RANGING IN IEEE 802.15.4A STANDARD

Anuj Sehgal
(Networks and Distributed Systems Seminar - 2008)
Introduction

- IEEE 802.15.4a standard
- Ranging methods in the standard
- Conclusion / Review
Introduction

IEEE 802.15.4a standard

Ranging methods in the standard

Conclusion / Review
IEEE 802.15.4a uses impulse radio (IR) UWB and chirp spread spectrum (CSS) signals.

IR-UWB is used for ranging support.

CSS is used for data communication.

<table>
<thead>
<tr>
<th>Signaling Format</th>
<th>250 - 750 MHz</th>
<th>2.4 - 2.4835 GHz</th>
<th>3.244 - 4.744 GHz</th>
<th>5.944 - 10.234 GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR-UWB</td>
<td></td>
<td>CSS</td>
<td>IR-UWB</td>
<td>IR-UWB</td>
</tr>
</tbody>
</table>

*Table 1. Bands used by IR-UWB and CSS Signaling*
Information conveyed by position and polarities of *pulse bursts*.

- Larger bandwidths provide high time resolution.
- Higher probability of establishing line-of-sight.
- High SNR and/or wider bandwidth reduce ranging error.
The packet consists of:

- SHR Preamble - synchronization header
  - Preamble
  - SFD - Start of frame delimiter
- PHR - physical layer (PHY) header
- Data
- Introduction
- IEEE 802.15.4a standard
- Ranging methods in the standard
- Conclusion / Review
IEEE 802.15.4a uses TW-TOA.
RDEV-A sends RFRAME to RDEV-B and awaits receipt.

Total Travel Time for RFRAME:
\[ T_r = 2T_t + T_a \]
Ranging Protocols

- Mandatory Ranging Protocol
- Optional Symmetric Double Sided TW-TOA (SDS TW-TOA)
- Optional Private Ranging Protocol
Mandatory TW-TOA

- Uses only the D2, A2, D4 and A4 data packets for the entire operation.

- A detailed time stamp report containing 16-octets generated.

- Confidence interval of 100 ps, 300 ps, 1 ns or 3 ns.

\[
T^W_t = T_t + \frac{1}{2} \delta (e_a - e_b)
\]

\[
T^B_{ta} = T^A_{ta} + \delta \quad T_t << \delta
\]
TIME STAMP DATA

- Ranging counter start value
- Ranging counter stop value
- RDEV-A crystal characterization value
- RDEV-B crystal characterization value
- Figure-of-merit (FoM)
- Uses D2, A2, D3, D4 and A4 data packets for the entire operation.

- Addition of the D3 data packet reduces effect of crystal tolerances.

\[
T^TW_t = T_t + \frac{1}{4}\delta(e_a - e_b)
\]

\[
T^B_{ta} = T^A_{ta} + \delta \quad T_t << \delta
\]
PRIVATE RANGING

- Snooper attack - *a device listens on the exchanged packets to detect RDEV positions.*
- Impostor attack - *a device transmits RFRAME to RDEVs in order to confuse acquisition and ranging.*
- Jamming attack - *a device jams transmissions of RFRAMEs.*
Authentication phase.

- RDEV-A sends *range authentication packet* to RDEV-B.
- $DPS_{rx}$ and $DPS_{tx}$ randomly chosen from preamble set.
- Acknowledgment if found genuine.
Ranging Phase

- RDEV-A transmits RFRAME that uses $DPS_{rx}$ as the preamble symbol.
- RDEV-B replies with acknowledgement RFRAME that uses $DPS_{tx}$ as preamble.
Introduction

IEEE 802.15.4a standard

Ranging methods in the standard

Conclusion / Review
IEEE 802.15.4a standard uses IR-UWB for ranging communication.

IR-UWB useful as it provides high LOS probability and low error probability.

The ranging protocols are based upon TW-TOA:

- A mandatory TW-TOA implementation.
- Optional SDS TW-TOA implementation (lower crystal error).
- Optional Private Ranging:
  - Ensures identity.
  - Encrypted data for security.
  - Randomly $DPS_{rx}$ and $DPS_{tx}$ varied make replay attacks difficult.
THAT'S ALL FOLKS!