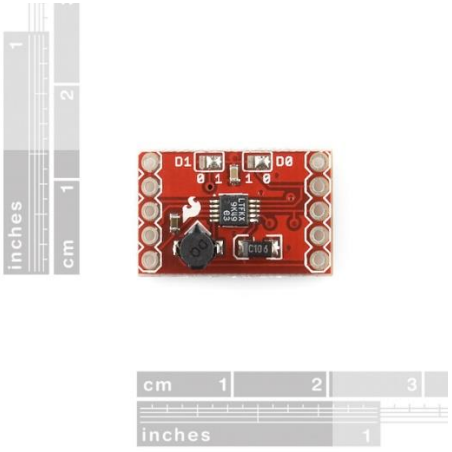
5.3.4. Photovoltaikmodul/Solarpanel

Das im Projekt verwendete Photovoltaikmodul ist ein 112mm x 8mm großes Mini-Solar-Panel der Firma Zimo, welches in Darstellung 30 abgebildet ist. Den angegebenen Spezifikationen des Herstellers zufolge soll es bei maximaler Sonneneinstrahlung eine Ausgangsspannung von 6V bei einer Leistung von bis zu 1,1 Watt erzielen. Das Photovoltaikmodul soll in der Lage sein, eine maximale Stromstärke von 200mA produzieren zu können. [79]

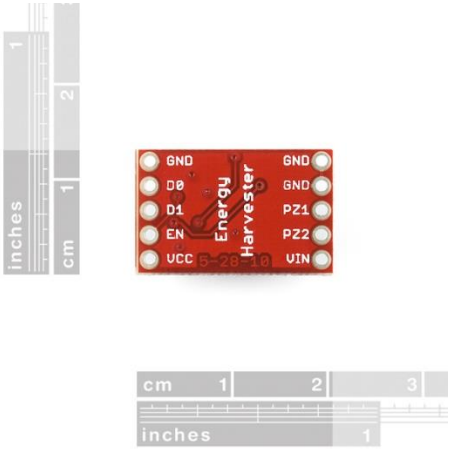
Darstellung 30. Solarzelle der Firma Zimo, Eigene Darstellung

Da bei der Recherche nach günstigen Solarmodulen für den Privatgebrauch viele Rezensionen unterschiedlicher Produkte und Hersteller Aussagen darüber lieferten, dass die angegebenen Werte nicht erreicht werden konnten, wurde sich bewusst für ein Solarpanel dieser Größe entschieden. So konnte sichergestellt werden, genügend Strom für einen Sendevorgang produzieren zu können, selbst wenn die Sonne einmal von leichten Wolken bedeckt sein sollte. Zur Sicherheit wurden eigene Messungen bei direkter Sonneneinstrahlung mit einem Multimeter ausgeführt. Dabei konnten Maximalwerte zwischen 180mA und 190mA für den Strom erzielt werden. Die gemessene Spannung schwankte jedoch sehr stark zwischen 5V und 9V. Dies ist zwar nicht unüblich für Solarzellen, jedoch kann es dadurch bei unsachgemäßem Anschluss an einen Stromkreis zur Zerstörung der angeschlossenen Geräte kommen.

5.3.5. SparkFun Energy-Harvesting-Board



Darstellung 31. Vorderseite des SparkFun Energy-Harvesting-Boards [80]



Darstellung 32. Rückseite des SparkFun Energy-Harvesting-Boards [80]

Bei der SparkFun Energy-Harvesting-Board handelt es sich um einen sehr effizienten Abwärtsregler, im englischen buck-regulator genannt. Ein Abwärtsregler oder Abwärtswandler sind elektrotechnische Bauteile, die eine Eingangsspannung U_e in eine geringer Ausgangsspannung U_a. Man findet diese besonders häufig bei kinetisch betriebenen Kleingeräten wie LED-Fahrradbeleuchtung oder Netzteilen zur Ladung von Akkumulatoren für Smartphones oder mobile Computer. [81]

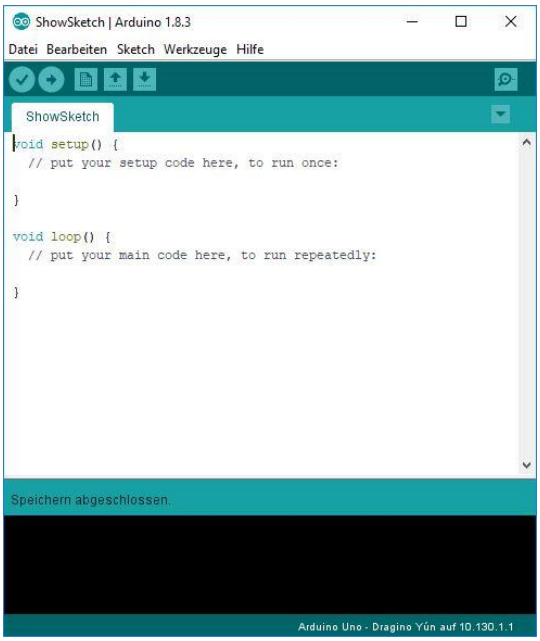
Die Funktion dieses Energy-Harvesting-Boards löst das Problem der schwankenden Stromspannung und -stärke. Es ist in der Lage einen bis zu 20V starken Strom auf 1,8V, 2,5V, 3,3V oder 6V herunter zu regeln. Die Vorkonfiguration des Boards gibt zudem bei dem 3,3V Ausgangspin eine kontinuierliche Spannung von 100mA ab, ist jedoch in der Lage kurzfristig einen kleinen Burst mit einer höheren Spannung abzugeben. [80]

5.4. Software, Entwicklungsumgebung

5.4.1 Entwicklungsumgebung

Arduino IDE

Arduino IDE ist die von Arduino verfügbare Entwicklungsumgebung und ermöglicht es Algorithmen für Arduino-basierte Mikrocontroller zu schreiben, den fertigen Code kompilieren zu lassen und anschließend auf den ausgewählten Mikrocontroller hochzuladen.



Darstellung 33. Arduino IDE, Eigene Darstellung

Hochgeladen werden kann der Code über ein USB-Kabel zwischen dem Mikrocontroller und dem Computer oder - sofern vorhanden - einer WiFi/Ethernet-Verbindung zwischen beiden Geräten. Die Entwicklungsumgebung ist in der Lage externe Bibliotheken per Datei oder über ein eingebautes Suchsystem einzubinden. Arduino IDE bietet zudem die Möglichkeit für Hersteller und Bibliotheks-Ersteller, Beispielcodes vorzubereiten, die direkt im Programm geöffnet werden können.

Neuerdings gibt es die Möglichkeit eine webbasierte Variante der Entwicklungsumgebung zu nutzen, das installierbare Programm kann jedoch unter:

https://www.arduino.cc/en/Main/Software

heruntergeladen werden. [82]

5.4.2. Genutzte Bibliotheken

Um die nötigen Komponenten für LoRa- und GPS-Konnektivität nutzen zu können, müssen diverse Bibliotheken eingebunden werden, um die genutzten Mikrochips, Empfänger und Sensoren ansprechen und auslesen zu können. Die im Verlauf der Arbeit genutzten Bibliotheken werden im Folgenden vorgestellt und ihr Funktionsumfang aufgezeigt.

5.4.2.1. YunBridge Library

Das im Beispielprojekt verwendete Dragino LG01 LoRa-Gateway basiert auf einem Arduino mit einem aufgesteckten Yún Shield, welches den Arduino um einen linuxfähigen Prozessor erweitert. Somit besitzt das System neben dem üblichen ATmega einen zweiten Prozessor, den Atheros AR9331, auf dem neben einer eigene Linux-Distribution zusätzlich der Wireless-Stack OpenWrt läuft. Der Prozessor ermöglicht dem Arduino Skripte auf der Linuxdistribution aufzurufen und erweitert die Funktionalität des Boards unter anderem um die WLAN-Konnektivität. Zusätzlich stellt der zweite Prozessor die Möglichkeit zur Nutzung diverser Internetservices her, wie zum Beispiel die Erstellung eines Linux basierten HTTP-Clients oder -Servers. Bei einem handelsüblichen Arduino Yún sind bereits beide Prozessoren miteinander verbunden, nutzt man jedoch das aufsteckbare Yún Shield, kommunizieren die Prozessoren über ihre serielle Schnittstelle miteinander. Die YunBridge Library verfügt über eine Vielzahl unterschiedlicher Klassen, von denen nun zwei weiter beleuchtet werden.

Bridge.h

Zur Übertragung von Sketches oder dem Auslesen des Konsolen-Logs wird im Regelfall die serielle Schnittstelle verwendet. Um eine vereinfachte Kommunikation zwischen dem Arduino und dem Yún Shield zu gewährleisten, wird die Bridge.h-Bibliothek benötigt. Das Gateway nutzt die Bibliotheken Bridge.h und die darauf basierende Console.h, um mit der verbauten Wireless-Komponente neue Sketches aufzuspielen sowie den Konsoleninhalt darzustellen. Die Bridge startet hierbei ein vom Gateway ausgehendes WLAN, in dem es selbst als Server fungiert. Treten nun andere Teilnehmer dem Drahtlosnetzwerk bei, können sich diese als Client mit dem Gateway verbinden, da dieses im Listen-Mode ist und auf die Verbindung eines Clients wartet. Datenübertragungen werden hierbei geparsed und mittels dem REST-Protocol übertragen.

Console.h

Console.h beschreibt eine Unterklasse der Bridge-Bibliothek, welche es ermöglicht Konsolendaten über die drahtlose Schnittstelle des Gateways auf den des Netzwerkmonitors der Arduino IDE auszugeben, statt über den seriellen Port. Die Funktionsweise ist dabei fast identisch mit der der Klasse Serial aus dem Standardrepertoir

der Arduino DIE. So wird aus `serial.write(„Hello World“);` beispielsweise ein `Console.write(„Hello World“);`.

5.4.2.2. SoftwareSerial.h

Arduino-Computer besitzen standardmäßig eine serielle Schnittstelle, die zur Datenübertragung zwischen dem Arduino und dem Computer oder anderer Peripherie genutzt wird. Realisiert wird dies durch eine in den Chip des Mikrocontrollers verbaute Hardwarekomponente, welche universal asynchronous receiver/transmitter (UART) genannt wird. Dieser UART ermöglicht es dem Arduino serielle Datenübertragung zu erhalten, selbst während er andere Rechenaufgaben bearbeitet. Dieses Bauteil ist bei handelsüblichen Arduinos mit den Pins 0 und 1 gekoppelt und stellt über diese eine direkte Verbindung zur USB-Schnittstelle bereit.

Um eine serielle Kommunikation mit anderen Peripheriegeräten zu ermöglichen, wurde die Bibliothek SoftwareSerial.h entwickelt. Sie ermöglicht es, serielle Kommunikation über andere der vorhandenen Digital-Pins eines Arduinos abzuwickeln. Um die Funktionen des verbauten UARTs zu replizieren, werden dessen Funktionen von der Hardwarelogik softwaretechnisch emuliert. Die Programmierung ersetzt also die Notwendigkeit eines UARTs zur seriellen Kommunikation über Digital-Pins des Mikrocontrollers.

Der UART ist jedoch nicht unabdingbar, da man mit der Bibliothek zwar mehrere softwaregestützte Seriellschnittstellen erzeugen kann, diese jedoch eine geringere Datenrate als ihr Hardware-Gegenstück haben. Zudem sind nicht alle Pins des Arduinos darauf ausgelegt Interrupts zu unterstützen und bei der Nutzung mehrerer Software-Serial-Ports muss darauf geachtet werden, dass immer nur jeweils einer der Ports Daten empfangen kann. Zudem kann die Nutzung von Software-Serial-Ports sehr CPU-intensiv sein, während der UART diese Aufgabe mit deutlich geringerem Ressourcenverbrauch abwickeln kann [83]. Für das Projekt ist die Bibliothek notwendig, da sie die serielle Kommunikation zwischen dem Arduino und dem LoRa/GPS-Shield herstellt und abwickelt. [84]

5.4.2.3. SPI.h – Serial Peripheral Interface

Das Serial Peripheral Interface (SPI) ist ein synchron arbeitendes Protokoll zur seriellen Datenübertragung zwischen einem einzigen Master-Device und einem oder mehreren Slave-Devices. Im Regelfall nimmt hierbei ein Mikrocontroller (beispielsweise ein Arduino) die Rolle des Masters ein und Aufsteckplatinen, Shields, Sensor- und Aktorsysteme werden diesem als Slaves untergeordnet.

Jede Komponente in diesem System verfügt über folgende drei Kanäle:

- MISO (Master In Slave Out):
  Von Slaves genutzter Kanal zur Datenübertragung an den Master.

- MOSI (Master Out Slave In):

Vom Master genutzter Kanal zur Datenübertragung an die angeschlossenen Peripheriegeräte.

- SCK (Serial Clock):
  Synchronisationskanal des Masters, der die Datenübertragungen zwischen den Geräten aufeinander abstimmt.

Jedes Peripheriegerät besitzt zudem jeweils einen spezifischen Kanal, um vom Master gesteuert zu werden, dem sogenannten Slave Select (SS). Zur korrekten Übertragung über das SPI müssen zu Beginn für jedes neue Gerät die maximal mögliche SPI-Übertragungsrate in MHz angegeben werden. So sollten beispielsweise 15Mhz im Code mit dem Wert 15000000 angegeben werden. Als weitere Parameter muss angegeben werden in welcher Reihenfolge der Master die Bits der Übertragung erwarten soll, also ob zuerst das most-significant-bit (MSBFIRST) oder das least-significant-bit (LSBFIRST) übertragen wird. Des Weiteren muss deklariert werden, in welchem Wartezustand sich die Übertragungsschnittstelle beim Sendevorgang und beim Empfangsvorgang befindet. Das Signal kann hierbei abfallen oder ansteigen. [85]

5.4.2.4. RH_RF95.h – Radio Head

Die Radiohead RF95 Bibliothek fungiert als Treiber für LoRa-fähige Sendemodule wie zum Beispiel die Semtech SX1276/77/78/79 Reihe von low-cost ISM Transceiver Chips. Diese Klasse ermöglicht das Senden und Empfangen von einfachen unadressierten, unzuverlässigen Paketübertragungen von bis zu 251 Achtbitzeichen. Diese Übertragungen werden über eine vom Nutzer gewählte Frequenz zwischen 240MHz und 960MHz gesendet, die Übertragungsreichweite wird hierbei von vordefinierten Einstellungen zur Bandbreite, dem Spreadingfaktor, der Coding Rate sowie dem Leistungspegel bestimmt. [86]

5.4.2.5. TinyGPS.h

Diese Bibliothek ermöglicht dem Arduino das Auslesen von den notwendigsten GPS-Daten wie Position in Längen- und Breitengrad, Datum, Uhrzeit, Höhe, Geschwindigkeit sowie den nautischen Kurs. Die Bibliothek versucht durch die Beschränkung des Auslesens auf diese wichtigen Kerninformationen die benötigte Rechenleistung möglichst gering zu halten, was gerade für kleine Systeme wie einen Arduino sehr vorteilhaft ist. Die TinyGPS-Klasse fungiert - einmal initialisiert - als Parser für die empfangenen Satellitendaten und überträgt diese in einen Datenstrom aus Zeichen (character). Weiterhin verfügt die TinyGPS-Bibliothek über diverse nützliche Methoden, so zum Beispiel die Methode encode(char c) die eintreffenden Zeichen aus dem Datenstrom nacheinander darauf untersucht, ob sie Teil eines validen GPS-Signals sind. So wird dem Anwender ermöglicht, erst mit dem Auslesen der Daten zu beginnen, wenn ein korrektes Signal beim System ankommt.

Die GPS Daten, die vom Satellit gesendet werden, werden standardmäßig als integrale Werte ausgegeben. Zudem sind die empfangenen Werte spezielle Messeinheiten, die häufig um einiges nützlicher für den ursprünglichen Zweck der GPS-Technologie - der Navigation

sind - als für industrielle Nutzung oder Heimanwendungen für Verbraucher. So liefert die Methode speed() zum Beispiel den Geschwindigkeitswert des GPS-Moduls in einem Einhundertstel eines Knotens an. Durch die Hinzunahme anderer Methoden unter Berücksichtigung des steigenden Ressourcenverbrauchs können jedoch praktischere Rückgabewerte erzielt werden. Die Bibliothek umfasst nämlich ebenfalls Methoden wie f_speed_kmph() oder f_speed_mps(), die die Geschwindigkeit in km/h oder m/s als Gleitpunktzahl ausgeben können. [87]

5.4.4. Webapplikation GPSWOX

GPSWOX ist eine englische Firma die Softwarelösungen für Tracking und Flottenmanagement anbietet. Die angebotenen Lösungen umfassen eine Live-Auswertung von GPS-Daten auf der Homepage sowie über eine kostenlose Mobile App. Die Anmeldung und das Live-Tracking eines Gerätes ist gratis, es können jedoch nicht alle Funktionen der Software genutzt werden. Die Firma bietet Pakete an, welche monatlich abgerechnet werden die die Funktionalität des Trackings sowie die Anzahl der trackbaren Geräte erhöhen. [88]

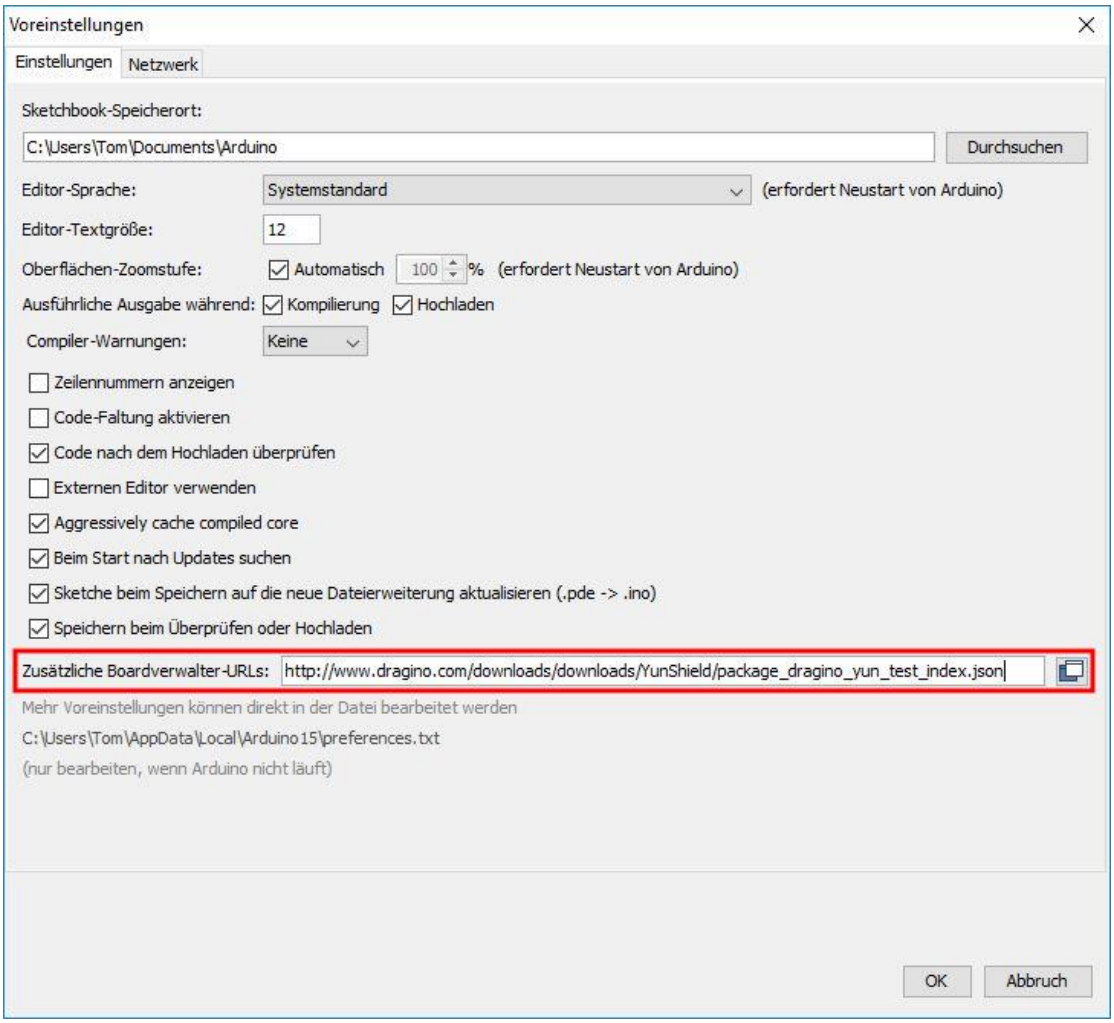
5.5. Implementierung

5.5.1. Vorbereitung der Entwicklungsumgebung

Einbinden der Hardwarespezifikationen des Geräteherstellers

Der erste Schritt bei der Implementierung des Projekts stellt die Vorbereitung der Entwicklungsumgebung dar, um die genutzten Sketches korrekt für die jeweilige Komponente kompilieren und später auf diese übertragen zu können.

Um beginnen zu können wird vorausgesetzt, dass die neuste Version der Arduino IDE heruntergeladen und installiert wurde. Um die nötigen Boardinformationen der im Projekt genutzten Dragino-Geräte zum Gerätemanager der Entwicklungsumgebung hinzufügen können, muss zuerst die von Dragino bereitgestellte URL mit diesen Informationen im Programm eingegeben zu werden.

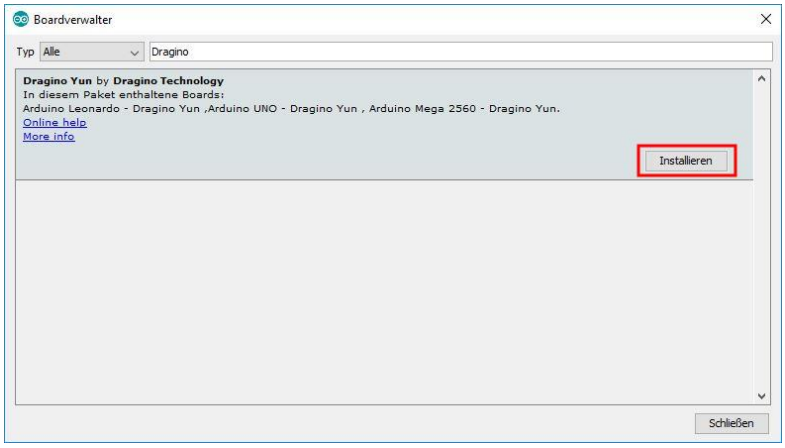


Darstellung 34. Eingabe der Boardverwalter URL, Eigene Darstellung

Öffnet man in der Aktionsleiste des Programms *Datei -> Voreinstellungen,* kann man folgende URL dem Textfeld *Zusätzliche Boardverwalter-URLs* hinzufügen.

```
http://www.dragino.com/downloads/downloads/YunShield/package_dragino_yun_test_index.json
```

Nun ist es möglich, die vom Hardwarehersteller zusammengestellte Boardinformationssammlung über den von der Entwicklungsumgebung bereitgestellten Softwarebrowser herunterzuladen und zu installieren. Dazu öffnet man in der Aktionsleiste den Pfad *Werkzeuge -> Boards -> Boardverwalter…* und gibt im Suchfeld *Dragino* ein.



Darstellung 35. Suche und Installation von Dragino Boardinformationen in der Arduino IDE, Eigene Darstellung

Ist der Suchvorgang beendet, sollte das Fenster wie in Darstellung 35 aussehen. Nun kann der Installieren-Button gedrückt werden. Nach kurzem Warten wurden die nötigen Daten heruntergeladen und installiert. Die Entwicklungsumgebung kann nun bei der Kompilierung die Hardwarespezifikationen der Dragino-Geräte berücksichtigen und man ist in der Lage unter *Werkzeuge -> Boards* die von Dragino vertriebenen Boards auszuwählen.

Für die Programmierung des Dragino LG01 LoRa-Gateways wird die Voreinstellung für das Dragino Yún Board verwendet. Im Programm findet man dieses unter:

Werkzeuge -> Boards: -> Arduino Uno – Dragino Yún

Einbinden der verwendeten Bibliotheken

Um die verwendeten Komponenten später im Code ansprechen und ihre Methoden korrekt kompilieren zu können, müssen die benötigten Bibliotheken zur Entwicklungsumgebung hinzugefügt werden. Zusätzlich zu den bereits vorinstallierten Bibliotheken können die Bibliotheken RadioHead und TinyGPS unter nachfolgenden Links heruntergeladen werden. Für die korrekte Implementierung sollte jedoch eine vom Hersteller angepasste Version der RadioHead-Bibliothek genutzt werden.

RadioHead

http://www.airspayce.com/mikem/arduino/RadioHead/

RadioHead Dragino Version

https://www.github.com/dragino/RadioHead

TinyGPS

http://arduiniana.org/libraries/tinygps/

Um diese Einzubinden lädt man sich die zugehörige .ZIP-Datei herunter und liest diese über den folgenden Aktionsleistenpfad ein.

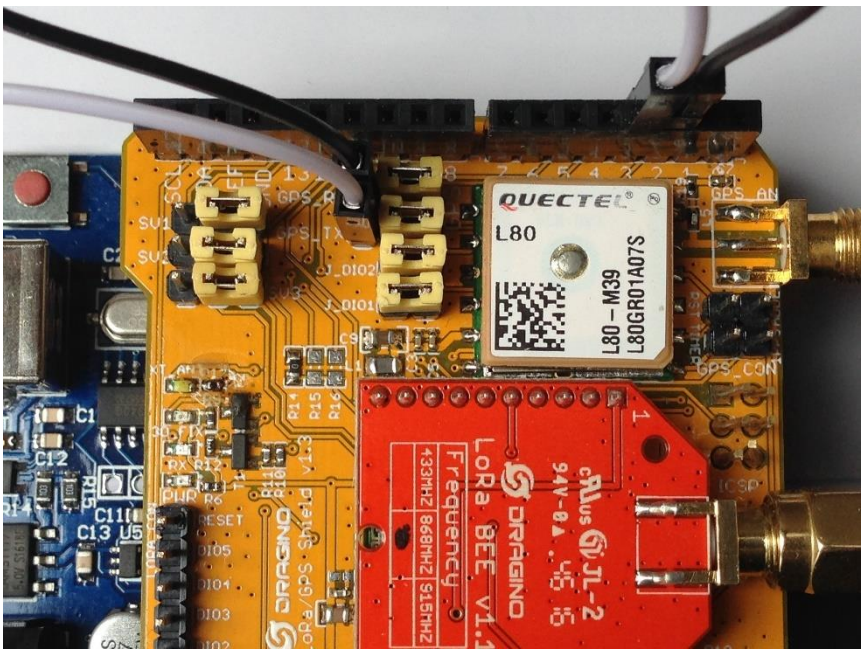
```
Sketch -> Bibliothek einbinden -> .ZIP-Bibliothek hinzufügen…
```

Von da an ist die Entwicklungsumgebung in der Lage, die Methoden der Bibliothek zu interpretieren.

5.5.2. Hardware-Vorbereitung des LoRa-Node-Systems

Zur Vorbereitung des Projekts muss das LoRa-Bee-Modul - falls noch nicht geschehen - auf das LoRa/GPS-Shield aufgesteckt werden und die zugehörige Antenne angebracht werden. Der zweite Antennenanschluss der sich am Shield befindet kann genutzt werden, um eine externe GPS-Antenne anzubringen. Dies ist jedoch nicht nötig, da das GPS Modul über eine interne Antenne verfügt.

Um nun das GPS-Modul zu aktivieren, muss der Jumperstecker von den mittig auf dem Shield zu findenden GPS_RXD und dem GPS_TXD Pins entfernt werden. Ist dies geschehen, können nun Kabelverbindungen zwischen dem D3 Digitalpin des Arduinos (zu finden auf dem Shield) und dem GPS_RXD Pin sowie zwischen dem D4 Pin und dem GPS_TXD Pin mithilfe von Jumperkabeln hergestellt werden. Nach der korrekten Verkabelung sollte die Sendeeinheit wie in der folgenden Abbildung aussehen:



Darstellung 36. Korrekte Verkabelung des GPS Moduls mit dem LoRa GPS Shield, Eigene Darstellung

Zur weiteren Vorbereitung der Hardware muss nun je ein Kabel an den Pluspol und den Minuspol des Solarpanels gelötet werden, um den Stromfluss des Panels abgreifen zu können. Weitere Vorbereitungen am Solarpanel müssen nicht vorgenommen werden.

Möchte man dem System einen Akku oder ähnliche Energiespeicher hinzufügen, werden diese nun in Reihe vom Pluspol des Solarpanels ausgehend angeschlossen. In diesem Projekt wurden testweise zwei Superkapazitatoren verwendet. Um sicherzugehen, dass keine Kriech- oder Kurzschlussströme das Solarpanel beschädigen, sollte eine Sperrdiode angebracht werden, wie das beispielhafte Schaltbild zeigt.

Mit oder ohne die Energiespeicher-Option verbindet man anschließend den Pluspol mit dem VIN Pol des SparkFun Energy-Harvesting-Boards, welches den Strom des Solarpanels für den sicheren Betrieb der Funkeinheit transformieren soll. Der Minuspol wird am äußeren Massepol des Boards angeschlossen, welcher mit GND markiert ist. Man nutzt den äußeren GND Pol, da dieser mit dem äquivalenten GND-Gegenstück auf der Ausgabeseite des Energy-Harvesting-Boards verbunden ist. Auf der Ausgabeseite schließt man nun den Pluspol an den VCC Pin an, um eine Ausgangspannung von 3,3V mit einer Stromstärke von 100mA zu erhalten. Der Minuspol verläuft über den GND Pin der Ausgabeseite. Um den Arduino mit aufgesetztem LoRa/GPS-Shield mit Strom zu versorgen, schließt man den Pluspol an den 3V3/VCC Pin des Shields an und schließt den Stromkreis durch verbinden des Minuspols an den GND Pin auf dem Shield.

Nun ist das System technisch in der Lage - bei genügend Sonneneinstrahlung - eine GPS-Verbindung aufzubauen und die gesammelten Daten über die 868MHz-Frequenz an das LoRa-Gateway zu senden. Bei Bedarf kann dem VIN-Eingangs des Energie-Harvesting-Boards noch ein Kippschalter hinzugefügt werden, um den Beacon manuell ein- und ausschalten zu können.

Der Code, der zur Funktionalität benötigt wird, wird im kommenden Abschnitt zur Software erläutert, nachdem die Einrichtung des Gateways beschrieben wurde.

5.5.3. Vorbereitung des LG01 Single-Channel Gateways

Das Dragino LG01 Single-Channel LoRa-Gateway bedarf keiner weiteren Hardwareanpassung. Es muss lediglich die beiliegende Antenne an dem zugehörigen Anschluss angebracht werden.

Auf die Linux-Partition des Gateways kann mit FTP oder SHH zugegriffen werden. Sobald das Gateway mit Strom versorgt wird, fährt es hoch und sendet ein 2,4GHz-WLAN-Signal aus. Die IP des Gateways ist standardmäßig die **10.130.1.1**, der zu nutzende Benutzer ist **root** und das benötigte Passwort zur Anmeldung ist **dragino**. Bei Bedarf kann dies natürlich geändert werden, jedoch wird im Zuge dieses Projektes darauf verzichtet.

Für die Anbindung des Gateways an die GPSWOX-Webapplikation muss die Firmware Version 4.2.1 auf das Gateway gespielt werden. Diese kann unter dem Link:

http://www.dragino.com/downloads/index.php?dir=motherboards/ms14/Firmware/IoT/

heruntergeladen und über das Webinterface des Gateways aufgespielt werden. Sobald man seinen Rechner mit dem dragino-WLAN verbunden hat, kann man über einen Browser auf das Webinterface zugreifen und sich mit oben genannten Login-Daten anmelden.

Darstellung 37. Aufspielen einer neuen Firmware auf das Dragino LG01-Gateway, Dragino User Manual [74]

Die heruntergeladene Datei kann nun im Reiter „System“ unter dem Punkt „Backup and Flash Firmware“ ausgewählt und auf das Gateway hochgeladen werden, wie in Darstellung 37 gezeigt wird. Dabei kann ausgewählt werden, andere Einstellung beizubehalten oder diese auf Werkseinstellung zurückzusetzen.

Nach kurzer Wartezeit hat sich das Gerät neugestartet und man kann sich erneut anmelden.

Einrichten des GPS Webservices

Verwendet man die Firmware-Version 4.2.1. findet man im Reiter „Sensor“ des Webinterfaces den neu hinzugefügten Punkt „GPS Track Server“, unter dem man den aus dem Abschnitt 5.4.4. bekannten GPS Service GPSWOX auswählen kann. Um diese Funktionalität nutzen zu können, muss man einen Account bei dem Webdienst GPSWOX anlegen, was erlaubt ein kostenloses GPS-Gerät tracken zu lassen.

Ist man bei GPSWOX angemeldet, wählt man zunächst den gewünschten Trackingserver und kann anschließend ein Gerät anlegen, welches getracked werden soll. Im vorliegenden Beispiel nutzen wir den für Europa bereitgestellten Server. Legt man ein neues Gerät an, vergibt man zunächst dem neu erstellten Gerät einen Namen, der nur zu reinen Anzeigezwecken im Webdienst dient, sowie einen Device Identifier, unter welchem das Gerät angesprochen werden kann. Diese Device ID ist der nötige Parameter, um die gesammelten GPS-Daten später dem Gerät zuordnen zu können. Im vorliegenden Beispiel wurde der Name „*EmergencyBeacon*“ und die DeviceID „*foo1337*“ gewählt. Bei der Wahl der Device ID sollte zur Vermeidung von Übertragungsfehlern auf die Nutzung von Sonderzeichen verzichtet werden.

Hat man einen Account erstellt und ein Gerät eingerichtet, müssen im Webinterface des Gateways die Login-Daten von GPSWOX sowie der zuvor ausgewählte Server angegeben werden. Auf dem Dragino LG01 Gateway ist ein vorprogrammiertes Shellscript namens

send_gps_data.sh hinterlegt, welches die GPS-Daten an den Tracking-Server weiterleiten kann. Dieses Script benötigt die Parameter DeviceID (-d), den Breiten- und Längengrad (-l, -n), sowie die Höhe über Normalnull (-a). Ein Aufruf aus der Shell könnte also so aussehen:

```
send_gps_data.sh -d foo1337 -l 7.952970 -n 48.480476 -a 106.5
```

Später muss sich dieser Aufruf aus den gesammelten Daten der GPS-Node zusammensetzen, damit das Gateway die Live-Daten an den Trackingserver senden kann.

5.5.4. Programmierung der Microcontrollereinheit des Gateways

Die Programmierungen der Microcontrollereinheiten in diesem Projekt werden in der Programmiersprache C umgesetzt. Im folgenden Abschnitt werden zunächst die wichtigsten Codeabschnitte des Gateway-Sketches erläutert und im Anschluss die der Programmierung der GPS-Node. Den vollständigen C-Code kann man den Anhängen X für das Gateway und X für die GPS-Node entnehmen. Der verwendete Code wurde mithilfe von Beispielprogrammen des Hardware-Herstellers Dragino erstellt und auf dieses Setup umgeschrieben, der Originalcode stammt von Edwin Chen, CEO der Firma Dragino Tech und ist im Anhang angehängt.

Anfangs werden die für das Gateway benötigten Bibliotheken geladen und eine Instanz der RadioHead-Funkklasse angelegt.

```
#include <Console.h>
#include <Process.h>
#include <SPI.h>
#include <RH_RF95.h>

RH_RF95 rf95;
```

Anschließend werden leere Char-Arrays angelegt die später mit den GPS-Daten Längengrad, Breitengrad und Höhe (longitude, latitude, altitude) sowie der DeviceID gefüllt werden, sobald die verbundene Node diese Daten sendet.

```
char DeviceID[20]="\0", lon[20]="\0, lat[20]="\0", alt[20]="\0";
```

Vor Beginn der Ausführung ruft der Arduino-Sketch die setup()-Methode auf, um die nötigen Grundeinstellungen des Boards zu initialisieren. Zuerst wird hierbei die Übertragungsrate zwischen dem Mikrocontroller und dem Linux-Prozessor festgelegt, die Konsole gestartet und gewartet bis diese aktiv ist.

```
void setup() {
  Bridge.begin(115200);
```

```
  Console.begin();
  while (!Console);
```

Anschließend wird geprüft ob die Funkinstanz initialisiert werden konnte und eine Fehlermeldung ausgegeben solange dies nicht passiert ist.

```
   if (!rf95.init()) {
    Console.println("LoRa could not be started.");
    while (1);
  }
```

Wurde sie initialisiert, können die wichtigen Parameter zur Übertragung gesetzt werden. Im Beispiel soll auf 868MHz mit einer Übertragungsleistung von 20dBm gesendet werden. Wurden die Parameter gesetzt, gibt die Konsole „Ready to receive!“ aus und setup()-Methode ist abgeschlossen.

```
rf95.setFrequency(868);
rf95.setTxPower(20);
Console.println("Ready to receive!");
}
```

Die Loop-Methode ruft beim Gateway lediglich die Funktion receivepacket(); auf, die alle wichtigen Programmteile enthält. Aufgrund des Modularisierungsprinzips wurden diese jedoch ausgelagert, um bei Bedarf problemlos weitere Methoden zur loop(); hinzufügen zu können.

```
void loop(){
 receivepacket();
}
```

Auf die Methode void getTimeStamp() wird hier nicht weiter eingegangen, da diese lediglich dazu dient einen Zeitstempel zur Einordnung der Rückgabe zu generieren. Eine der wichtigsten Methoden ist die run_send_gps_data()-Methode. Diese Methode führt den Befehl aus, der in Abschnitt 5.5.3. „Einrichten des GPS-Webservices“ erklärt wurde.

send_gps_data.sh -d DeviceID -l latitude -n longitude -a altitude

Zunächst wird ein neuer Prozess angelegt, welcher sogleich das Script aufruft.

```
void run_send_gps_data() {//
  Process p;
  p.begin("send_gps_data.sh");
```

Vor der Ausführung auf der Linux-Partition müssen jedoch noch die Parameter angehängt werden. Die nötigen Daten werden aus den vorher angelegten Char-Arrays entnommen, die durch die Methode receivepacket() erst Empfangen und anschließend so geparsed werden, dass die korrekten Informationen in den jeweiligen Char-Array geschrieben werden. Sind die Parameter gesetzt, wird der Prozess mit p.run(); ausgeführt.

```
  p.addParameter("-d");
  p.addParameter(DeviceID);
  p.addParameter("-l");
  p.addParameter(lat);
  p.addParameter("-n");
  p.addParameter(lon);
  p.addParameter("-a");
  p.addParameter(alt);
  p.run();}
```

In der Funktion receivepacket() wird einerseits das von der GPS-Node gesendete Paket empfangen und dessen Inhalt auf die Char-Arrays aufgeteilt sowie ein Acknowledgement an die Node gesendet. Zu Beginn wird überprüft, ob die RadioHead-Funkanwendung verfügbar ist. Ist dies der Fall werden Variablen deklariert, die zum korrekten Parsing der Nachricht nötig sind. Parsing ist eine Technik zum Herausfiltern einzelner Informationsbruchstücke aus einer zusammenhängenden Nachricht. So sendet beispielsweise die LoRa-Node gleichzeitig die GPS-Daten zu Höhen- und Breitengrad sowie der nautischen Höhe als eine Nachricht und das Parsing erlaubt, es die Informationen in einzelne Char-Arrays aufzuteilen und so zu nutzen. Die Länge des Buffers und der Message wird hier auf 50 gesetzt, da bekannt ist, dass die eintreffende Nachricht diese Größe nicht überschreitet.

```
void receivepacket() {
   if (rf95.available())
  {
    Console.print("New GPS Coordinates: ");
    int i = 0,j=0,code[4];
    int m1=0,m2=0,m3=0,m4=0;
    uint8_t buf[50];
    char message[50]="\0";
    uint8_t len = sizeof(buf);
```

Kommt ein Paket an, liest rf95.recv() die Nachricht komplett in einen Buffer, merkt sich die Länge der Nachricht und schreibt diese in den Char-Array *message*. Um die Nachricht später genau parsen zu können, sendet die LoRa-Node zwischen jedem Informationsbruchstück ein Komma, welches im folgenden Code gesucht wird. Ein Zähler für jede übertragene

Information speichert hierbei die Länge des Informationsbruchstücks in einem Vektor ab, um dieses später korrekt in einen eigenen Container übertragen zu können.

```
if (rf95.recv(buf, &len)){
  strcpy(message,(char *)buf);
  while(i<50)
  {if(message[i]==','){
    code[j]=i; j++;} i++;}}
```

Ist dies geschehen, können die Informationsbruchstücke mithilfe der abgespeicherten Codewortlänge aus dem Char-Array message[ ] in die den Daten zugeordneten Char-Arrays lon[ ], lat[ ], alt[ ] und DeviceID[ ] geparsed werden.

```
for(int k=0;k<code[0];k++)
  {
    lon[m1]=message[k];
    m1++;
  }
   for(int k=code[0]+1;k<code[1];k++)
  {
    lat[m2]=message[k];
    m2++;
  }
   for(int k=code[1]+1;k<code[2];k++)
  {
    alt[m3]=message[k];
    m3++;
  }
  for(int k=code[2]+1;k<code[3];k++)
  {
    DeviceID[m4]=message[k];
    m4++;
  }
```

Sind die Char-Arrays befüllt kann nun die Methode run_send_gps_data() gestartet und so der Prozess in der Linux-Shell aufgerufen werden. Ist dies abgeschlossen, gibt die Konsole die weitergeleiteten Daten aus und sendet eine Antwortnachricht an die Node, um das Ende des Zyklus anzuzeigen.

```
run_send_gps_data();
```

```
    Console.print((char*)buf);
    Console.print("  with RSSI: ");
    Console.print(rf95.lastRssi(), DEC);
    Console.print("  ");getTimeStamp();
    uint8_t data[] = "Gateway received GPS data";
    rf95.send(data, sizeof(data));
    rf95.waitPacketSent();
    Console.println("Reply sent to Node.");} }
```

5.5.4. Programmierung der Microcontrollereinheit der LoRa-Node

Die LoRa-Node muss so programmiert werden, dass sie zwei Aufgaben erfüllt:

1) Die LoRa-Node baut eine GPS-Verbindung auf und liest die benötigten Daten aus.
2) Sie schreibt die Daten in eine Nachricht und sendet diese über 868MHz an das Gateway.

Beim Hochladen des Codes mit der Arduino IDE kann es zu Fehlermeldungen kommen. Um diese zu beheben muss lediglich der RST-Knopf seitlich des LoRa/GPS Shields gedrückt gehalten werden bis der Sketch fertig hochgeladen wurde.

Wie auch bei dem Gateway müssen Anfangs die benötigten Bibliotheken eingebunden und Instanzen der Klassen deklariert werden. Zudem werden der softwarebasierten seriellen Schnittstelle die PINs übergeben, an die in Abschnitt 5.5.2. mittels Jumperkabeln das GPS-Modul angeschlossen wurde.

```
#include <SoftwareSerial.h>
#include <TinyGPS.h>
#include <SPI.h>
#include <RH_RF95.h>
TinyGPS gps;
RH_RF95 rf95;
SoftwareSerial ss(3, 4);
```

Im Anschluss werden die nötigen Variablen und Char-Arrays deklariert. Besonders wichtig ist hierbei die korrekte DeviceID anzugeben, da diese im Paket übertragen wird, um das GPS-fähige Gerät bei dem Sendevorgang zu GPSWOX identifizieren zu können.

```
char DeviceID[10]="foo1337";

String datastring1="";
String datastring2="";
```

```
String datastring3="";
uint8_t datasend[50]; // LoRa Nachricht

char gps_lon[50]={"\0"}; //Longitude
char gps_lat[20]={"\0"}; //Latitude
char gps_alt[20]={"\0"}; //Altitude
```

Im Anschluss daran wird die setup()-Methode aufgerufen. Zuerst werden die serielle Schnittstelle sowie die softwarebasierte serielle Schnittstelle initialisiert. Die serielle Schnittstelle gibt die GPS-Informationen hierbei an den Seriellen Monitor der Arduino DIE weiter, die softwarebasierte serielle Schnittstelle übernimmt die Kommunikation zum angeschlossenen LoRa-GPS-Shield. Der übergebene INT-Wert bestimmt hierbei die benötigte Übertragungsrate.

```
void setup()
{
  Serial.begin(9600);
  ss.begin(9600);
  while (!Serial);
```

Darauffolgend wird wie bei dem Gateway das Funkmodul initialisiert und die Funkparameter festgelegt. Ist dies ohne Probleme geschehen, wird ein „Ready to send“ ausgegeben.

```
  if (!rf95.init()) {
    Serial.println("LoRa could not be started.");
    while (1);
  }
  rf95.setFrequency(868);
  rf95.setTxPower(20);

  Serial.println("Ready to send!");
}
```

In der Loop-Methode des LoRa-GPS-Shields werden nun Variablen angelegt, um diese mit den zugehörigen GPS-Daten Longitude *flon*, Latitude *flat*, Altitude *falt* füllen zu können. Dann werden die GPS-Daten mit der Methode gps.f_get_position(&flat, &flon, &age); abgerufen und anschließend in die deklarieren Floats übertragen.

```
void loop()
{
```

```
  float flat, flon, falt;
  unsigned long age;
  gps.f_get_position(&flat, &flon, &age);
  falt=gps.f_altitude();
  flon == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flon, 6;
  flat == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flat, 6;
  falt == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : falt, 2;
```

Um die Daten besser übertragen zu können, werden diese durch die dtostrf()-Methode von Floats in Char-Arrays übertragen und anschließend durch die strcat()-Methode aneinandergehängt. Dabei ist unbedingt darauf zu achten, dass die Informationen durch ein Komma getrennt werden, da das Gateway später dieses Komma nutzt, um das Ende einer Information herauszufinden.

```
  datastring1 +=dtostrf(flat, 0, 6, gps_lat);
  datastring2 +=dtostrf(flon, 0, 6, gps_lon);
  datastring3 +=dtostrf(falt, 0, 2, gps_alt);
  if(flon!=1000.000000)
  {
  strcat(gps_lon,",");
  strcat(gps_lon,gps_lat);
  strcat(gps_lon,",");
  strcat(gps_lon,gps_alt);
  strcat(gps_lon,",");
  strcat(gps_lon,DeviceID);
  strcat(gps_lon,",");
```

Anschließend wird der zusammengesetzte Char-Array in den Char-Array *datasend* übertragen, im Monitor ausgegeben und über rf95 gesendet.

```
strcpy((char *)datasend,gps_lon);
Serial.println((char *)datasend);
  rf95.send(datasend, sizeof(datasend));
  rf95.waitPacketSent();
```

Anschließend wird auf die Antwort des Gateways gewartet und in einem intelligenten Delay die nächsten GPS-Daten abgerufen.

```
  receivepacket();
  }
```

```
  smartdelay(1000);
}
```

Die implementierte receivepacket()-Methode überprüft, ob das Gateway eine Nachricht zurückgesendet hat. Am Anfang der Methode werden die zwei Variablen *indatabuff* und *len* des Integertyps uint8_t deklariert, welche später mit der erhaltenen Antwort und deren Länge gefüllt werden.

```
void receivepacket(){
    uint8_t indatabuf[RH_RF95_MAX_MESSAGE_LEN];
    uint8_t len = sizeof(indatabuf);
```

Nach kurzer Wartezeit wird die eingehende Nachricht und deren Länge durch die rf95-recv()-Methode in die zwei Variablen gespeichert und anschließend ausgegeben. Um an der Node sichtbar zu machen, dass eine Nachricht eingeht, wird eine LED angeschaltet und die erhaltene Nachricht über die Konsole ausgegeben. Wenn kein Paket innerhalb des Wartefensters eingeht, wird „receive failed!“ in der Konsole ausgegeben und die LED wird ausgeschaltet.

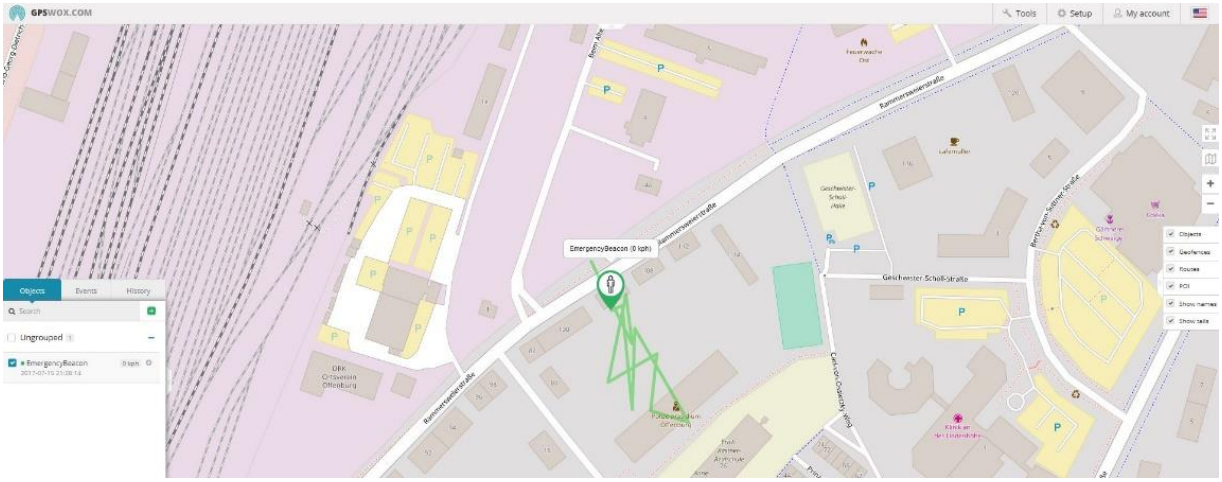
```
    if (rf95.waitAvailableTimeout(3000))
     {
       if (rf95.recv(indatabuf, &len))
         {
         Serial.println((char*)indatabuf);
         digitalWrite(LED, HIGH);
         }
         else
         {
          digitalWrite(LED, LOW);
          Serial.println("receive failed!");
         }
    }
    else
    {
      digitalWrite(LED, LOW);
    }
}
```

Die Funktion smartdelay() hält für eine eingegebene Anzahl von Millisekunden den Programmablauf und überprüft - wenn die serielle Schnittstelle zum GPS-Modul aktiv ist - durch gps.encode(ss.read()) ob ein valides GPS-Signal bei der Einheit eingeht. Dies ermöglicht die Vorbereitung für den nächsten Programmzyklus.

```
static void smartdelay(unsigned long ms)
{
  unsigned long start = millis();
  do
  {
    while (ss.available())
    {
      gps.encode(ss.read());
    }
  } while (millis() - start < ms);
}
```

5.5.5. Anzeige des GPS-Verlaufs durch GPSWOX

Wenn das System einen Zyklus durchlaufen hat, wurden die GPS-Daten von der Node an das Gateway gesendet und über ein Shell-Script an den GPS-Trackingserver des Webdienstes GPSWOX übertragen. Dort werden die letzten zehn Positionen des Gerätes mit der ID foo1337 gespeichert und durch einen Trail miteinander verbunden. Die GPS-Location des letzten Pakets wird mit einem auswählbaren Icon gekennzeichnet und dessen Zeitstempel wird in der Legende angezeigt.



Darstellung 38. Einrichten und erste Trackingversuche mit GPSWOX, Eigene Darstellung

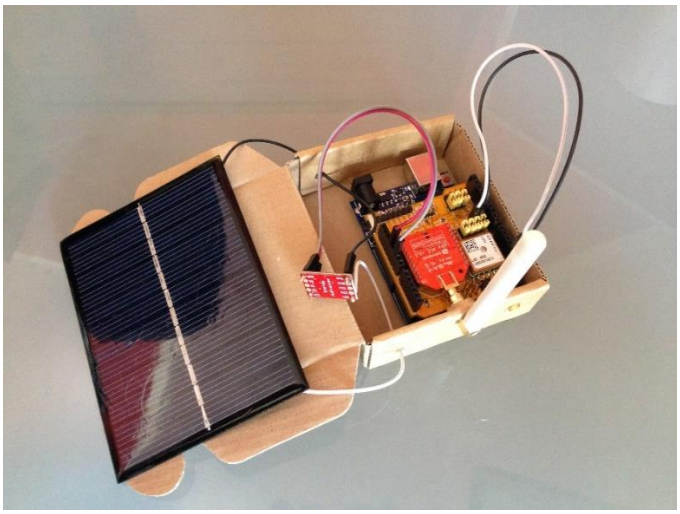
5.6. Evaluation des Projekts

Zur technischen Evaluation des Projektes „Emergency Beacon“ wurde die Basisstation fensternah in einem Raum auf der dritten Etage eines Hochschulgebäudes aufgestellt und mit dem Hochschulnetzwerk verbunden. Ein Rechner überwachte die eingehenden

Nachrichten auf der Ausgabekonsole der Arduino IDE sowie den GPS-Pfad der solarbetrieben GPS-Einheit.

Darstellung 39. Versuchsaufbau zum Reichweitentest des Emergency-Beacons, Eigene Darstellung

Die mobile Einheit wurde mit dem Energy Harvesting-Board verlötet und mit dem Solarpanel in einer handlichen, passenden Schachtel befestigt. Für diesen sehr mobilen Aufbau wurde auf das Einbinden der Superkapazitatoren als Energiespeicher verzichtet.

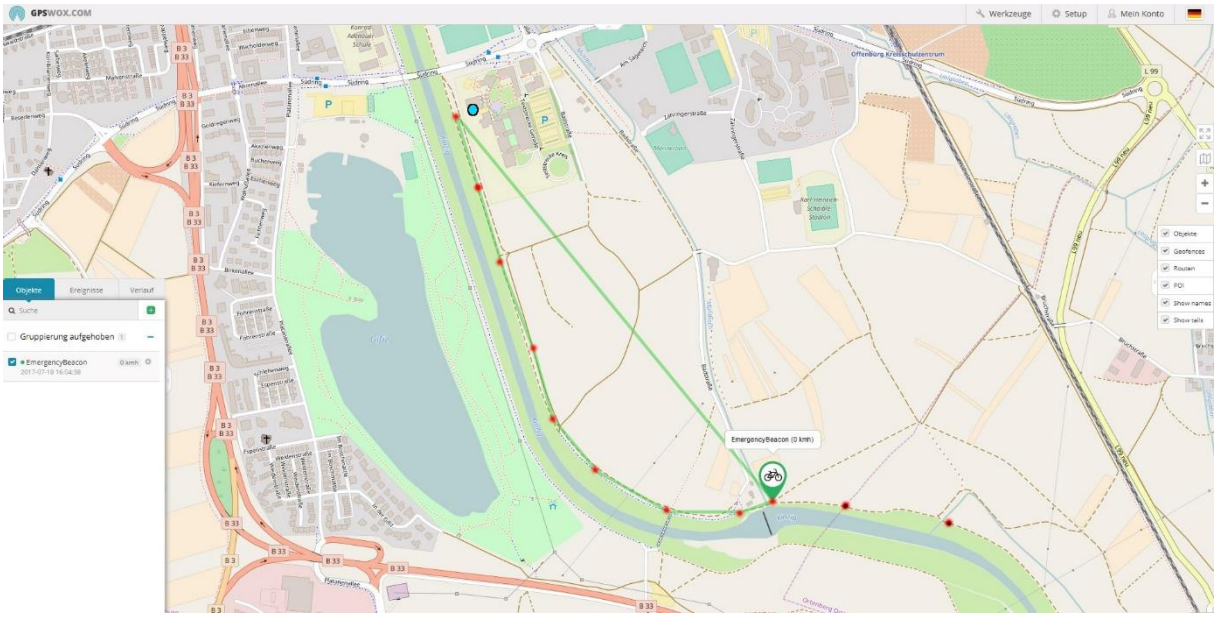


Darstellung 40. Einsatzbereiter GPS-LoRa-Beacon mit Solarzelle und Energy-Harversting Board, Eigene Darstellung

5.6.1. Reichweite

Um die Reichweite der Einheit zu testen, wurde der GPS-Beacon mittels Fahrrad langsam von der Basisstation entfernt und in größer werdendem Abstand aufgebaut. Die folgende Darstellung 41 zeigt das LoRa-Gateway als blauen Kreis mit schwarzer Kontur und die

Messpunkte des Emergency-Beacon als roten Kreis auf einer grünen Spur. Rote Kreise die mit einem schwarzen Punkt versehen sind und nicht auf der Linie liegen, zeigen die Positionen von Messpunkten an denen keine Nachricht beim Gateway eingegangen ist.



Darstellung 41. GPS Track des Versuchs von dem Webdienst GPSWOX mit eigenen Markierungen, Eigene Darstellung

Die Messdaten in der folgenden tabellarischen Darstellung 42 starten vom Gateway ausgehend entlang des Flusses in Richtung Süden. Angegeben sind die Entfernung zum Gateway in direkter Linie, Längen- und Breitengrad, Höhenmeter, DeviceID sowie der gemessenen RSSI der die Signalstärke in dBm anzeigt.

Darstellung 42. Tabelle mit Messwerten des Reichweitentests des Emergency-Beacons, Eigene Darstellung

Entfernung	Längengrad	Breitengrad	Höhenmeter	DeviceID	RSSI
50m	7.940398	48.457870	166.80	foo1337	-61dBm
200m	7.941312	48.455864	154.50	foo1337	-75dBm
400m	7.942033	48.454315	160.90	foo1337	-83dBm
600m	7.943043	48.452560	172.70	foo1337	-92dBm
800m	7.943685	48.451027	157.00	foo1337	-84dBm
950m	7.945198	48.449837	159.60	foo1337	-90dBm
1100m	7.947642	48.448929	162.90	foo1337	-94dBm
1200m	7.950133	48.448936	161.90	foo1337	-89dBm
1400m	Keine Messung				
1500m	Keine Messung				
1240m	7.951190	48.449173	161.40	foo1337	-94dBm

Darstellung 43. Maximale Reichweite des Versuchsaufbaus, Google Maps

Da der Messpunkt auf 1400m in einer Talsenke lag, wurde mit dem nächsten höhergelegenen Punkt bei 1500m fortgefahren. Als von dort ebenfalls keine Nachricht am Gateway angekommen ist, wurde in kurzen Schritten zurückgegangen bis wieder eine Nachricht empfangen wurde. Die höchste gemessene Entfernung bei einer Übertragung waren 1240m zwischen dem Gateway und der GPS-Node. Wie auf Darstellung 43 erkennbar, lagen zwischen beiden Geräten lediglich Wiesen, Felder und Bäume. Bei diesem Versuch war kein direkter Sichtkontakt zwischen beiden Geräten vorhanden.

Um zu überprüfen, ob eine größere Entfernung möglich ist, wenn Sichtkontakt besteht, wurde eine weitere Messung auf der Spitze des Hauptturms des 2800m entfernten Schloss Ortenberg durchgeführt. In folgender Darstellung 44 ist im Vordergrund das eingeschaltete Gateway und dessen Antenne zu sehen und rot eingekreist sichtbar die Spitze des Schlossturms.

Darstellung 44. Sichtkontakt zwischen dem Emergency-Beacon und dem LoRa-Gateway

Bei dem Versuch konnte trotz direktem Sichtkontakt und der erhöhten Lage beider Geräte keine Funkübertragung erreicht werden.

5.6.2. Stromverbrauch

Herstellerangaben zu der verwendeten Einheit besagen, dass sie bei der verwendeten Sendeleistung von 20dBM einen Verbrauch von 80mA aufweist. Tests mit reinen Paketübertragungen ohne den Anschluss der GPS-Einheit haben ergeben, dass bei gleicher Sendeleistung 74mA zur Übertragung einer Nachricht ausreichten.

Das GPS-Modul selbst benötigt einen Betriebsstrom von 25mA um die Verbindung zu einem Satelliten aufbauen und die Daten über die serielle Schnittstelle weitergeben zu können. Während der Tests reichten die von dem Energy-Harvesting-Board kontinuierlich ausgesendeten 100mA immer aus, um die Funkeinheit mit Strom zu versorgen. Da es bei den Messungen nie zu Energieproblemen kam, kann bei dem Versuch davon ausgegangen werden, dass eine Energiespitze nie lange über 100mA war oder dass die Bauteile einen niedrigeren Energiebedarf haben, als angegeben.

5.6.3. Fazit des Projekts

Im Rahmen dieser Arbeit wurde eine solarbetriebene Anwendung erstellt, die allein durch die Energiegeneration eines Solarpanels in der Lage ist, GPS-Daten zu sammeln und mittels LoRaWAN-Funktechnik über 1240 Meter an ein Gateway zu senden. Dieses sendet die Daten via Shell-Script an einen Webdienst, der die Daten visuell auf einer Karte sichtbar macht.

Zu Beginn der Hardwaresuche wurde zusätzlich ein kleineres LoRaWAN-Modul ohne GPS-Fähigkeit erworben, für den Fall, dass die Solarenergie nicht für die Stromversorgung des Arduinos, des GPS-Moduls sowie des LoRa-Moduls ausreichte. Nach ausreichenden Test wurde jedoch festgestellt, dass die von dem Energy-Harvesting-System bereitgestellte Energie genügt, um das große System mit Strom zu versorgen. Es wurde sich bewusst für Solarenergie entschieden, da ein solches System autark arbeiten kann, was bei der Sammlung von Bewegungsenergie nicht gewährleistet ist. Ein Nachteil dieses Systems ist es natürlich, dass ab einer bestimmten Wetterlage kein Strom mehr produziert werden kann und Maßnahmen getroffen werden müssen, um den in Sonnenstunden produzierten Strom zwischenzuspeichern.

Die im Test erbrachte maximale Reichweite lag zwar deutlich unter dem erwarteten Wert, jedoch kann dies auch mit unbekannten Störquellen und der Leistung der mitgelieferten Antennen zusammenhängen. Solange sich die LoRaWAN-Node im Sendebereich befand, konnten immer Nachrichten ausgetauscht werden, bis die Verbindung völlig abbrach. Fehlerhafte Ausgaben kamen nicht vor. Der nachgeschobene Test mit einer höheren Reichweite bei dem Sichtkontakt gegeben war, unterstützt die These, dass die Sendeleistung der Module einfach an ihre Grenzen gekommen ist. Da zwischen den beiden Punkten auf dem Boden nur wenige Gebäude und Störquellen lagen, kann davon ausgegangen werden, dass das Signal zu schwach war, um über diese Entfernung gesendet zu werden.

Die erworbenen Mikrocontroller und Sendemodule war bereits für den Einsatz in einem fertigen System vorbereitet und mussten nicht selbst zusammengelötet werden. Der Preis lag zwar etwas höher als bei vergleichbaren Einzelprodukten, aber boten für den Preis die Garantie, dass die Komponenten störungsfrei miteinander arbeiten können. Es wäre möglich gewesen, eine kleine Programmiereinheit mit einer LoRa-fähigen Platine und einem eigenständigen GPS-Modul zu verbinden, jedoch wäre dies über den Rahmen der

Arbeit hinausgegangen und hätte ein höheres elektrotechnisches Risiko mit sich gebracht, die Module bei Testversuchen zu zerstören.

Als nächste Schritte zur Weiterentwicklung des Projektes hätte man diverse Ansätze verfolgen können. So wäre es möglich gewesen, leistungsstärkere Antennen zu erwerben und mit den Systemen zu verbinden, um herauszufinden ob dies die Reichweite der Signalübertragung erhöht. Des Weiteren hätten zusätzliche Sensoren wie Temperatur-, Licht- oder Ultraschallsensoren an der LoRa-Node angebracht werden können, bis die Energieversorgung durch das Solarpanel nicht für die Versorgung der Bauteile ausgereicht hätte. Damit hätte man die Kapazität des Solarpanels ausschöpfen können.

Ein anderer Ansatz ist die Reduzierung der Gesamtgröße des mobilen Systems. Ein effizienteres, kleineres Solarpanel könnte in den Schaltkreis eingebaut werden, um die Einheit noch kleiner und handlicher zu machen als sie ohnehin bereits ist. Dazu wäre es passend, eine geeignete Art der Energiezwischenspeicherung hinzuzufügen, sei es durch eine Lithiumionenbatterie oder einige Superkapazitatoren.

Zusammenfassend kann gesagt werden, dass die Möglichkeiten solcher Systeme noch lange nicht ausgeschöpft sind und es viele Einsatzgebiete für sie gibt. In den kommenden Jahren werden LPWAN-System voraussichtlich immer mehr in den Vordergrund der Anwendungsentwicklung im Internet der Dinge treten.

6. Zusammenfassung der Arbeit und Ausblick

Das Internet der Dinge wird in den kommenden Jahren in immer mehr Bereichen des Lebens und Arbeitens Einzug erhalten. Neben dem Consumerbereich, in denen das Internet der Dinge hauptsächlich zur Mediasteuerung und der Gebäudeautomation eingesetzt wird, trägt das Internet der Dinge im Rahmen der Industrie 4.0 auch zu immer weiterentwickelten und optimierten Herstellungsprozessen in der Wirtschaft bei. Es scheint, dass derzeit jedes Unternehmen versucht, Marktanteile in dem Bereich der M2M-Kommunikation für sich zu sichern. Das große Problem dabei ist, dass oft die Interoperabilität zwischen den Systemen verschiedener Hersteller nicht gewährleistet wird, da scheinbar jeder ein eigenes Protokoll zur M2M-Kommunikation verwendet. Es wäre dringend notwendig, dass sich große Unternehmen auf einen zertifizierten Standard einigen, der im Idealfall die Vorteile der meisten Technologien unter sich vereint.

Genauso verhält es sich mit der drahtlosen Kommunikation im Internet der Dinge. Viele Unternehmen entwickeln an eigenen Lösungen die sie wiederrum als den einzig wahren Standard präsentieren. Wie aus dem Vergleich in dieser Arbeit hervorgeht, haben alle der vorgestellten Anbieter unterschiedliche Ansätze, was es schwierig macht sie in einem direkten Vergleich gegenüberzustellen. So wäre es sinnvoll, die Technologien nach Anwendungsgebieten miteinander zu vergleichen. Die EnOcean-Technologie zählt per Definition zu den LPWAN-Technologien, tendiert aber aufgrund der geringen Reichweite des Systems eher dazu mit Short-Range-Systemen wie WiFi oder Bluetooth verglichen zu werden, die jedoch meist über einen bei weitem höheren Energieverbrauch verfügen. Anbieter wie LoRa, SigFox oder Ingenu sind in der Lage große Flächen abzudecken, was einen Vergleich mit Mobilfunklösungen nahelegt. In der Zukunft könnte es unter Umständen noch dazu kommen, dass die kommenden Mobilfunk-Technologie in der Lage ist kostenbezogen mit den in dieser Arbeit vorgestellten LPWAN-Anbietern mitzuhalten. Mobilfunk besitzt im Vergleich zu LPWAN-Systemen eine niedrigere mögliche Durchdringung von Gebäuden und ist eingeschränkter was die Einsatzorte angeht, während LPWAN-Systemen selbst unter der Erde installiert und betrieben werden können, an denen keine Verbindung zu Mobilfunknetzen möglich ist.

Desweiteren wurde in der Arbeit ein kurzer Exkurs zum Energy-Harvesting gegeben und vorgestellt, welche Möglichkeiten zur Energiegewinnung aus Umweltressourcen existieren. EnOcean bietet bereits seit Jahren batterieloser Funktechnik an und entwickelt diese stetig weiter, aber auch die anderen vorgestellten Technologien benötigen wenig Energie und können durch Umweltressourcen mit Strom versorgt werden. Die Möglichkeiten zur Energiesammlung in Verbindung mit den vorgestellten LPWAN-Technologien haben ein großes Potential, da so dem Internet ermöglicht wird unerschlossene Gebiete ohne Strom- oder Netzwerkanschlüssen mit wartungsfreien und energieautarken Sensor- und Steuerungseinheiten zu erschließen und zu vernetzen.

Im praktischen Teil der Arbeit wurde versucht ein LoRaWAN-System mit Solarenergie zu betreiben, um GPS-Daten an eine Basisstation zu senden und auswerten zu lassen. Dieser Versuch hat gezeigt, dass es möglich ist mit den bereits verfügbaren LPWAN-Bauteilen und günstigen Solarmodulen schnell und einfach ein batterieloses System einzurichten. Die dazu benötigte Software steht oft Open Source zur Verfügung und ist hervorragend dokumentiert. Zudem stehen solchen Systemen ab dem Zeitpunkt des Eintreffens der Nachricht am Gateway sämtliche Möglichkeiten des Internets der Dinge zur Verfügung. So können die Daten durch verschiedene Webdienste wie beispielsweise ThingSpeak dargestellt und für die Anzeige im Web vorbereitet werden oder wie im vorgestellten Beispiel können die GPS-Daten mit GPSWOX auf einer Karte verzeichnet werden. Da das gezeigte Beispielprojekt auf einem Arduino basiert und nur wenige der verfügbaren Schnittstellen des Mikrocontrollers nutzt, kann die Anwendung zu Steuerungszwecken oder durch weitere Sensorik erweitert werden, solange genügend Energie zur Verfügung steht.

Zum Abschluss kann zusammenfassend gesagt werden, dass drahtlose Kommunikation im Internet der Dinge besonders im Bereich von low-power Netzwerken in den kommenden Jahren an Bedeutung gewinnen wird. Die Möglichkeit, energieautarke Funknetzwerke an beliebigen Orten einzurichten ist ein großer Gewinn für das Internet der Dinge und die Machine-to-Machine Kommunikation. Derzeit sind die vorgestellten Technologien zwar einsatzbereit, jedoch oft noch nicht zu einhundert Prozent marktreif. Besonders bei den Ansätzen die auf unternehmenseigenen Netzwerken aufbauen, ist die fehlende existierenden Abdeckung ein großes Problem, welches angegangen werden sollte. Zudem arbeiten zwar viele große Unternehmen in eigenen Allianzen zusammen an der Entwicklung eines großen Standards für diese Art von drahtloser Kommunikation, jedoch sind es immer noch zu viele verschiedene Technologien die alle miteinander konkurrieren. Es sollte versucht werden, eine einheitlichere Struktur der Protokolle und deren Interoperabilität anzustreben, um eine möglichst hohe Vernetzung erzielen zu können.

Literaturverzeichnis

[1] S. Horvath, *Aktueller Begriff, Internet der Dinge.* [Online] Available: https://www.bundestag.de/blob/192512/cfa9e76cdcf46f34a941298efa7e85c9/internet_der_dinge-data.pdf. Accessed on: May 25 2017.

[2] IEEE Conference on Local Computer Networks; Institute of Electrical and Electronics Engineers; Computer Society; Annual IEEE Conference on Local Computer Networks; LCN, *2016 IEEE 41st Conference on Local Computer Networks: LCN 2016 : 7-10 November 2016, Dubai, United Arab Emirates : proceedings*. Piscataway, NJ: IEEE, 2016.

[3] Hong, Steven, et al., *Applications of self-interference cancellation in 5G and beyond.*

[4] J. F. Kurose and K. W. Ross, *Computernetzwerke: Der Top-Down-Ansatz,* 5th ed. München: Pearson Studium, 2012.

[5] C. Baun, *Computernetze kompakt,* 3rd ed. Berlin u.a.: Springer Vieweg, 2015.

[6] FHEMWiki, *1% Regel im Funk.* [Online] Available: https://wiki.fhem.de/wiki/1%25_Regel. Accessed on: Jul. 16 2017.

[7] *Frequenzband :: frequency band :: ITWissen.info.* [Online] Available: http://www.itwissen.info/Frequenzband-frequency-band.html. Accessed on: Jun. 25 2017.

[8] *Grundlagen Funktechnik.* [Online] Available: http://www.elektronik-kompendium.de/sites/kom/0810301.htm. Accessed on: Jun. 16 2017.

[9] *dBm (decibel milliwatt) :: Dezibel Milliwatt :: ITWissen.info.* [Online] Available: http://www.itwissen.info/dBm-decibel-milliwatt-Dezibel-Milliwatt.html. Accessed on: Jun. 25 2017.

[10] *S/N (Signal-Rausch-Verhältnis) :: SNR (signal to noise ratio) :: ITWissen.info.* [Online] Available: http://www.itwissen.info/Signal-Rausch-Verhaeltnis-S-N-signal-to-noise-ratio-SNR.html. Accessed on: Jul. 04 2017.

[11] A. M. J. Goiser, *Handbuch der Spread-Spectrum Technik*. Vienna: Springer Vienna, 1998.

[12] r. v. 1. 121 *et al., The Constrained Application Protocol (CoAP).* [Online] Available: https://tools.ietf.org/html/rfc7252. Accessed on: Apr. 12 2017.

[13] Wikipedia, *File:Drzewo ciagow ortogonalnych.png - Wikipedia.* [Online] Available: https://en.wikipedia.org/wiki/File:Drzewo_ciagow_ortogonalnych.png. Accessed on: Jul. 19 2017.

[14] *Leistungsübertragungsbilanz :: link budget :: ITWissen.info.* [Online] Available: http://www.itwissen.info/Leistungsuebertragungsbilanz-link-budget.html. Accessed on: Jul. 19 2017.

[15] Prof. Dr. Christian Plätz, Dipl.-Ing. (FH) André Volkmar, “Stört LTE 800 das 868-MHz-Band?,” *wireless*, 01 Oct., pp. 34–38, 2013, https://www.tu-chemnitz.de/etit/sse/szee/rsrc/StoertLTE800.pdf.

[16] *Bluetooth Core Specification | Bluetooth Technology Website.* [Online] Available: https://www.bluetooth.com/specifications/bluetooth-core-specification. Accessed on: Jun. 21 2017.

[17] *IEEE 802.* Accessed on: Jun. 23 2017.

[18] *Certification | Wi-Fi Alliance.* [Online] Available: http://www.wi-fi.org/certification. Accessed on: Jun. 23 2017.
[19] *Zigbee IP and 920IP | Zigbee Alliance.* [Online] Available: http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeeip/. Accessed on: Jul. 03 2017.
[20] *Zigbee RF4CE | Zigbee Alliance.* [Online] Available: http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeerf4ce/. Accessed on: Jul. 03 2017.
[21] *Zigbee PRO with Green Power | Zigbee Alliance.* [Online] Available: http://www.zigbee.org/zigbee-for-developers/network-specifications/zigbeepro/. Accessed on: Jul. 03 2017.
[22] *About the Technology - NFC Forum.* [Online] Available: http://nfc-forum.org/what-is-nfc/about-the-technology/. Accessed on: Jul. 03 2017.
[23] G. Tamm and C. Tribowski, *RFID*. Berlin Heidelberg: Springer-Verlag Berlin Heidelberg, 2010.
[24] *The State of LTE - OpenSignal.* [Online] Available: https://opensignal.com/reports/2017/06/state-of-lte. Accessed on: Jul. 19 2017.
[25] K. Flynn, *3GPP Release 15 (5G).* [Online] Available: http://www.3gpp.org/release-15. Accessed on: May 28 2017.
[26] 3GPP, *About 3GPP Home.* [Online] Available: http://www.3gpp.org/about-3gpp/about-3gpp. Accessed on: May 26 2017.
[27] K. Flynn, *Release 13.* [Online] Available: http://www.3gpp.org/release-13. Accessed on: Jun. 16 2017.
[28] A. Kainz and M. Bürger, “Die IoT-Kommunikation der Zukunft – LPWAN & LTE Evolution,” *Elektrotech. Inftech.*, vol. 133, no. 7, pp. 348–350, 2016.
[29] Technical Marketing Workgroup LoRa Alliance, *LoRaWAN What is it?: A technical overview of LoRa and LoRaWAN.* [Online] Available: https://www.lora-alliance.org/portals/0/documents/whitepapers/LoRaWAN101.pdf. Accessed on: May 27 2017.
[30] *MQTT Version 3.1.1.* [Online] Available: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.html. Accessed on: Apr. 12 2017.
[31] *About LoRa Alliance.* [Online] Available: https://www.lora-alliance.org/The-Alliance/About-the-Alliance. Accessed on: May 22 2017.
[32] LoRa Alliance Technical committee, *LoRaWAN Regional Parameters.* [Online] Available: https://www.lora-alliance.org/for-developers. Accessed on: Jul. 19 2017.
[33] N. (. Sornin, M. (. Luis, T. (. Eirich, and T. (. Kramp, *LoRaWAN Specification 1.0.2.* [Online] Available: https://www.lora-alliance.org/for-developers. Accessed on: Jul. 19 2017.
[34] Sigfox, *Our story | Sigfox: Sigfox Timeline.* [Online] Available: https://www.sigfox.com/en/sigfox-story. Accessed on: May 28 2017.
[35] *Radio Technology Keypoints | Sigfox.* [Online] Available: https://www.sigfox.com/en/sigfox-iot-radio-technology. Accessed on: Jul. 19 2017.
[36] *What Is The Sigfox Protocol Stack?* [Online] Available: https://www.youtube.com/watch?v=tGmFgaxKPRU. Accessed on: Jul. 19 2017.
[37] Sigfox, *Coverage | Sigfox.* [Online] Available: https://www.sigfox.com/en/coverage. Accessed on: May 29 2017.

[38] Wikipedia, *Ingenu - Wikipedia.* [Online] Available: https://en.wikipedia.org/w/index.php?oldid=756696009. Accessed on: Jun. 16 2017.
[39] Ingenu Inc., *How RPMA works: The Making of RPMA.* [Online] Available: http://www.ingenu.com/portfolio/how-rpma-works-the-making-of-rpma/.
[40] *Machine Network Nationwide Coverage - Ingenu.* [Online] Available: https://www.ingenu.com/technology/machine-network/coverage-tracker/. Accessed on: Jul. 18 2017.
[41] *Software - Ingenu.* [Online] Available: https://www.ingenu.com/get-started/software/. Accessed on: Jul. 19 2017.
[42] J. Kurtz and B. Wortman, *ASP.NET Web API 2: Building a REST Service from Start to Finish*, 2014.
[43] EnOcean GmbH | Kolpingring 18a | D-82041 Oberhaching, *Unternehmensprofil | EnOcean - Über uns.* [Online] Available: https://www.enocean.com/de/company-profile/. Accessed on: Jul. 19 2017.
[44] *EnOcean-Funkstandard.* [Online] Available: https://www.enocean-alliance.org/de/was-ist-enocean/enocean-funkstandard/. Accessed on: Jul. 19 2017.
[45] EnOcean GmbH, *EnOcean Radio Protocol 2: Technical Specification.* [Online] Available: https://www.enocean.com/fileadmin/redaktion/pdf/tec_docs/EnOceanRadioProtocol2.pdf. Accessed on: Jul. 19 2017.
[46] EnOcean GmbH, *EnOcean Radio Protocol 1: Technical Specification.* [Online] Available: https://www.enocean.com/fileadmin/redaktion/pdf/tec_docs/EnOceanRadioProtocol.pdf. Accessed on: Jul. 19 2017.
[47] Prof. William Webb, *Weightless: The technology to finally realise the M2M vision.* [Online] Available: http://www.weightless.org/news/introduction-to-weightless-technology. Accessed on: Jul. 04 2017.
[48] *Wi-Fi Alliance® introduces low power, long range Wi-Fi HaLow™ | Wi-Fi Alliance.* [Online] Available: http://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-low-power-long-range-wi-fi-halow. Accessed on: Jul. 04 2017.
[49] M. Alioto, *Enabling the Internet of Things: From Integrated Circuits to Integrated Systems*. Cham: Springer International Publishing, 2017.
[50] The Things Network, *The Things Network Wiki: LoRaWAN Technology.* [Online] Available: https://www.thethingsnetwork.org/wiki/LoRaWAN/Home. Accessed on: Jul. 14 2017.
[51] V. Kostic and R. Janke, *Die Zukunft hat mit LoRa begonnen: Low-Power-Netze für das Internet der Dinge.* [Online] Available: https://www.telent.de/fileadmin/av_telent/telent-PDF/Publikationen/NET9-16_LoRa.pdf. Accessed on: Jul. 13 2017.
[52] Semtech, *Wireless & RF Selector Guide.* [Online] Available: https://www.semtech.com/images/mediacenter/collateral/ism_sg.pdf. Accessed on: Jul. 14 2017.
[53] *LoRa Technology.* [Online] Available: https://www.lora-alliance.org/What-Is-LoRa/Technology. Accessed on: May 22 2017.

[54] *LPWAN Cost Webinar.* [Online] Available: https://www.slideshare.net/BrianRay10/lpwan-sost-webinar. Accessed on: Jul. 16 2017.
[55] G. Schatz, *SigFox Vs. LoRa: A Comparison Between Technologies & Business Models.* [Online] Available: https://www.link-labs.com/blog/sigfox-vs-lora. Accessed on: Jul. 16 2017.
[56] The Things Network, *The Things Network Coverage.* [Online] Available: https://www.thethingsnetwork.org/map. Accessed on: Jul. 16 2017.
[57] *Sigfox Developer Portal.* [Online] Available: http://makers.sigfox.com/. Accessed on: Jul. 18 2017.
[58] Ingenu Inc., *How RPMA handles Interference: White Paper by Ingenu.* [Online] Available: https://www.ingenu.com/portfolio/how-rpma-handles-interference/. Accessed on: Jul. 19 2017.
[59] *One day at SigFox.* [Online] Available: https://www.disk91.com/2015/news/technologies/one-day-at-sigfox/. Accessed on: Jul. 17 2017.
[60] M. Centenaro, L. Vangelista, A. Zanella, and M. Zorzi, "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios," *IEEE Wireless Commun.*, vol. 23, no. 5, pp. 60–67, 2016.
[61] *Machine Network - Ingenu.* [Online] Available: https://www.ingenu.com/technology/machine-network/. Accessed on: Jul. 19 2017.
[62] Ingenu Inc., *RPMA Technology: For the Internet of Things.* [Online] Available: http://theinternetofthings.report/Resources/Whitepapers/4cbc5e5e-6ef8-4455-b8cd-f6e3888624cb_RPMA%20Technology.pdf. Accessed on: Jul. 16 2017.
[63] ublox AG, *NANO S100 Data Sheet: Technical data sheet describing the NANO-S100 cellular module.* [Online] Available: https://www.u-blox.com/sites/default/files/NANO-S100_DataSheet_%28UBX-16025707%29.pdf. Accessed on: Jul. 19 2017.
[64] *Device Library - Ingenu.* [Online] Available: http://www.ingenu.com/solutions/device-library/. Accessed on: Jul. 19 2017.
[65] *EVK-S10NANO Kit.* [Online] Available: https://www.u-blox.com/de/product/evk-s10nano-kit#product-information. Accessed on: Jul. 19 2017.
[66] EnOcean GmbH, *EnOcean Product Integration Whitepaper.* Accessed on: Jul. 14 2017.
[67] EnOcean GmbH | Kolpingring 18a | D-82041 Oberhaching, *Energy Harvesting Wireless Standard for Buildings | EnOcean - Case Studies.* [Online] Available: https://www.enocean.com/en/internet-of-things-applications/case-studies/. Accessed on: Jul. 14 2017.
[68] F. Electronics, *Elektronische Bauelemente von den Besten - Future Electronics.* [Online] Available: http://de.futureelectronics.com/de/Seiten/index.aspx. Accessed on: Jul. 19 2017.
[69] S. Priya and D. J. Inman, *Energy harvesting technologies*. New York: Springer, 2010.
[70] EnOcean GmbH, *EnOcean EnergyHarvesting in the IoT Whitepaper.* Accessed on: Jul. 14 2017.

[71] *Referenzen.* [Online] Available: https://www.enocean-alliance.org/de/loesungen/referenzen/. Accessed on: Jul. 19 2017.
[72] *Energy Harvesting: Hose und Schlafsack wandeln Körperwärme in Strom um - Golem.de.* [Online] Available: https://www.golem.de/news/energy-harvesting-hose-und-schlafsack-wandeln-koerperwaerme-in-strom-um-1306-99830.html. Accessed on: Jul. 19 2017.
[73] *Energie: Den Strom der Zukunft gewinnen wir im Vorbeigehen - WELT.* [Online] Available: https://www.welt.de/wissenschaft/article119738185/Den-Strom-der-Zukunft-gewinnen-wir-im-Vorbeigehen.html. Accessed on: Jul. 19 2017.
[74] E. Chen, *LG01 LoRa Gateway User Manual.* [Online] Available: www.dragino.com/downloads/index.php?dir=UserManual/&file=LG01_LoRa_Gateway_User_Manual.pdf. Accessed on: Jul. 19 2017.
[75] *Dragino LG01 Picture.* [Online] Available: http://wiki.dragino.com/images/5/54/Ms14_11.jpg. Accessed on: Jul. 19 2017.
[76] *Arduino Uno Rev3.* [Online] Available: https://store.arduino.cc/arduino-uno-rev3. Accessed on: Jul. 19 2017.
[77] *GPS_Shield_with_Lora_BEE.jpg (JPEG-Grafik, 750 × 750 Pixel).* [Online] Available: http://wiki.dragino.com/images/3/33/GPS_Shield_with_Lora_BEE.jpg. Accessed on: Jul. 22 2017.
[78] *Lora/GPS Shield - Wiki for Dragino Project.* [Online] Available: http://wiki.dragino.com/index.php?title=Lora/GPS_Shield#Packaging_Includes. Accessed on: Jul. 19 2017.
[79] *Zimo® 5V/6V Mini Solar Panel Ladegerät Solarmodul DIY Batterie Solarzelle zur Aufladung in verschiedenen Mustern zum Auswahl (6V/1.1W/200mA): Amazon.de: Küche & Haushalt.* [Online] Available: https://www.amazon.de/Zimo-Ladeger%C3%A4t-Solarmodul-Solarzelle-verschiedenen/dp/B01AEH7HMM/ref=sr_1_1?ie=UTF8&qid=1500502218&sr=8-1&keywords=zimo+solar. Accessed on: Jul. 20 2017.
[80] *SparkFun Energy Harvester Breakout - LTC3588 - BOB-09946 - SparkFun Electronics.* [Online] Available: https://www.sparkfun.com/products/9946. Accessed on: Jul. 20 2017.
[81] Vogel Business Media GmbH & Co. KG, *Buck-Boost-Spannungsregelung mit einem Abwärtsregler.* [Online] Available: http://www.elektronikpraxis.vogel.de/hardwareentwicklung/articles/287055/. Accessed on: Jul. 16 2017.
[82] *Arduino - Software.* [Online] Available: https://www.arduino.cc/en/Main/Software. Accessed on: Jul. 16 2017.
[83] Wikipedia, *Universal asynchronous receiver/transmitter - Wikipedia.* [Online] Available: https://en.wikipedia.org/w/index.php?oldid=785438061. Accessed on: Jun. 15 2017.
[84] Arduino, *SoftwareSerial Library.* [Online] Available: https://www.arduino.cc/en/Reference/SoftwareSerial. Accessed on: Jun. 15 2017.
[85] *Arduino - SPI.* [Online] Available: https://www.arduino.cc/en/Reference/SPI. Accessed on: Jul. 07 2017.

[86] AirSpayce Pty Ltd, *RadioHead: RH_RF95 Class Reference.* [Online] Available: http://www.airspayce.com/mikem/arduino/RadioHead/classRH__RF95.html. Accessed on: Jun. 16 2017.
[87] *TinyGPS | Arduiniana.* [Online] Available: http://arduiniana.org/libraries/tinygps/. Accessed on: Jun. 16 2017.
[88] *Vehicle GPS tracking software: white label gps server online | GPS Tracking Software - GPSWOX.COM.* [Online] Available: https://www.gpswox.com/. Accessed on: Jul. 17 2017.

Anhang

Grundlage des erstellten Codes zur Programmierung des Dragino LG01 LoRa-Gateway:

```
/*
  LoRa Simple Yun Server :
  Support Devices: LG01.

  Example sketch showing how to create a simple messageing server,
  with the RH_RF95 class. RH_RF95 class does not provide for addressing or
  reliability, so you should only use RH_RF95 if you do not need the higher
  level messaging abilities.

  It is designed to work with the other example LoRa Simple Client

  modified 16 11 2016
  by Edwin Chen <support@dragino.com>
  Dragino Technology Co., Limited
*/
//If you use Dragino IoT Mesh Firmware, uncomment below lines.
//For product: LG01.

#define BAUDRATE 115200
#include <Console.h>
#include <SPI.h>
#include <Process.h>
#include <RH_RF95.h>

// Singleton instance of the radio driver
RH_RF95 rf95;
```

```
int led = A2;
float frequency = 868.0;
String dataString = "",lon = "",lat = "";
char lonChar[50]={"\0"};
char latChar[50]={"\0"};
char command[50]={"\0"};
boolean gpsdata=true;


void setup()
{
  pinMode(led, OUTPUT);
  Bridge.begin(BAUDRATE);
  Console.begin();
  while (!Console) ; // Wait for console port to be available
  while (!Serial);
  Console.println("Start Sketch");
  if (!rf95.init())
    Console.println("init failed");
  // Setup ISM frequency
  rf95.setFrequency(frequency);
  // Setup Power,dBm
  rf95.setTxPower(20);
  // Defaults BW Bw = 125 kHz, Cr = 4/5, Sf = 128chips/symbol, CRC on
  Console.print("Listening on frequency: ");
  Console.println(frequency);
}

void loop()
{
  Process p;
  dataString = "";
  if (rf95.available())
  {
    // Should be a message for us now
    uint8_t buf[RH_RF95_MAX_MESSAGE_LEN];
```

```
uint8_t len = sizeof(buf);

if (rf95.recv(buf, &len))
{
  digitalWrite(led, HIGH);

  dataString += String((char*)buf);
  //dataString += ",";

  if(gpsdata==true){
  RH_RF95::printBuffer("request: ", buf, len);
  Console.print("lon: ");
  Console.println(dataString);
  lon=dataString;
  Console.print("RSSI: ");
  Console.println(rf95.lastRssi(), DEC);
  }else{
  RH_RF95::printBuffer("request: ", buf, len);
  Console.print("lat: ");
  Console.println(dataString);
  lat=dataString;
  Console.print("RSSI: ");
  Console.println(rf95.lastRssi(), DEC);
  }

  // Send a reply to client as ACK
  uint8_t data[] = "200 OK";
  rf95.send(data, sizeof(data));
  rf95.waitPacketSent();
  Console.println("Sent a reply");

  if(gpsdata==true)
  gpsdata=false;
  else{
  gpsdata=true;
  lon.toCharArray(lonChar, len);
  lat.toCharArray(latChar, len);
```

```
      strcat(command, "/send_gps_data.sh | -d41133741133741 -l ");
      strcat(command, lonChar);
      strcat(command, " -n ");
      strcat(command, latChar);
      strcat(command, " -a 30.5");
      p.runShellCommand(command);
      while(p.running());
      }
      digitalWrite(led, LOW);
    }
    else
    {
      Serial.println("recv failed");
    }
  }
}
```

Grundlage des erstellten Codes zur Programmierung der GPS/LoRa-Node:

```
/*
In this project,we'll show how to get GPS data from a remote Arduino via
Wireless Lora Protocol
and show the track on the GoogleEarth.The construction of this project is
similar to my last one:
1) Client Side: Arduino + Lora/GPS Shield (868Mhz).
2) Server Side: Arduino + Lora Shield (868Mhz) + Yun Shield + USB flash.
Client side will get GPS data and keep sending out to the server via Lora
wireless. Server side
will listin on the Lora wireless frequency, once it get the data from
Client side, it will
turn on the LED and log the sensor data to a USB flash.
Note: Over here we use the hardware serial to connect with the GPS and
check the serial print by
the software serial.You should make sure the GPS get fixed(3D_Fix LED
flash).
Press the "RST" button when you upload the sketch.
More about this example, please see:
*/
#include <SoftwareSerial.h>
#include <TinyGPS.h>
/* This sample code demonstrates the normal use of a TinyGPS object.
```

```
   It requires the use of SoftwareSerial, and assumes that you have a
   9600-baud serial GPS device hooked up on pins 3(rx) and 4(tx).
*/
#include <SPI.h>
#include <RH_RF95.h>

// Singleton instance of the radio driver
RH_RF95 rf95;
float frequency = 868.0;

TinyGPS gps;
SoftwareSerial ss(3, 4);
String datastring="";
String datastring1="";
char databuf[100];
uint8_t dataoutgoing[100];
char gps_lon[20]={"\0"};
char gps_lat[20]={"\0"};
boolean gpsreply=false;

void setup()
{
  Serial.begin(9600);
  ss.begin(9600);
    if (!rf95.init())
    Serial.println("init failed");

    rf95.setFrequency(frequency);
    // Setup Power,dBm
    //rf95.setModemConfig(RH_RF95::Bw31_25Cr48Sf512);  //set for pre-
configured long range

    //rf95.setSpreadingFactor(12);
    rf95.setTxPower(20);

    ss.print("Simple TinyGPS library v. ");
ss.println(TinyGPS::library_version());
    Serial.println();
```

```
}

void loop()
{
  // Print Sending to rf95_server
  ss.println("Sending to rf95_server");
  bool newData = false;
  unsigned long chars;
  unsigned short sentences, failed;

  // For one second we parse GPS data and report some key values
  for (unsigned long start = millis(); millis() - start < 1000;)
  {
    while (Serial.available())
    {
      char c = Serial.read();
      Serial.write(c); // uncomment this line if you want to see the GPS
data flowing

      if (gps.encode(c)){ // Did a new valid sentence come in?
        newData = true;
        Serial.write("\n\n");
      }
    }
  }
  //Get the GPS data
  if (newData)
  {
    float flat, flon;
    unsigned long age;
    gps.f_get_position(&flat, &flon, &age);
    ss.print("LAT=");
    ss.print(flat == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flat, 6);
    ss.print(" LON=");
    ss.print(flon == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flon, 6);
    ss.print(" SAT=");
    ss.print(gps.satellites() == TinyGPS::GPS_INVALID_SATELLITES ? 0 :
gps.satellites());
```

```
ss.print(" PREC=");
ss.print(gps.hdop() == TinyGPS::GPS_INVALID_HDOP ? 0 : gps.hdop());
flat == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flat, 6;
flon == TinyGPS::GPS_INVALID_F_ANGLE ? 0.0 : flon, 6;
Serial.write("\n\n Geschafft: GPS");
// Once the GPS fixed,send the data to the server.
datastring +=dtostrf(flat, 0, 6, gps_lat);
datastring1 +=dtostrf(flon, 0, 6, gps_lon);

/*Once the GPS fixed,send the data to the server.
datastring +=dtostrf(flat, 0, 6, gps_lat);
datastring1 +=dtostrf(flon, 0, 6, gps_lon);
ss.println(strcat(strcat(gps_lon,","),gps_lat));
strcpy(gps_lat,gps_lon);
ss.println(gps_lat); //Print gps_lon and gps_lat
strcpy((char *)dataoutgoing,gps_lat);
// Send the data to server
rf95.send(dataoutgoing, sizeof(dataoutgoing));*/

if(gpsreply==false){
strcpy((char *)dataoutgoing,gps_lat);
Serial.write(gps_lat);
Serial.write("\n\n Geschafft: LAT");
}else{
strcpy((char *)dataoutgoing,gps_lon);
Serial.write("\n\n Geschafft: LON");
Serial.write(gps_lon);
}

rf95.send(dataoutgoing, sizeof(dataoutgoing));
Serial.write("\n\n Geschafft: Gesendet");

if(gpsreply==false)
     gpsreply=true;
else
     gpsreply=false;
```

```
    // Now wait for a reply
    uint8_t indatabuf[RH_RF95_MAX_MESSAGE_LEN];
    uint8_t len = sizeof(indatabuf);

    if (rf95.waitAvailableTimeout(3000))
     {
       // Should be a reply message for us now
       if (rf95.recv(indatabuf, &len))
      {
         // Serial print "got reply:" and the reply message from the server
         ss.print("got reply: ");
         ss.println((char*)indatabuf);
      }
      else
      {
      ss.println("recv failed");
      }
    }
    else
    {
      // Serial print "No reply, is rf95_server running?" if don't get the
reply .
      ss.println("No reply, is rf95_server running?");
    }
  delay(400);

 }

  gps.stats(&chars, &sentences, &failed);
  ss.print(" CHARS=");
  ss.print(chars);
  ss.print(" SENTENCES=");
  ss.print(sentences);
  ss.print(" CSUM ERR=");
  ss.println(failed);
  if (chars == 0)
  ss.println("** No characters received from GPS: check wiring **");}
```

Eigenständigkeitserklärung

Tom Martin Jung, Studiengang M+I, Mat.-Nr.: 176720

Hiermit erkläre ich, dass ich die vorliegende Bachelor Thesis zum Thema „Vergleich aktueller LPWAN-Technologien im Internet der Dinge unter Einbindung von Energy-Harvesting“ selbstständig und ohne fremde Hilfe verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Weiterhin wurden von mir alle Stellen der Arbeit, an denen mit Wort- und Gedankengut aus fremden Quellen gearbeitet wurde, als solche gekennzeichnet. Diese Arbeit wurde bisher keinem anderen Prüfungsamt in gleicher oder vergleichbarer Form vorgelegt. Sie wurde bisher auch nicht veröffentlicht.

Ort, Datum	Unterschrift