Technische Hochschule Rosenheim

Bluetooth Low Energy - Funktionsweise und Einordnung in den Bereich der IOT Kommunikationsprotokolle

Thomas Randl
Fakultät für Informatik

WS 2019/20

In dieser Arbeit wird der Aufbau und die Funktionsweise der Funktechnik Bluetooth Low Energy (BLE) erläutert. Dabei wird zuerst der Protokollstack im Bezug auf die einzelnen Layer und die BLE spezifischen Profile betrachtet. Anschließend wird genauer auf die Kommunikation zwischen den einzelnen Verbindungspartnern eingegangen. Dabei wird insbesondere erklärt, welche Schritte notwendig sind um Datenpakete zu übertragen. Des Weiteren wird erläutert, wie der Verbindungsaufbau zwischen den Kommunikationspartnern abläuft und welche Rollen die jeweiligen Partner dabei einnehmen. Nachdem die Funktionsweise erläutert wurde, wird das „Featureset“ von BLE erklärt und mit aktuellen Internet of Things (IOT) Protokollen verglichen. Anhand der erarbeiteten Informationen wird dann am konkreten Beispiel der „iBeacons“ erläutert, wie BLE in der Praxis Anwendung findet.

Inhaltsverzeichnis

Abkürzungsverzeichnis

BLE Bluetooth Low Energy

HCI Host Controller Interface

IOT Internet of Things

ISM Industrial, Scientific, and Medical

RSSI Received Signal Strength Indication

SIG Special Interest Group

1 Einleitung

1.1 Ein Abschnitt der Einleitung

2 Technische Grundlagen und Implementierungen

Im folgenden Kapitel wird ein Überblick über die zentralsten BLE Anwendungen gegeben. Zusätzlich wird die Hardwareebene im Bezug auf die physikalischen Voraussetzungen und die genutzten Frequenzbereiche näher betrachtet.

2.1 Beispiele für Implementierungen

Im einundzwanzigsten Jahrhundert steigt die Verwendung von Geräten, welche drahtlos mit einem Empfangsgerät kommunizieren können. Vor allem die Einführung des Smartphones hat an diesem Punkt die drahtlose Kommunikation vorangetrieben. Nutzer wollen viele Funktionen zur Verfügung gestellt bekommen, um den persönlichen Alltag einfacher gestalten zu können.

Schon vor der Einführung des Smartphones war das Kommunikationsprotokoll „Bluetooth“ auf Mobiltelefonen verfügbar. Dabei wurde es hauptsächlich zum Datentransfer zwischen zwei Bluetoothfähigen Endgeräten verwendet. Das Hauptproblem, welches der Nutzer dabei erfahren musste, ist, dass diese Form der Datenübertragung sehr viel Zeit in Anspruch genommen hat. Dies lässt sich auf die geringe Datenmenge zurückführen, die pro Paket möglich ist.

Nachdem das Smartphone immer mehr an Beliebtheit gewonnen hat und sich der Begriff des IOT entwickelt hat, reagierte die Bluetooth Special Interest Group (SIG), indem sie ein Protokoll erarbeiteten, welches einen möglichst geringen Stromverbrauch, eine geringe Bandbreite und niedrige Komplexität bietet [Tow14, Seite 1].

Mit der Einführung von BLE kam die Möglichkeit kleine Datensignale zwischen Geräten auszutauschen. Ein aktuell sehr bekanntes Beispiel sind dabei sogenannte „Smartwatches“. Diese bieten neben der Möglichkeit die Uhrzeit bereitzustellen viele weitere Funktionen, wie beispielsweise die Steuerung von Telefongesprächen, oder die Fernsteuerung der Musikwiedergabe. Der Nutzer erhält durch ein derartiges Gerät die Möglichkeit, sein Smartphone in gewissen Bereichen fernzusteuern.

Beinahe jeder Mensch in der heutigen Zeit besitzt und nutzt ein Smartphone. Jedes Smartphone ist dabei mit einer Bluetoothschnittstelle ausgestattet. Dieser Sachverhalt liefert die Möglichkeit, nicht nur eine „Smartwatch“ mit dem Smartphone zu verbinden, sondern jegliches Empfangsgerät, welches der Nutzer benötigen könnte. Besonders beliebt sind dabei Fitnessgeräte, die dem Nutzer Informationen über sein Fitnesslevel liefern.

Allerdings liefert der Sachverhalt, dass beinahe jeder Nutzer Bluetooth nutzt auch andere „Usecases“. Mit sogenannten „Beacons“ (siehe Kapitel 4) kann man beispielsweise mit

einem Smartphone Informationen von einem oder mehreren „Beacons“ erfassen und in einer App oder im Browser gesammelt aufbereitet anzeigen. Ein „Beacon“ ist ein BLE Gerät, welches ausschließlich Informationen sendet. So kann man beispielsweise in einem Raum mit mehreren solchen Geräten stehen und Informationen über verschiedene Lebensmittel, oder deren Preise erhalten. Mit dieser Möglichkeit kann ein Nutzer noch besser und zielgerichteter mit sachdienlichen Informationen versorgt werden.

Sollte man die Absicht haben, ein eigenes Gerät zu entwickeln, welches mittels BLE kommuniziert, gibt es mehrere Anbieter für Hardwarekomponenten für verschiedene Anwendungsfälle. Besonders nennenswert sind dabei die Firmen „Nordic“ und „Texas Instruments“.

Die Firma „Nordic“, welche Komponononenten für verschiedenste Kommunikationsprotokolle anbietet, ist Mitglied bei der Bluetooth SIG und hat einen signifikanten Beitrag zum fortschritt von BLE beigetragen. Sie war auch eine der ersten Firmen, die günstige BLE Komponenten auf den Markt gebracht haben [Tow14, Seite 75].

Die Firma „Texas Instruments“ hingegen war als erstes dazu in der Lage, ein BLE fähiges Peripheriegerät auf den Markt zu bringen. Zusätzlich ist „Texas Instruments“ als einiger Anbieter „Feature complete“. Das heißt, dass die Geräte den kompletten Funktionsumfang des BLE Stacks anbieten [Tow14, Seite 79].

2.2 Hardware

2.3 Frequenzbereich

Da BLE ein Teil des Bluetoothstacks ist, sind die physikalischen Eigenschaften, die sowohl hinter Bluetooth Klassik, als auch BLE stecken identisch. Der Frequenzbereich, indem Bluetooth sendet ist dementsprechend auch der selbe. Allerdings gibt es einen Unterschied, was die Kanäle angeht, in denen gesendet wird.

Der Frequenzbereich in dem sich Bluetooth bewegt liegt zwischen 2,4GHz und 2,4835GHz auf dem Industrial, Scientific, and Medical (ISM) Band [Tow14, Seite 16]. Diesen Bereich teilt sich Bluetooth mit einigen anderen Kommunikationsprotokollen, weshalb es zwischen den Protokollen zu Kollisionen bei der Übertragung kommen kann. Aus diesem Grund teilt Bluetooth seinen Bereich in mehrere Kanäle auf. Bei Bluetooth Klassik ist der Frequenzbereich in insgesamt 79 Kanäle unterteilt [Sau18, Seite 410]. BLE teilt den Bereich allerdings nur in 40 Kanäle auf [Tow14, Seite 16]. Daraus resultiert, dass die Kanäle bei BLE doppelt so groß sind wie bei Bluetooth Klassik. Der Grund für diese Kanalunterteilung ist das sogenannte „Frequency Hopping“, welches unter Kapitel 3.1.1 näher betrachtet wird.

3 Funktionsweise Bluetooth Low Energy

beispielsweise Im nachfolgenden Kapitel wird nun auf die Softwareseitigen Aspekte des BLE Stacks eingegangen. Dabei finden die Architektur und die Kommunikation besondere Beachtung. Zusätzlich wird ein Überblick geboten, welche Möglichkeiten diese Technologie dem Nutzer bietet.

3.1 Protokollstack

In Abbildung 1 ist der Protokollstack von BLE zu sehen. Dabei sind die drei Ebenen „Controller“, „Host“ und „Application“ zu erkennen. Auf der untersten Ebene liegt der „Controller“, in welchem das „Physical Layer“ und das „Linked Layer“ enthalten sind. Zwischen „Host und „Controller“ liegt das sogenannte Host Controller Interface (HCI), welches die Schnittstelle zwischen den beiden Kommunikationspartnern darstellt. Im „Host“ wiederum befinden sich sämtliche Protokolle und Profile, die notwendig sind, um Kommunikation zu ermöglichen. An der Spitze des Protokollstacks befindet sich die „Applikation“ in der die Logik und Nutzerschnittstelle des aktuellen Anwendungsfalls liegt [Tow14, 15]. Wie diese einzelnen Komponenten funktionieren und untereinander kommunizieren ist in den nachfolgenden Abschnitten erläutert.

3.1.1 Physical Layer

Das sogenannte „Physical Layer“ bildet die Basis der Kommunikation bei einer Großzahl von Gerätearchitekturen. In dieser Schicht werden digitale Signale, also Bitfolgen, in analoge Signale umgewandelt. Dieser Vorgang wird zum Senden von Nachrichten über eine physikalische Schnittstelle benötigt. Die Rückübersetzung in eine digitale Bitfolge wird ebenfalls im „Physical Layer“ erledigt [Tow14, Seite 16]. Als physikalisches Medium bieten sich dabei eine Vielzahl von Möglichkeiten, wie unter anderem Magnetismus, Strom, oder Licht [Tan14, Seite 95 - 101].

Bei BLE ist die besagte physikalische Schnittstelle die Luft. BLE nutzt in dieser wie in Kapitel 2.3 erläutert einen definierten Frequenzbereich um Nachrichten zu übertragen. Dabei belegt BLE nur einen sehr kleinen Bereich des verfügbaren Spektrums. Insgesamt deckt der verfügbare Frequenzbereich in etwa einen Bereich von 30.000GHz ab. In ihm werden unter anderem Radiowellen, Fernsehübertragungen, Satellitensignale und viele weitere Nachrichtenpakete transportiert [Tan14, Seite 107]. Im Frequenzbereich in dem BLE übertragen wird befinden sich trotz des großen Spektrums einige konkurrierende Technologien, wie beispielsweise „Wireless LAN“ [Tow14, Seite 17]. Aus diesem Grund verwendet Bluetooth im allgemeinen das sogenannte „Frequency Hopping Spread Spectrum“. Dafür wird der verfügbare Frequenzbereich im Fall von BLE in 40 Kanäle aufgeteilt. Von diesen werden die letzten drei Kanäle zum „Advertisment“, also zur Bekanntmachung, verwendet. Über diese gibt sich ein Gerät zu erkennen, welches bereit zum Verbinden ist. Ein suchendes Gerät wiederum überprüft ausschließlich

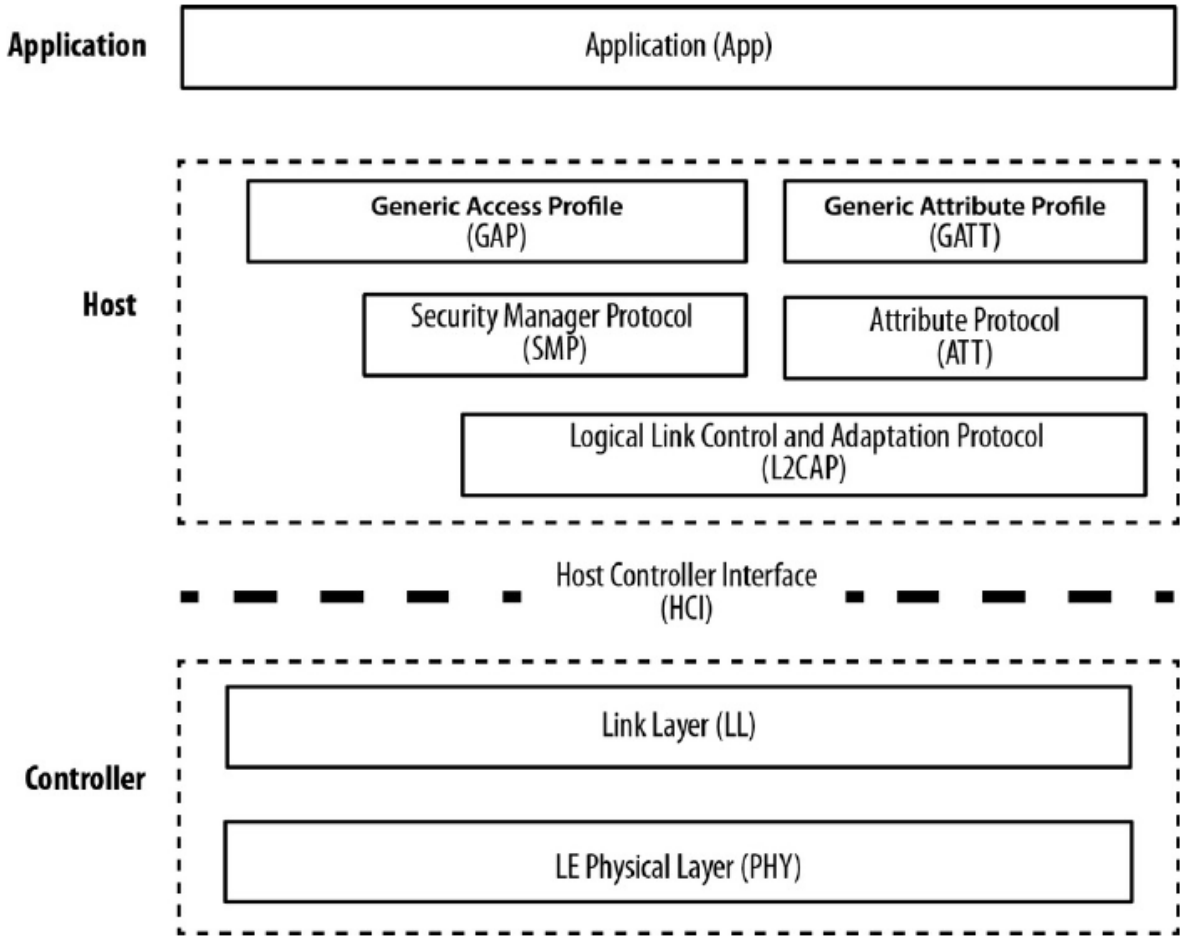

Abbildung 1: BLE Protokollstack [Tow14, Seite 16]

diese drei Kanäle nach verfügbaren Geräten. Die restlichen 37 Kanäle werden anschließend für die Übertragung verwendet. Dabei wird zu Beginn des Datenaustausches eine Sprungfrequenz vereinbart, welche daher für jede neue Verbindung voneinander abweicht. Nachdem die Verbindungsinformationen vereinbart wurden, beginnt der Datenaustausch. In Formel 1 ist zu erkennen, wie die Verbindungspartner gegenseitig abstimmen, in welchen Kanal sie als nächstes wechseln werden. Diese Berechnung führt jedes Gerät unter Berücksichtigung der vereinbarten Verbindungsinformationen selbst aus [Tow14, Seite 17].

$$Kanal = (aktuellerKanal + Sprungfrequenz) \mod 37 \tag{1}$$

Sollte dennoch ein Paket bei der Übertragung verloren gehen, wird dieses nach sofortigem Kanalwechsel erneut übertragen. Sollte es mehrfach zu Problemen mit einem oder mehreren Kanälen kommen führt Bluetooth eine Kanalabschätzung durch. Dabei wird eine „Channel Bitmap“ mit Kanälen erzeugt, welche eine hohe Interferenz aufweisen. Diese werden anschließend für die laufende Verbindung gesperrt. Um festzulegen, ob ein Kanal blockiert ist, gibt es die folgenden drei Möglichkeiten:

1. Received Signal Strength Indication (RSSI)

2. Eine hohe Packetfehlerrate

3. Informationen eines Endgerätes mit Zugriff auf konkurrierende Funktechnologien

Welche dieser Optionen verwendet wird ist allerdings vom Standard nicht vorgeschrieben und kann deshalb selbstständig definiert werden [Sau18, Seite 411].

3.1.2 Linked Layer

Das „Linked Layer“ liegt in der Architektur direkt auf dem „Physical Layer“. Dabei stellt es entweder die zu sendenden Daten bereit, oder verarbeitet die vom “Physical Layer“ empfangenen. Um dies bewerkstelligen zu können, werden Nachrichten nach einem definierten Schema in sogenannte „Frames“ gepackt. Diese enthalten zusätzlich zur eigentlichen Nachricht wichtige Informationen bezüglich des Paketes. Mit diesen kann unter anderem überprüft werden, ob es zu Fehlern bei der Übertragung gekommen ist, indem man eine „CRC Checksumme“ bildet [Tan14, Seite 194].

Das „Linked Layer“ wird bezüglich der zu verarbeitenden Daten für jede Kommunikationsart angepasst. Im Fall von BLE gibt es daher einige Eigenschaften, welche sich von anderen Protokollen unterscheiden. Zum einen gilt es zu beachten, dass die BLE Kommunikation auf einem Nachrichtenaustausch beruht, der sehr schmale Zeitfenster aufweist in denen Nachrichten gesendet werden können. Aus diesem Grund wird das „Linked Layer“ hier weitestgehend von den oberen Protokollschichten getrennt und kommuniziert nur über das HCI mit diesen. Daraus Folgt wiederum, dass das „Linked Layer“ sehr schnell in der Verarbeitung von Daten ist [Tow14, Seite 17f].

Jedes BLE Gerät verfügt über eine eindeutige Adresse. Diese ist Aufgebaut wie eine „MAC Adresse“. Diese Adresse kann das Gerät bei einem „Advertisement“ versuch broadcasten und andere Geräte können sich dann mit dieser Koppeln. Der Verbindungsprozess hat also verschiedene Rollenverteilungen die von der auszuführenden Aktion des Gerätes abhängen. So ist ein Gerät, welches auf einen Verbindungspartner wartet, ein „Advertiser“. Das bedeutet, dass dieses Gerät dauerhaft auf den Advertisementkanälen seine Adresse und andere wichtige Informationen für einen potentiellen Verbindungspartner preisgibt. Der potentielle Verbindungspartner in diesem Fall hat die Rolle des „Scanners“ inne. Das bedeutet, dass er gerne eine Verbindung eingehen würde. Um dies zu tun überprüft er die drei Advertisementkanäle nach „Advertisern“. Diese werden dann beispielsweise dem Nutzer in einer Liste angezeigt. Hier werden nur Geräte angezeigt, welche noch keine aktive Verbindung aufweisen. Das liegt daran, dass die Verbindungspartner bei einer erfolgten Verbindung ihre Rollen ändern. Der „Scanner“ wird zum „Master“ der Verbindung und steuert diese. Der „Advertiser“ wiederum wird zum „Slave“ der Verbindung und folgt den Anweisungen des „Masters“ bezüglich des Timings. In der Regel handelt es sich bei „Slave“ Geräten um einfache Geräte mit niedrigen Funktionalitäten, wohingegen der „Master“ meist ein leistungsstärkeres Gerät darstellt [Tow14, Seite 18f].

Bei BLE tritt gegenüber dem normalen Bluetoothprotokoll die Besonderheit auf, dass es nicht zwangsläufig zu einer Verbindung zwischen „Master“ und „Slave“ kommen muss. Geräte wie „Beacons“ beispielsweise arbeiten nur auf den Advertisementkanälen und senden dauerhaft Informationen an alle BLE Geräte in Reichweite [Gas, Seite 13]. Näheres hierzu findet sich unter Kapitel 4.

Wenn ein Gerät auf der Suche nach einem Verbindungspartner ist, hat es zwei Möglichkeiten. Zum einen kann es einen passiven Scan auf die Advertisementkanäle durchführen, bei dem der „Advertiser“ nicht mitbekommt, dass er erfasst wurde. Zum anderen kann ein aktiver Scan durchgeführt werden, mit dem eine aktive Anfrage an das zur Verfügung stehende Gerät gesendet wird, um weitere Informationen einzuholen und das Gerät über einen potentiellen Verbindungspartner zu informieren. Die Nachricht, welche bei einem aktiven Scan an den „Scanner“ gesendet wird enthält drei zentrale Informationen:

1. Die Möglichkeit einer Verbindung (Ja/Nein)
2. Die Möglichkeit einen aktiven Scan durchführen zu können (Ja/Nein)
3. Die Information, ob der „Advertiser“ ein „Broadcaster“ ist (Ja/Nein)

Sollte der „Advertiser“ ein „Broadcaster“ sein ist es erlaubt, nutzerspezifische Daten in den Nachrichten auszutauschen. In allen anderen Fällen werden hier ausschließlich verbindungsspezifische Daten ausgetauscht [Tow14, Seite 20f].

Für den Fall, dass der „Advertiser“ kein „Broadcaster“ ist, ergibt sich die Möglichkeit eine Verbindung aufzubauen. Um das zu bewerkstelligen sendet der „Scanner“ eine Verbindungsanfrage. Eine Verbindung in BLE steht für eine Abfolge von Verbindungsevents, bei denen Nachrichten ausgetauscht werden. Der „Scanner“ nimmt nun die Rolle des „Masters“ an und legt in der Verbindungsanfrage drei grundlegende Eckpunkte fest. Zum einen die Zeitspanne, die vergeht, bis ein neues Verbindungsevent stattfindet. Je größer diese Zeitspanne ist, desto weniger Energie wird verbraucht. Ein weiterer Punkt ist die Anzahl der Verbindungsevents, welche der „Slave“ überspringen darf, ohne die Verbindung zu beenden. Der letzte Punkt ist die Zeit, die vergehen darf, bis ein Timeout ausgelöst wird [Tow14, Seite 21f].

Im „Linked Layer“ wird die maximale Paketgröße festgelegt. In älteren Versionen von BLE lag die Payloadgröße, welche jedes Nachrichtenpaket maximal beinhalten konnte, bei 27 Byte. In Abbildung 2 ist der Aufbau eines Nachrichtenpaketes dargestellt. Besonders wichtig ist hierbei die Größe der Payload. Bezüglich dieser kann man erkennen, dass sich diese mit Version 4.2 auf 251 Bytes erhöht hat. Das wurde durch die Einführung der „Data Length Extension“ ermöglicht. Dieses Upgrade schafft die Voraussetzungen dafür, Nachrichten in weniger Zeit übertragen zu können, da mehr Informationen in ein Paket passen [Gup].

Sollte ein Paket fehlerhaft übertragen werden, wird dieses mittels der CRC Checksumme entdeckt und dieses Paket wird so lange wiederholt, bis die Checksumme korrekt ist.

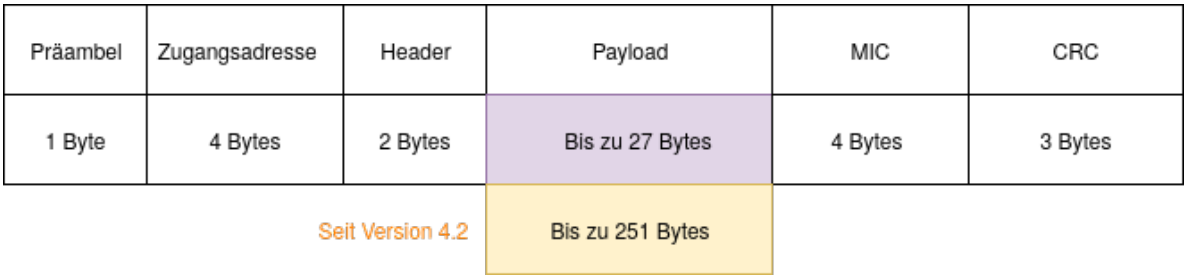

Abbildung 2: Aufbau eines Nachrichtenpaketes bei BLE

Dabei gibt es keine Obergrenze für die Anzahl an Wiederholungen [Tow14, Seite 23].

3.1.3 Profile

3.2 Kommunikation

3.2.1 Advertisement

3.2.2 Verbindung

3.2.3 Datenaustausch

3.3 Featureset (Kosten, Reichweite, Energieverbrauch, etc... am Titel muss ich noch schrauben)

4 Anwendungsbeispiel iBeacon

4.1 Funktionsweise

4.2 Kommunikation

5 Vergleich mit anderen Kommunikationsprotokollen

5.1 ZigBee

6 Fazit

A Erster Abschnitt des Anhangs

In diesem Anhang wird ...

Literatur

[Gas] M. Gast. In *Building Proximity Applications with iBeacon.*

[Gup] S. Gupta und R. Kumar. BLE v4.2: Creating Faster, More Secure, Power-Efficient Designs?Part 1. https://www.electronicdesign.com/communications/ble-v42-creating-faster-more-secure-power-efficient-designs-part-1. Last visit: 8 Dez 2019.

[Sau18] M. Sauter. LTE-Advanced Pro, UMTS, HSPA, GSM, GPRS, Wireless LAN und Bluetooth. In *Grundkurs Mobile Kommunikationssysteme*, Bd. 7, S. 410. Springer Vieweg, Wiesbaden (Deutschland), 2018.

[Tan14] A. Tanenbaum und D. Wetherall. In *Computer Networks*, Bd. 5, S. 95 – 104, 194. Pearson, Harlow (Vereinigtes Koenigreich), 2014.

[Tow14] K. Townsend, C. Cufi, Akiba und R.Davidson. Tools and techniques for lowpower networking. In *Getting Started with Bluetooth Low Energy*, S. 1, 15 – 23, 75, 79. O'Reilly Media Inc., Sebastopol (Vereinigte Staaten von Amerika), 2014.