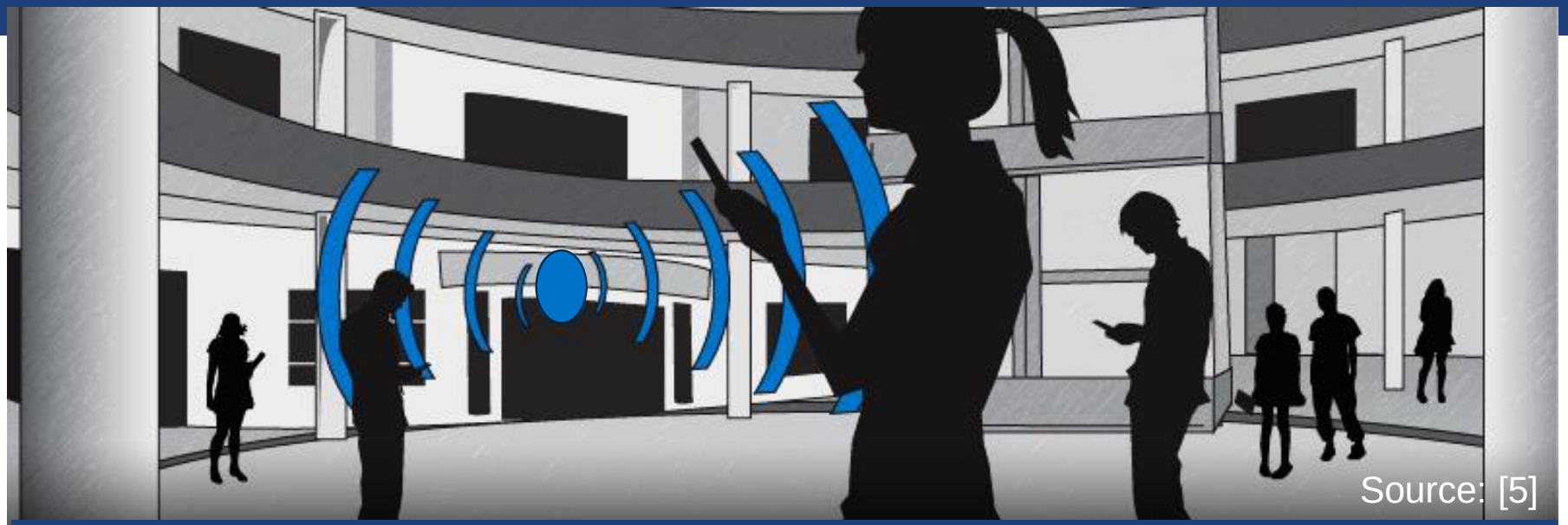


Seeing is Believing: Proximity-based Authentication

Peter Pilgerstorfer

Motivation

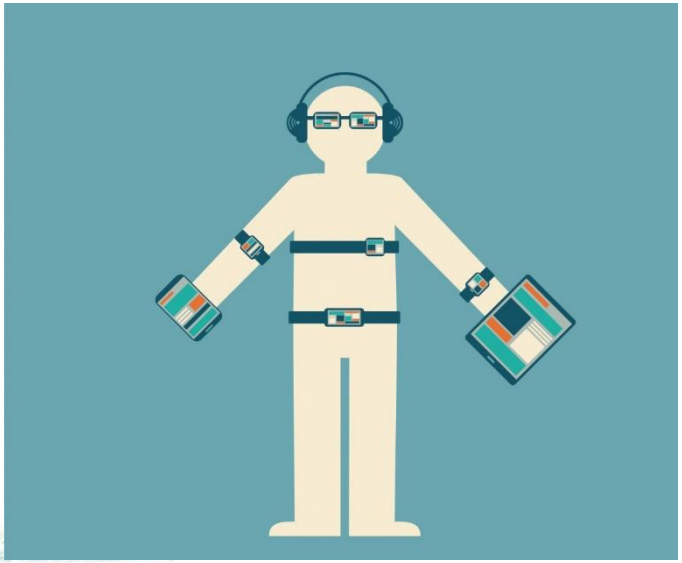
- Pairing without user interaction
- Traditional authentication
  - E.g. enter/confirm shared PIN
  - Not possible for certain IoT devices
  - Not scalable
- Use cases
  - NFC payments
  - Keyless entry and start systems
  - Secure pairing for implants
  - …

Goal

- A secure and authentic connection between two devices
  - Shared secret
  - Verify authenticity
- Assumption:
  Authentic if the devices are within proximity to each other

- Why does proximity lead to trust?
- How to determine proximity?

Why does proximity lead to trust?



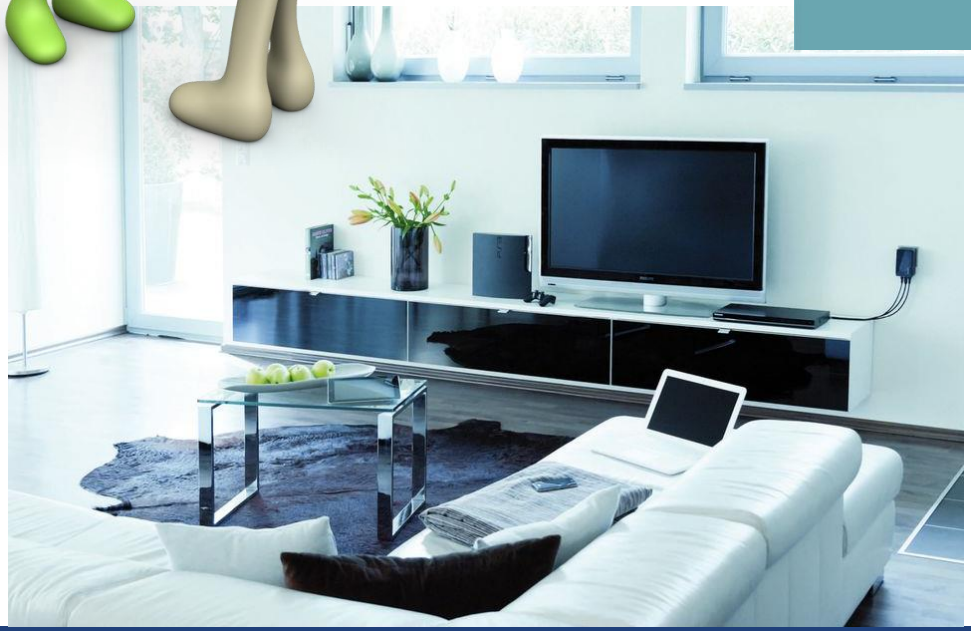


Image sources: [9-11]

How to determine proximity?

- Time of Flight
- Radio signal
- RSSI (Received Signal Strength Indicator)
- Accelerometer
- Illumination
- Audio signals
- …

Overview

- Wi-Fi Time of Flight, CoNext 2014
- Amigo, UbiComp 2007
- ProxiMate, MobiSys 2011

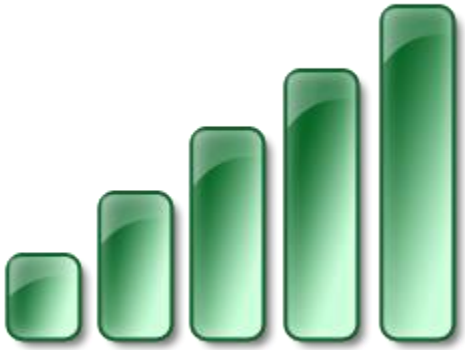


Image sources: [6-8]

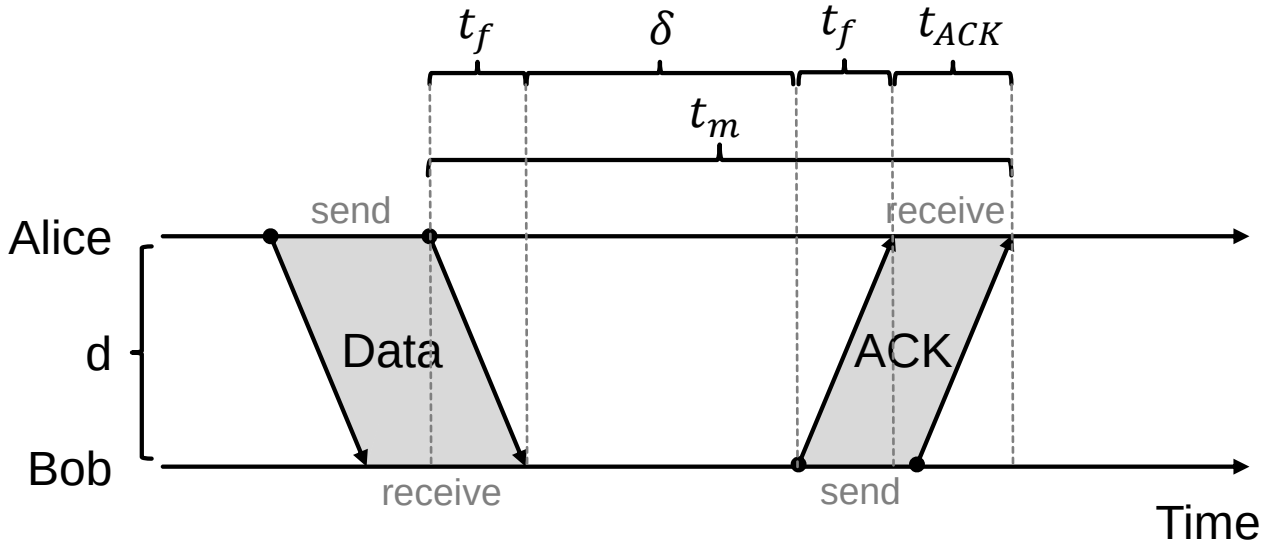
Wi-Fi Time of Flight

- Measure response time

$$\mathrm{t_f} = \frac{1}{2}(t_m - t_{ACK} - \delta)$$

- Calculate the distance

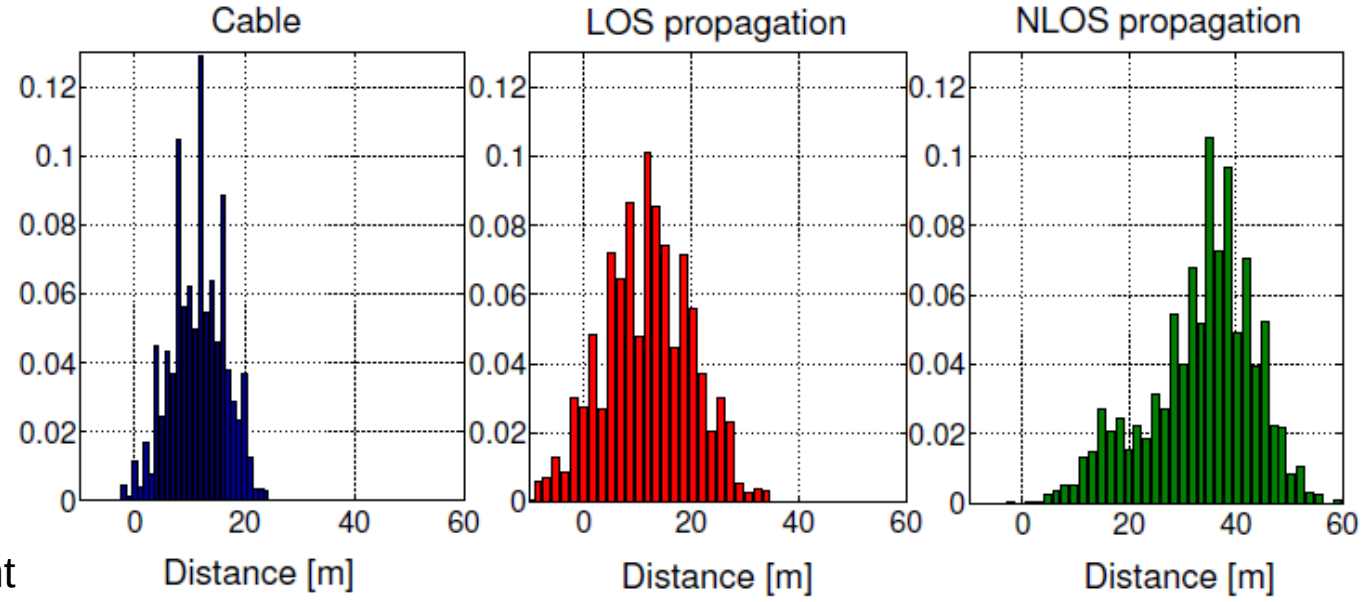
$$d = c \cdot t_f$$



Wi-Fi Time of Flight - Challenges

- Noisy measurements
  - Multiple paths
  - Imprecise hardware
- Consequences
  - Measure multiple times
  - Effective median error: $1.7 - 2.4m$

Image taken from Marcaletti et al [1]

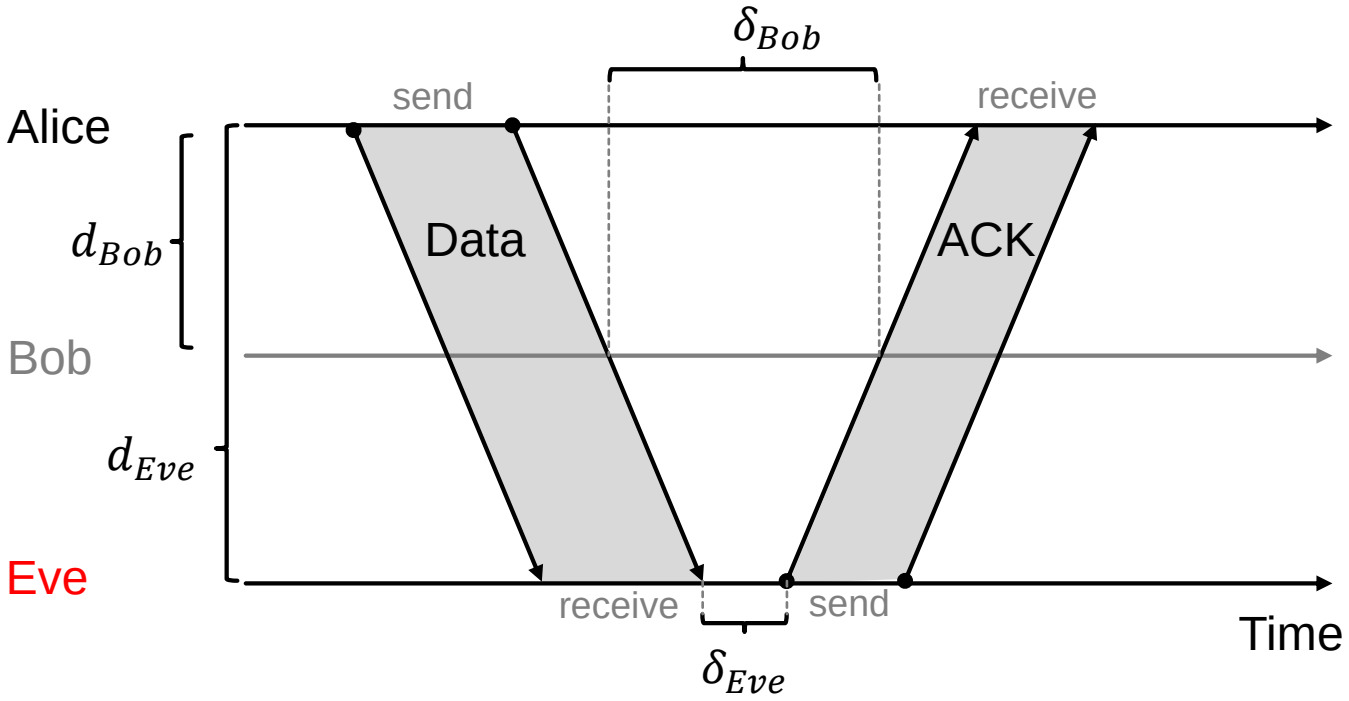


LOS: line-of-sight
NLOS: non-line-of-sight

Wi-Fi Time of Flight - Challenges

- Processing time
  - Keep δ as low as possible
  - What if attacker is faster?

    with $\delta = 10.2\ \mu s$, up to $\sim 1500\ m$ "closer"



Wi-Fi Time of Flight - Conclusion

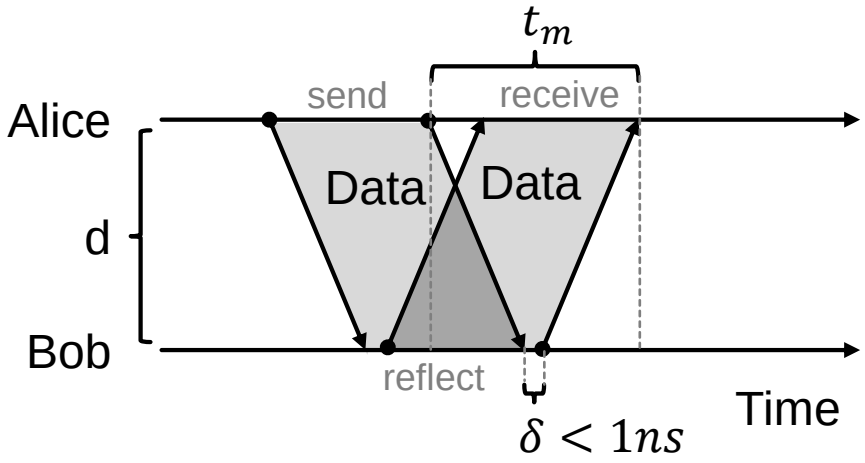
+ Works with standard Wi-Fi hardware

– Assumes that attacker doesn’t have access to faster hardware
– Not suitable for close distance pairing
– Many packets have to be sent

Wi-Fi Time of Flight - Improvement

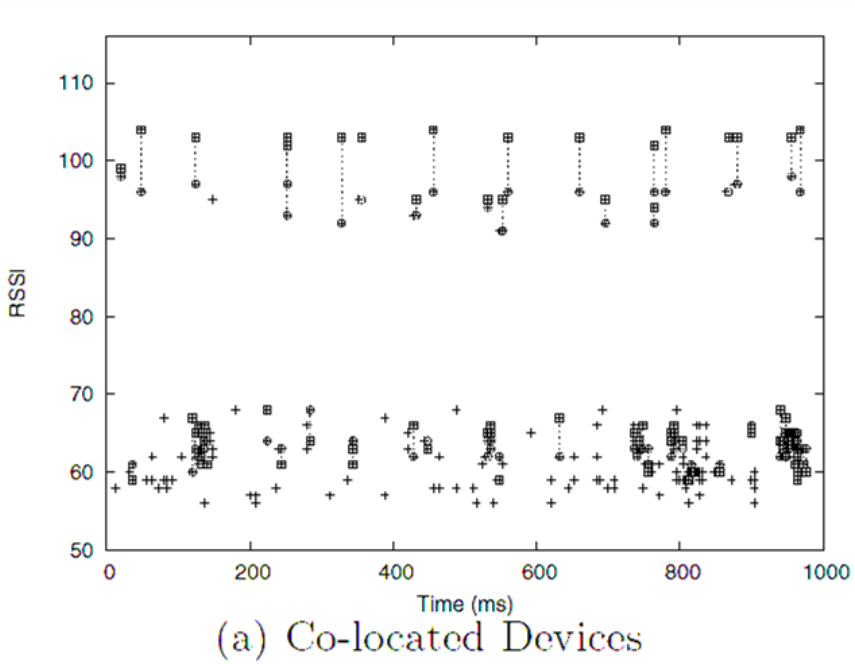
- Use special hardware to reduce processing time
  - With $\delta_T < 1ns$ an attacker can appear at most $\sim 15\ cm$ closer
- Reflect “instantly”
- Avoid demodulating signal

- Suitable for IoT devices

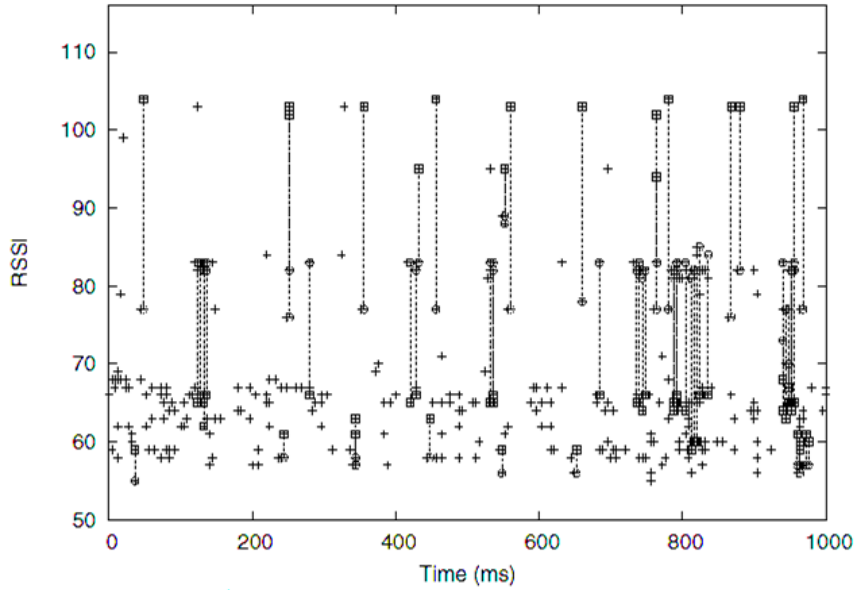


Amigo

- Radio environment is similar for devices in proximity
- Strategy: Passively observe received signal strength indicator (RSSI) for Wi-Fi packets



(a) Co-located Devices



(b) Devices 10m Apart

Images taken from Varshavsky et al [3]

Amigo – Observation

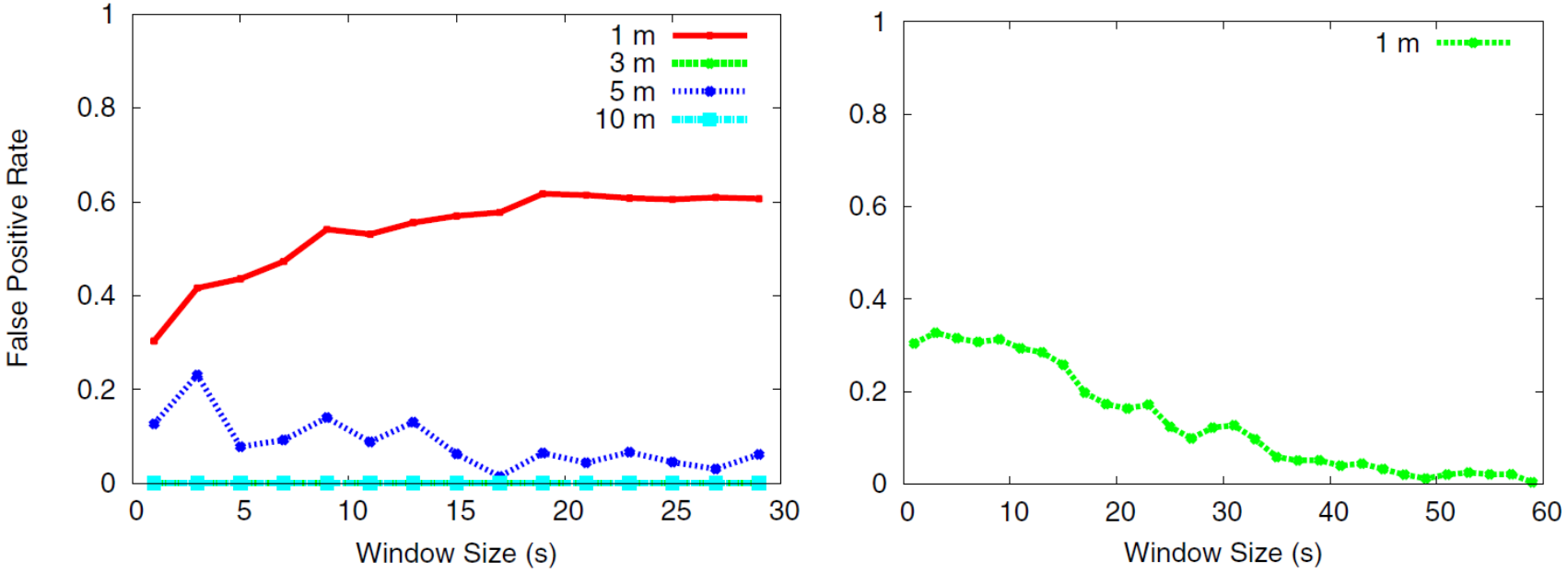
- Wi-Fi cards are set to promiscuous mode
  - Receive all packets
- Signature of the radio environment
  - Hash of every observed packet
  - RSSI of every observed packet
- RSSI
  - Defined in IEEE 802.11
  - Received power level

Amigo – Authentication

- Establish shared secret
- Observe packets transmitted via Wi-Fi
- Send signature to each other (hash and RSSI)
- Check if the other device made similar observations

Amigo – Results

- Attackers >=3m away can be detected within 5s
- Improve security by hand waving
  - Detect attackers within 1m



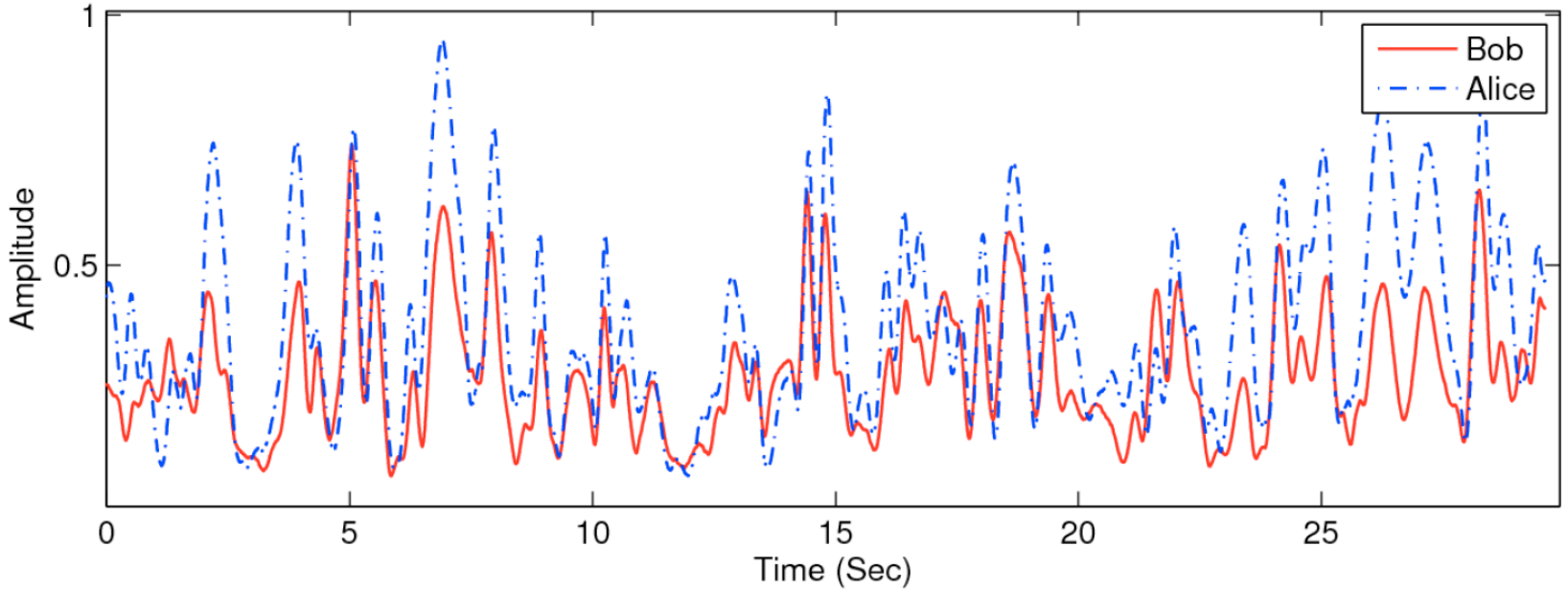
Amigo – Conclusion

+ Works with standard Wi-Fi hardware
+ Works reasonably well in close distances

– Paring time depends on Wi-Fi activity
– Diffie-Hellman key exchange is computationally intensive

ProxiMate

- Radio environment is similar for devices in proximity
- Strategy: Observe FM or TV radio signals directly instead of the received signal strength indicator



Images taken from Mathur et al [4]

ProxiMate – Wireless Channel

- Wireless channel
  - State described by complex number
  - Amplitude given by absolute value
  - Phase given by angle
- Features observed by ProxiMate:
  - Amplitude
  - Change of phase
- Use software-defined radio for measurements

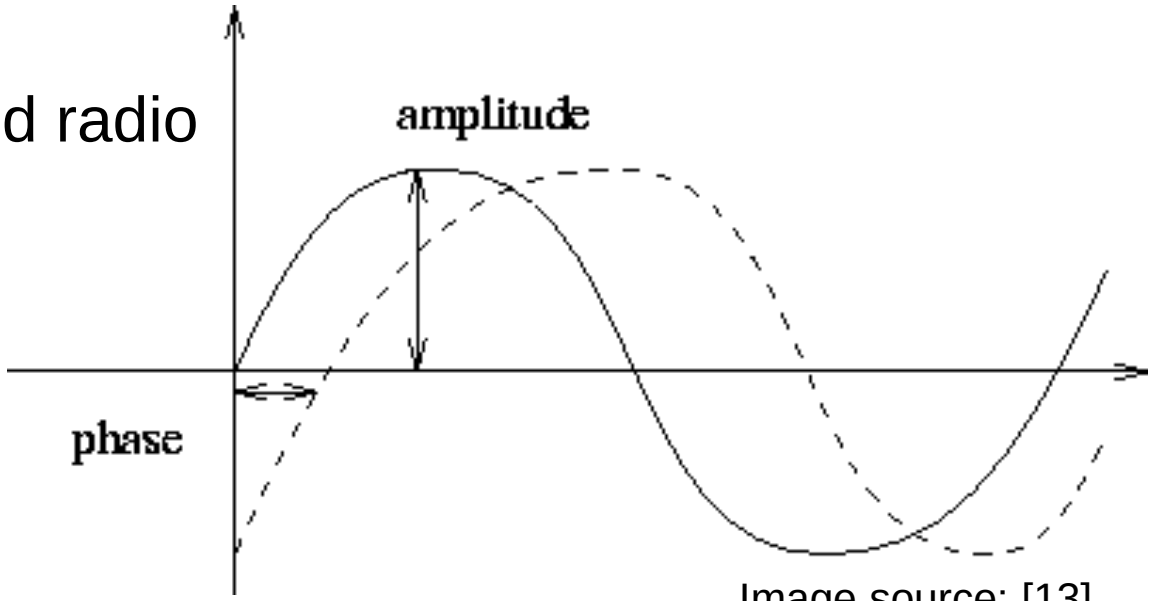


Image source: [13]

ProxiMate – FM/TV signal

- Frequency modulated
  - Amplitude constant
  - Amplitude variation not signal dependent
- TV: ~600 MHz
- FM: ~100 MHz

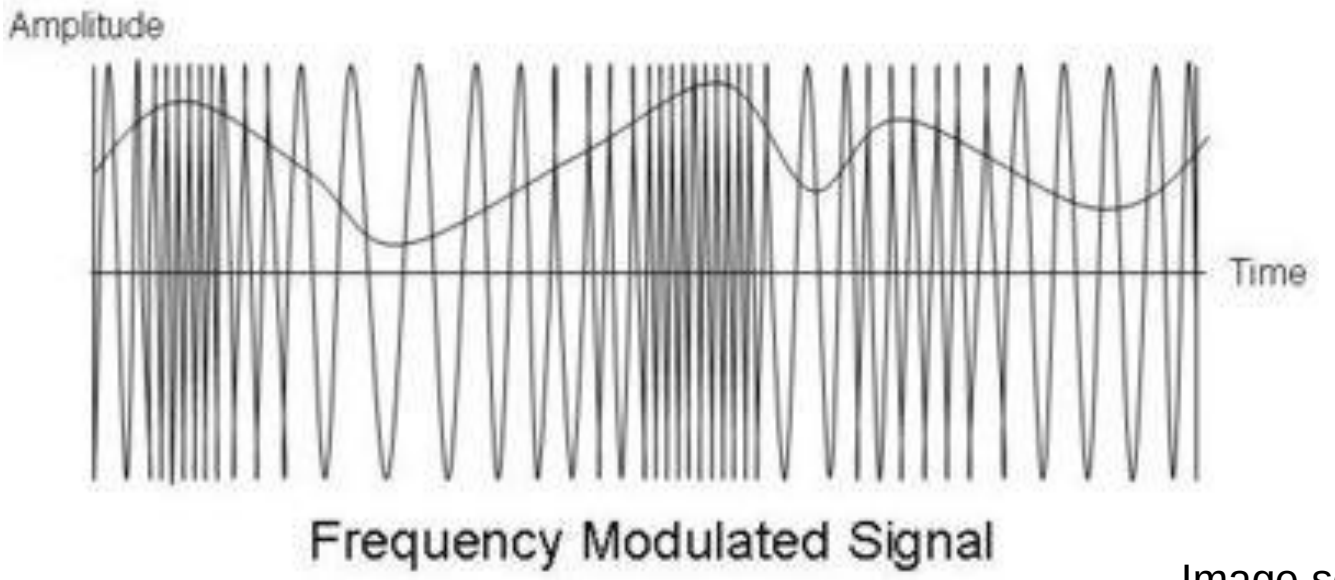


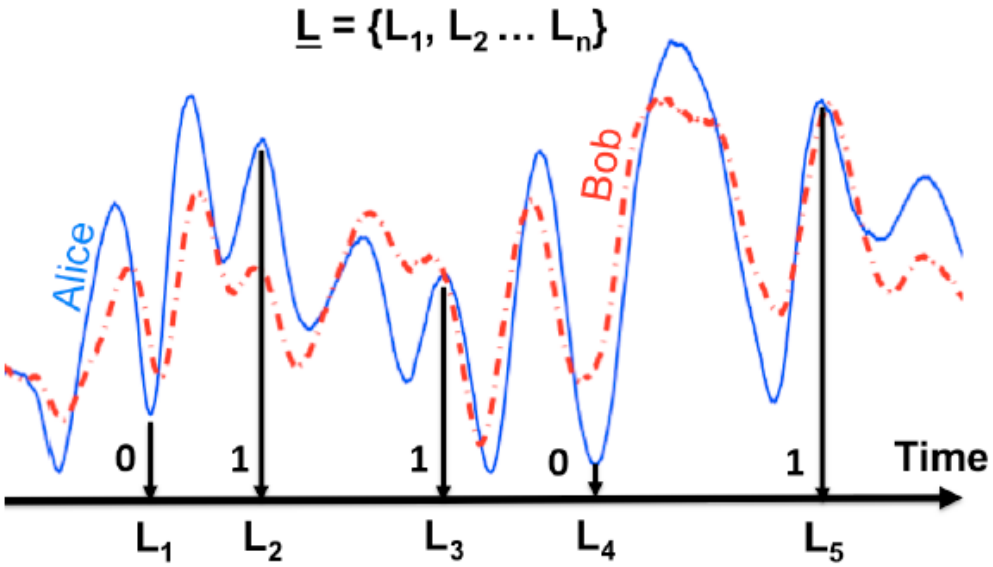
Image source: [12]

ProxiMate – Authentication

- Basic idea: generate a key out of the observed radio environment
  - Alice and Bob observe the environment
  - Alice collects timestamps of observed extrema (L)
  - Alice sends timestamps to Bob
  - Bob collects observed extrema at timestamps L
  - Extremas encode the key:

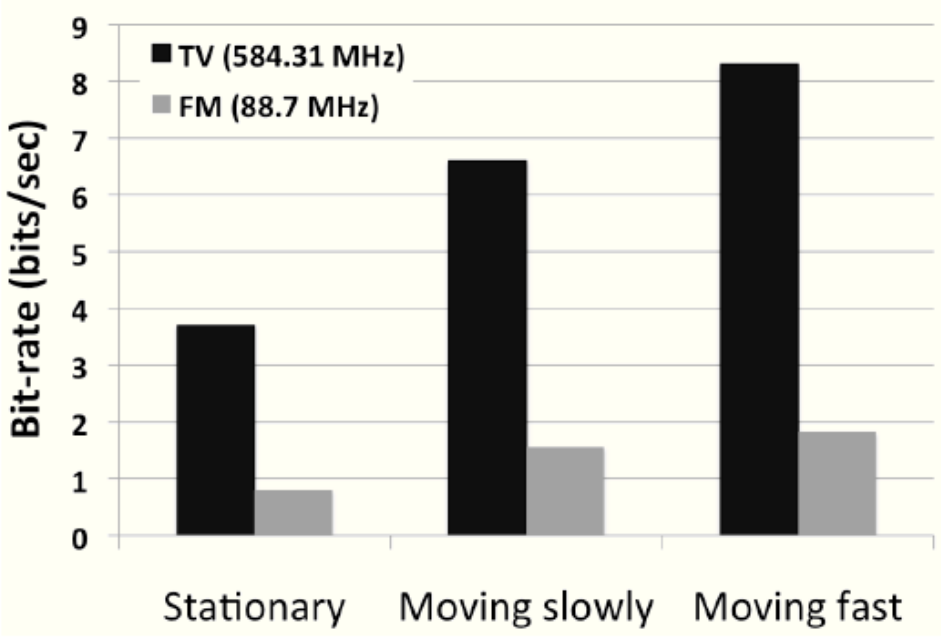
    Maximum … 1

    Minimum … 0



ProxiMate – Bit-rate

- Bit-rate limited
  - Wait long enough between two bits such that they are not correlated
- Bit errors occur and have to be corrected
  - Reduced effective bit-rate
- Improve Bit-rate
  - Use multiple radio stations simultaneously



ProxiMate – Results

- Pairing using 10 TV sources:
  - 3.3s at 2.4 cm distance
- Pairing using 10 FM sources:
  - 15s at 16.5 cm distance

- TV: ~600 MHz, ~50 cm wavelength
- FM: ~100 MHz, ~3 m wavelength

ProxiMate – Conclusion

+ Works reasonably fast in close distances
+ Pairing distance can be varied (using different radio channels)
+ Computationally lightweight

– Not yet applicable to todays devices

Conclusion

- Wi-Fi Time of Flight (by Capkun et al.)
  - + Potentially fastest
  - - Requires special-purpose hardware
- Amigo
  - + Can be implemented with standard Wi-Fi hardware
  - – Requires Wi-Fi communication
- ProxiMate
  - + Computationally cheap
  - – Requires more advanced radio interface

References

[1] MARCALETTI, Andreas, et al. Filtering Noisy 802.11 Time-of-Flight Ranging Measurements. In: *Proceedings of the 10th ACM International Conference on emerging Networking Experiments and Technologies*. ACM, 2014. S. 13-20.

[2] RASMUSSEN, Kasper Bonne; CAPKUN, Srdjan. Realization of RF Distance Bounding. In: *USENIX Security Symposium*. 2010. S. 389-402.

[3] VARSHAVSKY, Alex, et al. *Amigo: Proximity-based authentication of mobile devices*. Springer Berlin Heidelberg, 2007.

[4] MATHUR, Suhas, et al. Proximate: proximity-based secure pairing using ambient wireless signals. In: *Proceedings of the 9th international conference on Mobile systems, applications, and services*. ACM, 2011. S. 211-224.

Thank You

References

[5] http://crowdweaver.co.uk/2012/02/11/proximity-marketing-what-is-it/

[6] http://photo.elsoar.com/alarm-clocks-and-stopwatch-hot-colorful-images.html

[7] http://www.newgadget.org/mobile-phones/how-to-improve-your-phone-signal/

[8] http://www.naturapark.com.br/site/index.php/administradora/antcoletiva

[9] https://ibtx.wordpress.com/2015/01/06/wearables-time/

[10] http://www.connected-home.de/ratgeber/geraete-ins-heimnetz-einbinden-1472570.html

[11] http://how2mediate.com/2010/12/01/is-mediation-a-waste-of-time-2/

[12] http://www.hill2dot0.com/wiki/index.php?title=Frequency_modulation

[13] http://idmc.info/counter/22/amplitude-and-phase-spectrum-of-sine-wave