UCLA
Posters

Title
Distance Enlargement and Reduction Attacks on Ultrasound Ranging

Permalink
https://escholarship.org/uc/item/57q0q217

Authors
Sahar Sedighpour (NESL-UCLA)
Srdjan Capkun (IMM Technical University of Denmark)
et al.

Publication Date
2005
**Problem Description:** Distance Reduction And Enlargement

**Wormhole Attacks**
Exploits the fact that light travels faster than light

- Distance between A and B can be arbitrarily reduced.
- Attackers can pass the signal between them through a fast radio link, so that the signal would be to the listener much faster.

- This would only work if:
  \[
  \frac{x_1}{c} + \frac{x_2}{c} + P_{\text{US, receive}} + P_{\text{RF, send}} + P_{\text{RF, propagate}} + P_{\text{RF, receive}} + P_{\text{US, send}} + \frac{x_2}{V_{\text{US}}}
  \]

**Pulse-Delay Attacks**

- Distance between A and B can be arbitrarily increased.
- Attacker can make the distance seem longer by jamming the ultrasound signal from the beacon, and replay it at a later time.

---

**Prototype Implementation:**

We used Crickets from MIT with V2 Software:

Two Cricket nodes (A and B) are placed at distance \(d\). This distance is then measured using ultrasonic ranging: an ultrasonic signal and a radio signal are sent at the same time from node A to node B; node B then measures the difference between the reception time of the ultrasonic signal and the reception time of the radio signal; based on this difference, B estimates its distance to A. Case Study: M1 and M2 placed in 90° with respect to Beacon and Listener.

**Distance Reduction:**
Average distance measured with Attackers vs. Distance of Attackers to beacon and listener

**Distance Enlargement:**

When A1 also wait for US from B to send RF to A2

When original distance b/w L and B is 25 cm