CAESAR: Carrier Sense-Based Ranging in Off-The-Shelf 802.11 Wireless LAN

Domenico Giustiniano and Stefan Mangold
Disney Research Zurich, Switzerland
Summary

• Wireless LAN is crucial in navigation systems
• Current solutions do not meet a set of conflicting requirements
• We present CAESAR, a ranging technique that
  – combines time of flight and signal-to-noise ratio measurements to calculate the distance to a remote WLAN device
  – can be employed in off-the-shelf devices
  – shows high accuracy
  – can track the distance to smartphones
Outline

- Scenario
- Time of flight
- Problems
  - ACK detection time
  - Implementation in off-the-shelf devices
- Evaluation
- Conclusion
WLAN localization

• Advantages
  – WLAN *available* in most of today’s mobile devices
  – *no* additional infrastructure cost

• Problem
  – WLAN position based on *limited* device capabilities
Signal strength

1. SNR fingerprint of the environment
   • *cost of maintenance*

2. Signal strength-based *ranging* techniques
   - SNR of frames from remote stations
   - distance = f(SNR)
     • *Theoretical or empirical model*
Signal strength

Why are they used?

*Only software changes in off-the-shelf WLAN devices!*
Outline

• Scenario

• Time of flight

• Problems
  – ACK detection time
  – Implementation in off-the-shelf devices

• Evaluation

• Conclusion
TOF (time of flight) ranging

• Calculate the time of propagation $t_p$
  – From the remote station to the local station
  – *used in GPS*

• *Linear* function of the distance $d=c \cdot t_p$
  – $1 \, \mu s = 300 \, m$
  – Apart of the multi-path propagation

• *No offline measurements* for radio-mapping
TOF in WLAN?

• No reference 802.11 clock
  – *Echo techniques* (round-trip-time)
• Precision depends on the clock resolution
  – \(\rightarrow\) clock as *fast* as possible
• *Workload independent* estimation
  – of local station and network traffic
• *Software-based solution*
  – cost-effective, like in SNR-based ranging techniques
MAC Idle Time

• 802.11 WLAN uses a CSMA/CA protocol
  – Data/ACK pair

• Channel is *idle* between the data and ACK

• The idle time duration is
  – *predefined* and expected to be *constant*
    • MAC SIFS time ($t_{SIFS}$)
Variation of MAC Idle Time

• The idle time at the local station *varies*
  – with the *physical distance* between the two stations
  – because of time delay of $t_p$
CAESAR

• Key idea
  – exploit variation of idle time for ranging

• Variation based on channel state transitions of CSMA/CA → CAESAR: CArriEr Sense-baSed Ranging
Solved?

✓ Precise Time Measurement
  – CAESAR uses carrier sense samples
    • with resolution of the main WLAN clock
      – (44 MHz in 802.11b/g, at least 88 MHz in 802.11n)
      • \( \frac{300}{2 \cdot 44} = 3.4 \text{ m} \) of accuracy for the single sample
    – Short duration: no clock drift

✓ No protocol extensions
  – CAESAR only needs \textit{information at the local station}
    • E.g. \( t_{\text{MACidle}} \)
    – No need of any information from the remote station
      • \( t_{\text{SIFS}} \) is constant
Not really...

• CAESAR is a *MAC-based solution*
• $t_{\text{MACidle}}$ depends on MAC operations
  – *Delay* caused by ACK detection time
  – Synchronization on the *strongest* path
• no inherent support in WLAN hardware
  – for calculating $t_{\text{MACidle}}$
Outline

• Scenario
• Time of flight
• Problems
  – ACK detection time
  – Implementation in off-the-shelf devices
• Evaluation
• Conclusion
Problem: MAC Idle Time Distribution

- Two links, fixed distance (< 15 m)
- Multiple samples
- $t_{\text{MAC idle}}$ in the range of 500 - 530
  \[ 11.3 - 12 \mu s \text{ @44 MHz} > 10-10.1 \mu s \text{ expected!} \]
What causes this delay?

• ACK detection time $t_{FD}$

$$t_{MACidle} = 2t_p + t_{SIFS} + t_{FD}$$

$$d = c \cdot (t_{MACidle} - t_{SIFS} - t_{FD}) / 2$$
More details

- $t_{\text{MACidle}}$ distribution is bimodal
  - $\rightarrow$ two spikes on the same link
  - $\approx 20$ clock cycles
  - link A: 2$^{\text{nd}}$ spike at lower SNR
  - link B: 2$^{\text{nd}}$ spike at higher SNR
Frame detection time

\( t_{\text{MACidle}} \) is a function not only of the distance, but also of the SNR of the received ACK from the remote station.

\[
t_{\text{MACidle}} = f(\text{TOF}, \text{SNR})
\]

\[
t_{\text{MACidle}} = 2t_p + t_{\text{SIFS}} + t_{\text{FD}}
\]

\[
t_{\text{FD}} = f(\text{SNR})
\]
Automatic gain control

• When ACK is received, medium is declared busy:
  1. after the energy of ACK frame has been detected
  2. signal gain adjusted by the *Automatic Gain Control*
     • *function of the SNR*
AGC and SNR

• When the received signal is within a preferred range
  – PR: no operation (gain control) by the AGC

• For signals out of PR range
  – SSD = strong signal detection
  – WSD = weak signal detection

• SSD/WSD: AGC tunes the signal level to the desired range
  – *delay* in the ACK detection
Using the detection time for ranging estimates

- Multiple samples are then smoothed

\[
\begin{align*}
    t_{\text{MACidle}} &= 2t_p + t_{\text{SIFS}} + \bar{t}_{FD,s} \\
    d &= c \cdot \left( t_{\text{MACidle}} - t_{\text{SIFS}} - \bar{t}_{FD,s} \right) / 2
\end{align*}
\]
Map of detection states

- Based on MAC idle time and SNR
  - Frames are associated to states
  - Each frame is classified in WSD, PR or SSD state
Map of detection states

- Several tests, measurements of $t_{\text{MACidle}}$ and SNR
- We distinguish 3 different regions/states

![Diagram](image)
Using the detection time for ranging

\[ t_{\text{MACidle}} = 2t_p + t_{\text{SIFS}} + \bar{t}_{\text{FD,s}} \]

\[ d = c \cdot (t_{\text{MACidle}} - t_{\text{SIFS}} - \bar{t}_{\text{FD,s}})/2 \]
Using the ACK detection time for ranging

- the average detection time per state is used to estimate the distance

\[
\begin{align*}
t_{\text{MACidle}} &= 2t_p + t_{\text{SIFS}} + \bar{t}_{\text{FD,s}} \\
\bar{d} &= c \cdot (t_{\text{MACidle}} - t_{\text{SIFS}} - \bar{t}_{\text{FD,s}})/2
\end{align*}
\]

- PR frames: \( t_{FD} \) is only due to preamble detection
  - \( \sim 2 \) OFDM short symbols was measured

- SSD and WSD frames: A longer \( t_{FD} \)
  - L-STA AGC varies the amplifier gain of the ACK signal
  - an additional delay of \( \sim 0.4 \) \( \text{us} \) was measured
Outline

• Scenario
• Time of flight
• Problems
  – ACK detection time
  – Implementation in off-the-shelf devices
• Evaluation
• Conclusion
Problem: Measuring the Idle Time

- Channel state transitions
  - Occur only twice between the data and the ACK
    - At the end of the data transmission
    - When the ACK is received
  - We don’t need to continuously monitor the idle time

- Measuring the channel in two instants of time:
  1. when data transmission is ongoing
  2. when ACK reception is ongoing
Not trivial to implement

- *not trivial to implement*
  - $t_{\text{MACidle}}$ occurs in *very short period of time* (<12us)
  - the ACK duration is in the order of tens of secs
- *we require a fine-grained detection of the time of ongoing data transmission and ACK reception*
Outline

• Scenario
• Time of flight
• Problems
  – ACK detection time
  – Implementation in off-the-shelf devices
• Evaluation
• Conclusion
Map of evaluation

- STA1-STA5, WLAN Atheros chipset
- STA6, “HTC magic” smartphone
Indoors

• Average errors of $< 1$ m
  – in 8 links out of 10

• Absolute error of $< 2$ m after fewer than 25 samples
  – in 9 links out of 10
Tracking

- 7 positions: A, B, ... G
- CAESAR tracks the distance to a moving smartphone
- SNR is not a reliable indicator of distance

SNR = (similar values for different distances)
Conclusion

• Ranging technique is crucial in navigation system
• CAESAR measures the distance to remote WLAN devices
  – Key ideas based on MAC protocol operations for communication
  – high accuracy, high convergence, no changes in the network protocol, no offline calibration,...
• Effective technique to use in off-the-shelf devices
thank you for your attention !