

Hier steht der Titel der Diplom-/Studien-/Master-/ Bachelorarbeit

Diplomarbeit/Studienarbeit/Masterarbeit/Bachelorarbeit
von

Vorname Nachname

am Institut für Telematik
der Fakultät für Informatik

Erstgutachter:	Prof. Dr. ?. ??????????
Zweitgutachter:	Prof. Dr. ?. ??????????
Betreuender Mitarbeiter:	Dipl.-Inform. ?. ??????????

Bearbeitungszeit: ?? . Monat 20?? – ?? . Monat 20??

Ich erkläre hiermit, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt, die wörtlich oder inhaltlich übernommenen Stellen als solche kenntlich gemacht und die Satzung des KIT zur Sicherung guter wissenschaftlicher Praxis in der jeweils gültigen Fassung beachtet habe.

Karlsruhe, den ?? . ?????? 201?

Inhaltsverzeichnis

1	Einleitung	1
1.1	Zielsetzung der Arbeit	2
1.2	Anforderungen an das Bereichsortungssystem	2
1.3	Klassifizierung von Ortungssystemen	3
1.3.1	Protokoll	3
1.3.2	Topologie	3
1.3.3	Lokalisationsprinzip	3
1.3.4	Messgrößen	4
1.4	Gliederung der Arbeit	6
2	Vorherige Arbeiten	9
2.1	RADAR	9
2.1.1	Verbesserungen an RADAR	10
2.2	WiFi-LLS	10
2.2.1	Kommerzielle Lösungen	11
2.3	RSS-basierte Selbstlokalisierung	11
2.4	LANDMARC	11
2.5	Bluetooth	12
2.6	Time-of-flight Lokalisation	12
2.6.1	Ultraschall	13
2.7	Ortung ohne mobile Einheit	13
3	Hardware & Programmiermöglichkeiten	15
3.1	ESP8266	16
3.2	Texas Instruments SensorTag	16
	Literaturverzeichnis	17

1. Einleitung

Während die Ortung im Außenbereich fest in der Hand von Satellitensystemen wie dem Global Positioning System (GPS) liegen, bietet die Ortung im Innenraum eine Vielzahl verschiedener Technologien. Neben Technologien wie Bluetooth, Radio Frequency Identification (RFID) und Ultra Wide Band (UWB) weckt WLAN wegen seiner großen Verbreitung immer wieder Interesse in Forschung und Industrie.

So hat die Ortung mittels WLAN gerade im medizinischen Bereich durch kommerzielle Lösungen Verbreitung gefunden, Probleme finden sich aber bei Ortungsgenauigkeit gegenüber anderen Techniken und dem vergleichsweise hohen Energieverbrauch des Protokolls. Während viele wissenschaftliche Arbeiten sich der Ortungsgenauigkeit widmen, ist für den alltäglichen Einsatz die Batterielaufzeit der mobilen Einheiten hinderlich, wenn nicht gerade Smartphones als mobile Einheiten in Frage kommen.

Auch im Tunnelbau ist eine Ortung von Mitarbeitern und Besuchern von Nöten um in Notfällen bestimmen zu können, ob und wie viele Personen sich im Gefahrenbereich befinden, dies beeinflusst die Arbeit der Rettungskräfte. Das veränderliche Umfeld der Baustelle, auf der große Stahl- und Betonelemente bewegt werden, stellt dabei die genaue Ortung mittels Radiowellen vor große Probleme und es wird nur Bereichsortung durchgeführt, bei der jede Tunnelröhre in mehrere hundert Meter große Abschnitte aufgeteilt wird und der Wechsel der Mitarbeiter zwischen den Abschnitten beobachtet wird. Dies stellt zwar nur eine geringe Auflösung dar, erlaubt es aber bei Bränden zu erkennen welche Personen sich durch die Abschnitte Richtung Ausgang bewegen und welche in ihrem Abschnitt verharren, sie sind vermutlich entweder bewegungsunfähig oder eingeschlossen.

Die geringe Auflösung hat zudem Vorteile bezüglich des Datenschutzes, da sie verhindert, dass die Arbeiter mit Bewegungsprofilen analysiert werden und zum Beispiel geprüft wird wer sich wie lange im Pausenraum aufhält.

Die Ortung wird derzeit bei einem Referenzunternehmen mittels Bluetooth durchgeführt, dabei sind die Knoten eigenständige Bluetooth-Einheiten, die mit dem Ethernet Backbone verbunden sind, als mobile Einheiten kommen sowohl batteriebetriebene Tags als auch Smartphones zum Einsatz. Das zentrale Sicherheitssystem fragt die gesehenen mobilen Einheiten bei den Knoten an und bereitet die Ergebnisse graphisch auf.

1.1 Zielsetzung der Arbeit

Ziel der Arbeit soll der Entwurf und die Implementierung eines Bereichsortungssystems für Personen in Tunnelanlagen unter Verwendung eines bestehenden Netzwerks von WLAN Access Points (APs) sein. Bei einem Bereichsortungssystem handelt es sich um ein Ortungssystem bei dem die Positionen nicht genau bestimmt werden. Stattdessen wird das Areal auf dem geortet werden soll in einzelne Bereiche unterteilt und jede mobile Einheit beim Vorgang des ortens einem dieser Bereiche zugeordnet. Diese Arbeit grenzt sich von vorherigen Arbeiten dadurch ab, dass die Laufzeit beziehungsweise der Energieverbrauch der mobilen Einheiten im Vordergrund steht. Statt der nur wenige Tage umfassenden Laufzeiten anderer WLAN basierter Tags ist das Ziel dieser Arbeit eine Laufzeit von mehreren Monaten.

Der Entwurfsraum umfasst in einem ersten Schritt keine Änderungen an den Access Points, ihre Anzahl, Position, Software und Hardware ist gegeben.

Anschließend wird diese Beschränkung gelockert und die Software der APs kann verändert werden, bei diesen Veränderungen sollen aber die grundlegenden Mechanismen der 802.11 Spezifikation erhalten bleiben. So soll es nicht assoziierten Clients nicht möglich sein direkt mit Servern im Netzwerk zu kommunizieren, da dies die Sicherheit des gesamten Netzwerks gefährden könnte.

In einer zweiten Lockerung der Beschränkungen soll auch die Hardware veränderbar sein, dies widerspricht zwar der Annahme der bestehenden Struktur von WLAN APs, da diese potenziell ausgetauscht werden müssten, erweitert den Handlungsspielraum jedoch enorm und erlaubt es die vorherigen Implementierungen mit einer energetisch effizienten und potenziell nicht WLAN-basierten zu vergleichen.

Für jeden dieser Schritte müssen die angrenzenden Komponenten, Ortungsserver und mobile Einheiten, implementiert und hinsichtlich des Energieverbrauchs und der Erkennungssicherheit evaluiert werden. Abschließend sollen die drei Systeme miteinander verglichen werden.

1.2 Anforderungen an das Bereichsortungssystem

Da es sich um ein Bereichsortungssystem handeln soll werden keine direkten Anforderungen an die Genauigkeit der Ortung gestellt, jedoch soll ein klarer Wechsel zwischen zwei Bereichen, und damit zwei Access Points, zuverlässig erkannt werden. Bei den von den Zielpersonen getragenen Positionssendern, den sogenannten Tags, soll es in den ersten beiden Schritten um Geräte handeln, die auf WLAN Basis arbeiten und somit mit den Access Points kompatibel sind. Im dritten Schritt ist dies nicht erforderlich und die Kompatibilität wird durch technische Änderungen am AP wiederhergestellt. Die Tags sollen eine Laufzeit von bis zu 3 Jahren erreichen, sie müssen jedoch mindestens eine Laufzeit von 6 Monaten aufweisen um als verwendbar angesehen zu werden. Dabei sind Größe und Gewicht der Lösung zu beachten, zwar kann die Laufzeit eines Tags jederzeit durch die Vergrößerung des Energiespeichers herbeigeführt werden, die Tags müssen jedoch mühelos von den Zielpersonen an einem Band um den Hals getragen werden können. Zuletzt soll unter Rücksichtnahme auf das beschriebene Szenario die Komplexität der IT-Infrastruktur so gering wie möglich gehalten werden um ein stabiles und kostengünstiges System zu garantieren.

1.3 Klassifizierung von Ortungssystemen

Die Klassifikation von Ortungssystemen auf Funkbasis kann neben dem verwendeten Protokoll anhand der Topologie, dem Lokalisationsprinzip und der gemessenen Größen durchgeführt werden [LDBL07]. Außerdem wird zwischen zweidimensionaler und dreidimensionaler Lokalisation unterschieden.

1.3.1 Protokoll

Prinzipiell lassen sich verwendete Frequenzen, Modulationsverfahren und Sendeleistung frei wählen, solange sie die gesetzlichen Vorgaben für die Sender eingehalten werden. Wenn ein eigenes Protokoll verwendet wird kann die Kodierung der Informationen frei gewählt werden, ein Beispiel für ein solches Protokoll ist die Ortung mit Ultra-Breitband Signalen (UWB) mit dem Genauigkeiten im Zentimeterbereich erreicht werden können. Bestehende Protokolle zu verwenden hat dagegen den Vorteil, dass üblicherweise commodity-of-the-shelf Komponenten verwendet werden können, was die Kosten des Systems senkt. Im Gegenzug können für die Genauigkeit wichtige Parameter nicht mehr frei gewählt werden und der overhead des Protokolls muss übernommen werden, Beispiele für solche Protokolle sind 802.11 (WLAN), Bluetooth und Radio Frequency Identification (RFID).

1.3.2 Topologie

Die Topologie hat zwei Dimensionen, Fernlokalisierung versus Selbstlokalisierung und direkt versus indirekt und beschreibt wie Knoten und mobile Einheiten zusammenwirken.

Bei der direkten Fernlokalisierung werden von mobilen Einheiten gesendete Signale an Knotenpunkten gemessen und die Ergebnisse an einen zentralen Ortungsserver weitergegeben, dieser führt dann die Lokalisation durch. Das Ergebnis der Lokalisation ist nur zentral verfügbar.

Bei der direkten Selbstlokalisierung senden hingegen die Knoten und die mobilen Einheiten messen die eingehenden Signale. Anhand der Messergebnisse bestimmt jede mobile Einheit seine Position, die Ergebnisse der Lokalisation sind anschließend nur auf der mobilen Einheit verfügbar.

Die indirekte Fernlokalisierung gleicht der direkten Selbstlokalisierung, allerdings besteht zusätzlich eine Datenverbindung zu einem zentralen Ortungsserver, dem die berechnete Position mitgeteilt wird. Das Ergebnis steht nach kurzer Verzögerung sowohl auf der mobilen Einheit als auch zentral zur Verfügung, optional können dort die Daten von anderen mobilen Einheiten zugegriffen werden um sich über deren Positionen zu informieren.

Auch die indirekte Selbstlokalisierung erweitert die direkte Fernlokalisierung um eine Datenverbindung zwischen mobiler Einheit und zentralem Ortungsserver um sich über die eigene und eventuelle auch andere mobile Einheiten zu informieren. Dies kann insbesondere bei Verwendung von Mischtechnologien notwendig sein, wenn die zur Ortung genutzte Technik es nicht erlaubt an den mobilen Einheiten zu empfangen, aber dennoch eine Selbstlokalisierung durchgeführt werden soll.

1.3.3 Lokalisationsprinzip

Das einfachste Lokalisationsprinzip ist das Umgebungsprinzip, hier wird eine mobile Einheit dem Knoten mit dem stärksten Signal zugeordnet, der Knoten kann sowohl

als Sender als auch als Empfänger auftreten. Die gewonnene Position ist dabei nur symbolisch und ihre Genauigkeit ist abhängig von der Dichte des Netzes. Für eine erfolgreiche Lokalisation muss nur ein Knoten in Reichweite der mobilen Einheit sein, was diese Möglichkeit auch in komplexeren Lokalisationsprinzipien zu einer sinnvollen Ausweichmöglichkeit macht, falls nicht genügend Knoten in Reichweite sind.

Die geometrische Bestimmung der Position einer mobilen Einheit mit drei oder mehr Knoten nennt man Trilateration. Dabei wird üblicherweise für jeden Knoten die Distanz zur mobilen Einheit bestimmt, anschließend wird ein Kreis mit der gemessenen Distanz um jeden Knoten gebildet und der Schnittpunkt der drei Kreise bestimmt die Position der mobilen Einheit. Da die Distanzen aus den gemessenen Signalparametern geschätzt werden müssen sind sie fehlerbehaftet und es ergibt sich oft kein eindeutiger Schnittpunkt, dann wird zum Beispiel die Mitte der Schnittpunkte gewählt.

Die geometrische Bestimmung ist ebenfalls über die Berechnung der Winkel zu den Knoten möglich, dies nennt man Triangulation. Der Winkel kann zum Beispiel über die zeitlich Differenz der ankommenden Signale an den synchronisierten Knoten bestimmt werden, dann wird von jedem Knoten aus eine Halbgerade in diesem Winkel gefällt und der Schnittpunkt bestimmt die Position der mobilen Einheit. Wenn mit gerichteten Antennen gearbeitet wird kann der Winkel des eingehenden Signals direkt bestimmt werden, dann müssen nur 2 Knoten in Reichweite sein um die mobile Einheit zu lokalisieren.

Das aufwendigste Lokalisationsprinzip ist die Szenenanalyse. Hier werden zunächst in einer offline-Phase Vektoren $(m_1, m_2, \dots, m_n, p_x, p_y, p_z)^T$ aus Messgrößen und Positionsmarken gesammelt, anhand dieser Fingerabdrücke werden dann in der online-Phase die Positionen neuer Messergebnisse bestimmt. Üblicherweise kommen dabei Verfahren des maschinellen Lernens wie k-nearest-neighbour, neuronale Netze oder Support Vektor Machines (SVM) zum Einsatz um die Muster der Fingerabdrücke aus der offline-Phase zu erkennen und die Positionen $(p_x, p_y, p_z)^T$ in der online-phase aus den gemessenen Größen $(m_1, m_2, \dots, m_n)^T$ zu schätzen. Im zweidimensionalen Fall wird dabei $p_z = 0$ angenommen.

1.3.4 Messgrößen

Beliebte Messgrößen für die Positionsbestimmung sind Ankunftszeit des Signals (time of arrival, TOA), die Differenz der Ankunftszeiten (time difference of arrival, TDOA), die Paketumlaufzeit (roundtrip time of flight, RTOF) und die Stärke des empfangenen Signals (received signal strength, RSS). Es existieren aber noch mehr messbare Größen, wie etwa die Messung der empfangenen Phase des Signals (received signal phase, RSP) und die Messung des Einfallswinkel des Signals mit mehreren gerichteten Antennen (angle of arrival, AOA).

TOA beruht auf der begrenzten Ausbreitungsgeschwindigkeit des Signals, hochfrequente Signale breiten sich mit Lichtgeschwindigkeit $c = 299.792.458 \text{ m/s}$, Ultraschall mit Schallgeschwindigkeit $c \approx 343 \text{ m/s}$ bei 20°C aus, damit ergibt sich die Distanz $d = c * (t_{\text{empfangen},i} - t_{\text{gesendet}})$ mit i sei der empfangende Knoten. Die Position der mobilen Einheit kann dann mit der Methode der kleinsten Quadrate bestimmt werden, dazu wird die Kostenfunktion $F(x, y, t_{\text{gesendet}}) = \sum_{i=1}^N \alpha_i^2 f_i^2(x, y, t_{\text{gesendet}})$ mit $f_i(x, y, t_{\text{gesendet}}) = c * (t_{\text{empfangen},i} - t_{\text{gesendet}}) - \sqrt{(x_i - x)^2 + (y_i - y)^2}$ und α_i sei die Konfidenz von Knoten i , minimiert. Dies erfordert, dass die Knoten synchroni-

siert sind und die $t_{empfangen,i}$ möglichst ohne vorherige Verarbeitung bestimmt wird um Varianzen zu vermeiden. Zusätzlich ist es von Vorteil, wenn auch die mobile Einheit synchronisiert ist, da dann nur noch mit zwei Variablen optimiert werden muss, da $t_{gesendet}$ dann entsprechend der Synchronisation und dem Sendeintervall als gegeben angenommen werden kann. Die Forderung nach Synchronität ist jedoch für $c = 299.792.458m/s$ sehr stark, da das Signal nur $0.00000000336s/m$ benötigt und somit bereits kleine zeitliche Ungenauigkeiten große Fehler verursachen und erst durch zusätzliche Messungen oder Glättungstechniken hohe Genauigkeiten erreicht werden können. Skibniewski et al. konnten hohe Genauigkeit durch die Verwendung von Ultraschall erzielen, da sich durch die geringere Ausbreitungsgeschwindigkeit Imperfektionen in der Synchronisierung weniger stark auswirken [SkJa09]. Bei einer Selbstlokalisierung ist zu beachten, dass $t_{gesendet}$ den Sendezeitpunkt der Knoten darstellt, sie müssen also entweder alle gleichzeitig auf verschiedenen Frequenzen oder in einem vordefinierten Muster nacheinander senden, die Zeitdifferenz des tatsächlichen Sendezeitpunkts zu $t_{gesendet}$ muss dann vom Empfangszeitpunkt $t_{empfangen,i}$ abgezogen werden.

Bei TDOA wird statt der direkten Ankunftszeiten die Differenz dieser gemessen, dies erfordert üblicherweise Zeitsynchronität bei den Knoten, nicht jedoch bei der mobilen Einheit, da nur die Ankunftszeiten für die Berechnung relevant sind. Die mobile Einheit liegt dabei auf dem Schnittpunkt zweier Hyperboloiden, die jeweils zwischen den Knoten die TDOA gemessen haben und einem Referenzknoten aufgespannt werden. Die Hyperboloiden werden aufgestellt durch

$$R_{i,j} = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} - \sqrt{(x_j - x)^2 + (y_j - y)^2 + (z_j - z)^2}$$

mit (x_i, y_i, z_i) sei der jeweilige Messknoten, (x_j, y_j, z_j) sei der gemeinsame Referenzknoten und (x, y, z) sei die Position der mobilen Einheit. Abb. 1.1 zeigt die Lösung graphisch, Drane et. al. und Torrieri beschreiben die analytische Lösung der Gleichung mit nichtlinearer Regression [DrMS98] beziehungsweise Taylor-Entwicklung [Torr84]. Li et al. eliminiert zusätzlich die Forderung nach Synchronisation für mobile Einheiten, die sowohl senden als auch empfangen können [LPLaY00]. Dabei wird ein Datenpaket an die mobile Station gesendet und von dieser mit einem Acknowledgement beantwortet, diese Kommunikation wird von anderen Knoten beobachtet und die Differenz der Ankunftszeiten des Datenpakets und des Acknowledgements als $t_{i,1}$ mit $i \in Knoten$ protokolliert. Zusätzlich ist $t_{i,0}$ als die Differenz zwischen dem Senden des Datenpakets und dem Empfangen an den anderen Knoten durch die bekannte Position aller Knoten ebenfalls bekannt. Damit kann die Differenz der Ankunftszeit $TDOA_{i,j} = (t_{i,0} + t_{i,1}) - (t_{j,0} + t_{j,1})$ mit $i, j \in Knoten$ ohne vorherige Synchronisation berechnet werden.

Wird RTOF gemessen muss die mobile Einheit sowohl senden als auch empfangen können. Dabei wird die Zeit vom Aussenden eines Paketes bis zur Ankunft der Antwort gemessen, wichtig sind hier zum einen möglichst spät/früh gesetzten Zeitstempel beim senden/empfangen des Signals und eine sehr konstante Verarbeitungszeit des Kommunikationspartners. Zunächst muss dabei die Verarbeitungszeit gemessen werden, indem Knoten und mobile Einheit auf einen Abstand von 0 Metern gebracht werden, anschließend kann die Entfernung $d = c * (t_{empfangen} - t_{gesendet} - t_{Verarbeitung})$ bestimmt werden. Die Position wird dann analog zu TOA bestimmt. Diese Messgröße kann sowohl für die Fern- als auch für die Selbstlokalisierung verwendet werden, ist aber sehr anfällig gegenüber Schwankungen in der Verarbeitungszeit, die bei Protokollen wie 802.11 häufig auftreten.

RSS überprüft wie stark das empfangene Signal aus dem allgemeinen Rauschen auf der verwendeten Frequenz hervor sticht. Dafür ist es wichtig, dass immer mit der selben Leistung gesendet wird, dann kann mit einem theoretisch oder empirisch ermittelten Ausbreitungsmodell die Entfernung zwischen mobiler Einheit und Knoten anhand des Pfadverlustes bestimmt werden. Dann ist $d = F(S_{\text{gesendet}}, S_{\text{empfangen}})$ mit F sei das Ausbreitungsmodell. Um gute Ergebnisse zu erzielen sollten jeweils möglichst gleichförmige mobile Einheiten und Knoten verwendet werden, denn Lui et al. konnte für WLAN zeigen, dass unterschiedliche Hardware bei Knoten und mobiler Einheit erhebliche Varianz in den gemessenen RSS Werten erzeugt [LGLD⁺11]. Zusätzliche Probleme entstehen, wenn Protokolle wie Bluetooth eine Anpassung der Sendeleistung vorsehen [HoSo07], dann muss eine solche Anpassung eliminiert werden, bei Bluetooth geschieht das durch die Verwendung von Inquiry Paketen, diese dienen zur Entdeckung anderer Bluetooth-fähiger Geräte und werden immer mit voller Sendeleistung gesendet um möglichst alle Geräte in Reichweite zu erreichen. Ein weiteres Problem von RSS ist der starke Einfluss von Hindernissen und anderen Signalen auf dem selben Frequenzband. Gerade bei der Ortung in Innenräumen wirken diese Einflüsse begrenzend auf die Genauigkeit und oft muss eine Kalibrierung durchgeführt werden um die Einflüsse von Wänden und anderen Hindernissen zu eliminieren.

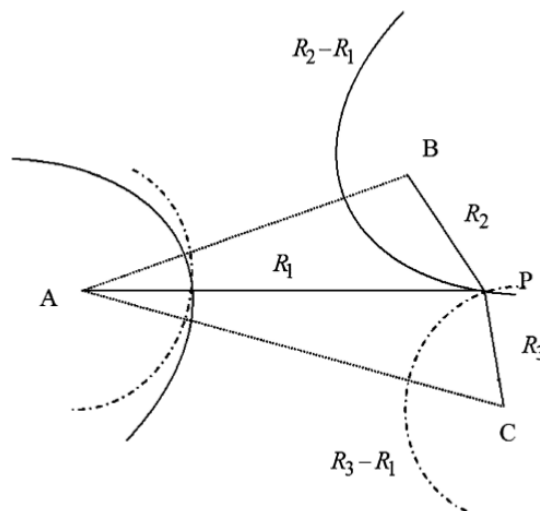


Abbildung 1.1: Positionsbestimmung mit der Differenz der Ankunftszeiten (TDOA), aus [LDBL07].

1.4 Gliederung der Arbeit

Im folgenden Kapitel 2 sollen zunächst einige wissenschaftliche und kommerzielle Lösungen zur Ortung in Innenräumen diskutiert werden. Anschließend wird in Kapitel 3 die Spezifikation 802.11, auch wireless LAN (WLAN) genannt, in einem für diese Arbeit notwendigem Maße erörtert. Dort werden auch die für das Ortungssystem nötigen Teile der Bluetooth 4.0 (Low Energy) Spezifikation erläutert. In Kapitel 4 wird eine Übersicht über die Hardware der Bluetooth und WLAN Tags und deren Programmiermöglichkeiten gegeben. Im Anschluss wird in Kapitel 5 der Entwurfsraum im Rahmen einer theoretischen Betrachtung abgesteckt. Die nachfolgenden Kapitel 6 und 7 widmen sich der Methodik und Ausführung von Experimenten bezüglich

Energieverbrauch und Reichweite der Tags. Die Implementierung der Ortungsserver und die Schnittstellen zu Access Points und Sicherheitssystem werden in Kapitel 8 beschrieben. Zum Schluss folgt ein Fazit, welches die Ergebnisse zusammenfasst und die evaluierten Lösungsansätze abschließend vergleicht.

2. Vorherige Arbeiten

In diesem Kapitel werden vorhandene Lösungen die für die gegebene Aufgabe der Bereichsortung in Tunneln in Frage kommen diskutiert. Es werden hauptsächlich Lösungen auf Basis der 802.11 Spezifikation ausgewählt, dabei aber auch solche Systeme einbezogen, die eine spezifische Position der mobilen Einheit angeben, da diese anschließend trivial einem Bereich zugeordnet werden kann. Es werden sowohl wissenschaftliche als auch kommerzielle Lösungen diskutiert. Auffällig ist bei der Recherche, dass wissenschaftliche Veröffentlichungen sich fast immer auf eines von zwei Aufgabenfeldern beziehen: Entweder soll die Ortungsgenauigkeit erhöht oder die Anforderungen ohne signifikanten Genauigkeitsverlust gesenkt werden. Diese Anforderungen können zum Beispiel Komplexität des Knoten-Netzwerks, des einzelnen Knotens, Synchronisation oder vorherige Kalibrierung sein.

An den Energieverbrauch der mobilen Einheiten werden üblicherweise keine Forderungen gestellt und oft von den Veröffentlichungen komplett ignoriert. Dies ist akzeptabel wenn davon ausgegangen wird, dass die mobile Einheit zusätzlichen Nutzen bietet und das Laden der Einheit in Nutzungsszenario des Anwenders bereits vorgesehen ist. So hat der Anwender in einem Szenario, bei dem sein Smartphone mittels direkter oder indirekter Selbstlokalisierung seine Position bestimmt um ihn zu navigieren nur minimale Anforderungen an den Energieverbrauch. In Szenarien mit direkter oder indirekter Fernlokalisierung hat die mobile Einheit für den Anwender oft keinen direkten Nutzen, deshalb ist eine Forderung nach täglichem oder wöchentlichem laden beziehungsweise wechseln der Batterie schwerer durchzusetzen.

2.1 RADAR

Das RADAR System von Bahl et al. (Microsoft Research) hat als eins der ersten WLAN-basierten Ortungssysteme viel Aufmerksamkeit erfahren [BaPa00]. Als Messgröße wird die Stärke des empfangenen Signals (received signal strength, RSS) genutzt, diese wird laut 802.11 Spezifikation als Index (RSSI) von der Hardware zurückgegeben. Das RADAR System ist auf eine offline-Phase angewiesen in der empirisch ein Signalausbreitungsmodell aufgebaut wird, es handelt sich also um ein

System mit Szenenanalyse. Die Verwendung einer offline-Phase ist im stark veränderlichen Baustellenumfeld nicht akzeptabel. Zum einen führt der ständige Baufortschritt dazu, dass regelmäßig neu kalibriert werden muss und zum anderen wirken sich auch die großen Baumaschinen auf die Signalausbreitung aus. Damit sich dies nicht im Modell wiederfindet müssten zunächst alle beweglichen Maschinen aus dem Bereich entfernt werden um anschließend in der online-Phase ihren Einfluss glätten zu können. Die offline-Phase ist deshalb wirtschaftlich gesehen nicht durchführbar und das empirisch ermittelte Signalausbreitungsmodell müsste durch ein theoretisches ersetzt werden, für eine grobkörnige Bereichsortung sollte dies jedoch ausreichend sein. Bei RADAR sendet die mobile Einheit 4 UDP-Pakete pro Sekunde aus, an den Knoten wird dann der RSSI gemessen, die Autoren weisen jedoch darauf hin, dass sich dieser Vorgang leicht umkehren ließe um von einer Fernlokalisierung auf eine Selbstlokalisierung zu kommen. Bezüglich des Energieverbrauchs äußern sie sich jedoch zu keiner der beiden Varianten. Die Position wird anschließend bestimmt indem aus den in der offline-Phase aufgenommenen Werten derjenige mit dem geringsten Abstand zu den gemessenen Werten gewählt wird, dies wird im *nearest neighbour in signal space (NNSS)* Algorithmus beschrieben. Für die Ortung wird mehrfach gemessen und dann gemittelt um im Median eine Genauigkeit von unter 3 Metern zu erhalten, das kurze Sendeintervall von 0,25 Sekunden führt auch bei bewegten Personen zu einer Genauigkeit von 3,5 Metern. Gleichzeitig führt das kurze Sendeintervall aber auch zu einem hohen Energieverbrauch auf Seiten der mobilen Einheit, eine Reduktion der Sendevorgänge sollte im Kontext der Bereichsortung angestrebt werden um den Energieverbrauch zu senken und die Batterielaufzeit der mobilen Einheit zu steigern.

2.1.1 Verbesserungen an RADAR

Bahl et al. veröffentlichten anschließend noch einige Verbesserungen für das ursprüngliche RADAR System [BaPB00]. Diese umfassen unter anderem den Einsatz von Access Points statt PCs als Knoten zu verwenden, verbesserte Ortung bewegter Personen und die Erkennung von hinzugekommenen Hindernissen wie etwa Personen. Letzteres geschieht durch die Analyse der Signalstärke von Beacon Frames anderer APs, da diese sich nicht bewegen können Veränderungen in der Signalstärke als Veränderungen auf dem Signalweg gesehen werden. Dies ließe sich auch auf größere Hindernisse übertragen, hängt aber stark von der strategischen Platzierung und möglichst dichten Verteilung der APs ab. Auch hier äußern sich die Autoren nicht zum Energieverbrauch, wohl auch deshalb weil sie einen Laptop als mobile Einheit verwenden.

2.2 WiFi-LLS

Chen et al. kritisieren den Einsatz von spezialisierten Access Points, deren Software muss verändert werden, da der RSSI nur am AP gemessen werden kann und somit vom AP für den Ortungsserver zugänglich gemacht werden muss. Sie wechseln daher auf eine indirekte Fernlokalisierung, bei der sie die Signalstärke von Paketen naher APs messen, in ein Paket packen und an den Ortungsserver senden. Dadurch lösen sie auch das Adressierungsproblem: RADAR stellt ursprünglich keinen Adressierungsmechanismus für mehrere mobile Einheiten zur Verfügung, vor dem Versenden des Pakets mit den Signalstärken kann nun leicht ein Identifikator wie etwa die

MAC-Adresse hinzugefügt werden.

Außerdem verwenden für ihr WiFi-based Local Location System (WiFi-LLS) ein theoretisches Signalausbreitungsmodell $P(d) = P(d_0) - 10 \log_{10}(\frac{d}{d_0})^n - OAF$ mit der Distanz d , der Signalstärke $P(d)$ und der Referenzdistanz $d_0 = 1m$. $P(d_0)$, der Pfadverlustexponent n und der Hindernisdämpfungsfaktor OAF müssen bestimmt werden, jedoch lassen sich $P(d_0)$ und n auf einer einzelnen Teststrecke mit unterschiedlichen Abständen von AP und mobiler Einheit bestimmen und OAF kann für einen Gebäudetyp bestimmt werden. Dadurch hat das Modell einen konstanten Aufwand, dies ist für Baustellen interessant, da sich diese Werte einmalig messen und dann sogar über mehrere gleichartige Baustellen übertragen ließen.

Auch in dieser Veröffentlichung steht die Ortungsgenauigkeit im Vordergrund und es werden keine Angaben zum Energieverbrauch gemacht. Als Referenz kann dienen, dass die mobile Einheit bei WiFi-LLS alle 5 Sekunden einen Scan (siehe Kapitel 3.x) durchführt, die Signalstärken der 3 signalstärksten APs zusammen mit der eigenen MAC-Adresse in XML codiert und das so erzeugte Paket an den Ortungsserver versendet.

2.2.1 Kommerzielle Lösungen

Hier sollen zum Beispiel Ekahau und AeroScout vorgestellt werden, muss dazu noch gesicherte Infos besorgen.

2.3 RSS-basierte Selbstlokalisierung

Prasithsangaree et al. stellen ein WiFi-LLS ähnliches System vor [PrKC02], welches aber auf eine offline-Phase zum sammeln von Fingerabdrücken für Positionen in einem Abstand von 1,5 beziehungsweise 3 Metern setzt. Dies ist natürlich im Sinne der Aufgabenstellung nicht sinnvoll, da für eine Tunnelbreite von 10m 4000 beziehungsweise 2000 Messungen pro Kilometer vorgenommen werden müssten.

Die Arbeit zeigt aber die Volatilität der empfangenen Signalstärke auf, dies wurde 2011 von Lui et al. genauer untersucht [LGLD⁺11]. Lui et al. zeigen, dass die gemessene empfangene Signalstärke stark von der beteiligten Hardware abhängt und die Systeme für jedes mal neu kalibriert werden müssen wenn sie auf ein neues AP-Modell portiert werden und auf dem Areal optimalerweise nur ein AP-Modell verwendet werden sollte.

Abb. 2.1 zeigt die gemessenen RSSI Werte für die von ihnen getesteten Netzwerkkarten mit unterschiedlichen Distanzen, für einige Karten korreliert die empfangene Signalstärke nur sehr schwach mit der Distanz zwischen Knoten und mobiler Einheit. Sie zeigen außerdem, dass einige AP-Modelle den RSSI speichern und nur bei größeren Veränderungen aktualisieren und dass die Antenne signifikanten Einfluss auf den protokollierten Wert hat, aber im Allgemeinen die Varianz der protokollierten Werte sehr hoch ist.

2.4 LANDMARC

Ni et al. stellen ein Ortungssystem auf Basis von Radio Frequency Identification (RFID) vor [NLLP04]. Dazu werden aktive RFID-Tags als mobile Einheiten eingesetzt, diese sind mit einer Batterie ausgestattet und senden regelmäßig ihre gespeicherte ID aus.

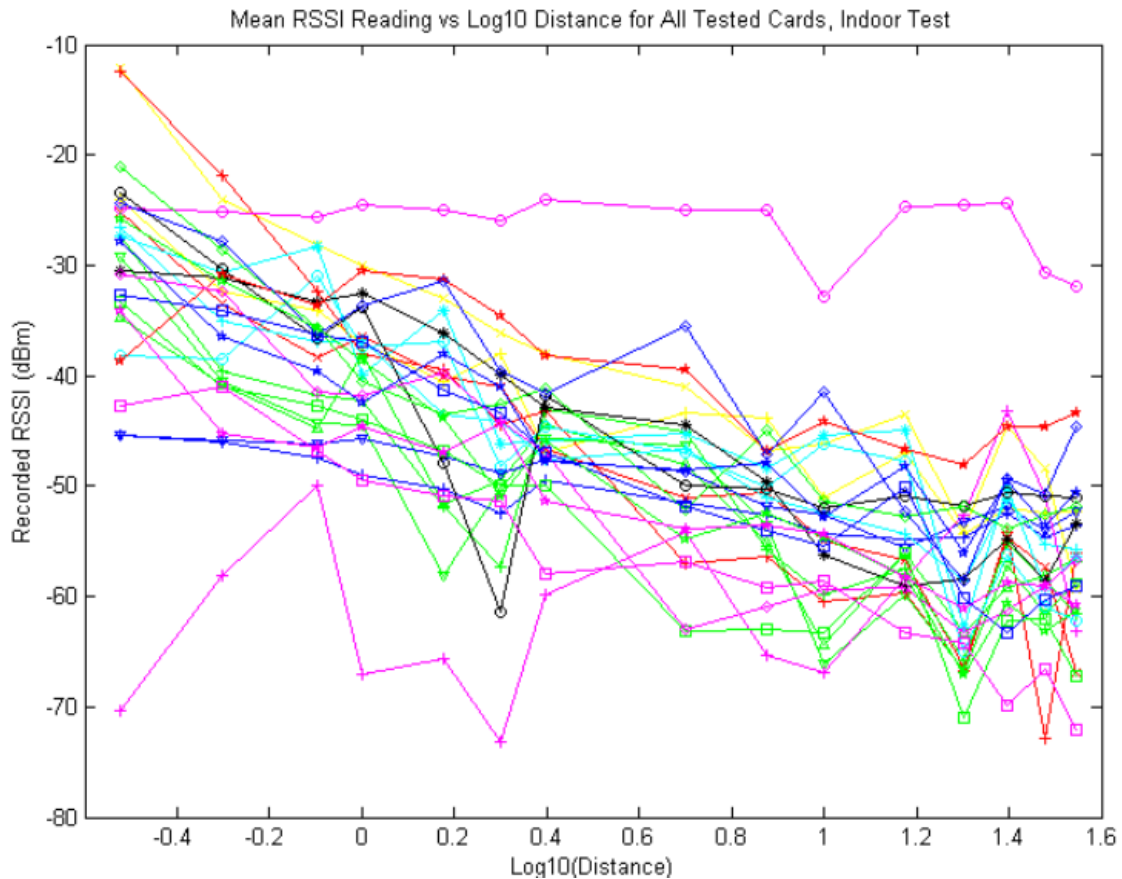


Abbildung 2.1: Gemessener RSSI mit verschiedenen Access Points und Distanzen, aus [LGLD⁺11].

Der Knoten ist mit einem Lesegerät (RFID-Reader) ausgestattet und empfängt die ID, der Knoten liefert dann die ID und ein Signalstärkelevel zwischen 1 und 8 zurück. Da das Signalstärkelevel nur eine sehr grobe Auflösung hat verbessern Ni et al. die Genauigkeit durch das Ausbringen von zusätzlichen Tags an bekannten, fixen Positionen, für die Bereichsortung ist dies aber nicht notwendig.

Die Autoren geben für ein Sendeintervall von 7,5 Sekunden eine Batterielaufzeit von 3-5 Jahren an, dabei sind die Tags klein genug und könnten, wie in der Einleitung gefordert, an einem Band um den Hals getragen werden.

2.5 Bluetooth

Hier habe ich noch kein Paper, es kommt aber fix noch mindestens ein System auf Bluetooth-Basis + Kritik an verschiedenen Bluetooth Parametern.

2.6 Time-of-flight Lokalisation

Aufgrund der Schwächen von RSS-basierten Systemen wurde auch über solche nachgedacht, die stattdessen oder zusätzlich die time-of-flight (TOF) messen, ein Beispiel für ein solches zeigen Wibowo et al. [WiKP09]. Sie fordern optimalerweise Zugriff auf die physische Schicht (PHY) des 802.11 Protokolls, da auf diesen aber üblicherweise kein Zugriff besteht messen sie TOF in der darüber liegenden MAC-Schicht.

Ein Knoten sendet einen Beacon Frame aus und protokollieren die Sendezeit, die mobile Einheit empfängt den Beacon Frame, protokolliert die Empfangszeit und die Sendezeit der gesendeten Antwort, der Knoten sichert die Empfangszeit der Antwort. Nun sendet die mobile Einheit die zwei gespeicherten Zeitstempel an den Knoten, der mit diesen die Verarbeitungszeit auf der mobilen Einheit berechnen kann um dann die Distanz $d = c * (\frac{t_{\text{empfangen}} - t_{\text{gesendet}} - t_{\text{Verarbeitung}}}{2})$ zur mobilen Einheit zu bestimmen. Dieses Schema lässt sich leicht von einer Fernlokalisierung in eine Selbstlokalisierung umwandeln indem man den Initiator des Vorgangs tauscht.

Die Notwendigkeit die Zeitstempel bereits in der PHY- beziehungsweise MAC-Schicht zu setzen erfordert Zugriff auf die Software des als Knoten verwendeten Access Points. Außerdem müssen die Zeitstempel im Bereich von Nanosekunden gesetzt werden und die Verarbeitungszeit vor/nach dem setzen muss sehr konstant sein, da eine Abweichung von $100ns$ bei $c = 299.792.458m/s$ bereits einen Fehler von $30m$ verursacht.

Muthukrishnan et al. beschreiben diese Problematik bei dem Versuch TOF ohne Zugriff auf die Software des APs umzusetzen [MKML06]. Sie kommen zu dem Ergebnis, dass sich die in der Spezifikation eingebauten Zeitstempelfunktionen wie das Network Time Protocol (NTP), Ping und die Zeitstempel in Beacon Frames nicht eignen, da sie zum einen nur eine Auflösung im Millisekundenbereich bieten und zum anderen von der Blockierungskontrolle von 802.11 (CSMA/CA) abhängen.

2.6.1 Ultraschall

Skibiniewski et al. nutzen Ultraschall für eine Fernlokalisierung mit TOF [SkJa09]. Ultraschall kann nicht von WLAN APs empfangen werden und es muss zusätzliche Hardware installiert werden, das System soll hier dennoch Beachtung finden, da es für die Ortung von Baumaterial auf Baustellen entwickelt wurde.

Bei diesem System sendet zunächst der Knoten einen Beacon Frame der ZigBee Spezifikation (802.15.4) an die mobile Einheit, diese antwortet und sendet unmittelbar danach das Ultraschallsignal. Das schnelle 2.4GHz ZigBee Signal dient dem Knoten dann als Referenz für den Sendezeitpunkt des Ultraschallsignals, welches wegen seiner langsamen Ausbreitungsgeschwindigkeit $c \approx 343m/s$ wesentlich weniger anfällig für ungenaue Zeitstempel ist. Außerdem kann die Zeit zwischen dem Aussenden des Beacon Frames und der Antwort gemessen werden um zusätzliche TOF-Informationen zu gewinnen.

Statt ZigBee ließe sich auch WLAN nutzen, ZigBee ist jedoch bereits auf niedrigen Energieverbrauch ausgelegt und wegen des Ultraschalls wäre trotzdem ein extra Knoten nötig. Problematisch an der Lösung ist entweder der Energieverbrauch der Ultraschalleinheit oder die Reichweite, ausreichend kleine Einheiten reichen keine 100m weit und leiden trotzdem unter kurzer Batterielaufzeit. Die Autoren schließen deshalb, dass noch Innovation in diesem Bereich notwendig ist um dieses System praktikabel zu machen.

2.7 Ortung ohne mobile Einheit

Eine Ortung ohne mobile Einheit erfüllt wegen ihrer Abwesenheit offensichtlich jede Anforderung an die Batterielaufzeit der mobilen Einheit. Mit MonoPHY stellen Abdel-Nasser et al. ein System zur Ortung ohne mobile Einheit vor [ANSSY13].

Dazu verwenden sie einen 802.11n-fähigen Laptop und Access Point und analysieren

die Channel State Information (CSI) der physischen Schicht (PHY) der zwischen AP und Laptop übertragenen Daten. Um die bestehende Struktur von APs zu nutzen sollte das System angepasst und die CSI zwischen den APs gemessen werden. Das System hat jedoch einige Aspekte, die es ungeeignet für die Aufgabenstellung machen.

Das System unterscheidet nicht zwischen Personen, sondern erkennt nur, dass jemand anwesend ist, außerdem ist es nur für eine Person in einem $100m^2$ gestaltet worden und müsste auf Baustellengröße und die Verfolgung mehrerer dutzend Personen erweitert werden. Aber auch dann ist fraglich, wie gesichert werden kann, dass alle Personen durchgehend erkannt werden können, zum Beispiel wenn sich mehrere Personen auf oder in einem Transportfahrzeug aufhalten. Auch ist es ohne Identifikation schwerer Fehler zu erkennen, wird fälschlicherweise angezeigt, dass sich noch eine Person im Tunnel befindet kann oft durch ausrufen des Betreffenden festgestellt werden, dass dieser nicht im Tunnel ist. Hat man dagegen nur die Information, dass sich noch eine Person im Tunnel befindet müsste jede Gruppe durchgezählt werden und selbst dann bestünde die Möglichkeit, dass eine Person ohne das Wissen anderer in den Tunnel gegangen ist und diesen nicht mehr verlassen hat.

Weitere Probleme entstehen durch die Baumaschinen und Container, diese haben einen starken Einfluss auf die CSI und verdecken dadurch möglicherweise nahe Personen und die Fahrzeugführer. Deshalb müssten diese Objekte ebenfalls als Entitäten angezeigt werden, die Anzeige diverser Kommandostände, Pausenräume und stehen gelassener Baumaschinen verwirrt im Notfall jedoch, da sich in jedem Objekt potentiell eine Person befinden könnte.

Die Veröffentlichung beruht außerdem auf der Verfügbarkeit der CSI, diese sind dort durch die Auswahl einer bestimmten Netzwerkkarte gegeben und sind nicht zwingend in einer bestehenden Struktur von APs verfügbar. Als letzter Kritikpunkt steht die Verwendung einer offline-Phase, die, wie bereits diskutiert, wirtschaftlich nicht umsetzbar ist.

Somit erfüllt die Ortung ohne mobile Einheit zwar die Anforderungen an den Energieverbrauch, jedoch nicht die Forderung nach sicherer Erkennung von Abschnittswechseln, deshalb scheidet diese Technik zumindestens für Baustellen aus.

3. Hardware & Programmiermöglichkeiten

In diesem Kapitel soll die für die mobilen Einheiten verwendete Hardware und ihre Programmiermöglichkeiten näher beleuchtet werden. Als mobile Einheiten werden in dieser Arbeit hauptsächlich Tags behandelt: Tags sind kleine Geräte, die ausschließlich zur Ortung und damit einhergehender Identifikation genutzt werden.

Diese Arbeit behandelt jedoch ebenfalls die Ortung mittels Smartphones mit dem Android Betriebssystem von Google [Goog17], um diese in das System einzugliedern und bei Personen, die ein Firmenhandy besitzen die Notwendigkeit eines zusätzlichen Tags zu eliminieren.

Ein Smartphone kann auch ohne Software für die Ortung nicht die geforderten 6 Monate Batterielaufzeit erfüllen, derartige Anforderungen werden deshalb fallen gelassen. Stattdessen muss ein Smartphone mindestens eine 12-stündige Schicht ohne Ladevorgang auskommen, da sonst ein Bereichswechsel nicht mehr erkannt werden kann. Lösungen mit geringem Energieverbrauch werden dennoch bevorzugt.

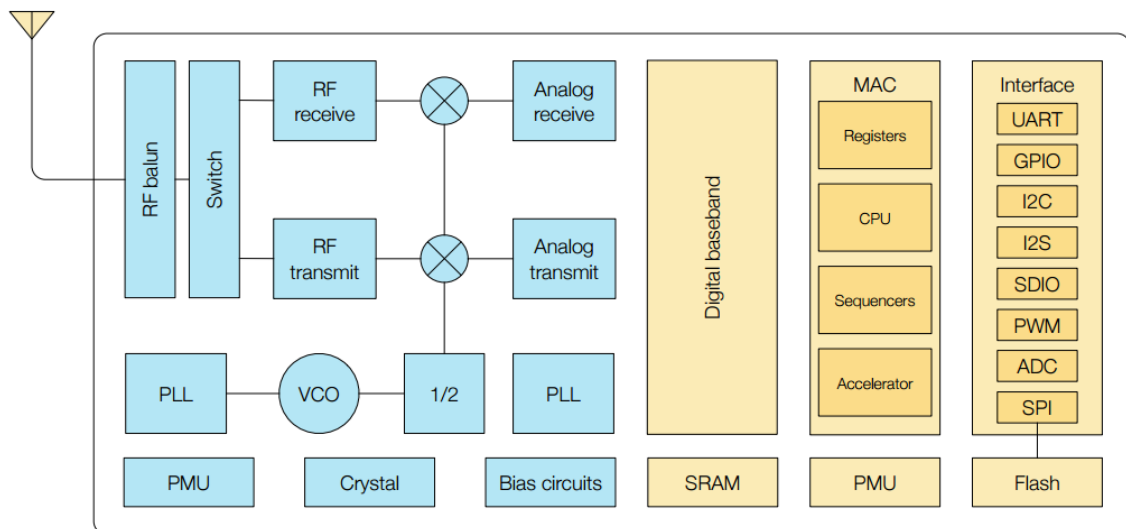


Abbildung 3.1: Blockdiagramm des ESP8266, aus [Team17]

3.1 ESP8266

Für WLAN-basierte Tags kommt der ESP8266 von Espressif in den Modulen ESP12-S beziehungsweise ESP12-F zum Einsatz. Der ESP8266 zeichnet sich durch einen niedrigen Energieverbrauch und viele Freiheiten bei der Programmierung aus, die Module ESP12-S und ESP 12-F unterscheiden sich dabei hauptsächlich durch ihre Antenne, siehe Abb. 3.2. Das neuere ESP12-F sollte eine höhere Reichweite entfalten, dies wird noch Gegenstand eines Experiments sein.

Der Esp8266 besitzt neben einer CPU eine 802.11b/g/n/e/i-fähige WLAN-Einheit und diverse andere, kabelgebundene Kommunikationsstandards wie zum Beispiel GPIO, I2C und SPI, siehe Abb. 3.1. Der Chip selbst besitzt weder einen Flashspeicher für Programme und Daten noch eine Antenne, diese werden auf dem Modul, z.B. ESP-12F, integriert [Team17]. Espressif gibt im Datenblatt auch Aufschluss über den Energieverbrauch des Chips, siehe dazu Abb. 3.3.

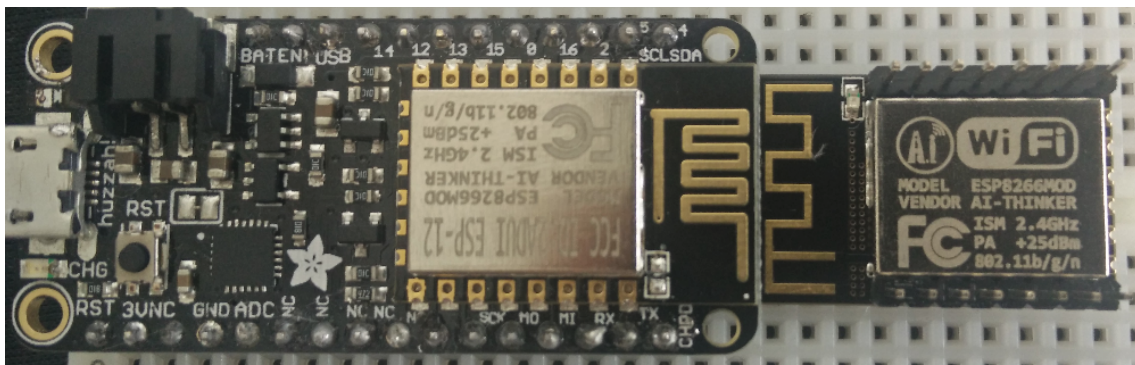


Abbildung 3.2: Vergleich der Antennen, links: ESP12-S verbaut auf einem Adafruit Feather Huzzah, rechts: ESP12-F

Parameters	Min	Typical	Max	Unit
Tx802.11b, CCK 11Mbps, P OUT=+17dBm	-	170	-	mA
Tx 802.11g, OFDM 54Mbps, P OUT =+15dBm	-	140	-	mA
Tx 802.11n, MCS7, P OUT =+13dBm	-	120	-	mA
Rx 802.11b, 1024 bytes packet length , -80dBm	-	50	-	mA
Rx 802.11g, 1024 bytes packet length, -70dBm	-	56	-	mA
Rx 802.11n, 1024 bytes packet length, -65dBm	-	56	-	mA
Modem-sleep ^①	-	15	-	mA
Light-sleep ^②	-	0.9	-	mA
Deep-sleep ^③	-	20	-	μA
Power Off	-	0.5	-	μA

Abbildung 3.3: Energieverbrauch des ESP8266 bei verschiedenen Operationen, aus [Team17]

3.2 Texas Instruments SensorTag

Für das Bluetooth-basierte Tag wird das SensorTag von Texas Instruments verwendet.

Literaturverzeichnis

- [ANSSY13] H. Abdel-Nasser, R. Samir, I. Sabek und M. Youssef. MonoPHY: Mono-stream-based device-free WLAN localization via physical layer information. In *Wireless communications and networking conference (WCNC), 2013 IEEE*. IEEE, 2013, S. 4546–4551.
- [BaPa00] P. Bahl und V. N. Padmanabhan. RADAR: An in-building RF-based user location and tracking system. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, Band 2. Ieee, 2000, S. 775–784.
- [BaPB00] P. Bahl, V. N. Padmanabhan und A. Balachandran. Enhancements to the RADAR user location and tracking system. *Microsoft Research* 2(MSR-TR-2000-12), 2000, S. 775–784.
- [ChLu07] Y. Chen und R. Luo. Design and implementation of a wifi-based local locating system. In *Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on*. IEEE, 2007, S. 1–5.
- [DrMS98] C. Drane, M. Macnaughtan und C. Scott. Positioning GSM telephones. *IEEE Communications Magazine* 36(4), 1998, S. 46–54.
- [Freu15] J. Freudiger. How talkative is your mobile device?: an experimental study of Wi-Fi probe requests. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2015, S. 8.
- [Goog17] Google. Offizielle Website des Android-Projekts. https://www.android.com/intl/de_de/phones/, 2017.
- [HoSo07] A. M. Hossain und W.-S. Soh. A comprehensive study of bluetooth signal parameters for localization. In *Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007. IEEE 18th International Symposium on*. IEEE, 2007, S. 1–5.
- [LDBL07] H. Liu, H. Darabi, P. Banerjee und J. Liu. Survey of wireless indoor positioning techniques and systems. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 37(6), 2007, S. 1067–1080.
- [LGLD⁺11] G. Lui, T. Gallagher, B. Li, A. G. Dempster und C. Rizos. Differences in RSSI readings made by different Wi-Fi chipsets: A limitation of WLAN localization. In *Localization and GNSS (ICL-GNSS), 2011 International Conference on*. IEEE, 2011, S. 53–57.

- [LPLaY00] X. Li, K. Pahlavan, M. Latva-aho und M. Ylianttila. Comparison of indoor geolocation methods in DSSS and OFDM wireless LAN systems. In *Vehicular Technology Conference, 2000. IEEE-VTS Fall VTC 2000. 52nd*, Band 6. IEEE, 2000, S. 3015–3020.
- [MiSA03] A. Mishra, M. Shin und W. Arbaugh. An empirical analysis of the IEEE 802.11 MAC layer handoff process. *ACM SIGCOMM Computer Communication Review* 33(2), 2003, S. 93–102.
- [MKML06] K. Muthukrishnan, G. Koprnikov, N. Meratnia und M. Lijding. Using time-of-flight for WLAN localization: feasibility study. 2006.
- [NLLP04] L. M. Ni, Y. Liu, Y. C. Lau und A. P. Patil. LANDMARC: indoor location sensing using active RFID. *Wireless networks* 10(6), 2004, S. 701–710.
- [PrKC02] P. Prasithsangaree, P. Krishnamurthy und P. Chrysanthis. On indoor position location with wireless LANs. In *Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on*, Band 2. IEEE, 2002, S. 720–724.
- [SkJa09] M. J. Skibniewski und W.-S. Jang. Simulation of Accuracy Performance for Wireless Sensor-Based Construction Asset Tracking. *Computer-Aided Civil and Infrastructure Engineering* 24(5), 2009, S. 335–345.
- [Team17] E. S. I. Team. ESP8266EX Datasheet. http://espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf, 2017.
- [Torr84] D. J. Torrieri. Statistical theory of passive location systems. *IEEE transactions on Aerospace and Electronic Systems* (2), 1984, S. 183–198.
- [WiKP09] S. B. Wibowo, M. Klepal und D. Pesch. Time of flight ranging using off-the-self ieee802. 11 wifi tags. In *Proceedings of the International Conference on Positioning and Context-Awareness (PoCA'09)*, 2009.