

Lokalisierung durch Messung von WLAN-Signallaufzeiten

Mario Haustein

Herbsttreffen der GI/ITG-Fachgruppe Betriebssysteme

11. November 2011

Motivation

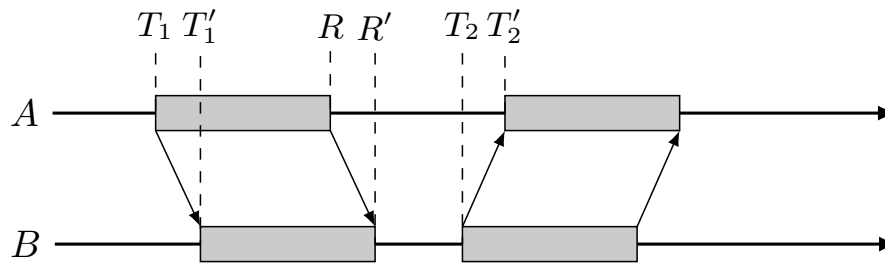
- ▶ WLAN-Laufzeitlokalisierung hat das Potential zum Indoor-GPS.
- ▶ Laufzeitmessungen werden im Vergleich zu Feldstärkemessungen weniger durch die Umwelt beeinflusst.
- ▶ Es gibt bereits ähnliche Ansätze.
 - ▶ Diese sind aber meist auf spezielle Hardware ausgelegt ...
 - ▶ ... oder tauschen Daten mit Teilnehmern „hinter“ dem Access Point aus.

Ziel: Weite Verbreitungsmöglichkeit sicherstellen.

- ▶ Keine Spezial-Hardware ⇒ „Off-the-shelf“
- ▶ Keine Firmware- oder Hardware-Modifikationen
- ▶ Keine Assoziierung mit Access Point
- ▶ Die Grenzen von IEEE 802.11 einhalten

Wie misst man die Signallaufzeit?

- ▶ Time-of-Flight-Verfahren: Nachrichtenaustausch $A \rightarrow B \rightarrow A$



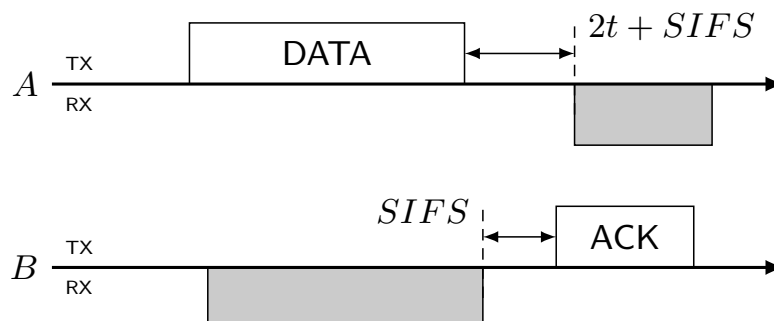
- ▶ Es ist keine Uhrensynchronisation notwendig.

$$\Delta = T_2' - T_1 = \underbrace{(T_1' - T_1)}_t + \underbrace{(R' - T_1')}_d + \underbrace{(T_2 - R')}_g + \underbrace{(T_2' - T_2)}_t = 2t + d + g$$

- ▶ Nach Umstellen erhält man: $t = \frac{1}{2} \cdot (\Delta - d - g)$

Die IEEE 802.11 MAC-Schicht

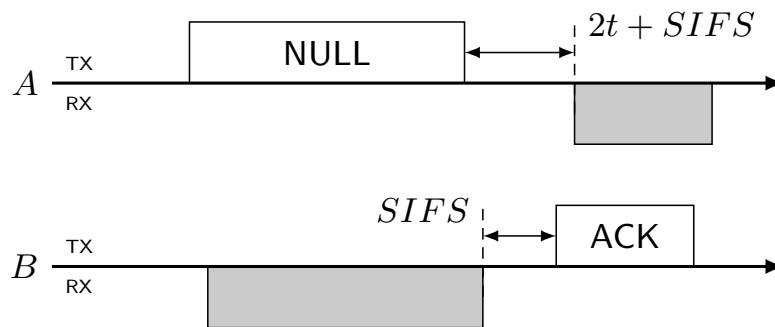
- ▶ IEEE 802.11 stellt die Zustellung von Frames bereits auf MAC-Ebene sicher.



- ▶ Dieser Mechanismus stellt eine TOF-Sequenz dar.
 - ▶ Wurde bereits in der Vergangenheit zur Lokalisierung genutzt.

Das NULL-ACK-Verfahren

- ▶ NULL-Frames transportieren keine Nutzlast.
- ▶ Sie dienen der Umsetzung von Stromsparfunktionen.



- + Keine Assoziierung mit dem Access Point notwendig
- + Keine Belastung des Netzwerks hinter dem Access Points
- + Keine Beeinflussung durch Verschlüsselung
- + Kürzere Durchlaufzeit
- Erzeugung nicht so einfach wie bei DATA-ACK-Sequenzen

Der TSF-Zähler

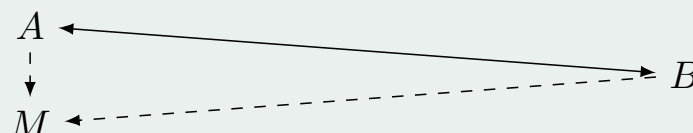
- ▶ Nach Kapitel 1.11 in IEEE 802.11 in jedem WLAN-Adapter vorhanden.
- ▶ Viele Adapter vermerken den Wert des TSF beim **Empfang** eines Frames.
- ▶ Auflösung: $1 \mu s$, Kein Jitter!

Problem

Benötigte Sendezeitstempel können nicht ohne Weiteres erfasst werden.

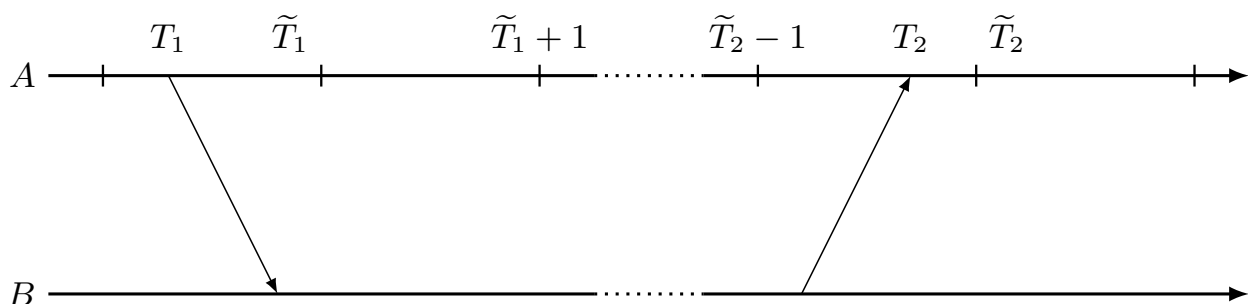
Lösung

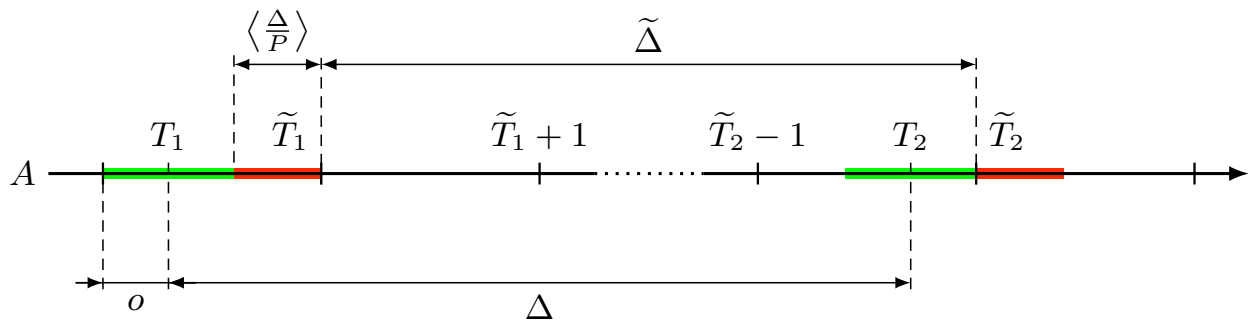
- ▶ Ein zweiter Monitor-Adapter in Nähe von A



⇒ Bei M müssen nur Empfangsereignisse gemessen werden.

Mittels wiederholter Messungen und statistischer Verfahren kommt man mit der groben Auflösung des TSF aus.





- ▶ $\tilde{\Delta}$ hängt vom Offset o ab.
- ▶ Ist o gleichverteilt, folgt $\tilde{\Delta}$ einer Zweipunktverteilung ($P \dots$ Auflösung).

$$\tilde{\Delta} = \begin{cases} \left\lfloor \frac{\Delta}{P} \right\rfloor & 0 < \frac{o}{P} < 1 - \left\langle \frac{\Delta}{P} \right\rangle \\ \left\lfloor \frac{\Delta}{P} \right\rfloor + 1 & 1 > \frac{o}{P} \geq 1 - \left\langle \frac{\Delta}{P} \right\rangle \end{cases}$$

- ▶ Es gilt:

$$E[\tilde{\Delta}] = \Delta$$

Erfassung und Erzeugung der NULL-ACK-Sequenzen

Erfassung

- ▶ Heutzutage überwiegend „SoftMAC“-Adapter im Einsatz
- ▶ Der Linux MAC80211-Stack erlaubt sog. Monitor-Schnittstellen.
 - ▶ 802.11-Frames werden samt Metainformationen¹ an Anwendungen weitergegeben.
 - ▶ Bitrate, TSF, Kanal / Frequenz, ...
- ▶ Gewöhnlicher Paket-Sniffer einsetzbar.

Keine Patches notwendig

Erzeugung

- ▶ Über Monitor-Schnittstellen können beliebige Frames in den normalen Paketstrom eingeschleust werden („Packet Injection“).
- ▶ Z.B. einfaches C-Programm in Verbindung mit libpcap.

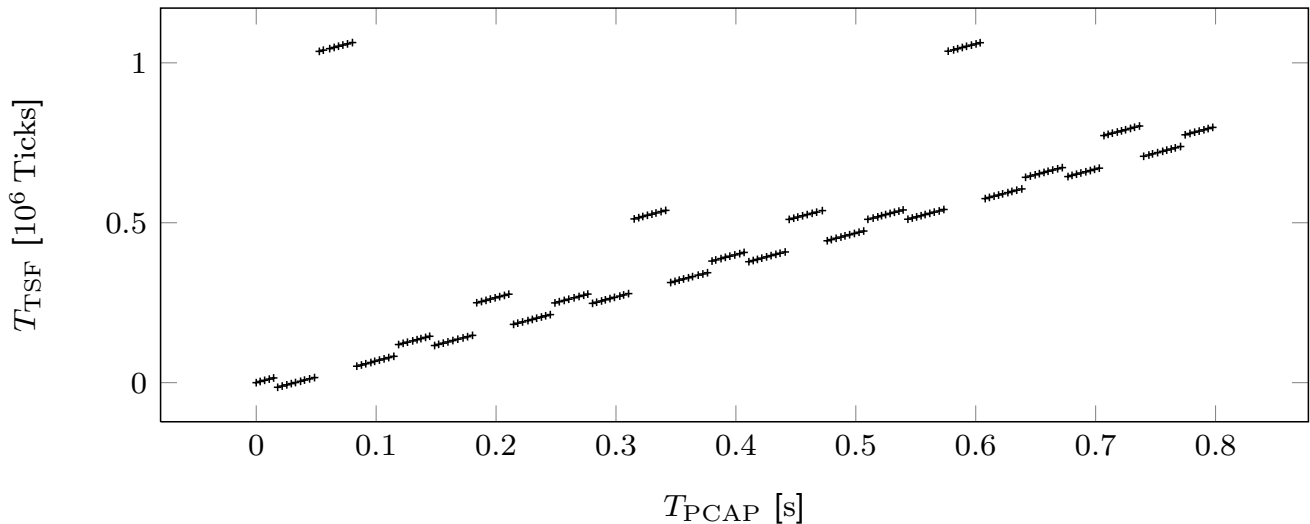
Kernelpatch zur Festlegung einer Bitrate

¹vgl. <http://www.radiotap.org/>

Die Auswertung von NULL-ACK-Sequenzen

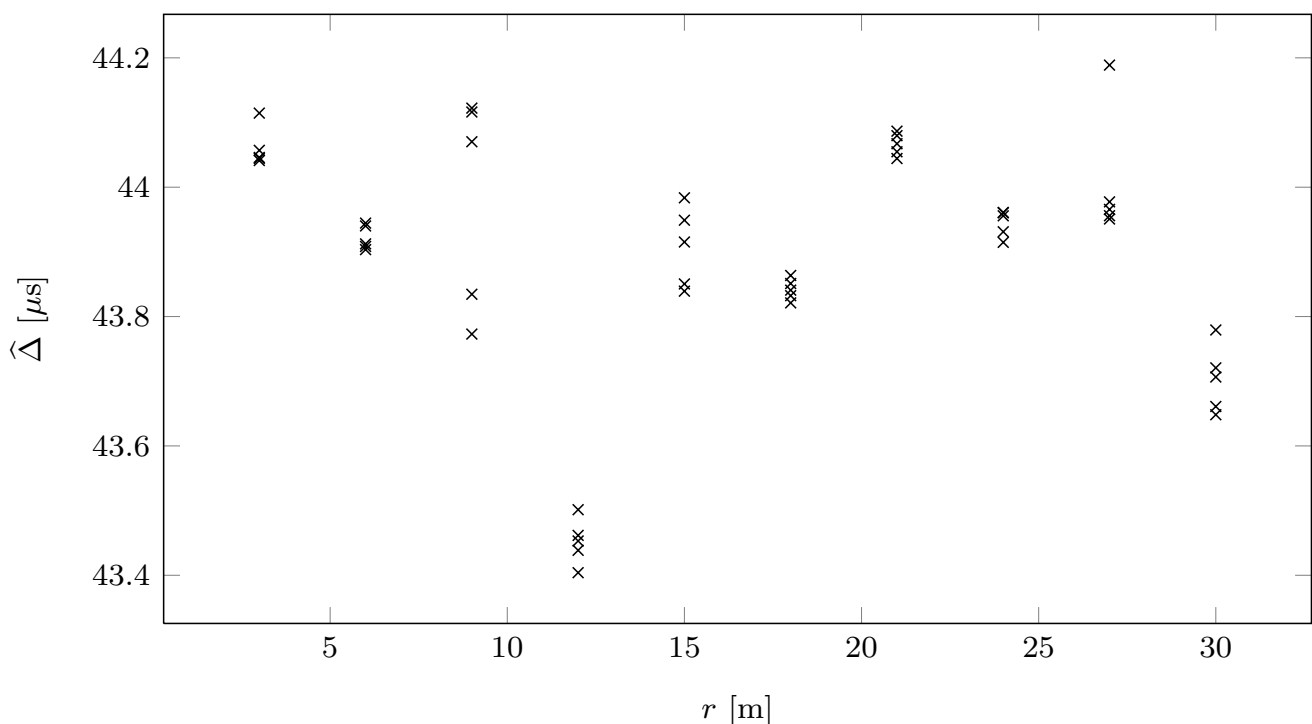
- ▶ Auswerten der Paket-Sniffer Aufzeichnungen.
 1. NULL-ACK-Sequenzen identifizieren.
 2. $\hat{\Delta}$ berechnen.
 3. Messfehler filtern.

Fehlerhafte TSF-Zähler machen eine Filterung notwendig:



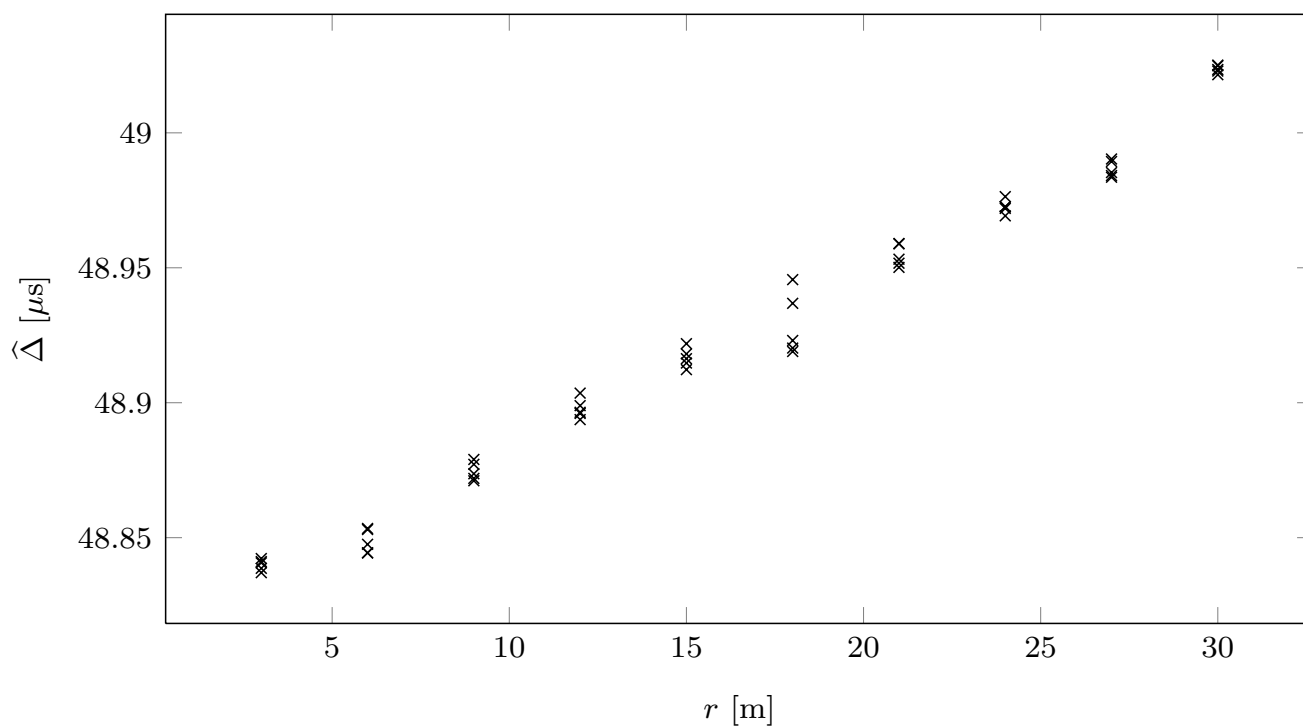
Versuchsergebnisse

54 MBit/s, Intel-Karte (IWL6000), ca. 7000 bis 9000 Einzelmessungen pro Schätzung

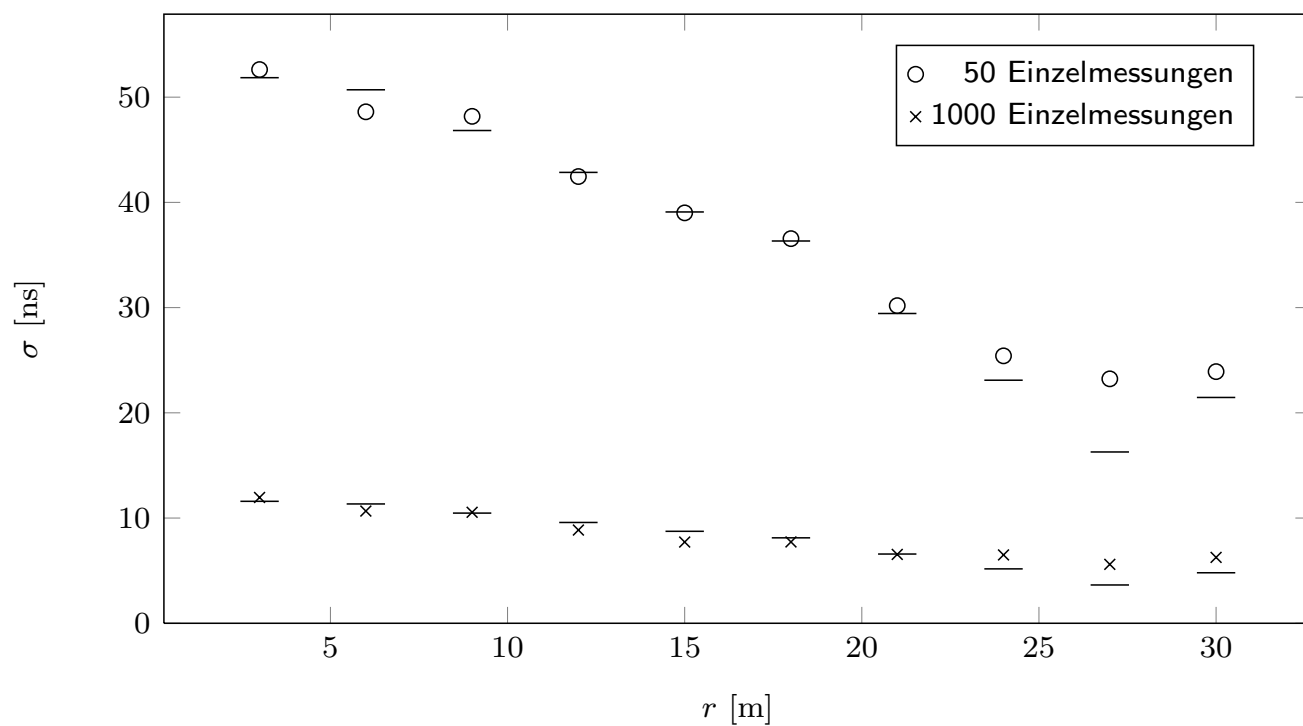


Versuchsergebnisse

54 MBit/s, Atheros-USB-Stick (TL-WN422G), ca. 7000 bis 9000 Einzelmessungen pro Schätzung



Genauigkeit



Ausblick

- ▶ Eine Software-basierte Laufzeitmessung ist möglich!
 - ▶ Erreichen Modellgenauigkeit.
 - ▶ Nicht jede Hardware-Plattform ist geeignet.
- ▶ Technische Schwierigkeiten erfordern ein zweites WLAN-Gerät
 - ▶ Kann evt. durch Firmwaremodifikationen behoben werden.
 - ▶ Treiber mit quelloffener Firmware: carl9170²
- ▶ In baulich schwierigen Umgebungen werden WLAN-Signale reflektiert und haben einen längeren „Funkweg“.
- ▶ IEEE 802.11y setzt die Laufzeitmessung in Zukunft Hardware-seitig um.

²<http://linuxwireless.org/en/users/Drivers/carl9170>