Secure Pairing of Wireless Devices by Multiple Antenna Diversity

Liang Cai

University of California, Davis

Joint work with Kai Zeng, Hao Chen, Prasant Mohapatra

Ubiquitous Wireless Devices

Most of these devices require ad-hoc connections!

Wi-Fi Direct

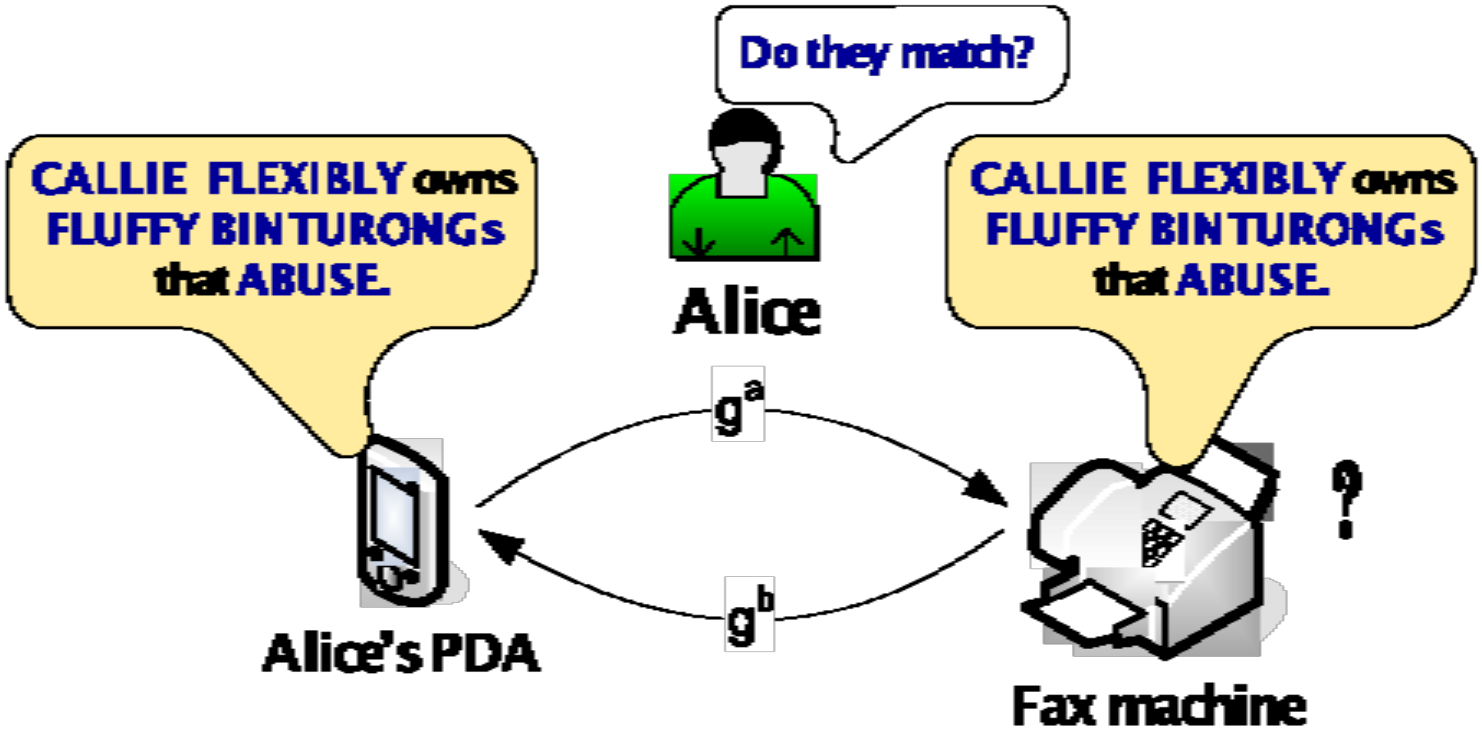
- Allows peer-to-peer Wi-Fi connection (without AP)
- Requires no new hardware
- Specification and certified devices are coming soon

Secure Device Pairing

- Bootstrap secure communication between two devices.
- Common approach: shared PIN code
- Problems
  - Many devices have no keyboard (so they hardcode secrets)
  - Potential user error and vulnerability
- Solution: using out-of-band (OOB) channels

Visual Channel (Seeing is Believing)

Acoustic Channel (Loud and Clear)



Motion Channel (Shake well before use)

Limitations of OOB Channels

- OOB channels are not ubiquitous on all devices
- Some OOB channels are vulnerable to attacks (Halevi etc. CCS ’10)

Desirable Device Pairing Scheme

- Use no out-of-band channel
- Does NOT require the user to
  - Enter secrets (simplify user tasks), or
  - Verify secrets (avoid user mistakes)

Our scheme: Good Neighbor

- Use the wireless channel
- Securely pair devices based on proximity

Why not using Distance-bounding Protocols

- Cryptographic protocol that allows verifier V to establish an upper bound on physical distance to a prover P.

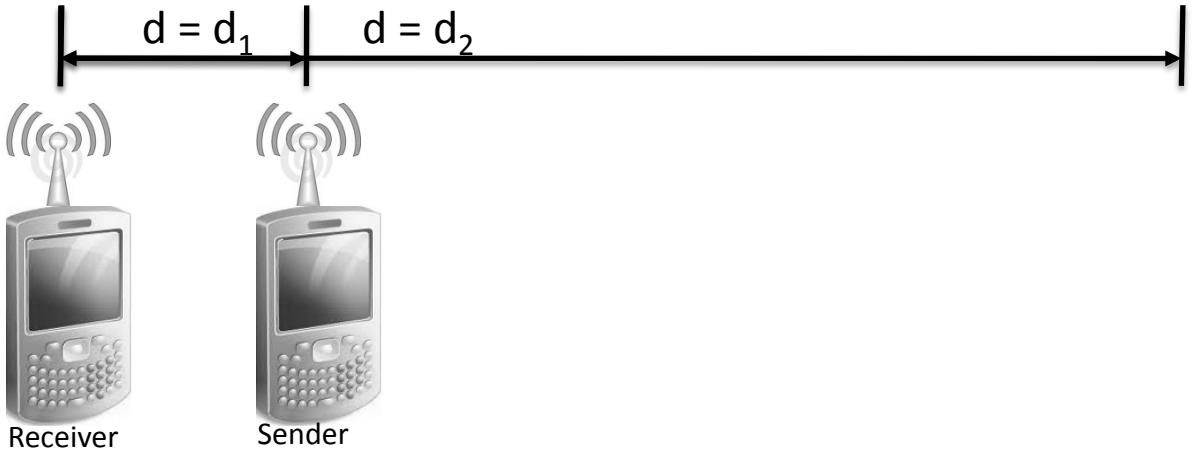
- Based on the fact that electro-magnetic waves travel nearly at the speed of light, but cannot travel faster
- Rely on a rapid bit exchange and require precise clocks to measure light-speed messages

Threat model

- Attackers can
  - Have powerful antennas
  - Have exact copies of the pairing devices
  - Know the exact location of the pairing devices
- Attackers can NOT
  - Come in close proximity of the receiver (Eg. less than 20cm).
  - Compromise the pairing devices.
  - Jam the channel

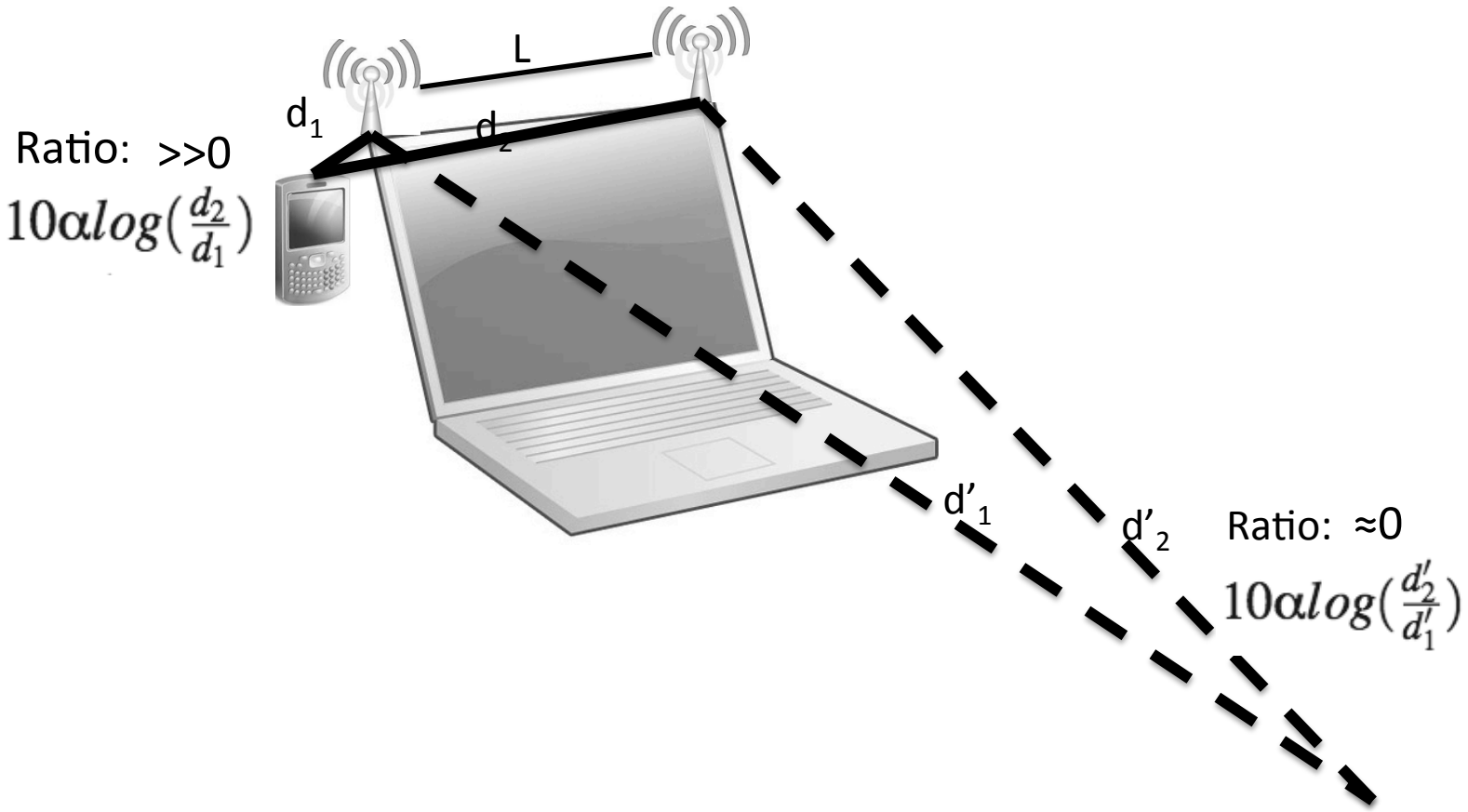
Naïve Approach: Inferring proximity by RSS

$$P_r[dBm] = P_0 - 10\alpha log(\frac{d}{d_0}) + X_\sigma$$

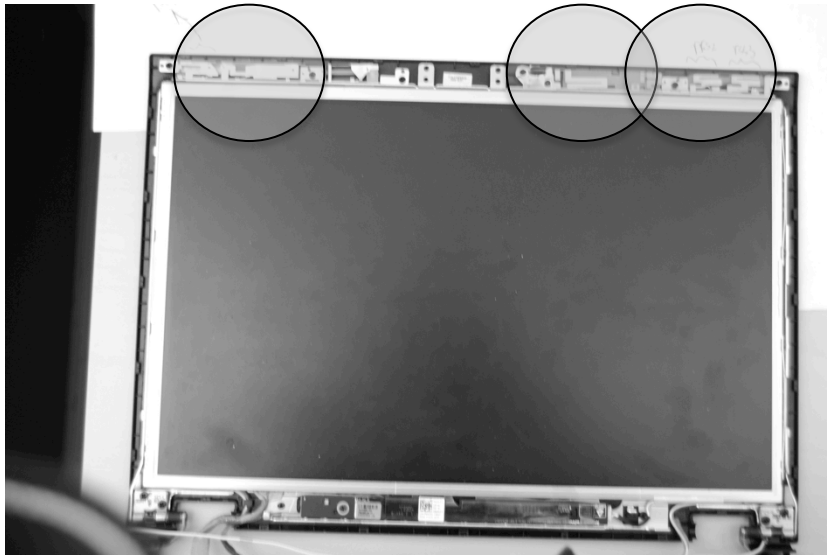


Changing P_0

Improvement: Inferring proximity by RSS ratio

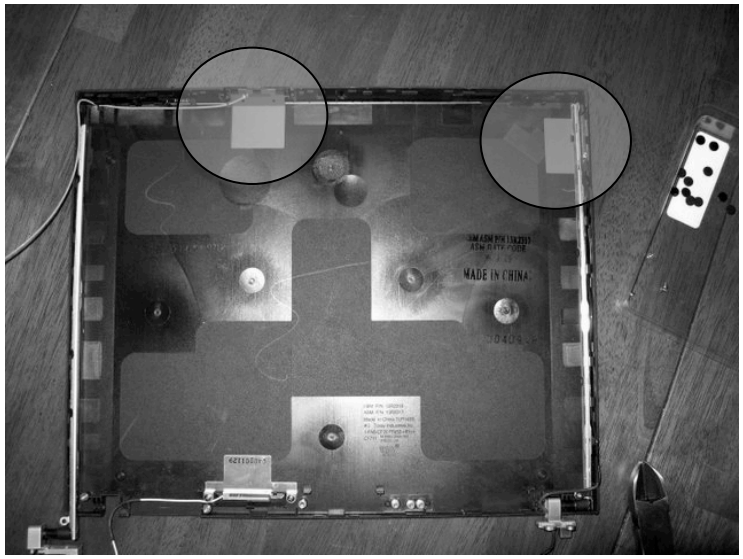


Antenna Diversity and IEEE 802.11n MIMO



Dell e5400 (MIMO antennas)

- MIMO
- Spatial multiplexing (From 54Mbps to 600 Mbps)



IBM T42P (Antennas diversity)

- Spatial diversity: to improve the quality and reliability of a wireless link

Practical Problem: Unstable RSS Values

- Problem:
  - RSS values may fluctuate
- Solution:
  - Sender (S) sends a series of packets
  - Receiver (R) calculates the mean and deviation of the RSS values

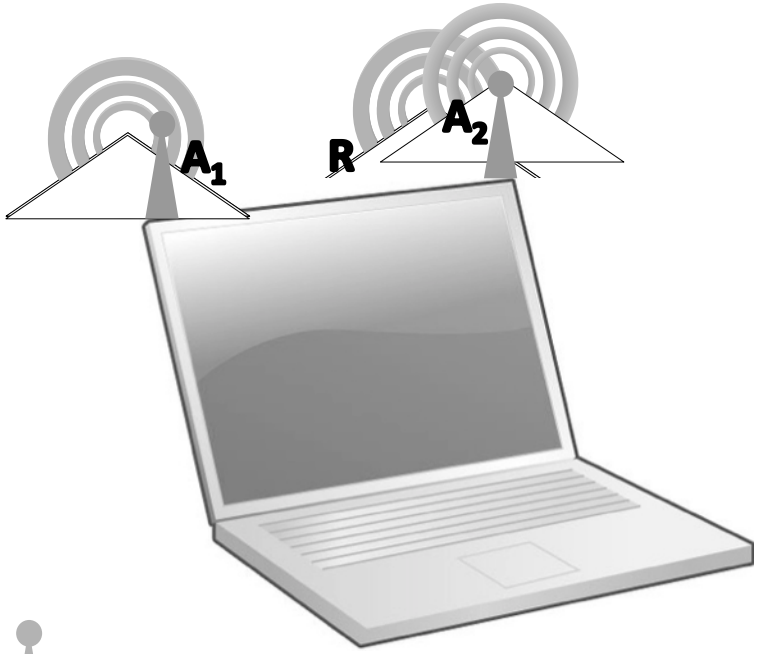
Practical Problem: RSS saturation

- Problem:
  - RSS value saturates when the signal is too strong or too weak.
- Solution: (power probing)
  - S sends probing packets with different transmission power levels
  - R chooses the optimal power level that results in the largest RSS ratio

Practical Problem: Automatic Rate Adaptation

- Problem:
  - Inconsistent RSS values if the Automatic Rate Adaptation feature is enabled.
- Solution:
  - Disable Automatic Rate Adaptation.

Final scheme



S R

Move S close to A_1 of R

AuthRequest()

AuthResponse(K_R)

PowerQuery(l,n)

PowerResponse(l)

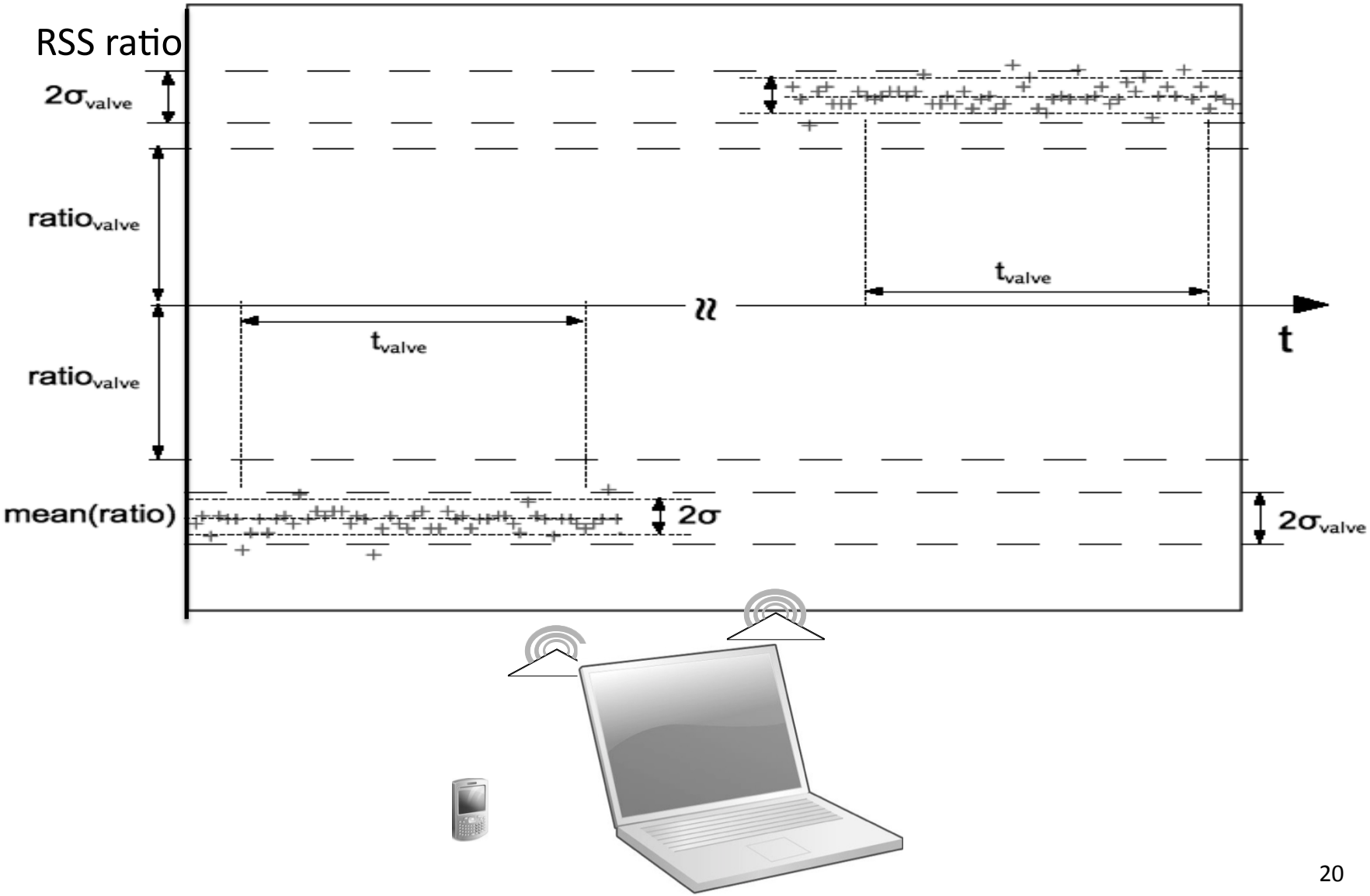
RSSMeasure(E_{KR}(k))

Move S close to A_2 of R

RSSMeasure(E_{KR}(k))

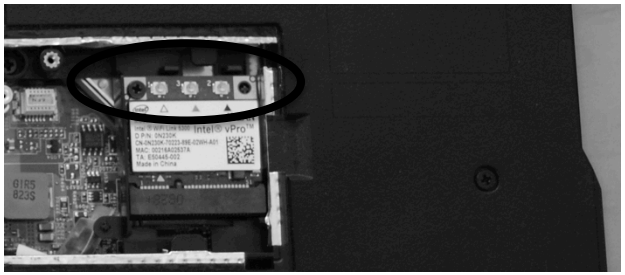
Success()

Typical RSS ratio of successful device pairing



Antennas used in our experiments

Type 1: internal antennas for Dell E5400 laptop

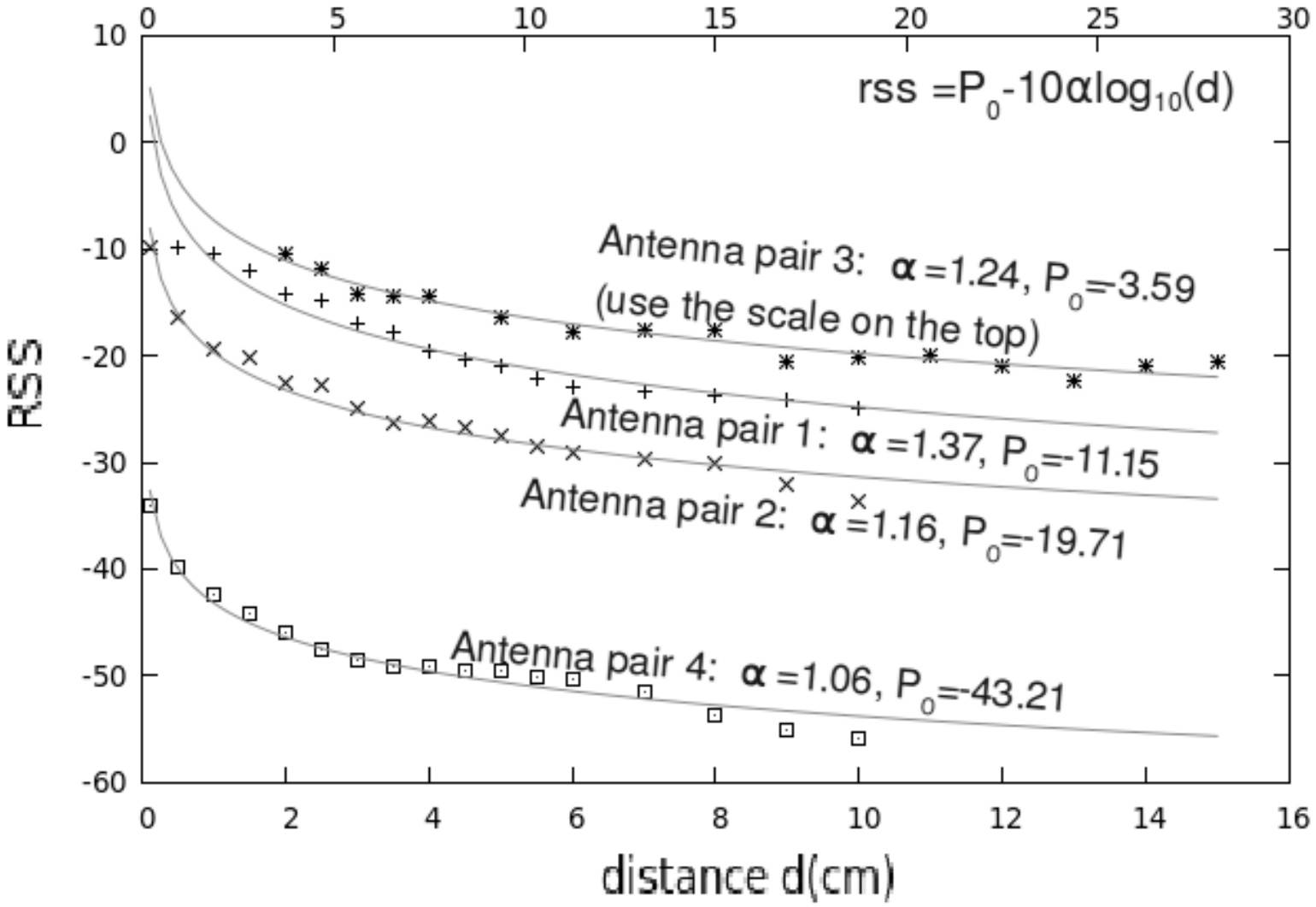


Type 4: Dipole antenna

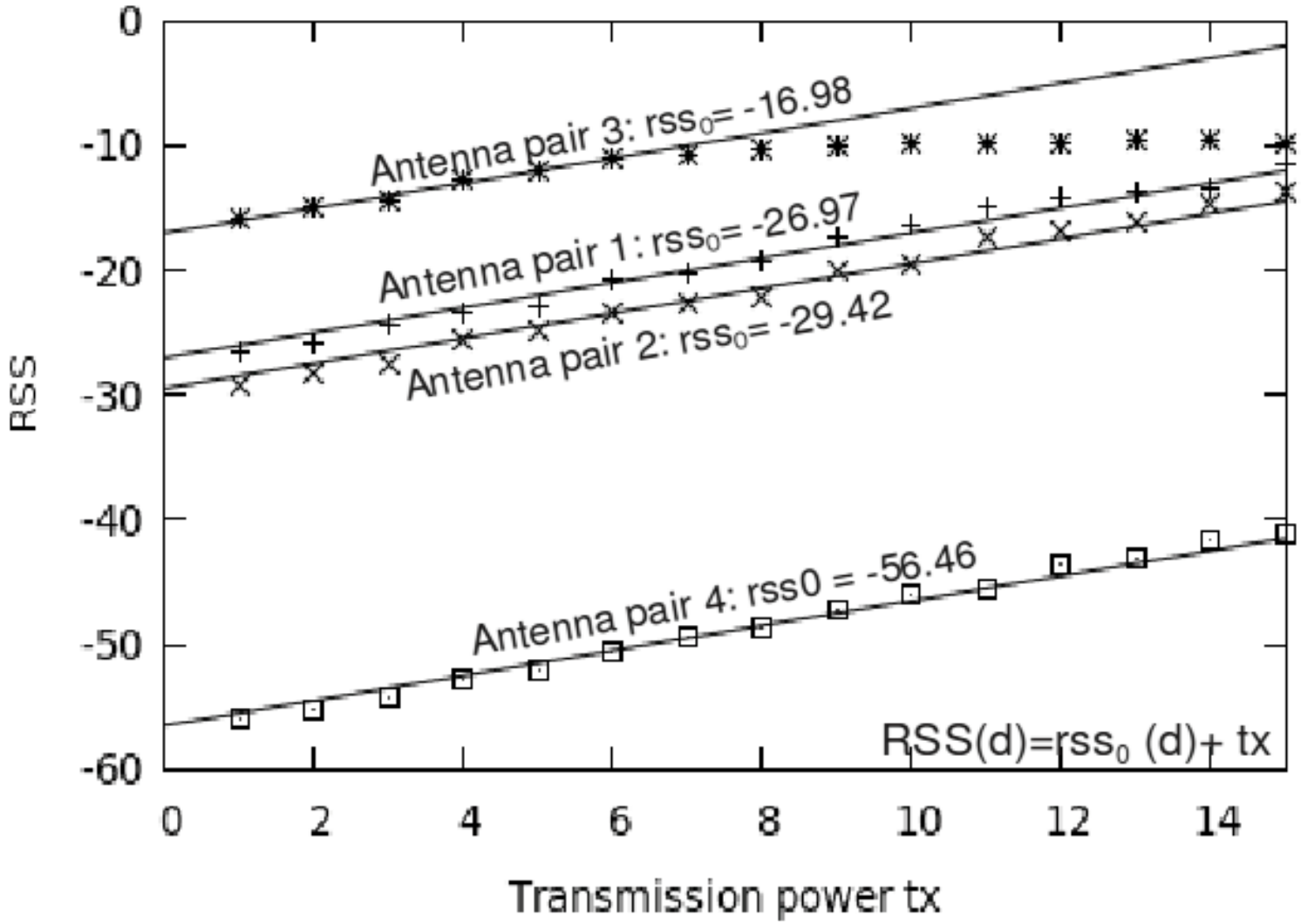
Type 2: antennas for laptop mini PCI cards

Type 3: RP-SMA (f) socket

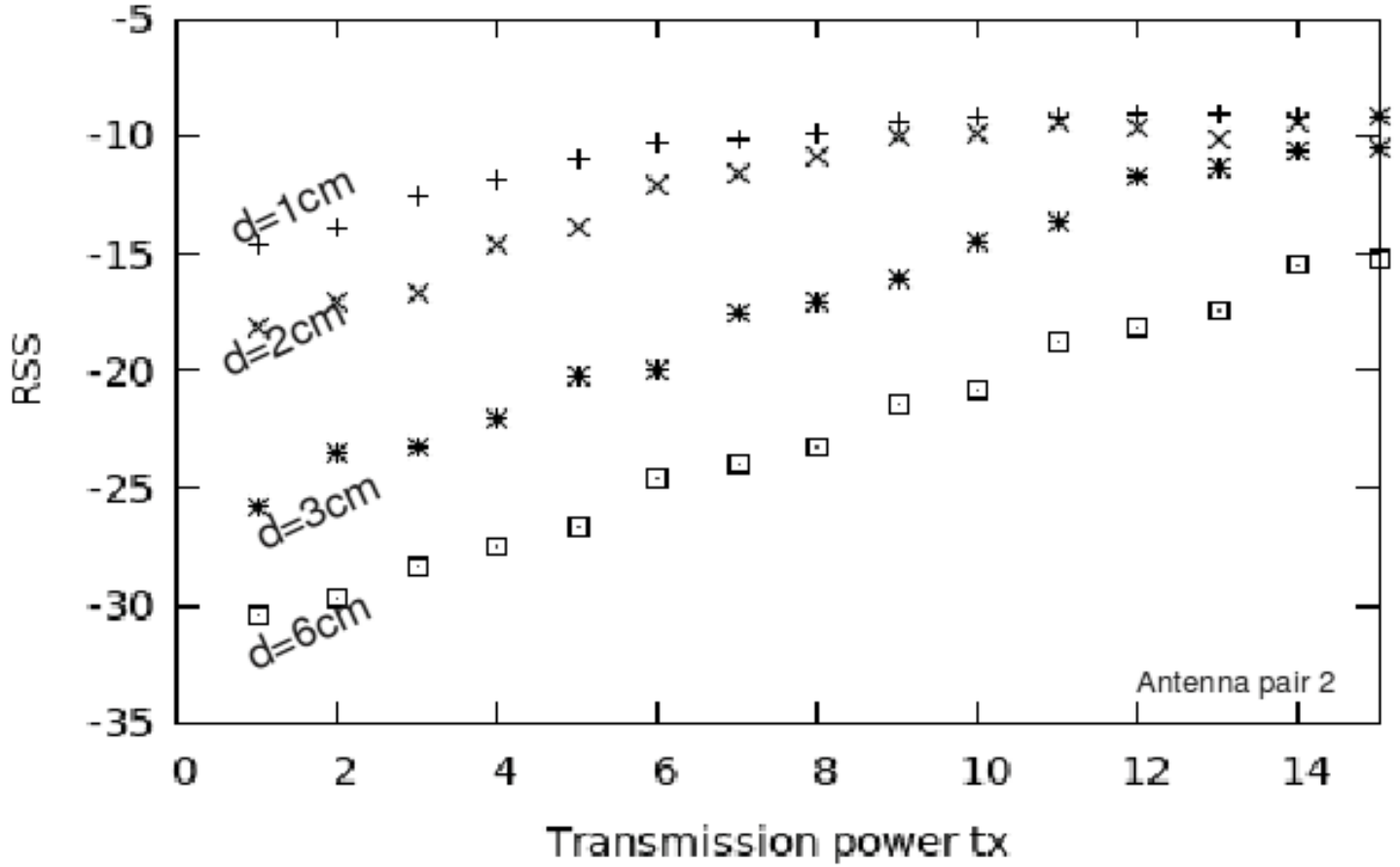
Logarithmic relationship between RSS value and the sender-receiver distance



Linear relationship between RSS value and the transmission power



RSS saturation is observed when the distance decreases



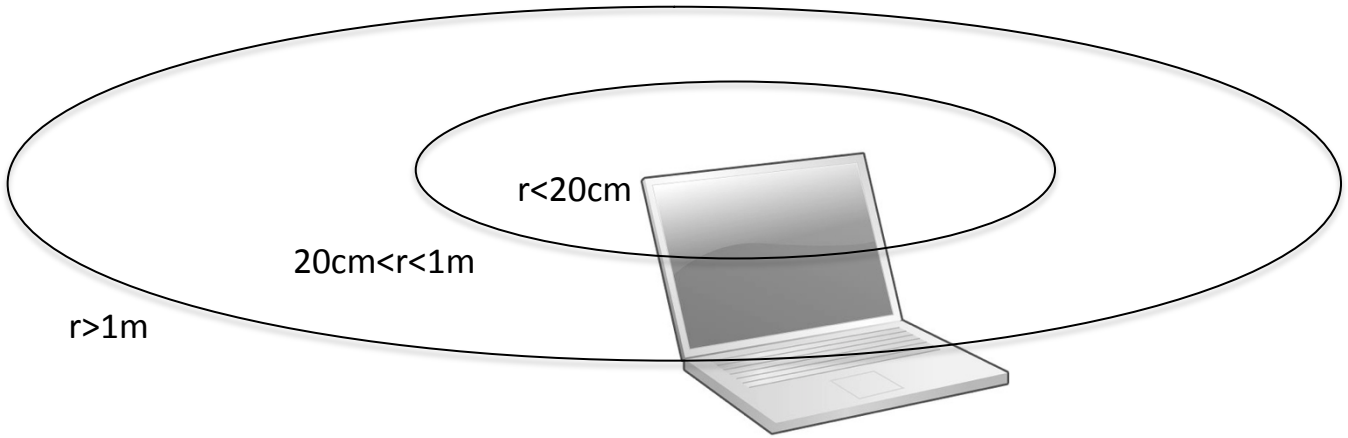
Prototype

Receiver


Sender

- Modify the driver to export RSS values seperately
- Threshold setting:
  - $r_H = -r_L = 11$
  - $\sigma_{valve} = 0.6$
  - $T_{valve} = 1s$

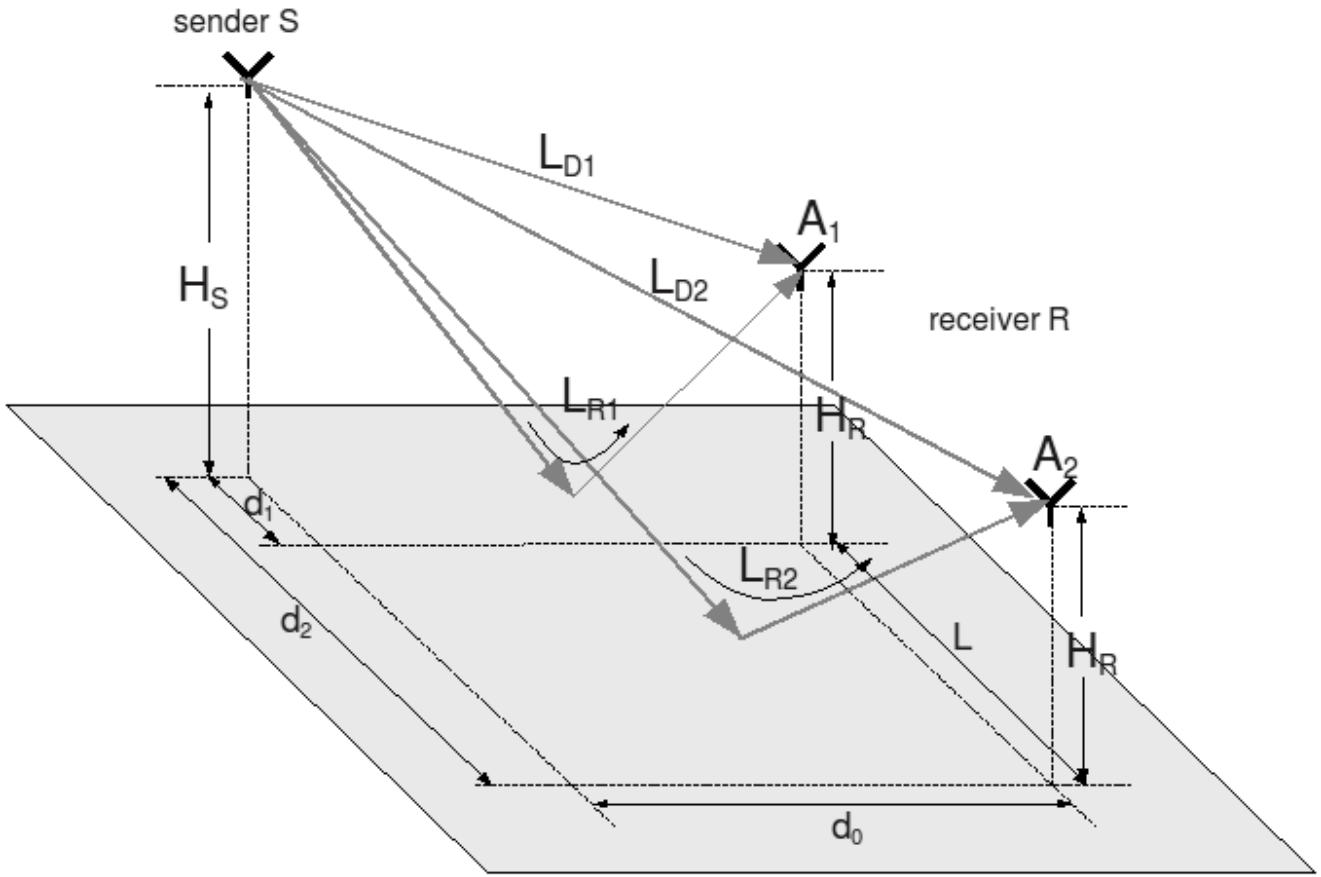
Prototype



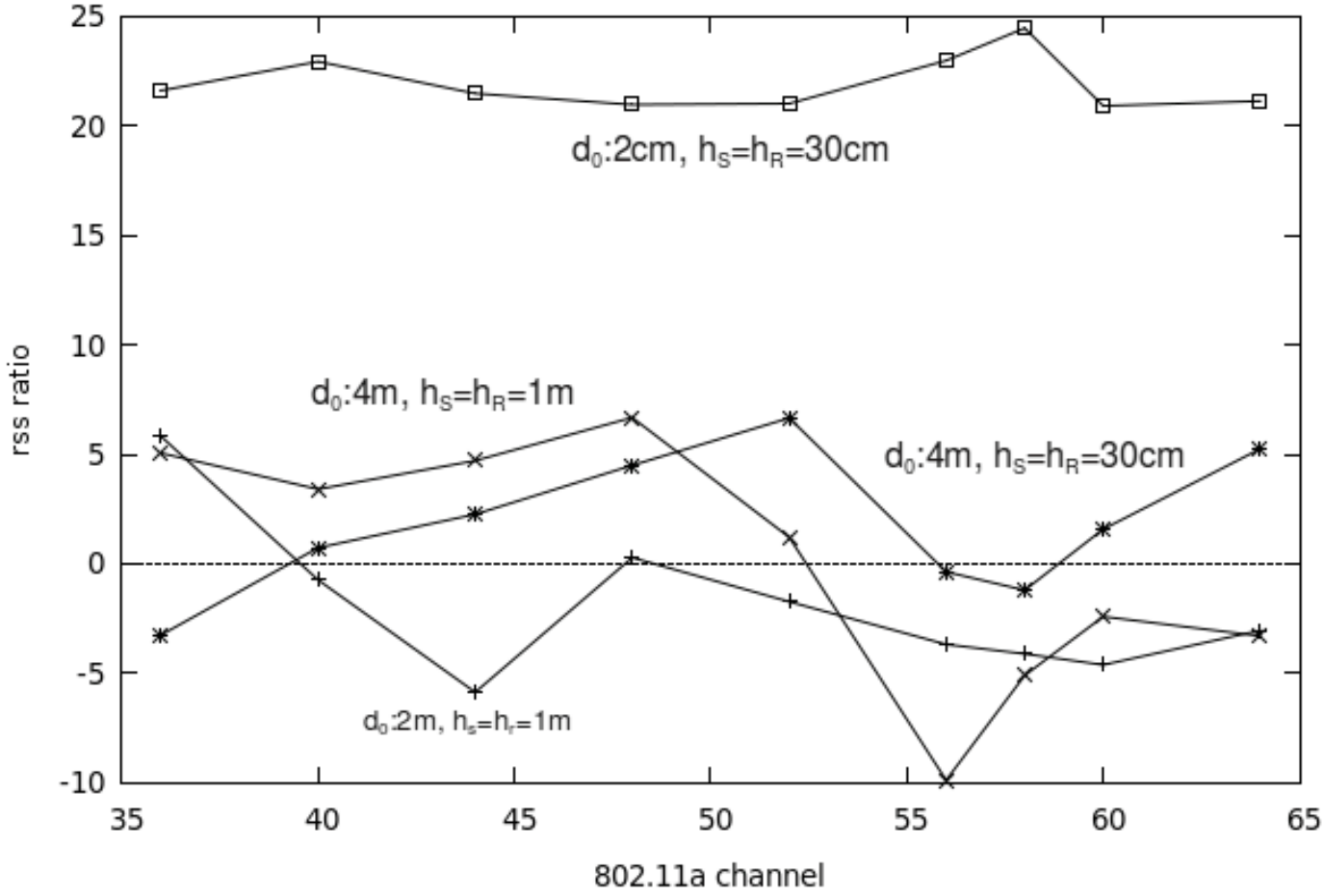
Distance range	$< 20cm$	$[20cm, 100cm]$	$> 100cm$
Success Rage	90%	0%	0%
Failure Rate	10%	100%	100%
Max Mean RSS Ratio	15.62	6.35	3.43

Potential Attack using Multipath Effect

- Attacker may exploit multipath effect to find faraway locations that cause large RSS ratios

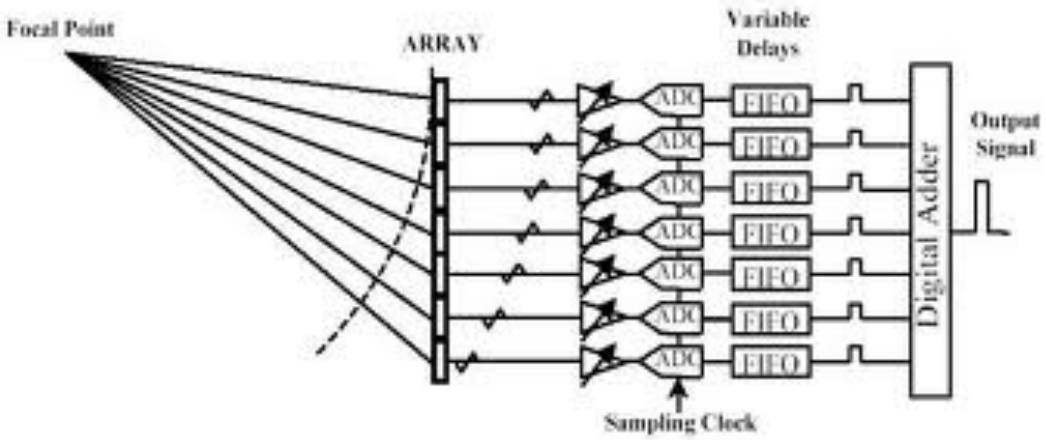


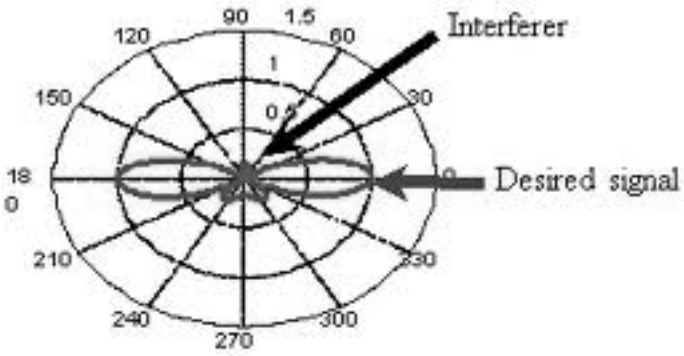
Mitigating with Frequency hopping



Potential Attack using Beam Forming

- Risk: Attackers may form a beam of signal with an antenna array
- Attackers need a very large antenna array (**size of hundreds of meters when L=20cm, d>10m**)





Future works

- Mutual authentication
- Apply our scheme to Bluetooth
- Applications that requires Near Field Communication

Conclusion

- A novel device-pairing scheme
  - Based on proximity
  - Requires no Out-of-Band Channel
  - Requires no user input or verification