

Bau eines Wardriving-Moduls

Christian Stahl
Nico Feld

17. Oktober 2018
Ausarbeitung
Hardwarenahe Systemprogrammierung
Prof. Dr. Sturm

1 Motivation und Idee

Diese Arbeit beschäftigt sich mit dem Erstellen eines Wardriving-Moduls. "Wardriving" bezeichnet dabei das systematische Erfassen von WLAN-Netzen an verschiedenen Positionen und deren Auswertung. Anschließend können dann die erfassten WLAN-Netze der Position zugeordnet werden und letztendlich kartographiert werden. Dafür wird ein extra Modul mit Positionsbestimmung (GPS) und eine WLAN-Komponente benötigt. Als Motivation kann einerseits das Finden von unsicheren Netzwerken und die anschließende Meldung an den Besitzer oder auch einfach die Kartographie von offenen WLAN-Netzen für Touristen o.Ä. stehen. Im Rahmen der Vorlesung "Hardware-nahe Programmierung" haben wir ein solches Modul gebaut und programmiert. Dabei haben wir das Modul um die Funktion Bluetooth-Geräte zu erfassen erweitert, die Erweiterung um die GSM-Abdeckung ist leider nicht geglückt.

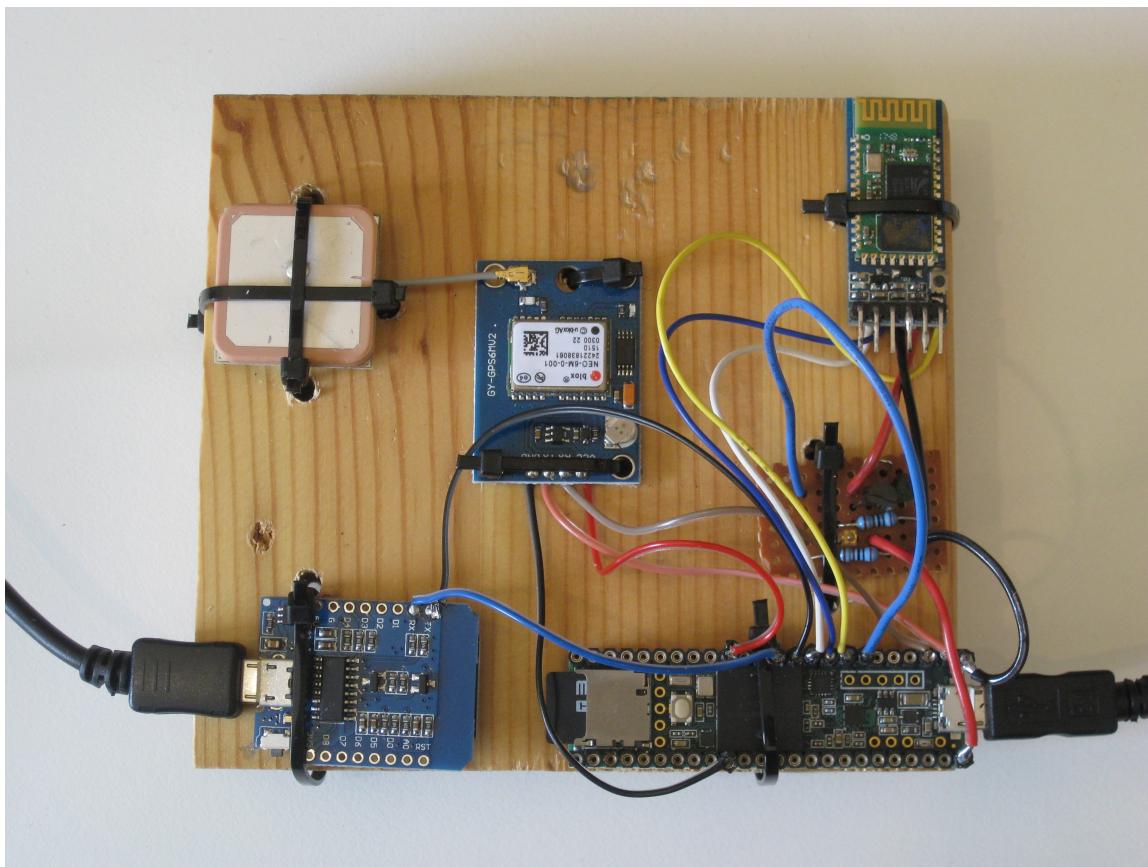


Abbildung 1: Aufbau unseres Wardriving-Moduls

2 Aufbau und Probleme

Zur Erfassung der GPS-Daten, der WLANs, der Bluetooth-Geräte, sowie der GSM-Abdeckung haben wir die verschiedenen Module sternförmig um einen Teensy 3.6 angeordnet, welcher die zentrale Koordination und Datenspeicherung übernimmt. Die verschiedenen Module werden per UART verbunden, die Spannungsversorgung liefert eine Powerbank per USB, teils wird sie über den Teensy weitergereicht. Dazu verwenden wir, wie in Abbildung 1 zu sehen, rote und schwarze Drähte, um sie von den Leitungen für logische Pegel zu unterscheiden.

Bei Start unseres Moduls initialisiert der Teensy die angeschlossenen Module. Anschließend wird in einer Schleife stets zunächst die GPS-Information abgefragt. Um Endlosschleifen zu vermeiden

wurden alle Module um eine Abbruchbedingung (kill-count) erweitert, sodass kein Modul den Gesamtablauf blockieren kann. Sollte nach der gegebenen Anzahl von Versuchen keine verwertbare Information erfasst worden sein, so bricht die Erfassung des einzelnen Moduls ab. Wird kein GPS-Punkt gefunden, so haben wir die anderen Module nicht abgefragt, sondern eine Wartezeit von 20 Sekunden eingebaut, um zu verhindern, dass die Module heiß laufen, was bei ersten Implementierungen zu Problemen führte.

2.1 Teensy 3.6

Als programmierbares “Herzstück“ des Moduls haben wir uns für den Teensy 3.6 entschieden, da er sowohl ausreichend Speicher besitzt um die ankommenden Daten zu verarbeiten, als auch über einen eingebauten SD-Karten Slot verfügt, wodurch wir die erfassten Daten auf eine SD-Karte schreiben können. Des Weiteren konnte er sehr einfach mittels der “PlatformIO“-Erweiterung des Editors “Atom“ programmiert und gestartet werden. Die hohe Anzahl der Pins, genauer der UART-Pins, erlaubte uns außerdem die viele anderen Module ohne Schwierigkeiten anzuschließen.

2.2 GPS-Modul

Für das GPS-Modul verwenden wir einen Ublox NEO 6M Chip. Das GPS-Modul stellt die wichtigste Komponente des Wardriving-Moduls dar, denn ohne die Positionsbestimmung kann keine Zuordnung der restlichen Daten erfolgen. Somit gibt dieses Modul auch den “Takt“ für die restlichen Module an: Erst wenn die Positionsbestimmung erfolgreich war, werden die Informationen der anderen Module (WLAN und Bluetooth) ausgewertet. Diese Positionsbestimmung erfolgt vom Modul jede Sekunden und wird per UART an den Teensy übertragen.

Die Informationen werden vom Modul im NMEA 0183-Standard¹ übermittelt. Dieser Standard beschreibt die Kodierung der erfassten Daten in ASCII-basierte Datensätze. Dabei werden vom Gerät mehrere dieser Datensätze pro Sekunde erfasst. In dieser Arbeit werden lediglich die beiden Datensätze *Recommended Minimum Sentence C (RMC)* und *Global Positioning System Fix Data (GGA)* ausgewertet. Jeder dieser Datensätze beginnt immer mit einem Identifier. In diesem Fall wären das die Identifier “\$GPRMC,“ und “\$GPGGA,“. Anschließend folgen die Informationen des Datensatzes separiert mit Kommata. Eine mögliche Kodierung eines RMC-Datensatzes wäre also:

```
$GPRMC,162614,A,5230.5900,N,01322.3900,E,10.0,90.0,131006,1.2,E,A*13
```

Aus diesen beiden Datensätzen werden in dieser Arbeit die Informationen *Status*, *Uhrzeit*, *Breitengrad*, *Längengrad*, *Anzahl der Satelliten* und *Höhe* ausgelesen. Falls der Status nicht “A“ beträgt, ist dies ein Zeichen dafür, dass die Positionsbestimmung nicht erfolgreich verlief. Falls dies der Fall ist wiederholt das GPS-Modul nach 20 Sekunden Pause die eine Positionsbestimmung bis letztendlich eine erfolgreiche Bestimmung erfolgte. Bei einer erfolgreichen Positionsbestimmung werden die restlichen Informationen in die “gps.csv“ auf der SD-Karte geschrieben. Anschließend werden die Informationen der anderen Module abgefragt, welche anhand der Uhrzeit nun eindeutig der bestimmten Position zugeordnet werden können.

2.3 WLAN-Modul

Für das WLAN-Modul verwenden wir ein WEMOS D1 MINI. Dieses Modul benötigt eine eigene Firmware, welche in unserem Fall lediglich jede Sekunde alle WLAN-Netze in der Umgebung

¹https://de.wikipedia.org/wiki/NMEA_0183

erkennt, anschließend jedes Netzwerk nach BSSID, Name (SSID), Typ der Verschlüsselung, Channel, Sichtbarkeit und RSSI (Verbindungsstärke) scannt und schließlich diese Daten per UART an den Teensy überträgt. Da die Abfrage im Teensy nach diesen Daten (`wifi->available()`) jederzeit eintreten kann, also auch während des Schreibprozesses des WLAN-Moduls, ist es wichtig nur die Daten auszuwerten wenn sie vollständig sind und erst zu beenden, wenn alle Daten übertragen wurden. Um dies zu gewährleisten fängt jede Zeile, die vom WLAN-Modul übertragen werden mit “42,” an und das Ende der Übertragung wird mit der Zeile “end“ gekennzeichnet. Eine mögliche Ausgabe des Moduls wäre somit:

```
42,54:67:51:42: CF:E0,KabelBox-6700,WPA2/PSK,1,0,-90  
42,46:67:51:42: CF:E0,Vodafone Hotspot,open,11,0,-94  
42,A0:E4:CB:C4:86:B1,irie,WPA2/PSK,6,0,-92  
42,D0:6F:82:C7:CF:35,WLAN-QNN5B4,WPA2/PSK,0,0,-91  
end
```

Diese wird wie folgt vom Teensy interpretiert: Beginnt eine Zeile weder mit “42,” noch mit “end“ wird diese Zeile verworfen, da es sich um Reste einer vorherigen Übertragung handelt. Andernfalls können durch die aktuelle Uhrzeit des GPS-Moduls die so übermittelten Daten der Position eindeutig zugeordnet werden. Um jedoch redundante Informationen, wie Name oder Typ der Verschlüsselung nicht jedes mal zu speichern, wenn ein Netzwerk entdeckt wird, werden zwei CSV-Dateien erzeugt. Wird ein Netzwerk mit bisher unbekannter BSSID erkannt so werden lediglich die Informationen *BSSID*, *Name*, *Verschlüsselung*, *Channel* und *Sichtbarkeit* in die “networks.csv“ geschrieben. Handelt es sich jedoch um ein bereits bekanntes Netzwerk so werden die Informationen *Uhrzeit*, *BSSID*, *RSSI* in die “wifi.csv“ geschrieben. So sind alle benötigten Informationen stets über die BSSID eindeutig zuordenbar ohne Informationen unnötig oft zu speichern.

2.4 Bluetooth-Modul HC-05

Zur Erfassung der verfügbaren Bluetooth-Geräte verwenden wir ein HC-05-Modul. Dieses verfügt über zwei Betriebsmodi. Der AT-Modus dient der Konfiguration des Moduls und ist aktiv, wenn der Enable-Pin des Moduls auf 3.3V (high) liegt und anschließend die Spannungsversorgung zugeschaltet wird. In diesem Modus blinkt die LED auf dem Bauteil langsam, etwa im Halbsekundentakt. Der zweite Betriebsmodus, der Inquire-Mode, ist aktiv wenn das Modul mit Betriebsspannung versorgt wird und am Enable-Pin logisch 0 (low) anliegt und wird durch schnelles Blinken der LED angezeigt.

Die besondere Schwierigkeit bei der Implementierung der Bluetooth-Geräteerfassung mithilfe des Moduls lag darin, dass das Modul, unseres Wissens nach aufgrund eines Firmware-Fehlers, nicht wie dokumentiert arbeitet. Der von uns benötigte Inquire-Modus soll laut Dokumentation mit dem Befehlscode „AT+INQ“ gestartet werden und soll mit „AT+INQC“ gestoppt werden können. Beide Befehle erzeugten bei unseren Tests lediglich Fehlermeldungen, wobei der von „AT+INQ“ geworfene Fehlercode „1F“ nicht dokumentiert ist.

Da wir den Inquire-Mode bereits beim Start des Moduls aktivieren können, das Modul jedoch dann durchgehend Daten an den Teensy sendet, haben wir ein Workaround entwickelt, um die beiden nicht-funktionsfähigen Befehle zu umgehen.

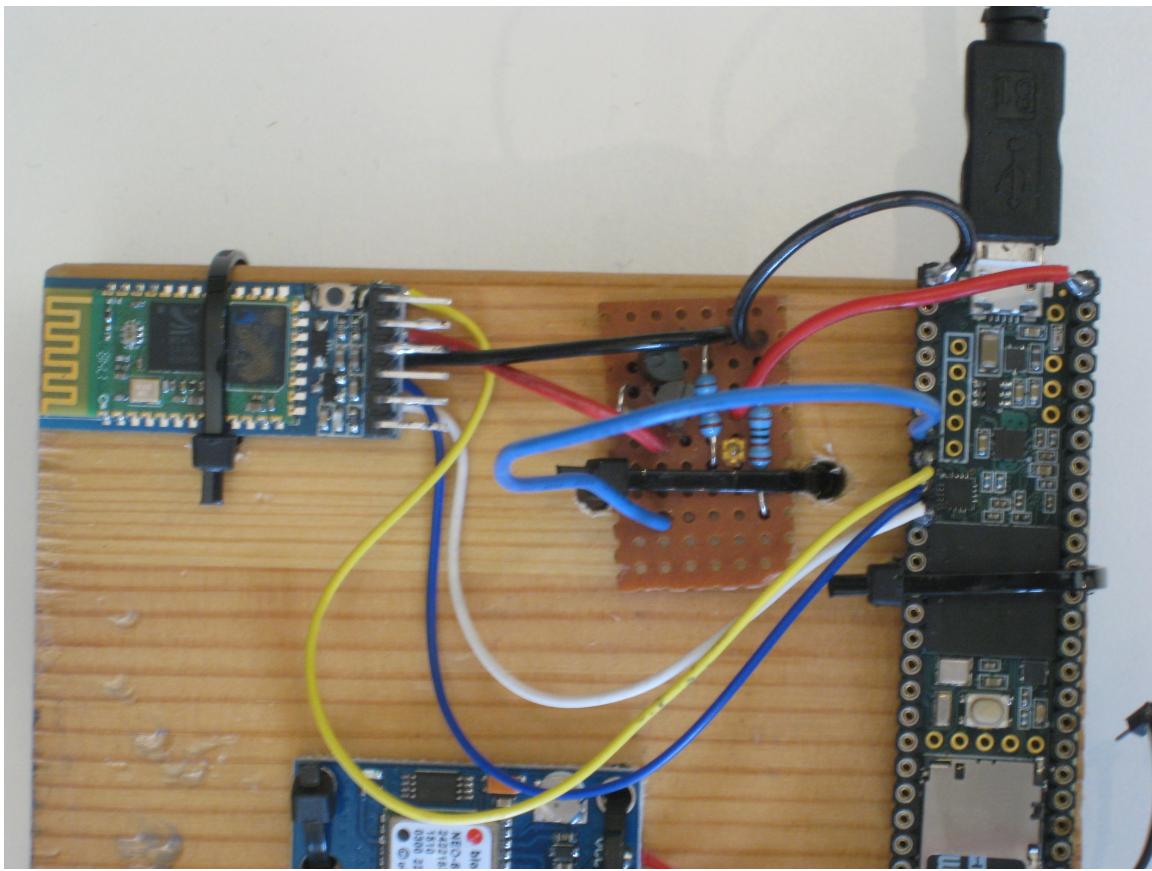


Abbildung 2: Bluetooth-Modul und Schaltung zur Spannungsversorgung

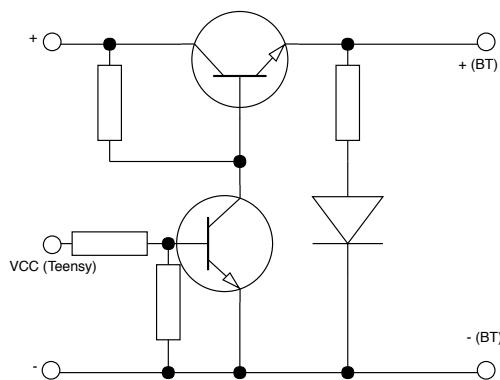


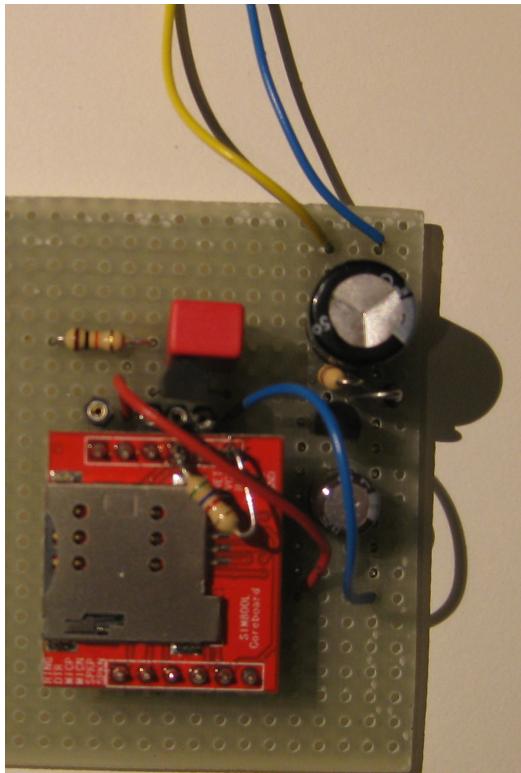
Abbildung 3: Schaltung zur Steuerung der Spannungsversorgung

Zunächst wird das Modul im AT-Modus konfiguriert und anschließend abgeschaltet, indem es von der Stromversorgung getrennt wird. Diese Trennung führen wir durch einen logischen Pegel (Im Foto hellblau, in Abbildung 3 links mittig) herbei, indem wir die nebenstehende Schaltung zwischen die Spannungsquelle (dem 5V-Pin, sowie einen Gnd-Pin des Teensy) und den VCC- und Gnd-Pins des Moduls eingebaut haben. Zu Debug-Zwecken ist auf der Platine eine LED (zwischen den beiden Widerständen) verbaut, die leuchtet, solange das Modul mit Strom versorgt ist. Aufgrund der Hardwarelatenzen benötigen wir zum An- und Abschalten des Moduls jeweils circa 1,5 Sekunden, was die Zeit zur Erfassung aller Daten an einem GPS-Punkt deutlich verlängert. Um mit der Datenerfassung zu beginnen, aktivieren wir das Modul im Inquire-Mode und lesen die ankommenden Daten ein. Nach 10 Sekunden schalten wir das Modul wieder ab und lesen die restlichen Daten, welche eventuell noch im Puffer des Teensy liegen, ein. Wir erhalten einen String, den wir an den Zeilenbrüchen trennen, um die einzelnen Datentupel zu isolieren. Anschließend filtern wir mithilfe regulärer Ausdrücke die validen Tupel, um sie weiter zu verarbeiten. Dabei gehen wir ab diesem Punkt analog zum WLAN vor.

Durch die Latenzen und die relativ lange Erfassungszeit dauert eine Abfrage der Bluetooth-Geräte

etwa 14,5 Sekunden und nimmt somit einen Großteil der gesamten Erfassungszeit ein. Diesen Kompromiss sind wir eingegangen, um die Erfassung der Bluetooth-Daten zu ermöglichen.

2.5 GSM-Modul SIM800L



Das SIM800L-Modul hat uns größere Schwierigkeiten bereitet, als alle anderen Module. Bis zuletzt war es uns nicht möglich es einzubinden. Eine Schwierigkeit bestand darin, dass verschiedene Bibliotheken für das Modul existieren, welche sich bereits bei der Initialisierung unterscheiden. Auch gibt es widersprüchliche Aussagen darüber, ob die verwendete Simkarte pingeschützt sein darf oder nicht.

Das größte Problem jedoch ist, dass das Modul, unabhängig von der verwendeten Bibliothek auf keine Eingaben reagiert. Es soll, wie alle anderen Module, per UART auf AT-Befehle reagieren, erzeugte bei unseren Tests jedoch nie eine Antwort. Für verschiedene Szenarien haben wir Schaltungen eingebaut und getestet. Ohne anliegende Spannung am Reset-Pin, mit Reset beim Start auf high und anschließend low, und konstant high oder low war es uns nicht möglich vom Modul eine Antwort zu erhalten. Somit mussten wir schließlich die Einbindung des GSM-Moudls aufgeben.

Abbildung 4: Platine mit GSM-Modul SIM800L

3 Kartographie

Um die Daten nun grafisch auszuwerten wurde das Geoinformationssystem “QGIS“ verwendet. Dieses erlaubt es die erstellten CSV-Dateien zu laden und als geographische Punkte darzustellen. Dazu ist es lediglich notwendig die Spalten “Longitude“ und “Latitude“ der gps.csv auszuwählen und als X- und Y-Koordinaten der Punkte zu kennzeichnen. Die anderen Datensätze können nun mit bekannten Datenbankbefehlen, wie z.B. JOIN verknüpft und ausgewertet werden. Folgende Abbildung zeigt dabei eine Heatmap über die Anzahl von WLAN-Netzen in Tarforst.

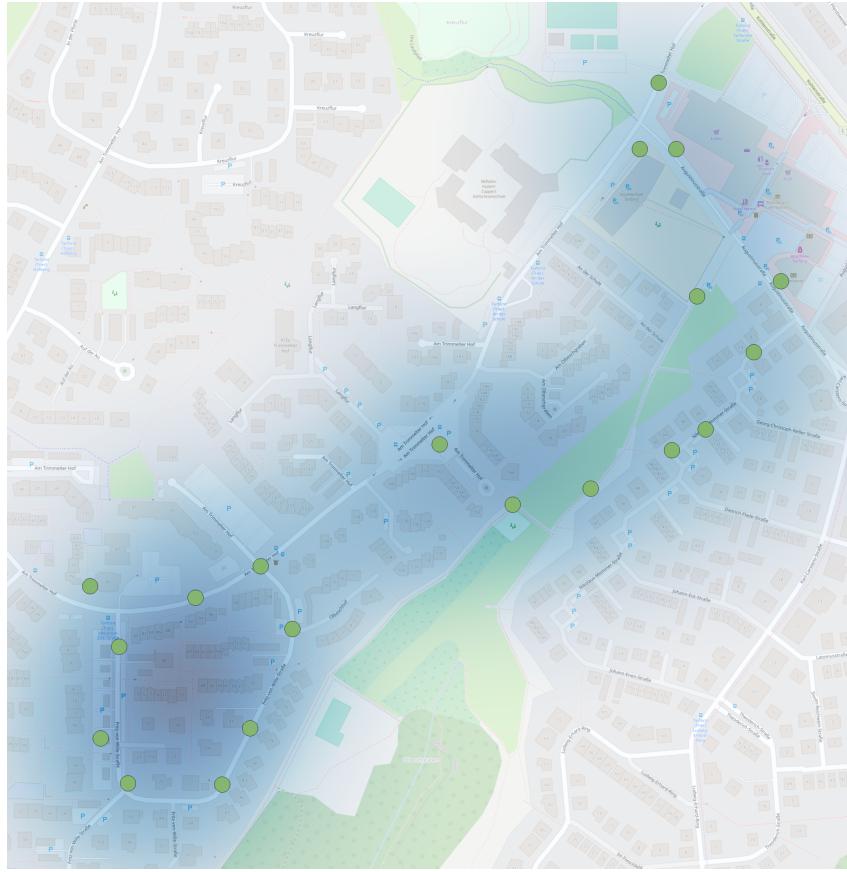


Abbildung 5: Heatmap von erfassten WLAN-Netzwerken

4 Fazit

Die Entwicklung des Wardriving-Moduls hat deutlich gemacht, dass die Hauptschwierigkeit bei der Entwicklung eines Projekts mit vielen einzelnen Komponenten darin liegt, sich mit deren genauen Funktionsweise auseinanderzusetzen und die Module letztendlich harmonisch miteinander kommunizieren zu lassen. Die Schwierigkeiten mit dem Bluetooth-Modul zeigten, dass eine richtige, vollständige Dokumentation nicht immer gegeben ist und man häufig auf eigene Workarounds und Tests angewiesen ist um die gewünschte Funktionalität zu gewährleisten.

So wurde auch durch das GSM-Modul deutlich, dass es bereits beim Anschließen der Komponenten zu nicht nachvollziehbaren Fehlern kommen kann, welche bis zum Schluss nicht gelöst werden konnten. Da es sich aber bei diesem Modul um ein “proof of concept“-Projekt handelt, waren die einzelnen Module im unteren Preisspektrum angeordnet. Hochwertigere und teurere Module könnten einige dieser Probleme nicht aufweisen und eine komplettere, gepflegtere Dokumentation besitzen, was die Arbeit damit erheblich vereinfachen würde. Die besondere Herausforderung durch die Schwierigkeiten waren eine interessante Komponente des Projekts und haben gezeigt, wie gegebene Umstände, in unserem Fall die (fehlerhaften) Komponenten, oder auch bestehende Infrastrukturen die Entwicklung eines Projekts beeinflussen und den Arbeitsaufwand verschieben können.

Letztendlich lässt sich jedoch zusammenfassen, dass die Entwicklung eines Wardriving-Moduls definitiv möglich ist. Auch Erweiterungen wie die Erkennung von Bluetooth-Geräten sind im Prinzip problemlos umsetzbar.

Den Quellcode des Projektes findet man unter:

<https://github.com/Cataract92/LookyLooky/tree/test>