

Ein autonomes System zur Erfassung von WLAN-Probe-Requests

Miriam Alina Scholz, *Robert Baumgartl*, Dirk Müller

HTW Dresden

Fakultät Informatik/Mathematik

robert.baumgartl@informatik.htw-dresden.de

21. November 2019

Ausgangspunkt: WiFi-Probe-Requests

- ▶ Smartphones, Tablets, usw. strahlen periodisch so genannte *WiFi Probe Requests* aus (Zweck: Suche und aktive Verbindung mit bekannten Netzen)

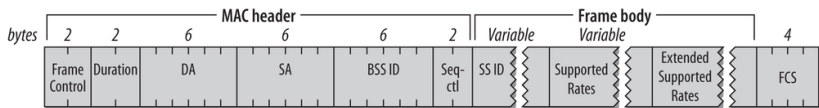


Abbildung: Format eines Probe Requests

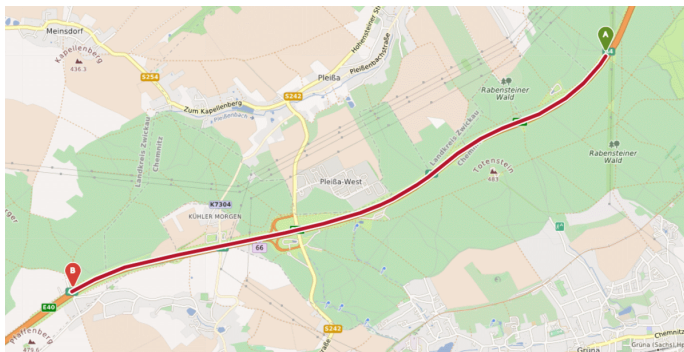
- ▶ *Probe Requests* können von jedem WiFi-Empfänger (im Monitor Mode) empfangen und aufgezeichnet werden

Ausschnitt einer Aufzeichnung an der BAB A4

<i>Zeitpunkt</i>	<i>S.-Stärke</i>	<i>MAC-Adresse</i>	<i>SSID-Feld</i>
⋮	⋮	⋮	⋮
16:40:17.496722	-83dBm	80:c5:e6:fe:d5:b4	dlink
16:40:18.072398	-44dBm	04:02:1f:dd:e3:c9	VodafoneWiFi
16:40:27.428133	-92dBm	00:6e:07:88:d5:79	FRITZ!Box 7362 SL
16:40:33.224335	-36dBm	04:02:1f:dd:e3:c9	Balveda
16:41:31.061595	-92dBm	00:27:10:93:78:fc	o2-WLAN99
16:41:36.921195	-98dBm	00:22:58:7b:3a:7a	FRITZ!Box 6320 Cable
16:41:42.004917	-72dBm	6c:8f:b5:04:7c:e4	Hotel Crystal 1.OG Z11
16:41:42.006160	-71dBm	6c:8f:b5:04:7c:e4	HUAWEI-E5220-4093
16:41:42.007367	-69dBm	6c:8f:b5:04:7c:e4	FritzBoxConrad
16:41:43.025213	-89dBm	34:af:2c:62:5f:eb	WLAN1-800797
16:43:05.041507	-87dBm	80:00:0b:02:39:e7	FRITZ!Box 6490 Cable E
⋮	⋮	⋮	⋮

Prinzipielle Funktionsweise (Fuxjäger, 2016)

- ▶ Idee: an zwei Positionen (z. B. an der Autobahn) bekannter Entfernung WLAN-Probe-Requests mit Zeitstempel aufzeichnen
- ▶ für übereinstimmende MAC-Adressen: $v = \frac{S}{\Delta t}$



Verbesserungen (Baumgartl, 2018)

1. Messeinrichtung: Notebook (+ externe Antenne) → Raspberry Pi 3
2. Messposition: zentral (Brücke) → seitlich (Fahrbahnrand)

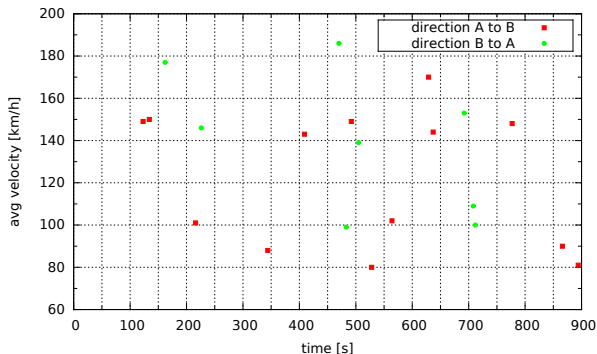
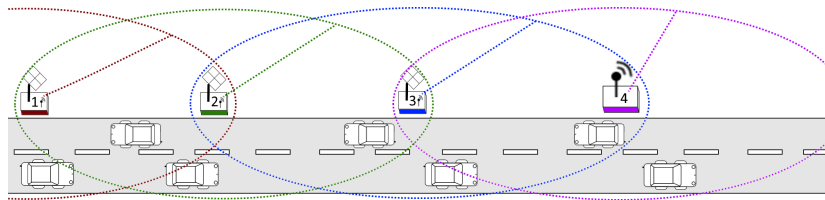


Abbildung: Ermittelte Geschwindigkeiten (Messintervall 15min)

Anwendung: Stauererkennung, Beobachtung von Verkehrsströmen



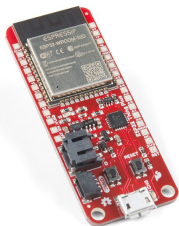
- ▶ autonome Arbeitsweise der Stationen notwendig → Energieversorgung?

Auswahl der Rechnerplattform

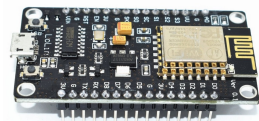
Kandidaten



Raspberry Pi Zero



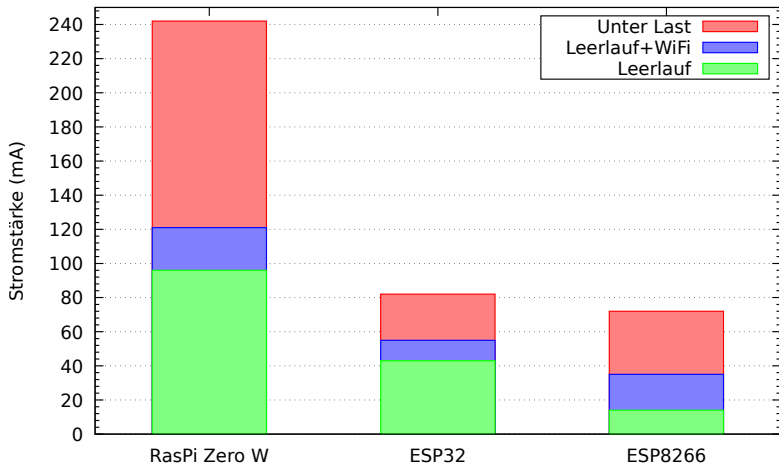
ESP32



ESP8266

Auswahl der Rechnerplattform

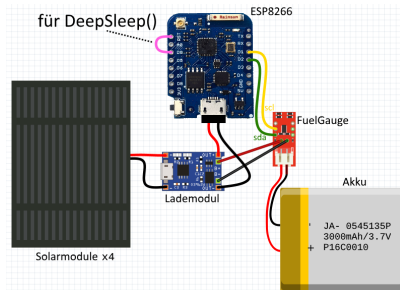
Vergleich des Energiebedarfs



Versuchsanordnung

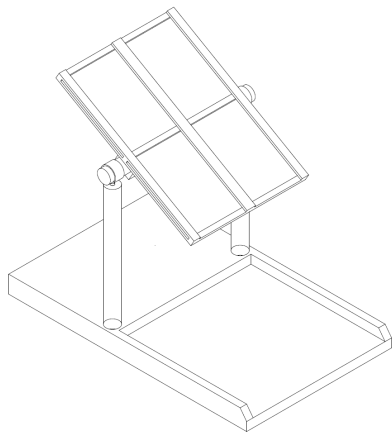
Erforderliche Komponenten

- ▶ ESP8266-Modul (Wemos D1 mini Pro)
- ▶ 4 Solarpanels 116x160mm, á 2.5W
- ▶ Laderegler TP4056
- ▶ LiPo-Akku 3000 mAh // 3,7 V 11 W
- ▶ Ladezustandsüberwachung (SparkFun LiPo Fuel Gauge mit MAX17043)
- ▶ (Spannungskonverter)



Schaltung der Komponenten

Praktischer Aufbau

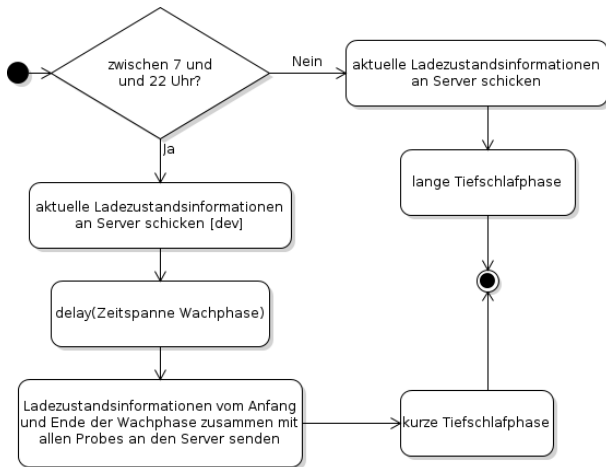


Entwurf des Gehäuses



Prototyp in Betrieb

Arbeitsregime der Sensorplattform



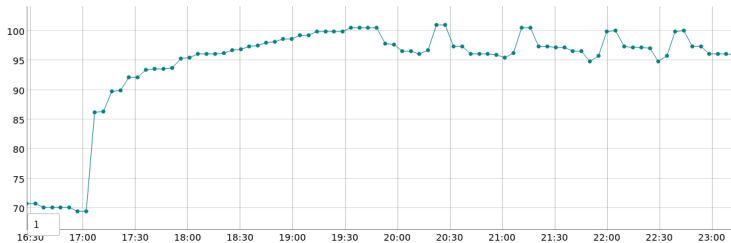
Prinzipieller Ablauf

Arbeitsregime des Gesamtsystems

- ▶ Sensorplattform arbeitet tagsüber zyklisch: 5 Minuten Aufzeichnung, 5 Minuten *Deep Sleep*
- ▶ empfangene Probe-Requests werden am Ende jedes Zyklus per HTTP-POST-REQUEST an einen Server übertragen
- ▶ dort in Datenbank abgelegt
- ▶ Auswertung erfolgt offline (PHP-Programm)

Ergebnisse

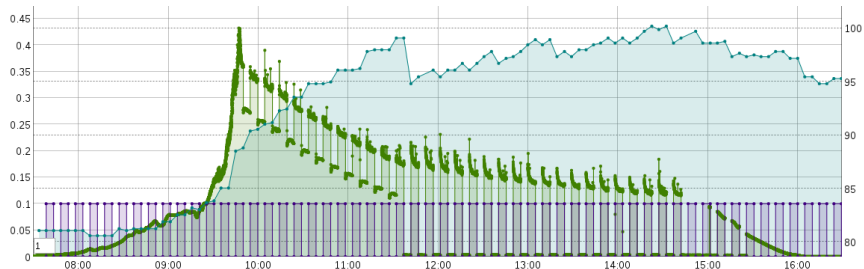
State of Charge:



Verlauf des Ladezustands des Akkus (blau, [%]) beim Ladevorgang

- ▶ keine PV angeschlossen; Ladevorgang startet 17.00 Uhr
- ▶ kontinuierlicher Betrieb des Moduls
- ▶ Nachweis Funktionsfähigkeit Laderegler

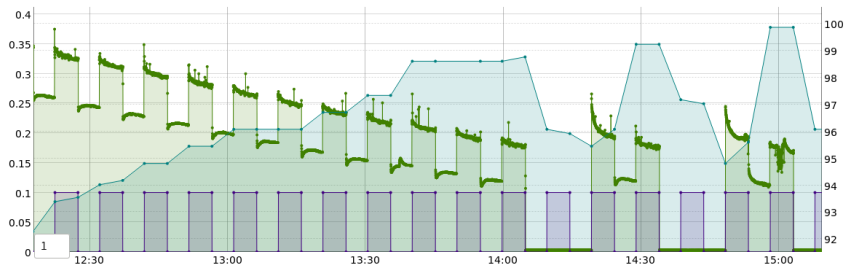
Ergebnisse



Ladestrom der Solarmodule (grün, [A]) vs. Ladezustand des Akkus (blau, [%]) und Aktivphasen des Systems (violett)

- ▶ Strommessung mit zwischengeschaltetem Digitalmultimeter
- ▶ Regler reduziert Ladestrom bei Erreichen eines hohen Ladestandes

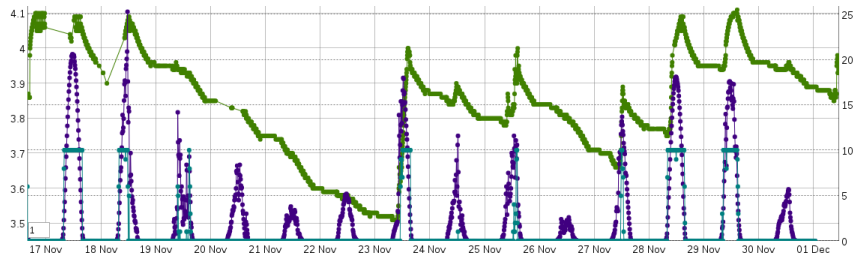
Ergebnisse



Ladestrom der Solarmodule (grün, [A]) vs. Ladezustand des Akkus (blau, [%]) und Aktivphasen des Systems (violett)

- ▶ Vergrößerung des vorangegangenen Bildes

Ergebnisse: Langzeittest



Ladespannung des Akkus (grün) vs Globalstrahlung (violett) und Sonnenscheindauer (blau)

- ▶ Globalstrahlung und Sonnenscheindauer aus Daten des DWD entnommen (Station Dresden-Klotzsche)
- ▶ Tage mit Sonnenschein reichen, um Akku wieder voll zu laden

- ▶ Autonom versorgte Plattform zur Erfassung von Probe Requests im Outdoor-Betrieb ist mit preiswerten Off-the-Shelf-Komponenten realisierbar.
- ▶ Plattform funktionierte nach einmaligem Aufladen des Akkus 14 Tage lang fehlerfrei (Ende November)
- ▶ autonomer Versorgung nachgewiesen (aber: periodische Arbeitsweise, Einschränkung im Nachtbetrieb, Akku im Winter?).
- ▶ variable Parameter: Akkukapazität, PV-Fläche, Duty-Cycle des Prozessors

Ausblick: Probleme, Herausforderungen, Hindernisse

1. Problem: ausgeschaltete Telefone, MAC Randomization → fällt bislang nicht ins Gewicht
2. Problem: relativ geringe Abstände der Messsysteme → Untersuchungen zum Einsatz von LoRaWAN zur Kommunikation zwischen Stationen und zur 'Zentrale'
3. Problem: was tun bei leerem Akku? → DutyCycle variabel auslegen!
4. Problem: leichtgewichtiges Kommunikationsprotokoll zwischen Stationen
5. Problem: Aufzeichnung & Speicherung der *Probe Requests* ist möglicherweise unzulässig → Pseudonymisierung, Löschung nach Geschwindigkeitsbestimmung

- ▶ Paul Fuxjaeger et al: *Towards Privacy-Preserving Wi-Fi Monitoring for Road Traffic Analysis*. IEEE Intelligent Transportation Systems Magazine, Vol. 8, No. 3, 2016
- ▶ Robert Baumgartl, Dirk Müller: *Raspberry Pi as an Inexpensive Platform for Real-Time Traffic Jam Analysis on the Road*. Proc. FedCSIS, Poznań, 2018
- ▶ Miriam Alina Scholz: *Autonome Energieversorgung für Plattformen zum automatischen Erfassen von WiFi-Probe-Requests*. Diplomarbeit, HTW Dresden, Dezember, 2018