April 25th, 2012

# Two-Way Wireless


## Amir K. Khandani

M.Sc. Tehran University, Ph.D. McGill University

Canada Research Chair

RIM-NSERC Industrial Research Chair

E&CE Department, University of Waterloo

khandani@uwaterloo.ca, 519-8851211 ext 35324


Ontario

Ontario Centres of Excellence

Canada Foundation for Innovation
Fondation canadienne pour l'innovation

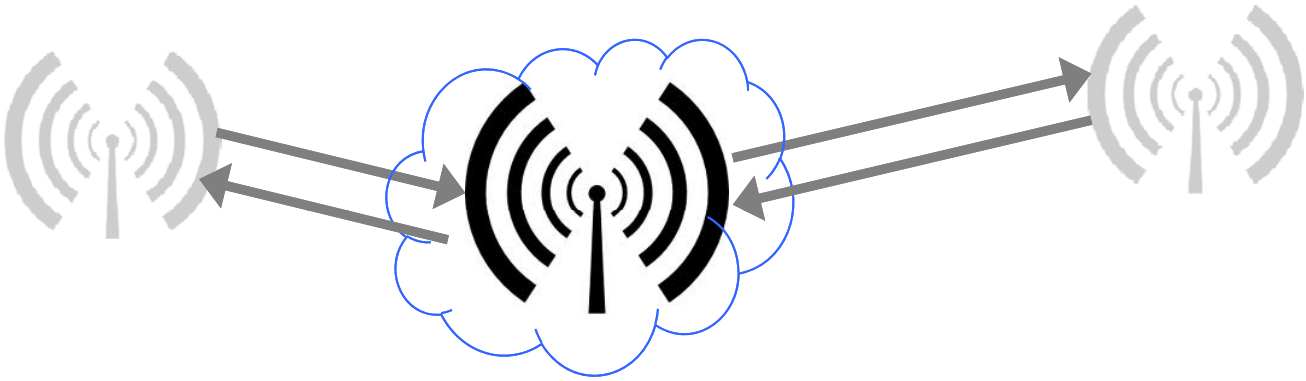
Canada Research Chairs

NSERC CRSNG

UNIVERSITY OF Waterloo

# Outline

# Introduction:
## Review of Main Objectives



- Establishing two-way wireless links with complete overlap in ***time*** and ***frequency***, with support for:
  - Half-duplex clients, as well as full-duplex clients
  - Asynchronous clients (joining without prior coordination)
  - Multiple-Input Multiple-Output (MIMO) antenna systems.

# Motivation

- Current wireless systems are one-way:
  - **Time Division Duplex**: Either talk or listen (walkie-talkie approach)
  - **Frequency Division Duplex:** Use two different bands to talk/listen
  - There is not even two-way OFDMA, nor two-way CDMA.
- Two-way wireless is theoretically possible, but complicated due to large amount of self interference.
- Two-way communications is used in ordinary phones, DSL, wireless with highly directional antennas, free space optics, and fiber.
- Impact on wireless networks (e.g., cellular, WLAN) is expected to be higher than above earlier applications.
  - Addresses networking and security issues, in addition to doubling the rate.

# A Brief Literature Survey

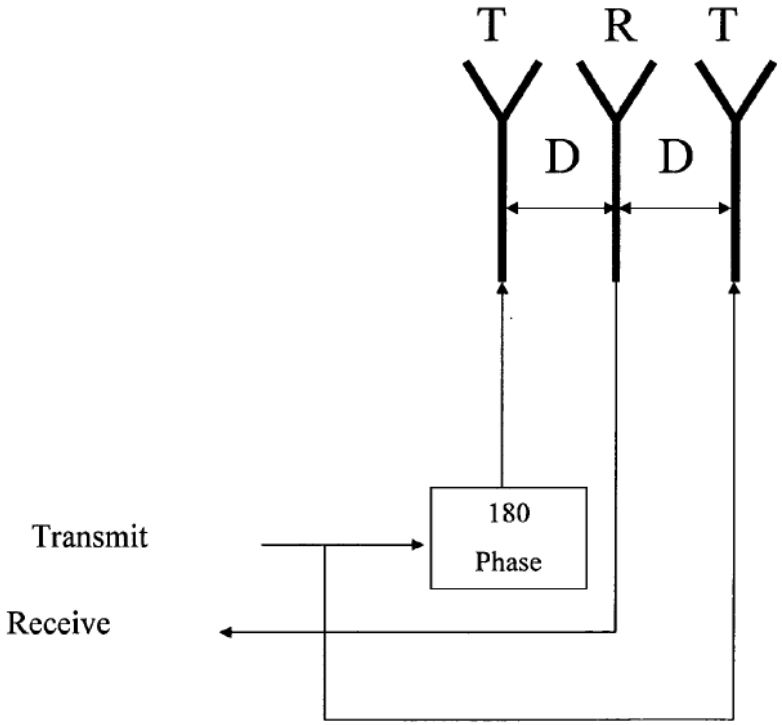
1. K. Tsubouchi, H. Nakase, A. Namba, K. Masu, "Full duplex transmission operation of a 2.45-GHz asynchronous spread spectrum using a SAW convolver", *IEEE Transactions on Ultrasonics, Ferroelectrics and Frequency Control*, **Sept. 1993** (Res. Inst. of Electr. Commun., Tohoku Univ., Japan)
   - Uses different CDMA codes in each directions, single antenna
2. S. Chen, M. A. Beach, J.P. McGeehan, "Division-free duplex for wireless applications," Electronics Letters, **Jan. 1998**, (Centre for Commun. Res., Bristol Univ.)
   - First true full duplex, separate TX and RX antennas
3. Amir K. Khandani, "Methods for spatial multiplexing of wireless two-way channels," US patent, filed Oct. 2006 (provisional patent filed **Oct. 2005**), issued **Oct. 2010**
   - Analog cancellation using multiple antennas
4. B. Radunovic, D. Gunawardena, P. Key, A. Proutiere, N. Singh, V. Balan, G. Dejean, "Rethinking Indoor Wireless: Low Power, Low Frequency, Full-duplex, "Microsoft Technical Report MSR-TR-2009-148", **July 2009**
   - Analog cancellation using noise cancelling chip Quellan QHx220
5. M. Duarte and A. Sabharwal, "Full-Duplex Wireless Communications Using Off-The-Shelf Radios: Feasibility and First Results", *Asilomar Conference on Signals, Systems, and Computers,* **Nov. 2010** (plus three more references from the same team to follow)
   - Analog active cancellation
6. J. Choiy, M. Jainy, K. Srinivasany, P. Levis, S. Katti, "Achieving Single Channel, Full Duplex Wireless Communication," *Mobicom 20*10, **Sept. 2010**
   - Based on antenna setup first introduced in speaker's patent above - Analog cancellation using noise cancelling chip Quellan QHx220
7. Announcement by Stanford University (**Feb. 2011**): http://www.youtube.com/watch?v=RiQb5NdDWgk
   - Based on the setup in reference 6 above and reference 11 (see next page)
8. Announcements by Rice University (**Sept. 2011**): http://www.youtube.com/watch?v=tXMwn2mm0VY
   - Based on the setup in reference 5 above and references 9,10,12 (see next page)

# A Brief Literature Survey (cont.)


9. A. Sahai, G. Patel and A. Sabharwal, "Pushing the Limits of Full-duplex: Design and Real-time Implementation", *Rice tech report,* **Feb. 2011**
10. M. Duarte, C. Dick and A. Sabharwal, "Experimental-driven Characterization of, “Full-Duplex Wireless Systems", submitted to IEEE Transactions on Wireless Communications, **June 2011**
11. M. Jain, J. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, P. Sinha, "Practical, Real-time, Full-Duplex Wireless", *Mobicom,* **Sept. 2011**
12. E. Everett, M. Duarte, C. Dick, and A. Sabharwal, "Exploiting Directional Diversity in Full-duplex Communications", *Asilomar Conference,* **Nov. 2011**


- ***300+ more references (articles and patents) on full duplex wireless, active cancellation, etc., with no overlap with the work presented here.***

# What is New w.r.t. Speaker's Issued Patent?



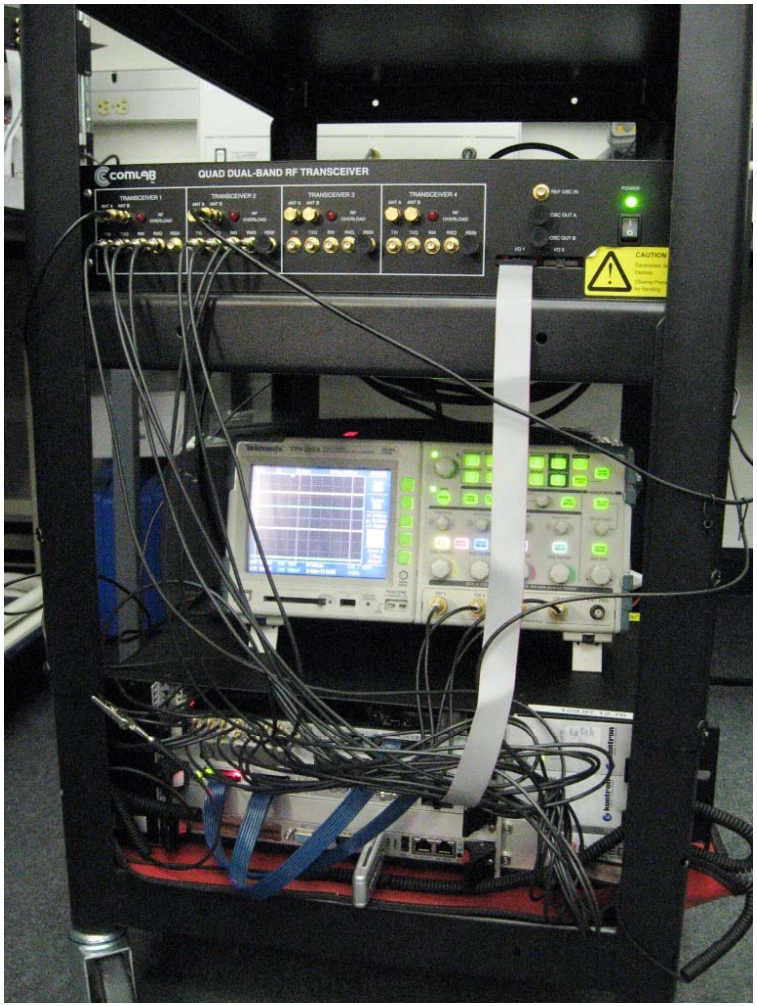

- New methods for antenna design
- New RF and base-band processing brings degradation in SNR due to self-interference close to zero.
- Support for asynchronous clients (superimposed networking)
- Support for MIMO
- New applications for full-duplex wireless
- Hardware, RF and DSP complexities are virtually the same as half-duplex units.

**Figure extracted from speaker's patent issued in 2010 – same antenna setup reported in references 6 (Sept 2010) and 7 (Feb. 2011)**

**United States Patent**
**Khandani**

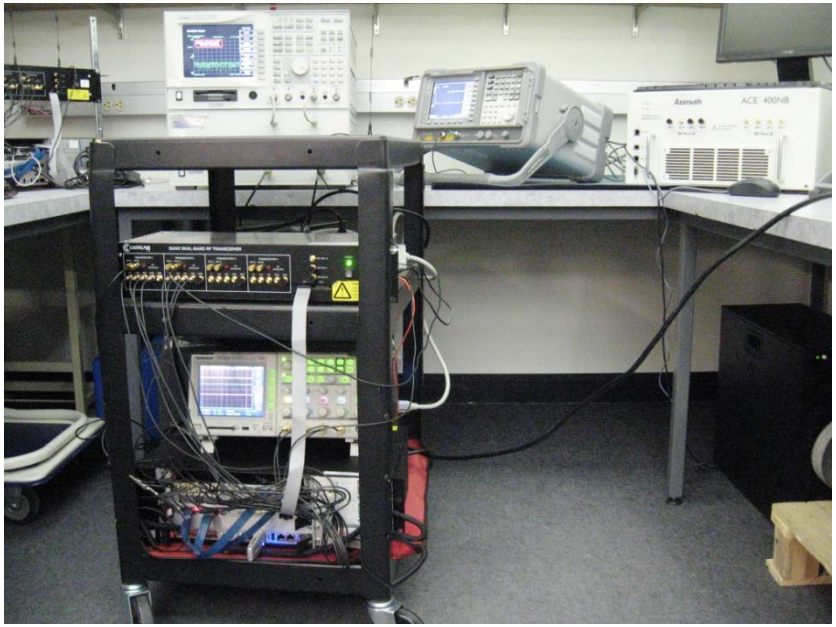
**Patent No.: US 7,817,641 B1**
**Date of Patent: Oct. 19, 2010**

# Hardware Implementation



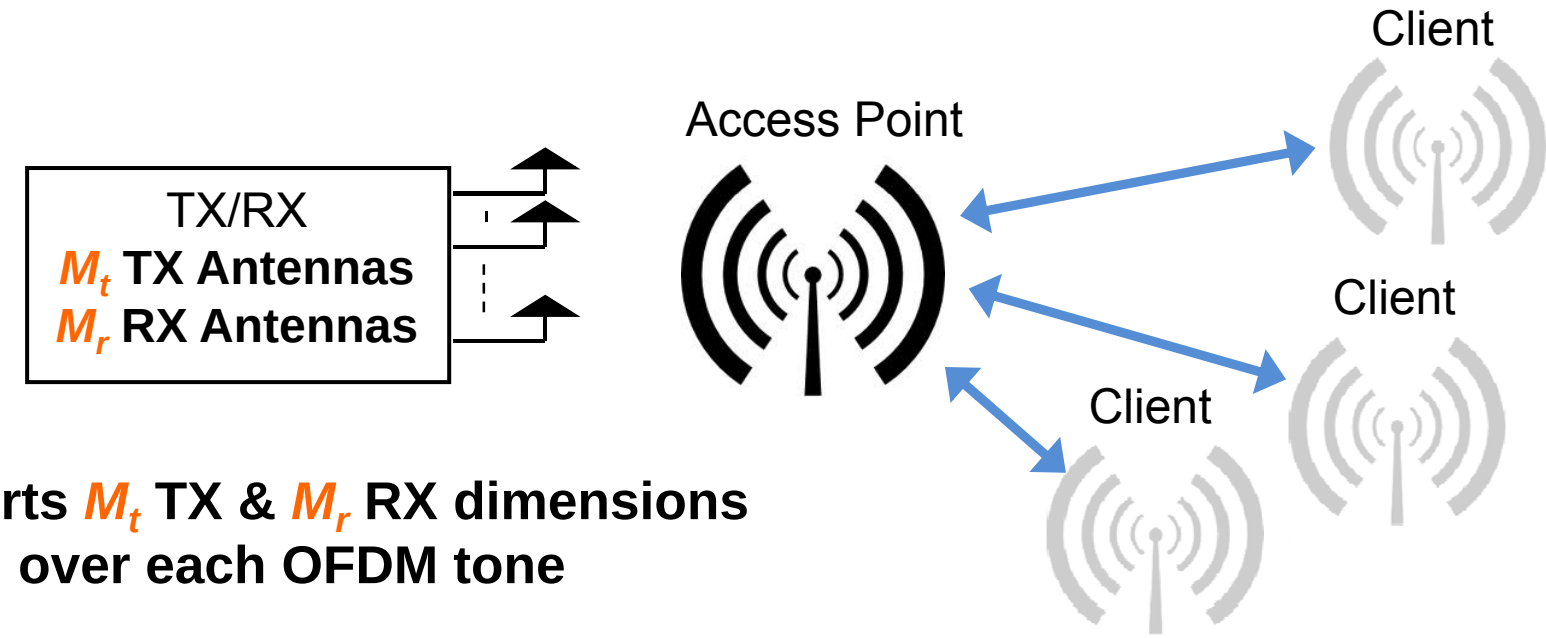

- Radio: 802.11
  - 20Mhz bandwidth @ 2.4Ghz ISM band, 64 tone OFDM, transmission power of 30dBm.
  - Similar results were obtained for the 5Ghz ISM band.
- Hardware:
  - Lyrtech Software defined radio platform, off-the-shelf components made for 802.11, no strict requirement on size, complexity, accuracy

# Hardware Implementation



- Implementation on Lyrtech software defined radio platform (real-time on DSP/FPGA).
- Tested in outdoor & (harsh) indoor environments
  - Works as reliably as a one-way system in similar conditions

# Basic Setup (User Multiplexing)




**Supports $M_t$ TX & $M_r$ RX dimensions over each OFDM tone**

- Divide OFDM tones among several clients (i.e., OFDMA) with two-way communications over each tone
  - Simple/small antennas, simple signal processing, off-the-shelf hardware
  - Support for MIMO in each tone
  - Clients do not need to be synchronized
  - **Clients do not require to have full-duplex capability**

# Benefits

- A paradigm shift in wireless networking:
  - Efficiency of WiFi is around 5%-10% due to its MAC.
  - Cellular networks have a higher efficiency, but at the cost of an expensive infrastructure.
    - Too expensive as we move towards smaller and smaller cells
  - Significant impact on security
  - Doubling Band-width with lower complexity than MIMO
- Likely to have a higher impact than Turbo-code, MIMO, SDMA, IA, as it impacts networking and security issues.
- Two-way wireless channel is different, and in many applications more powerful than two one-way channels.

# Contributions*

1. Interference mitigation in analog domain:
   - Antenna design, Signal injection/Corrective beam-forming
2. Complementary stages of digital signal processing:
   - Interference removal, Signal reconstruction
   - Handling asynchronous clients
3. Application of two-way wireless:
   - Media-based wireless: a new paradigm in connectivity
   - Facilitating multi-node co-operative communications
     - SDMA in both uplink and down-link
     - Interference Cancellation in two neighboring nodes
   - Facilitating MAC and QoS requirements
   - Security enhancement
   - Secret key generation
   - Higher rate in a point-to-point link by better synchronization,
   - improving ARQ, Adaptive Coding and Modulation, Power Control, etc)
4. (by my team): Implementation, and extensive measurements.

* Ideas and algorithms throughout this work are speaker's contributions. He is sole inventor on patents, and following UW IP policy 73, owner of the IP. Negotiations for IP commercialization involve only the speaker.

# History of this Work

- Basic hardware implementation functional in late 2009
- Avoid publicizing due to:
  - Aiming for  a stronger impact by a more mature system
    - Earlier reported designs in 1990 were forgotten as the solution did not meet industrial standards, they generally have a very limited functionality in terms of error performance, band-width, etc., and need a controlled/laboratory environment to establish even the basic connection, and consequently are far from what industry needs.
  - IP protection of different aspects
- Why Now?
  - It is mature:
    - Cannot be moved forward (at least not fast enough) without industry's involvement and wider academic research.
  - Academic duty:
    - Knowledge sharing to avoid rediscoveries.

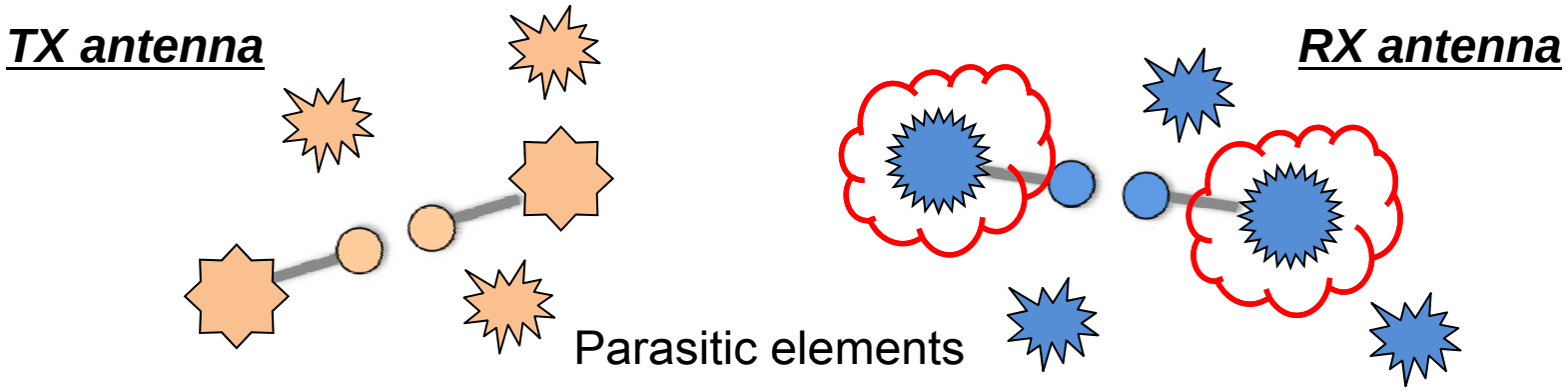
# Acknowledgments


- Implementation Team:
  - R. Hernandez, M. Baratvand, H. Attia
- Generous and visionary financial support from:
  - Salaries:
    - Ontario Ministry of Research & Innovation (ORF-RE)
    - Natural Sciences & Eng. Research Council of Canada (NSERC Strategic & NSERC Discovery)
    - Canada Research Chair Program
  - Equipment:
    - Canada Foundation for Innovation (CFI)
    - Ontario Ministry Research & Innovation (ORF-RI)
- UW general support and liberal IP policy

# First Stage of RF Cancellation: Antenna Design

# Objective in Antenna Design

- First part: separate antennas are used for TX & RX.




- **Small $S_{12}$= $S_{21}$**: A sinusoid at terminals of one antenna should induce a low (ideally zero) signal at terminals of the other one.
  - This should be the case over a large frequency range.
- **Small $S_{11}$& $S_{22}$:** Good radiation/reception

# Remarks

- Low coupling requirement in two-way wireless is different from that of MIMO.
- Low Coupling in MIMO:
  - Antenna gains to a distant antenna should be independent of each other.
  - Hard to satisfy in antennas are very close.
- Low Coupling in Two-way Wireless:
  - TX and RX antennas in a given unit should not induce a strong signal on each other.
  - **No obvious restriction on antenna separation**

# Starting Point

- Near field works to our advantage:
  - Strong but predictable, and as a result, totally manageable
- Maxwell equations indicate:
  - Linearity
  - **Geometrical symmetry** in:
    - Construct (shape, material, boundary conditions), and
    - Excitation (antenna feed terminals)

    cause **geometrical symmetry** in wave.
  - Symmetry in wave can be used to cancel signals.

# Maxwell Equations for a Single Frequency

- Linearity: A sinusoidal excitation results in a sinusoidal field of the same frequency at a point of interest (unless the system does not radiate/dissipate energy).
- Field equations for a single frequency $\omega$:

$$\nabla \times D = -j\omega B$$

$$\nabla \times B = J + j\omega D$$

$$\nabla \circ D = \rho$$

$$\nabla \circ B = 0$$

$D$: Electric Field (*E*-Field)

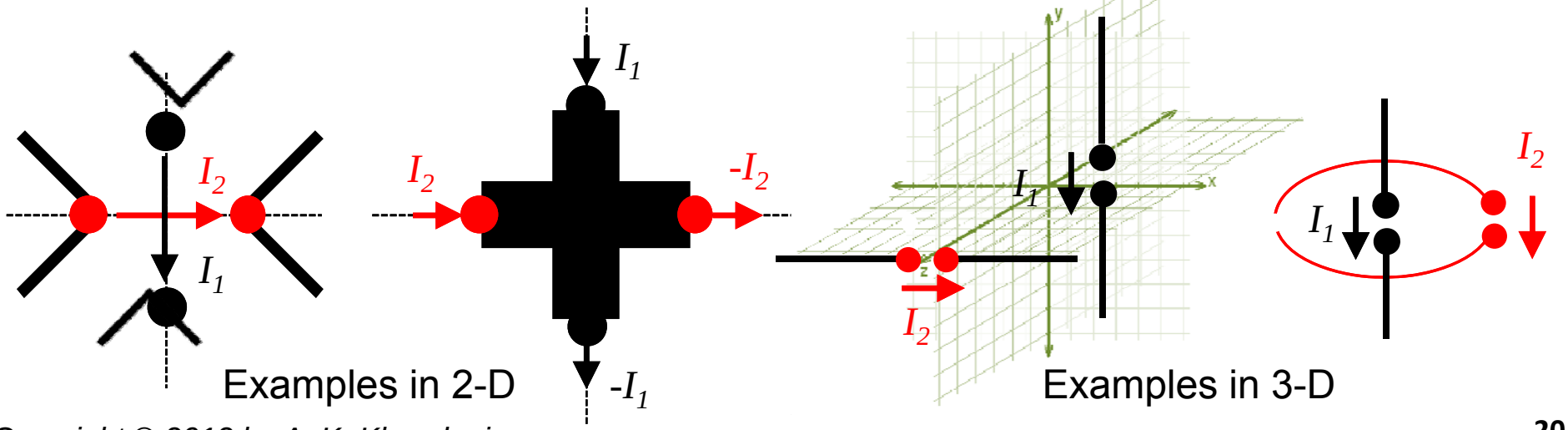
$B$: Magnetic Field (*M*-field)

$J$: Current

$\omega$: Frequency

# *Pair-wise Symmetrical* Antennas

- Each antenna is *Self Symmetrical*:
  - Two arms are image of each other with respect to a plane of symmetry (construct & excitation).
  - Note that arms can overlap (applicable to patch structures).
- Two antennas are *Mutually Symmetrical*:
  - Antennas have separate planes of symmetry, and are invariant under reflection in the plane of symmetry of each other.

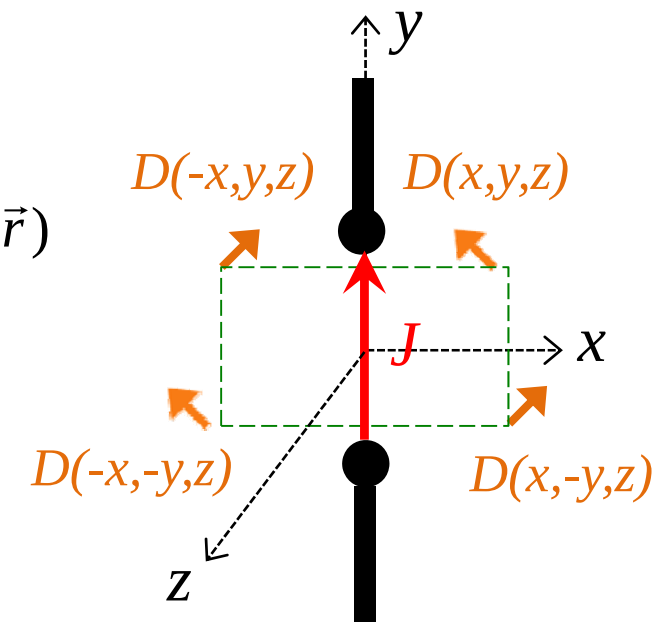


# Effect of Symmetry

- For a symmetrical antenna, we have:

  ***Theorem 1:*** *F*ield components (E & H) are invariant under any symmetry which does not change direction of the TX input current, and are invariant with sign change under a symmetry which changes the direction of the TX input current.

$$\nabla \times D(\vec{r}) = -j\omega B(\vec{r})$$
$$\nabla \times B(\vec{r}) = J + j\omega\varepsilon D(\vec{r})$$
$$\nabla \cdot D(\vec{r}) = \rho(\vec{r})$$
$$\nabla \cdot B(\vec{r}) = 0$$
$$\vec{r} = (x, y, z)$$




$x \rightarrow -x$ Does not Flips $J$

$y \rightarrow -y$ Flips $J$

$z \rightarrow -z$ Does not flip $J$

# Effect of Symmetry

- For pair-wise symmetrical TX/RX, we have:

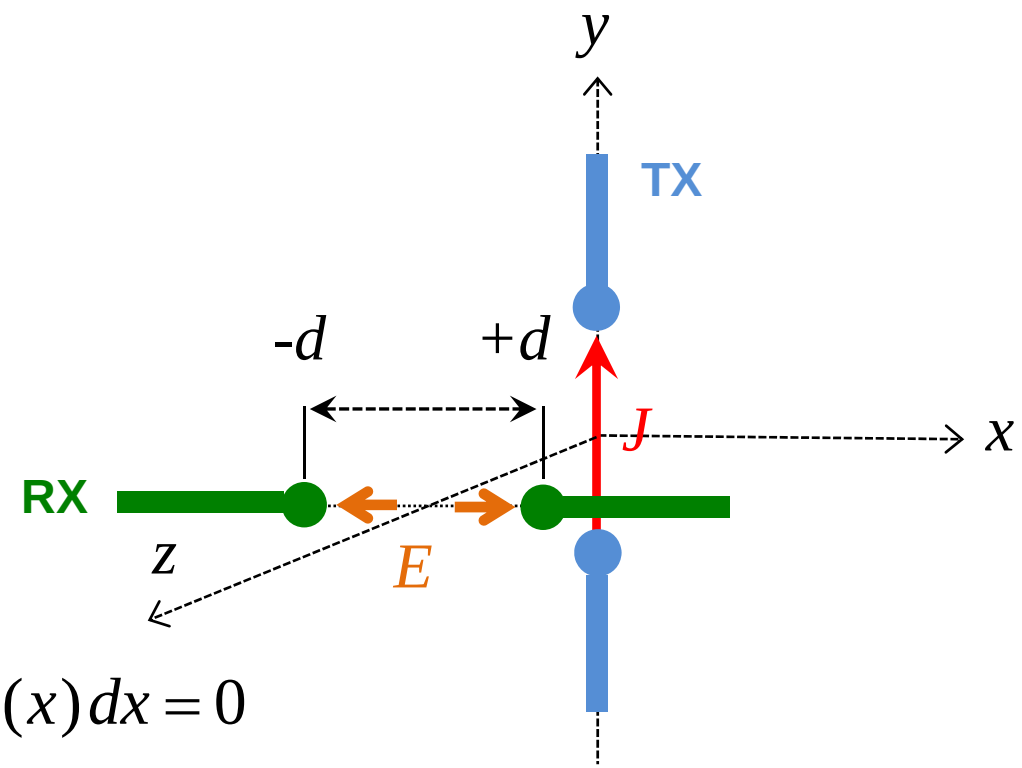
  ***Theorem 2:*** $S_{12}= S_{21}= 0$ independent of frequency.

  ***Proof****:* Follows relying on *Theorem* 1 and integrating *E*-field over the line connecting the terminal of the RX antenna.

$x \longrightarrow -x$ Does not Flips $J$

$y \longrightarrow -y$ Flips $J$

$z \longrightarrow -z$ Does not flip $J$

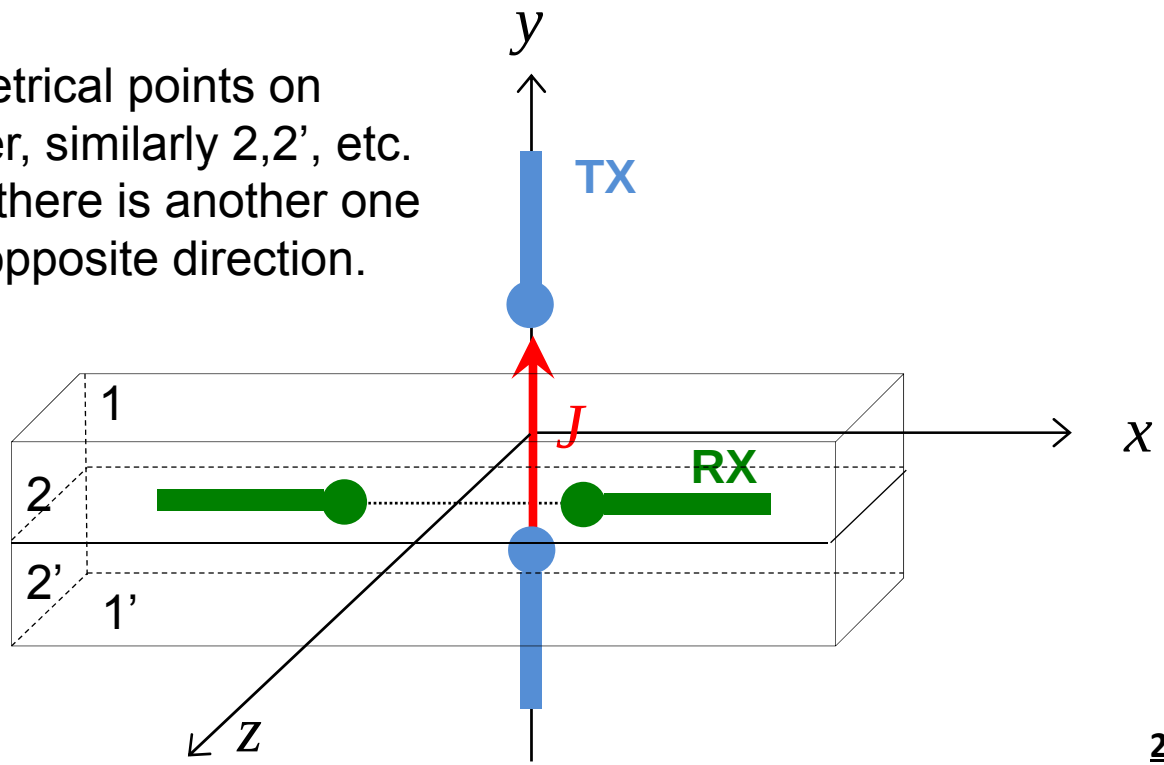



$$E(x) = -E(-x) \Rightarrow \Delta V = \int_{-d}^{+d} E(x)\,dx = 0$$

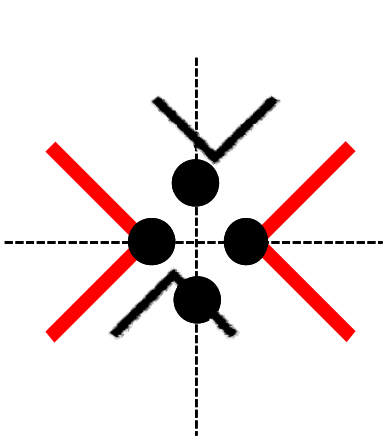
# A More Rigorous Proof

- Applying Poynting's theorem to a symmetrical surface (symmetrical with respect to the plane of symmetry of TX antenna) surrounding the RX antenna predicts zero energy flow.

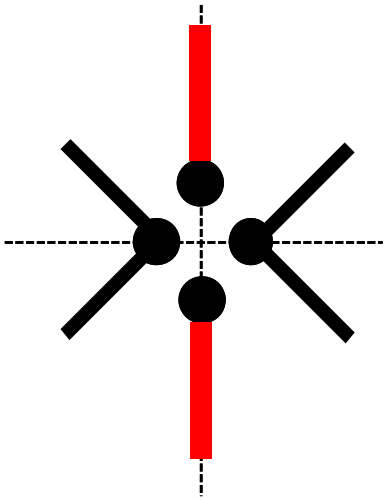
- Poynting's vectors on symmetrical points on surface 1,1' cancel each other, similarly 2,2', etc.
- For every Poynting's vector, there is another one with similar magnitude and opposite direction.



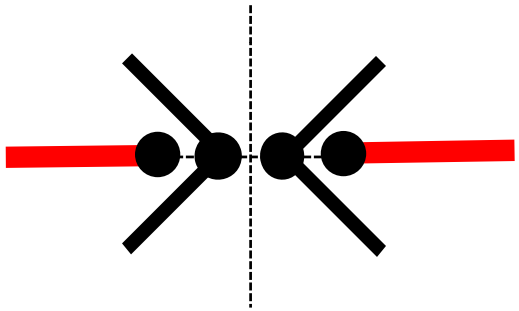
# Numerical Results Using HFSS



$S_{12} \approx$ -90dB



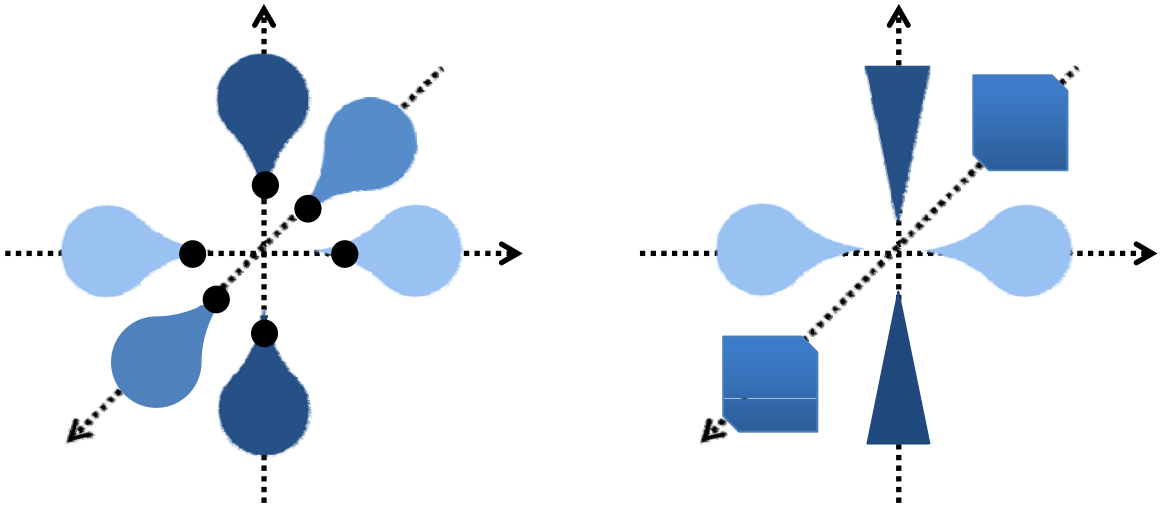
$S_{12} \approx$ -90dB



$S_{12} \approx$ -2dB

# *Triple-wise Symmetrical* Antennas

- Any two antennas are pair-wise symmetrical; no coupling between any pair
  - Diagonal S-matrix (independent of frequency)
  - Each antenna can switch between TX and RX modes asynchronous of other ones.

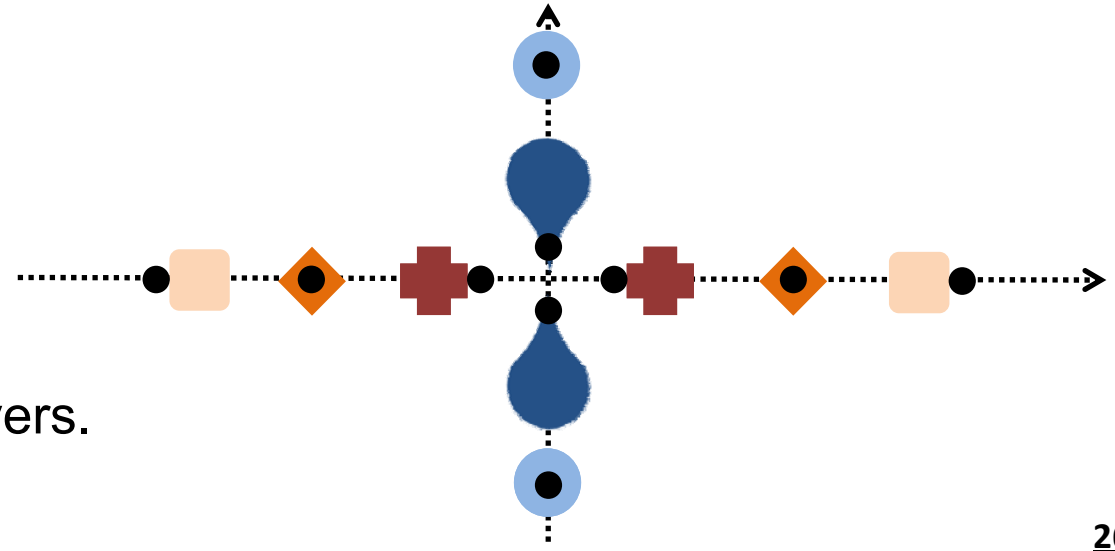


# Generalizations to MIMO

- Two sets of antennas in each unit, TX and RX
- Each antenna in TX set is pair-wise symmetrical w.r.t. all antennas in RX set and vice versa.
- A straightforward approach:
  - Use the symmetrical planes of TX and RX antennas to generate more elements in each set

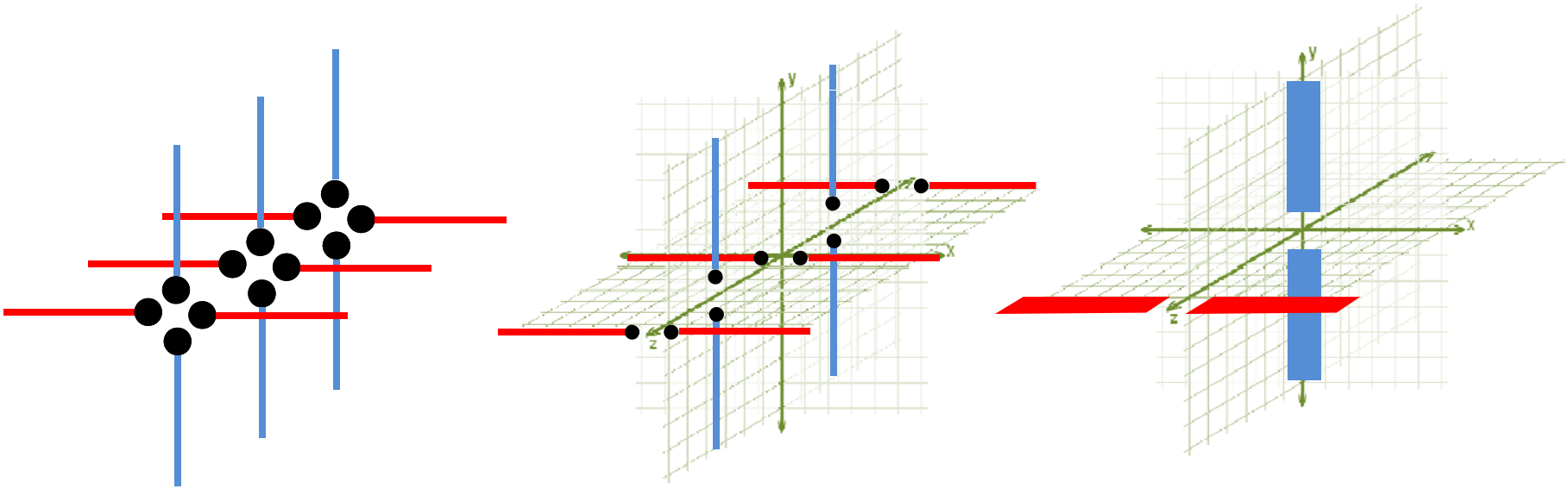
Can suffer from poor $S_{11}$

To improve $S_{11}$, arms can be brought closer by placing antennas on different PCB layers.



# MIMO in 3-D (Zero Coupling)

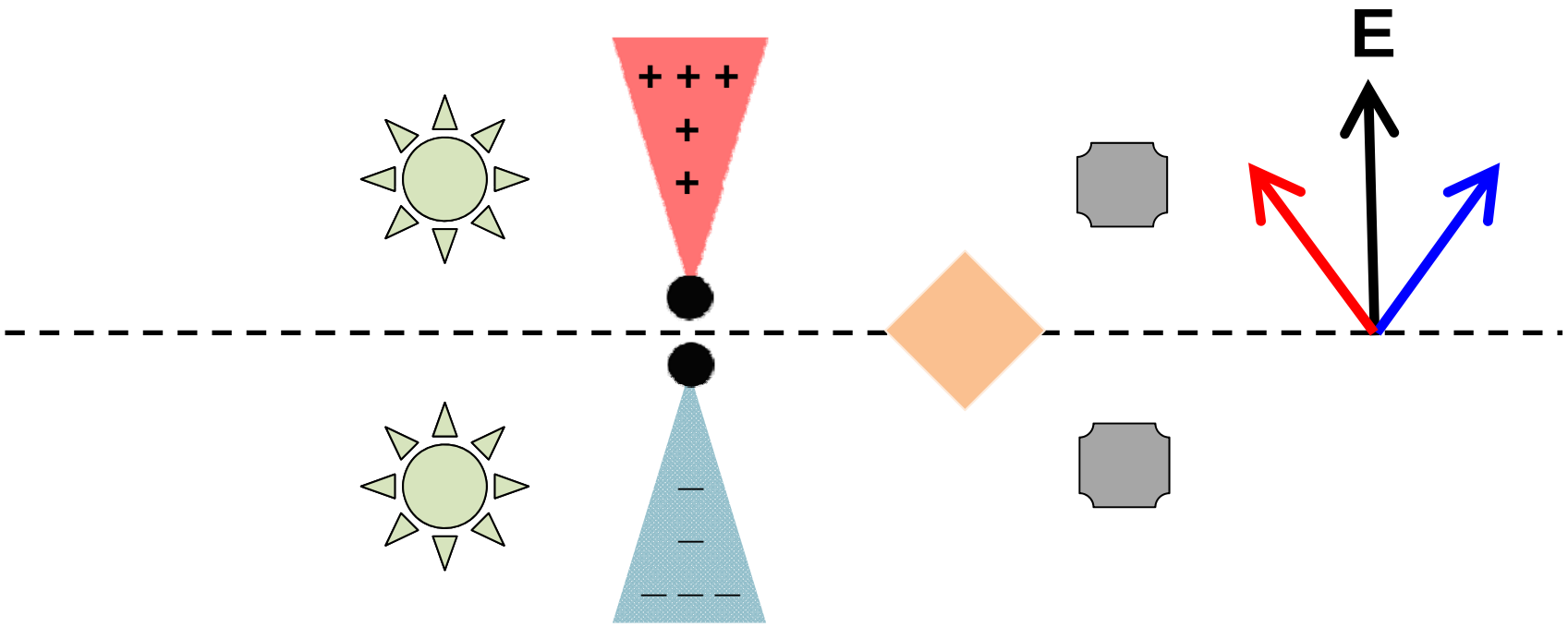
- More flexible (easier to implement) due to the possibility of reflections in three dimensions.




Antennas can be placed in any order, and can be of different lengths for multi-band operation.

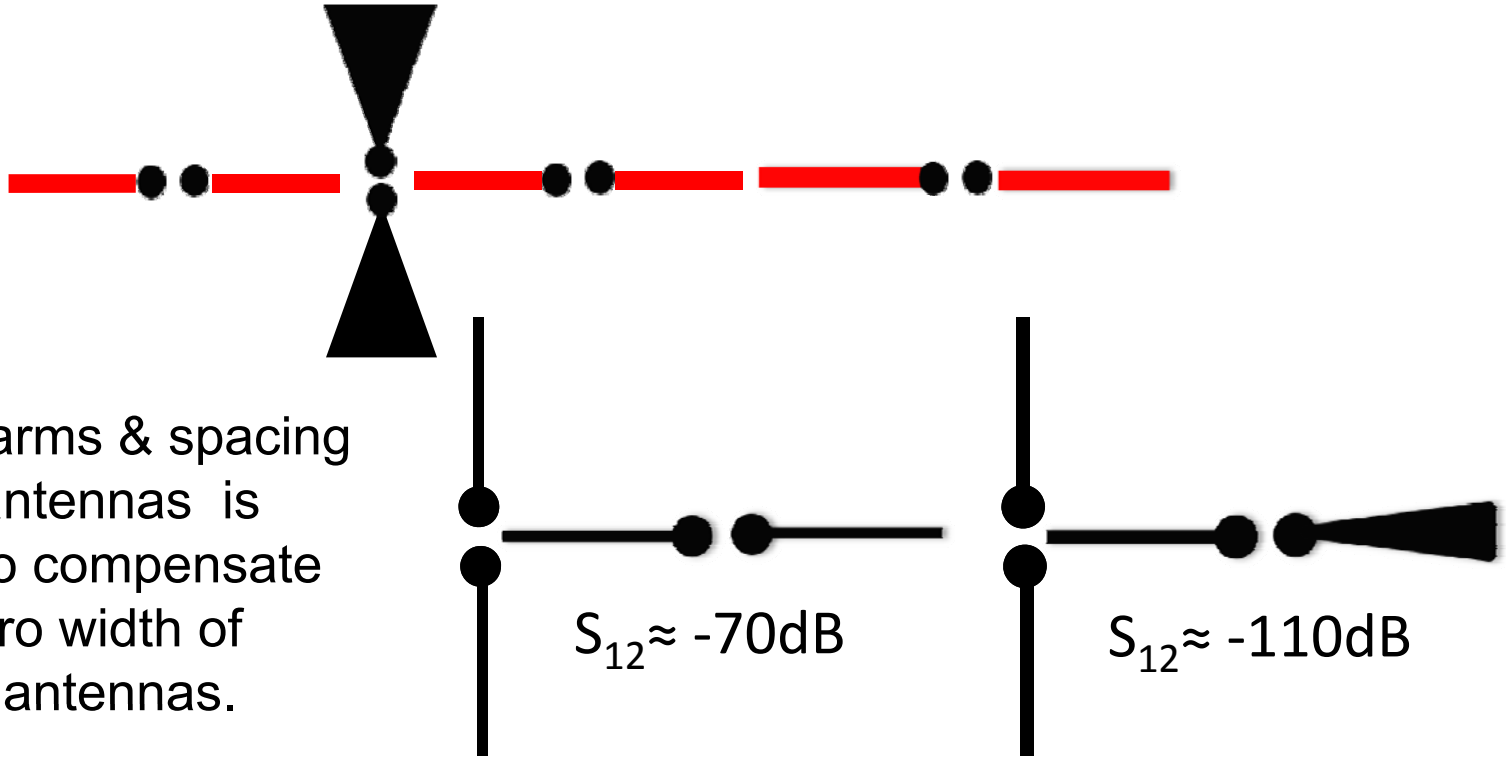
# Remarks

- *E*-field of a symmetrical antenna is orthogonal to its plane of symmetry bisecting its feed terminals.



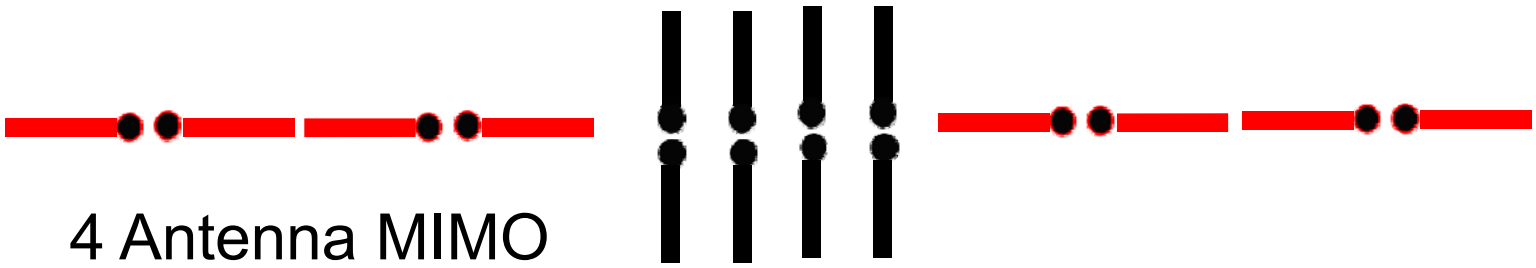
# Low Coupling Design in 2-D

- Place one set of the antennas along the symmetry plane of the other one(s).



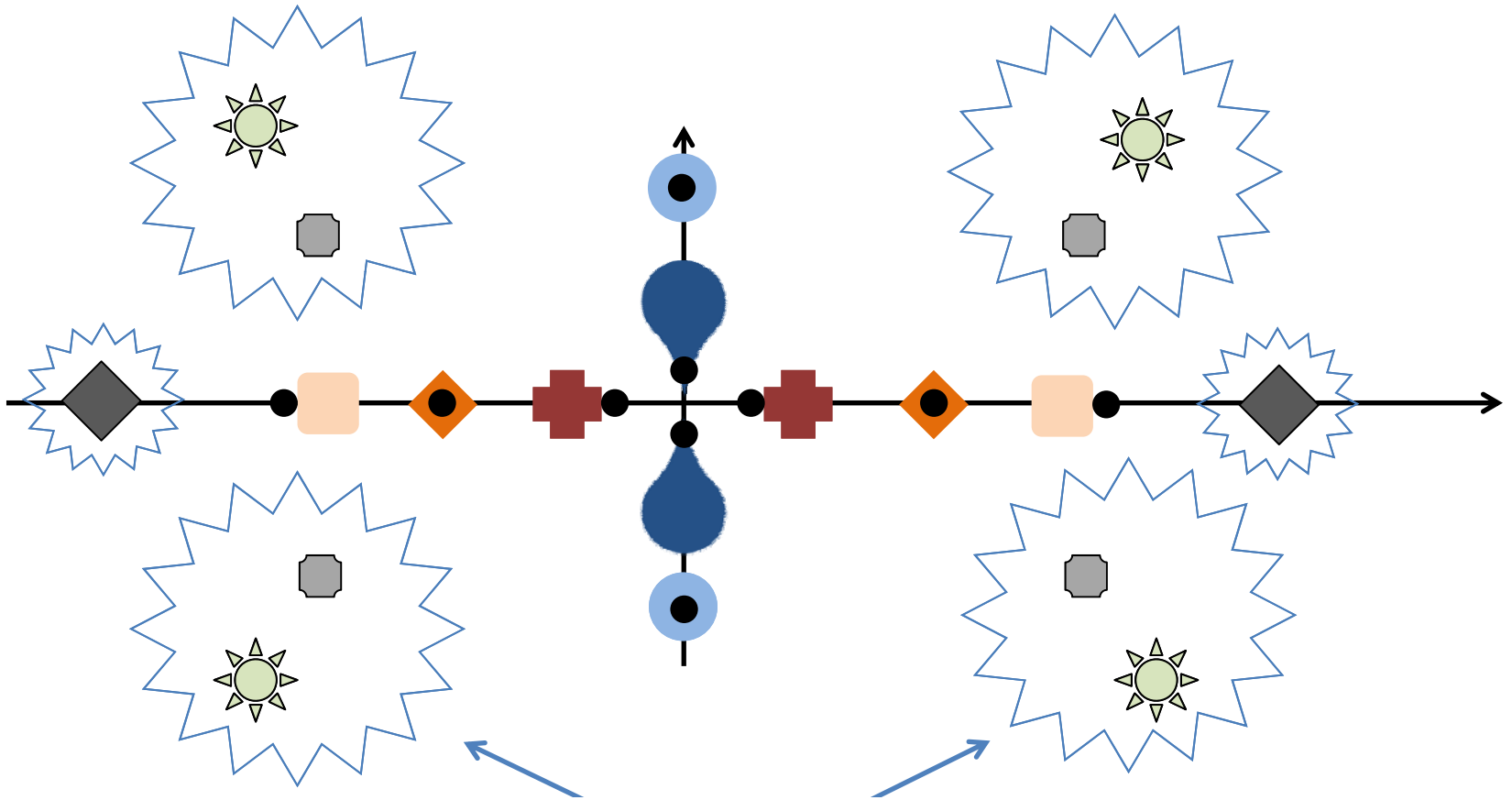

➢ Optimum spacing between vertical/horizontal antenna is very small.

# MIMO in 2-D (Low Coupling)



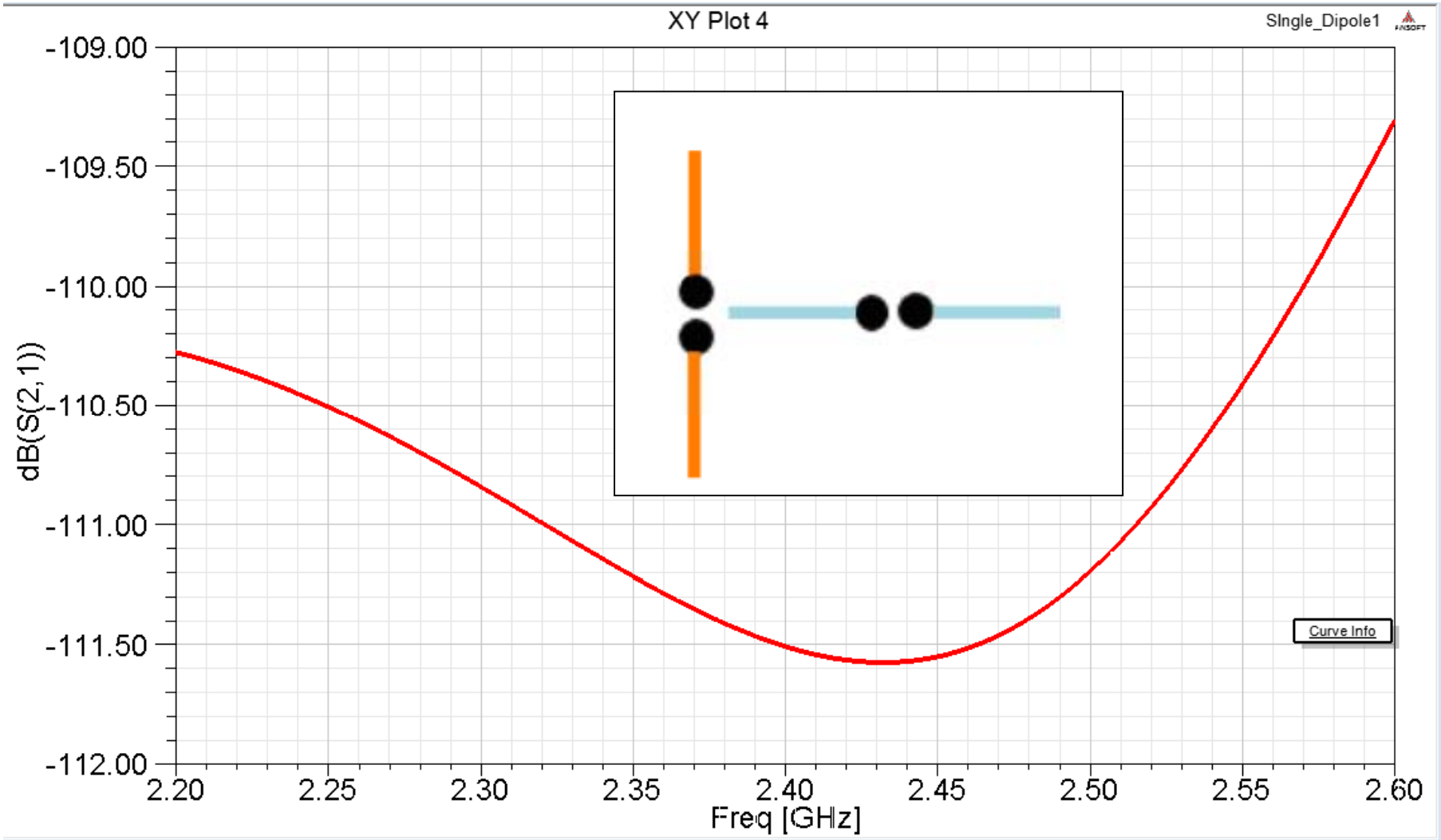

- Shape of arms & spacing between antennas is adjusted to compensate for non-zero width of horizontal antennas, as well as for MIMO requirements (independent gains).
- One arm can be generated by reflection in the ground plane: Mono-pole vs. Diploe

# Symmetry in Construct: Shape, Feed, Material and Parasitic Elements

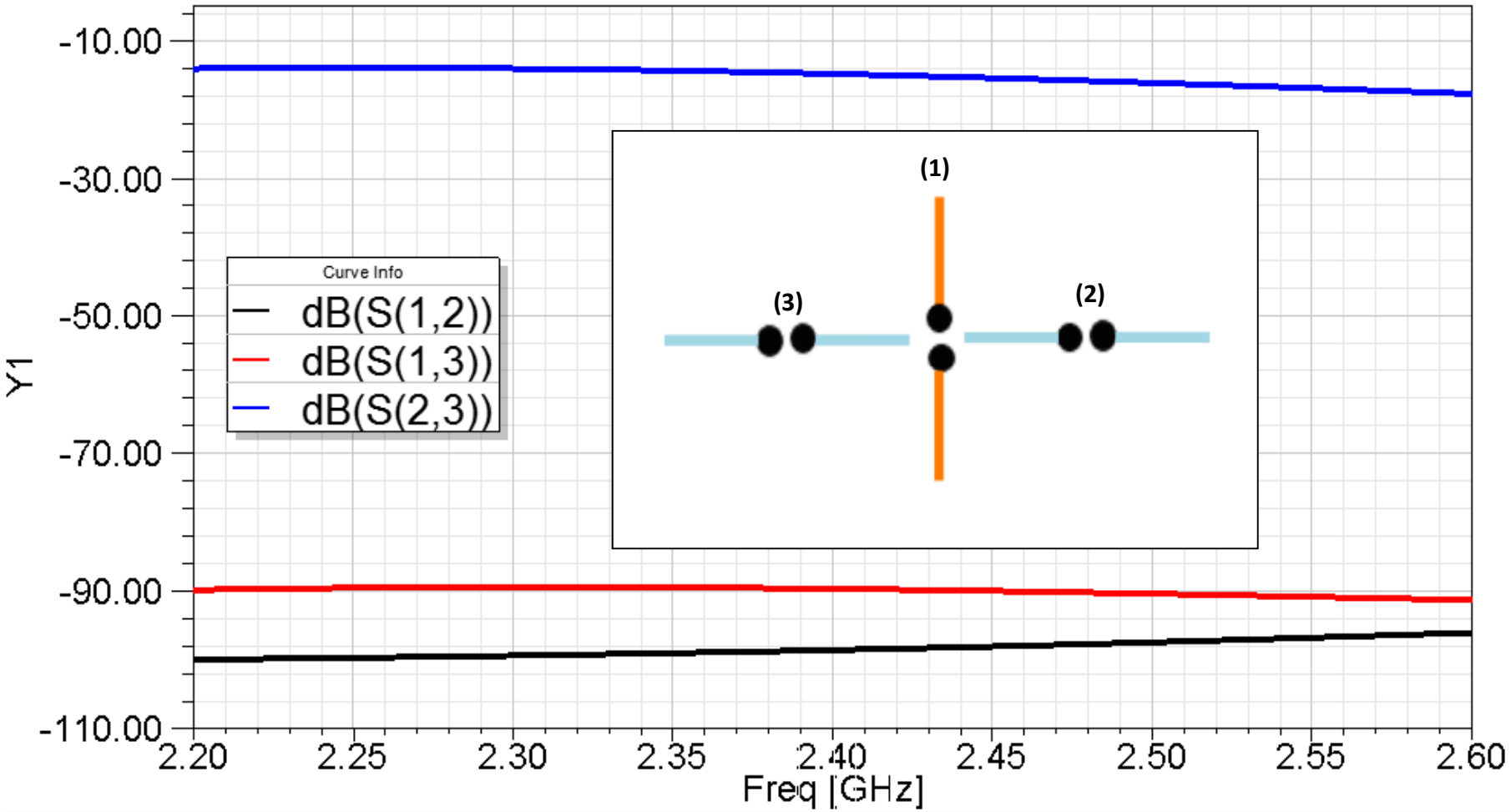


- Parasitic Elements: Human body, surroundings, PCB layers, circuit placement, etc.
- Elements are added towards providing balance with unavoidable/occasional parasitic elements (e.g.. Human body, tower, installation wall, container box, etc.).

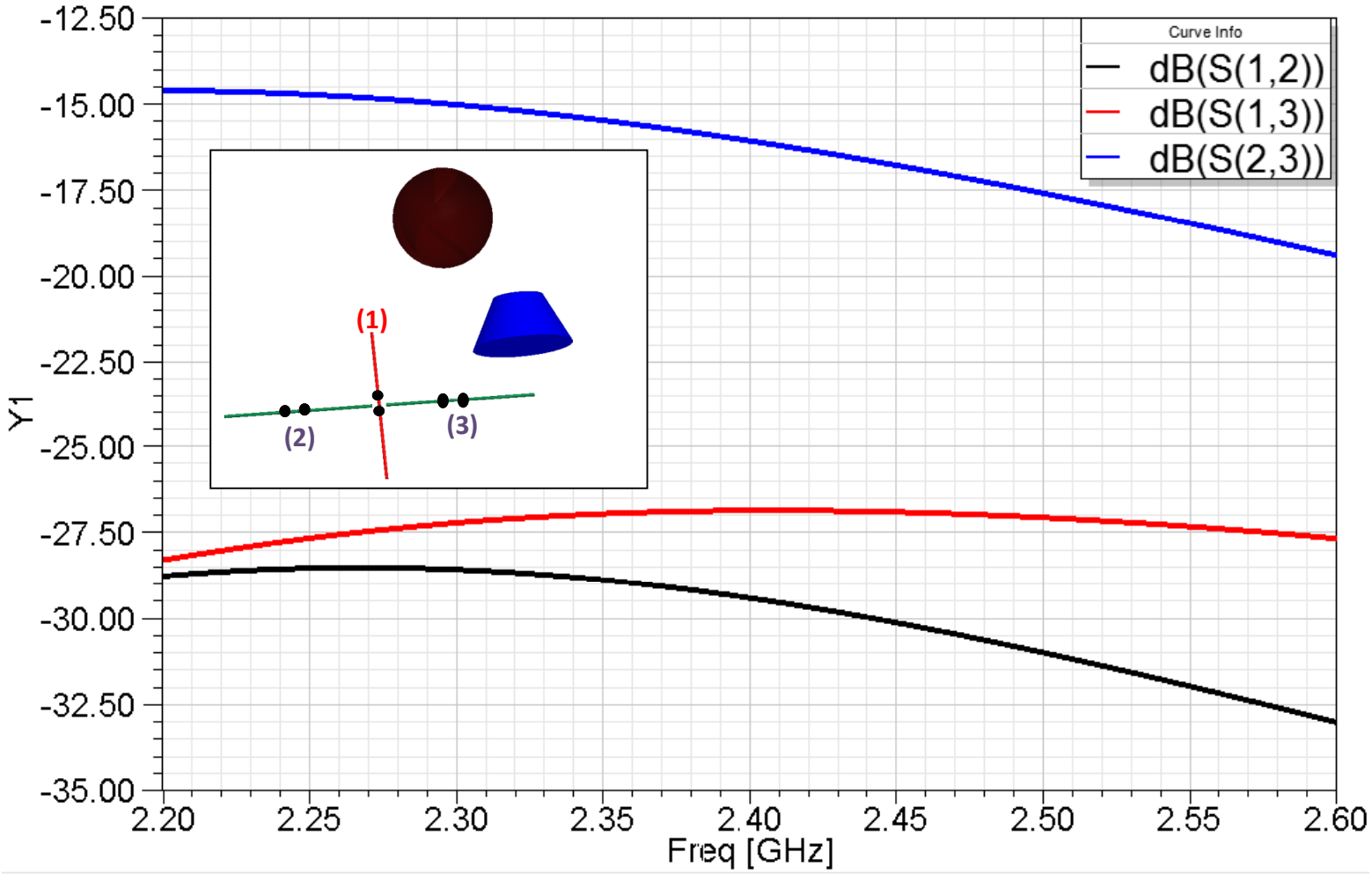
# Numerical Results Using HFSS



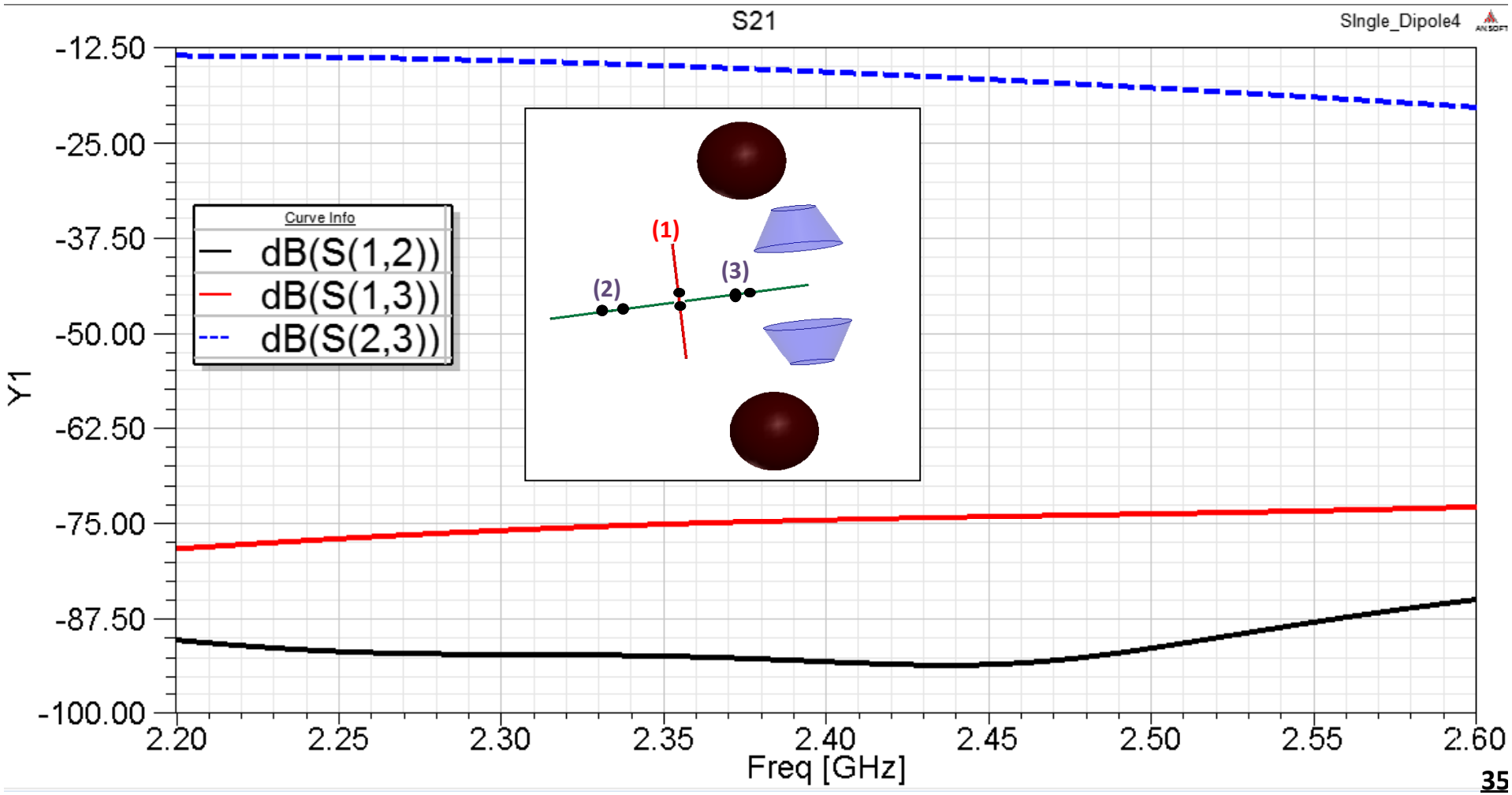
# Numerical Results Using HFSS



# Numerical Results Using HFSS

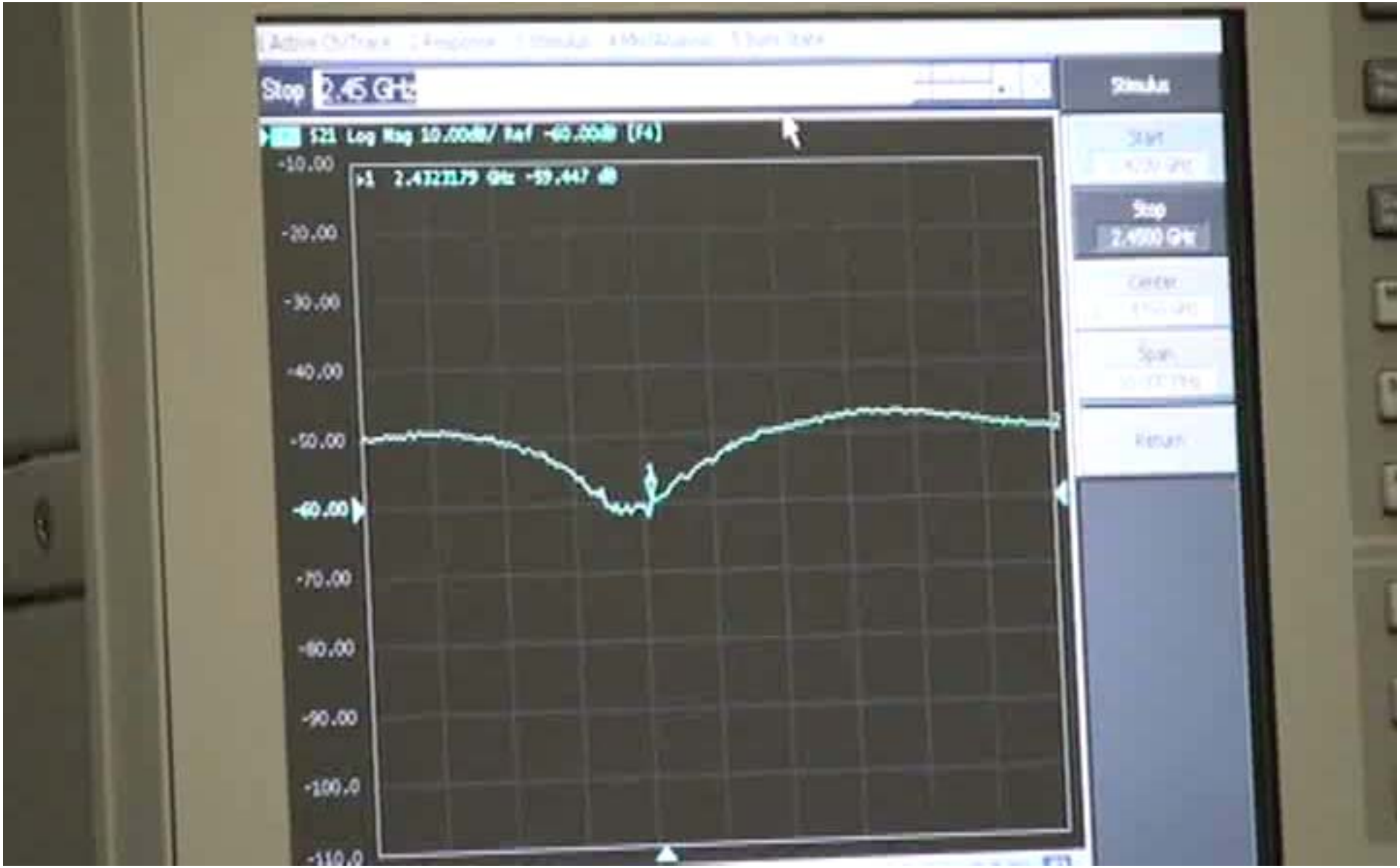


# Numerical Results Using HFSS



# Remarks

- Small coupling in symmetrical structures is not due to *polarization*, nor due to *antenna null*.
  - Neither is meaningful for near field.
- ***Question***: Are the sufficient conditions (based on provided symmetry conditions) for decoupled antennas necessary too?
  - Not clear without considering effect on $S_{11}$,$S_{22}$.
    - A more comprehensive theoretical analysis should include values of $S_{11}$,$S_{22}$.
    - For the symmetrical antennas introduced here, low coupling is achieved with good values for $S_{11}$,$S_{22}$.




2.4Ghz band,  Circuit area~ 7cm x 8 cm, $S_{11}$ & $S_{22}$ are around -15dB

# Second Stage of RF Cancellation: Active Cancellation

# Active Cancellation

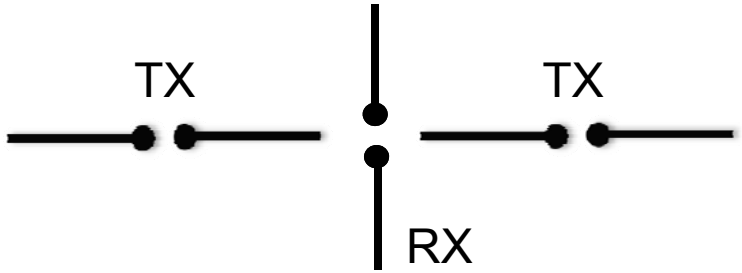
- Form an analog signal to subtract in the receive chain prior to A/D to reduce self-interference
  - RF signal combining is well established, e.g., I/Q combiner is commonly used.
- Can be also done by beam-forming within each unit
  - *Corrective Beam-forming*
  - Particularly useful if additional transmit chains are available within the unit
    - Most practical systems have several modes of operation (depending on circumstances/requirements) to improve performance and also enable various tradeoffs

# D/A Error in Signal Injection

- **A reasonable question**: Is signal injection just hiding the problem by replacing the issue of A/D error by and an equivalent D/A error?
- **NO**: D/A operation is linear and its effect is cancelled by subsequent interference cancellation in base-band.
- **NO**: Error caused by possible numerical inaccuracies (e.g., FFT/IFFT) can be computed digitally, and compensated in digital domain.

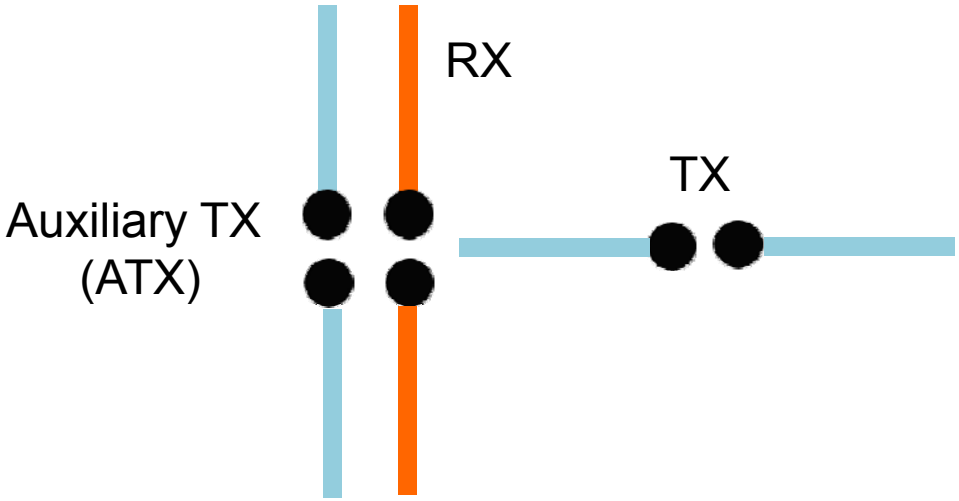
# Corrective Beam-forming for Reducing Self-interference

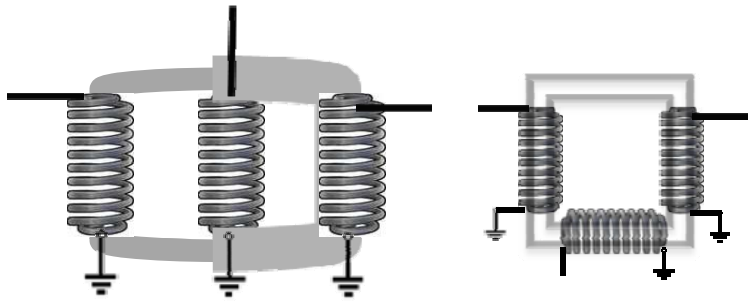
- Multiple transmit antennas are used to create null on the receive antenna(s).
  - Example of two TX and one RX antennas:




  - Restriction on the spacing is less than MIMO requirements (null creation is easier than independent gain requirement).
  - Multiple TX antennas may already exist in the unit to support different modes of operation for the unit.

# Simplification: Corrective Beam-forming with Auxiliary TX

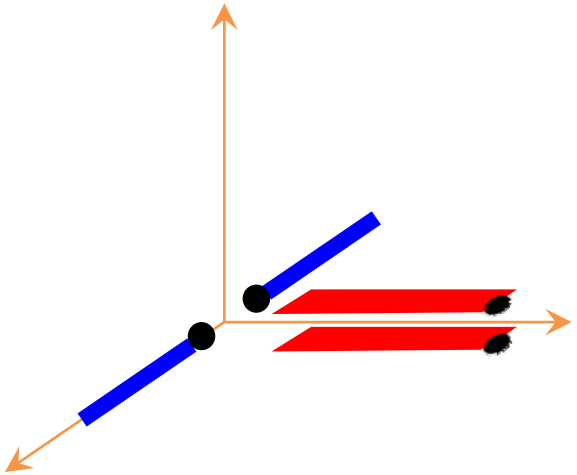


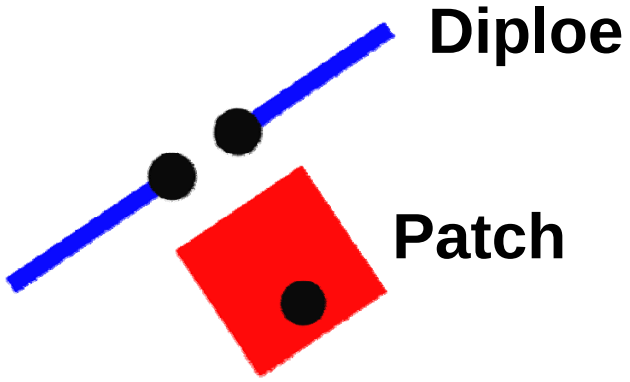



Signal injection is a form of ATX

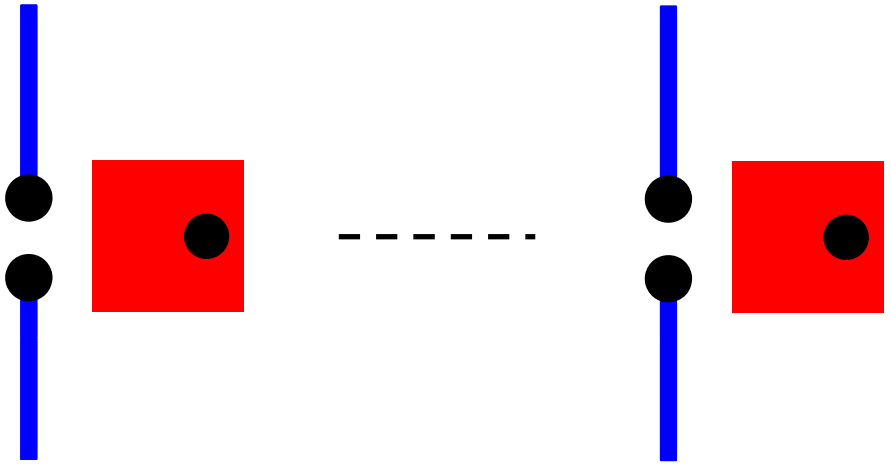
- Auxiliary TX (ATX) can have a simple structure in terms of size, feed, grounding, length, etc (creating null is simple).
- ATX can have a high coupling with RX and transmit with low power.
- ATX can be one of the antennas used in MIMO mode (as TX or TX/RX with circulator) and switched to act as ATX, when needed.
- Multiple ATX can be used for MIMO (flexible size/spacing).

# Another Form of Decoupled Antennas in 3-D (reality of 2-D)



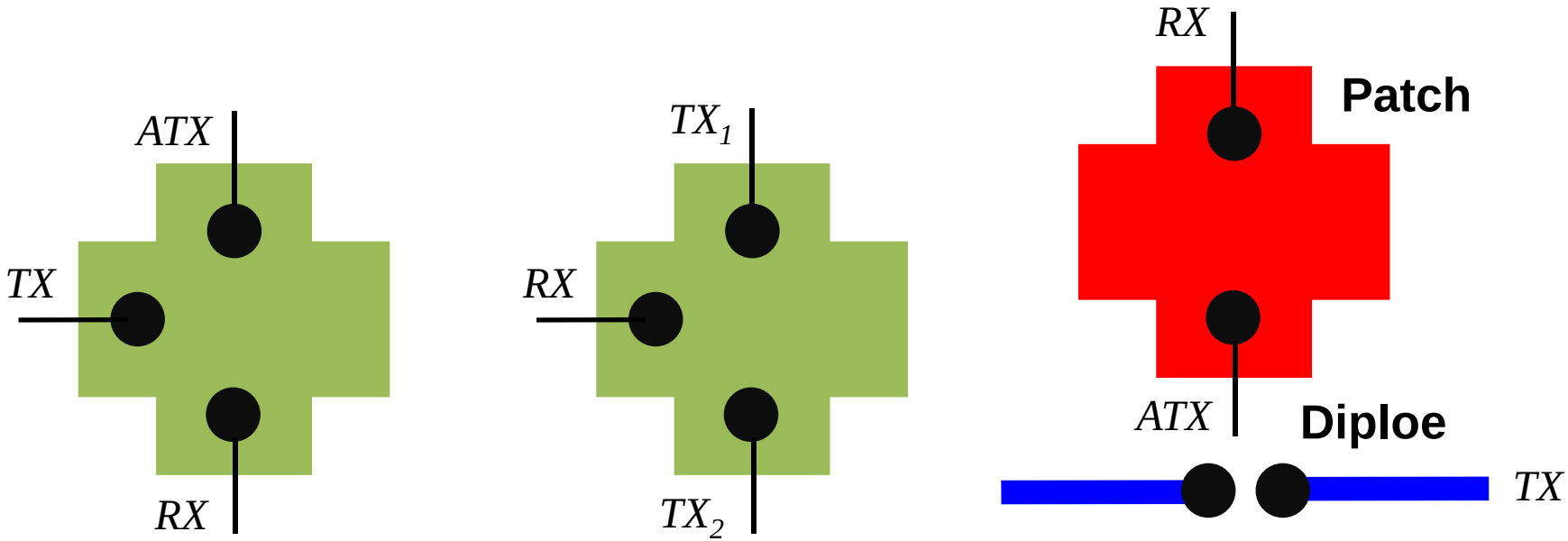



**Generalization to MIMO**



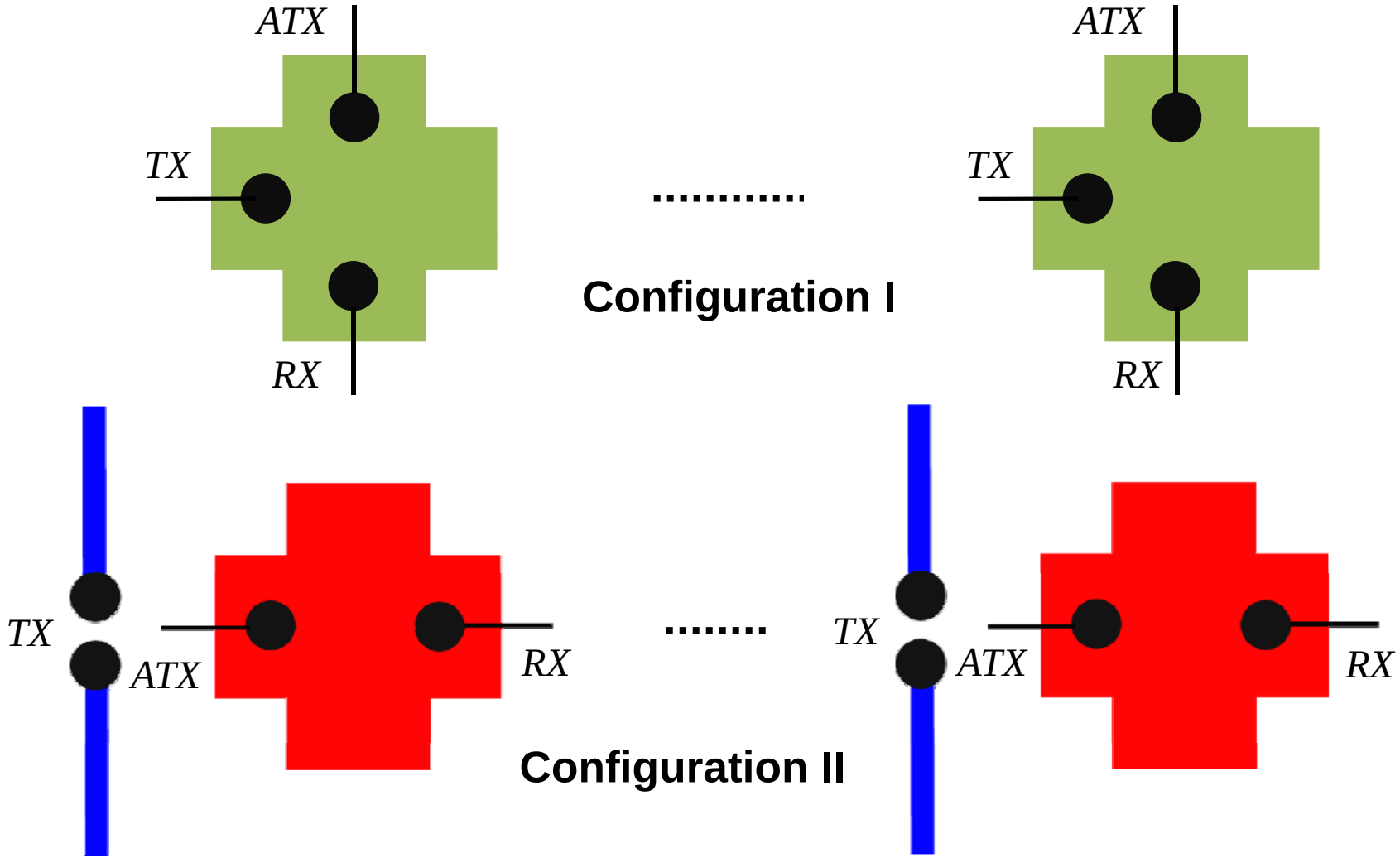
# Combined Design: Multi-terminal Antennas

- Transmit, receive and active cancellation are combined into a single arm above ground using patch antennas.




Shape of corner cuts and various sizes are optimized for best radiation efficiency and proper coupling.

# Generalization to MIMO: Each Radio has Shared TX/RX Antennas



# Signal Recovery at Base-band

# Interference Removal in Base-band

1) Pilots (disjoint in time) are transmitted from each TX antenna to measure corresponding channel, resulting in: $\mathrm{H}_1 + \Delta\mathrm{H}_1, \mathrm{H}_2 + \Delta\mathrm{H}_2$
2) Self-cancelling pilots with pre-coding (after fixing the weightings) are sent simultaneously:

$$\mathrm{H}_2(\mathrm{H}_1 + \Delta\mathrm{H}_1)(\mathrm{P} + \Delta\mathrm{P}) - \mathrm{H}_1(\mathrm{H}_2 + \Delta\mathrm{H}_2)(\mathrm{P} + \Delta\mathrm{P}) =$$

$$(\mathrm{H}_2\Delta\mathrm{H}_1 - \mathrm{H}_1\Delta\mathrm{H}_2)\mathrm{P} + (\mathrm{H}_2\Delta\mathrm{H}_1 - \mathrm{H}_1\Delta\mathrm{H}_2)\Delta\mathrm{P}$$

where $(\mathrm{H}_2\Delta\mathrm{H}_1 - \mathrm{H}_1\Delta\mathrm{H}_2)\Delta\mathrm{P} \approx 0$

– Residual self-interference channel: $\mathrm{H}_2\Delta\mathrm{H}_1 - \mathrm{H}_1\Delta\mathrm{H}_2$

# Interference Removal in Base-band

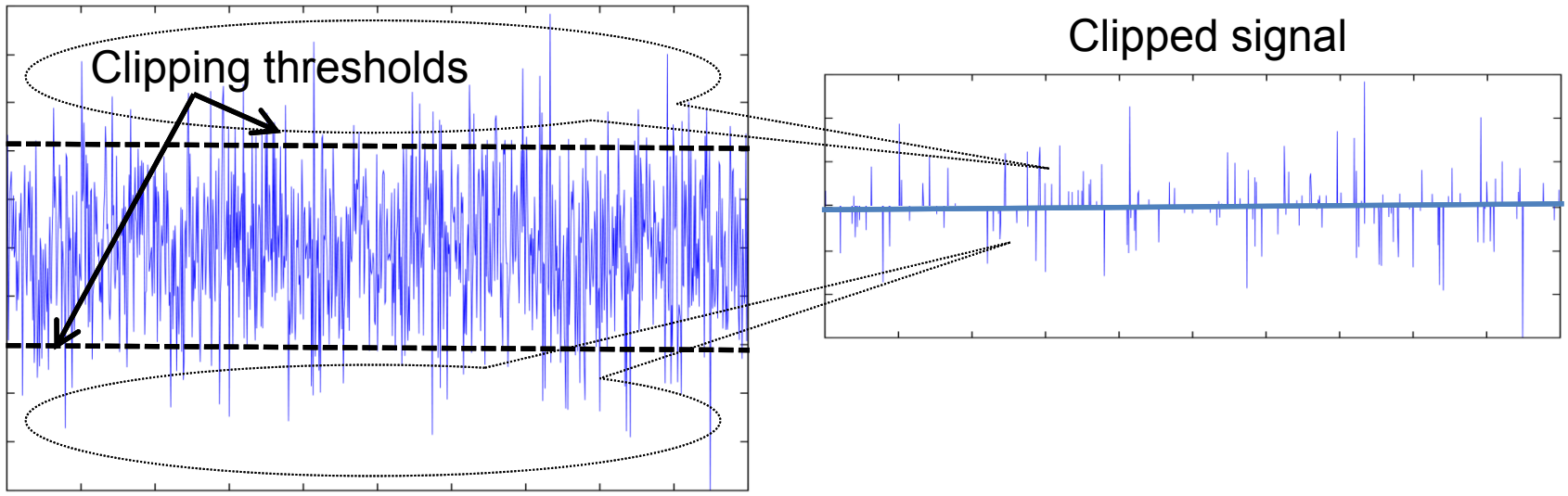
3) $\Gamma + \Delta\Gamma$ : OFDM data with computational error

$$H_2(H_1 + \Delta H_1)(\Gamma + \Delta\Gamma) - H_1(H_2 + \Delta H_2)(\Gamma + \Delta\Gamma) =$$
$$(H_2\Delta H_1 - H_1\Delta H_2)\Gamma + (H_2\Delta H_1 - H_1\Delta H_2)\Delta\Gamma$$

- $(H_2\Delta H_1 - H_1\Delta H_2)\Gamma$ is cancelled by base-band self-interference cancellation (equalization).
- $(H_2\Delta H_1 - H_1\Delta H_2)\Delta\Gamma$ is compensated digitally (all its components are known).

# Base-band Interference Removal & Clipped Signal Reconstruction

- Analog signal can be clipped prior to A/D and the clipped part is then digitally compensated (accounting for only the TX signal).

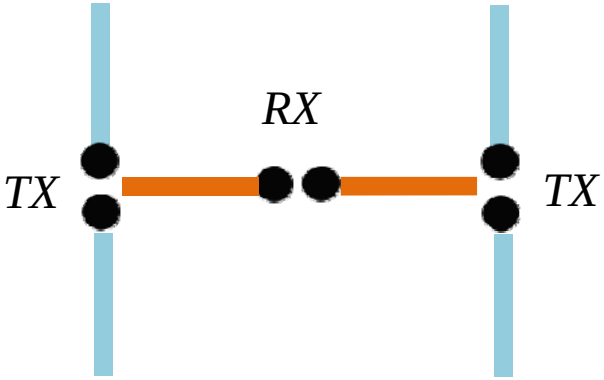


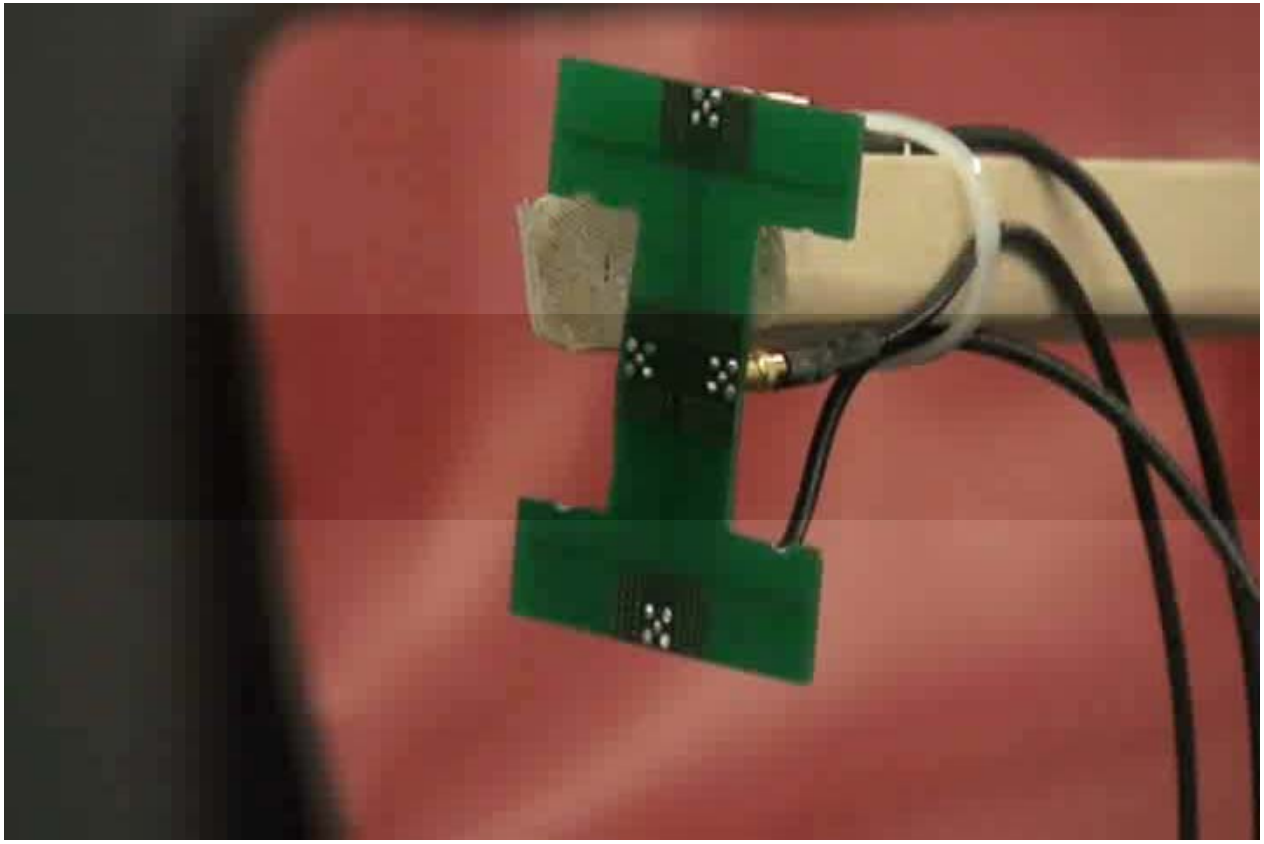
# Example of Performance

- Antenna structure shown in earlier video clip
- Transmit power about 30dBm (typical for cell phone power).
- Residual Self Interference to Noise Ratio:
  - Antenna structure alone: about 40dB
  - After corrective beam-forming: about 2dB
  - After base-band subtraction: about 0.4dB
    - **NOTE**: Observed degradation is less than typical degradations due to various mismatches in signaling between **separate** (distant) TX/RX units.

# Effects of Different Cancellation Algorithms in Base-band (Real-time)

**Dipole Antennas**

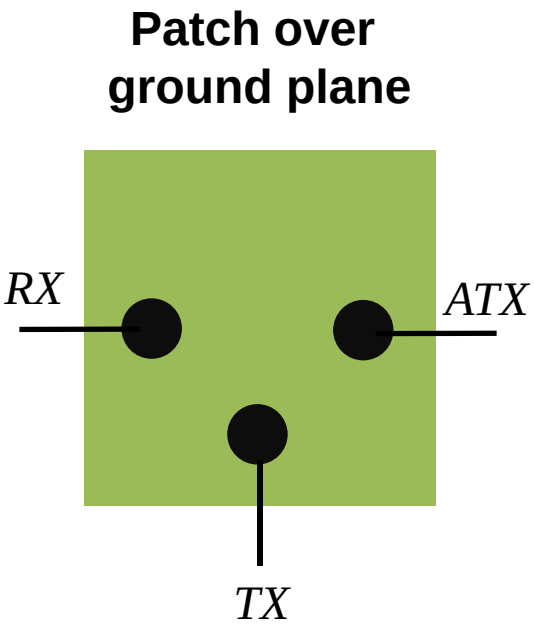


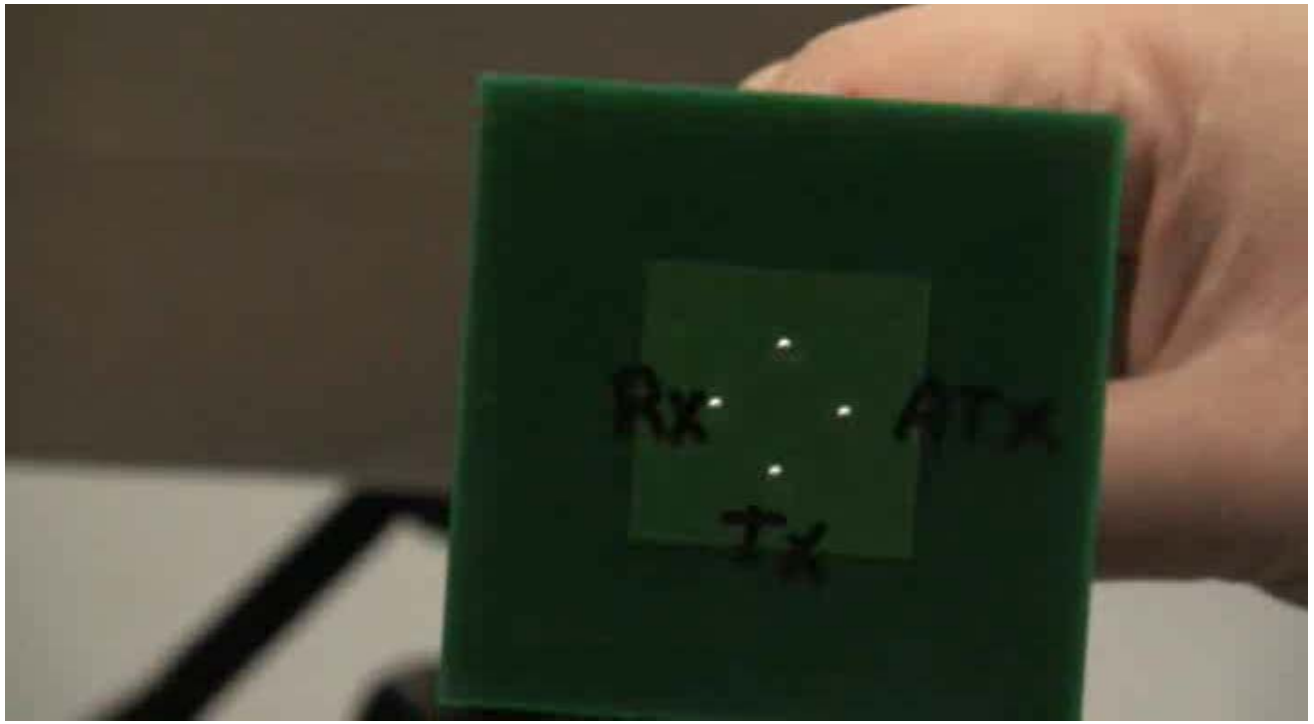



**20MHZ bandwidth@2.4Ghz, $S_{11}$ & $S_{22}$ around -15dB**

**Important:** Implementation is based on using two transmit antennas and corrective beam-forming. This is merely for the ease of implementation and also ease of measurements. In practice, signal injection after LNA would achieve the same goal.

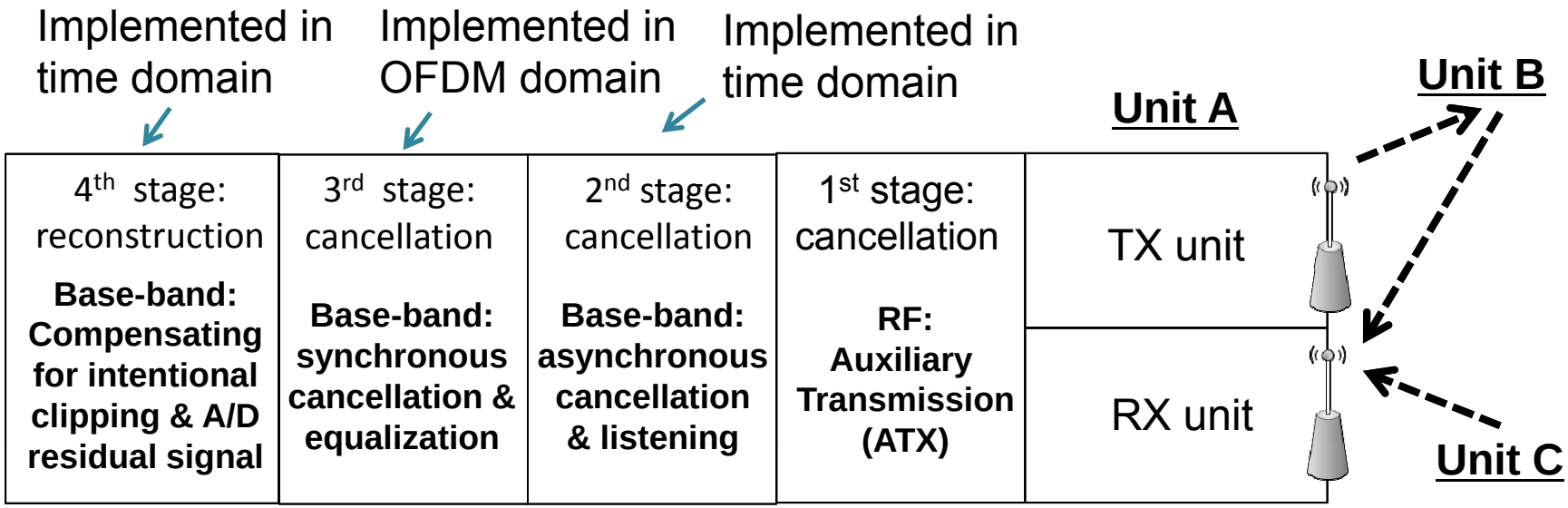
# Effects of Different Cancellation Algorithms in Base-band (Real-time)



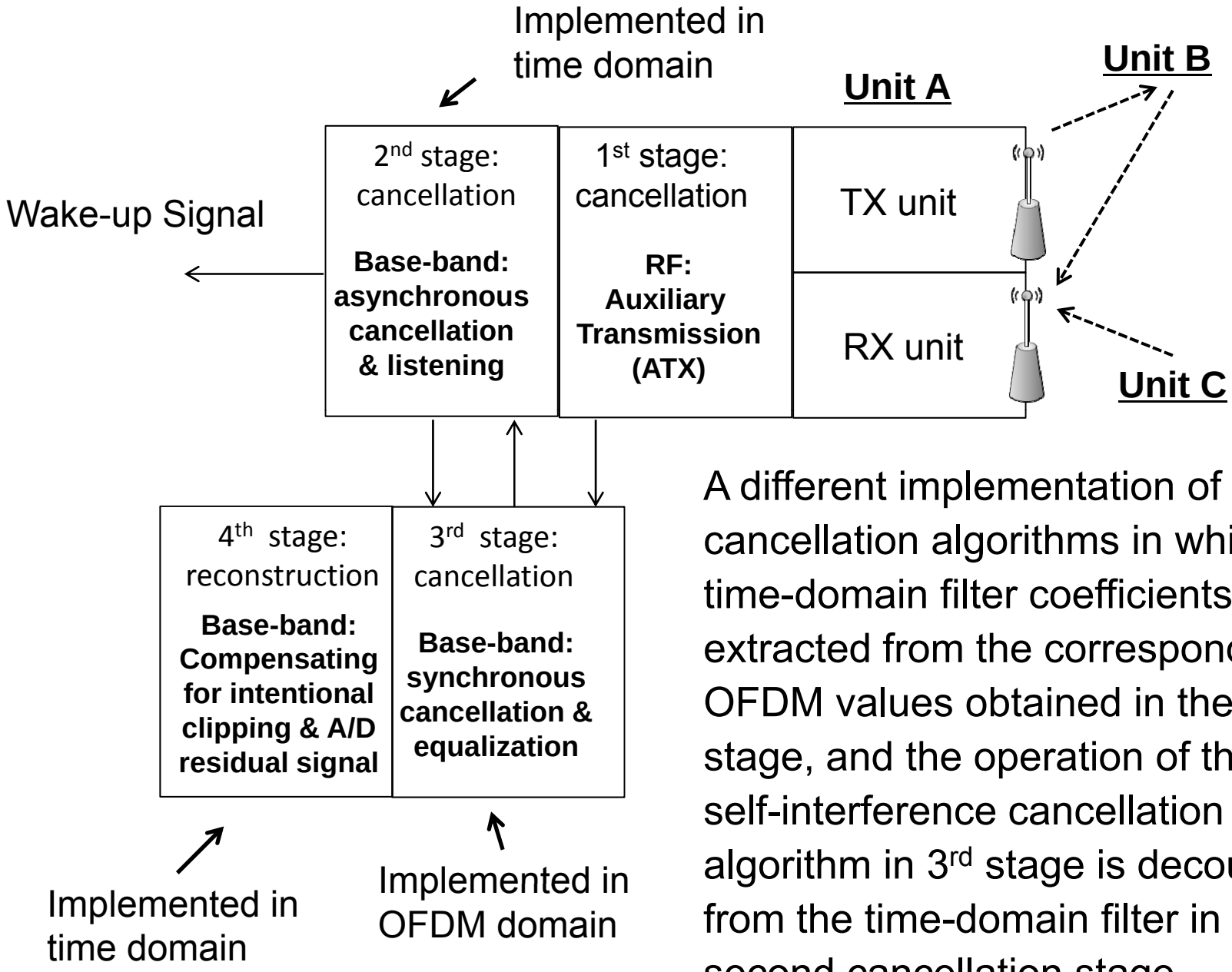




**20MHZ bandwidth@2.4Ghz, $S_{11}$ & $S_{22}$ around -15dB**

# Supporting Asynchronous Clients




- Receive and transmit connections are established to two separate clients in an asynchronous manner.
- Unit A is listening to detect a valid incoming signal, while transmitting to unit B. This is made possible by the 2nd stage of self-cancellation which is synchronous with unit A's transmit signal, but not necessarily synchronous with the incoming signal from Unit C.

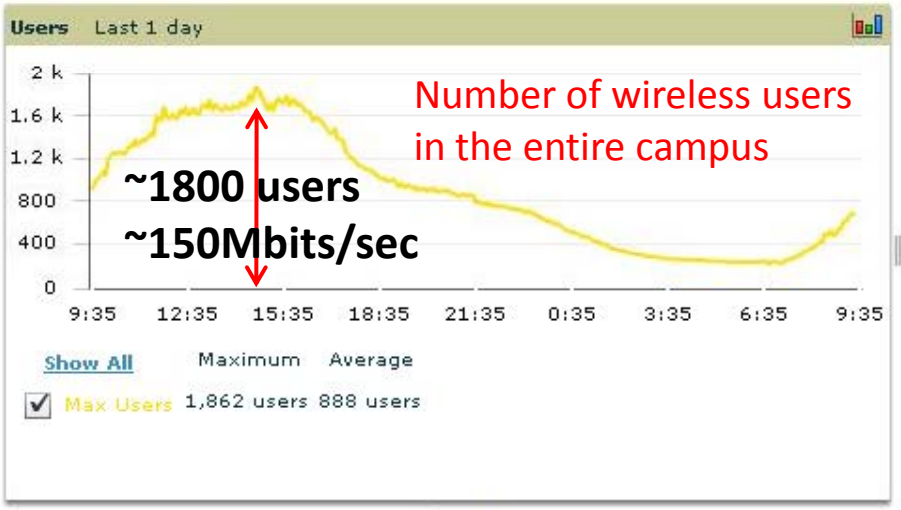


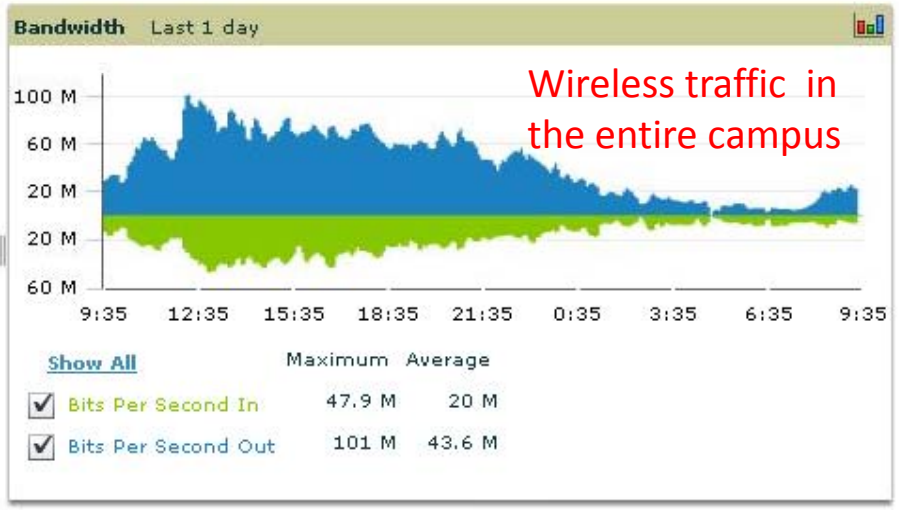

A different implementation of the cancellation algorithms in which the time-domain filter coefficients are extracted from the corresponding OFDM values obtained in the 3rd stage, and the operation of the main self-interference cancellation algorithm in 3rd stage is decoupled from the time-domain filter in the second cancellation stage.

# Network Applications

# **WLAN Traffic**: Bursty, Delay Sensitive & Inefficient

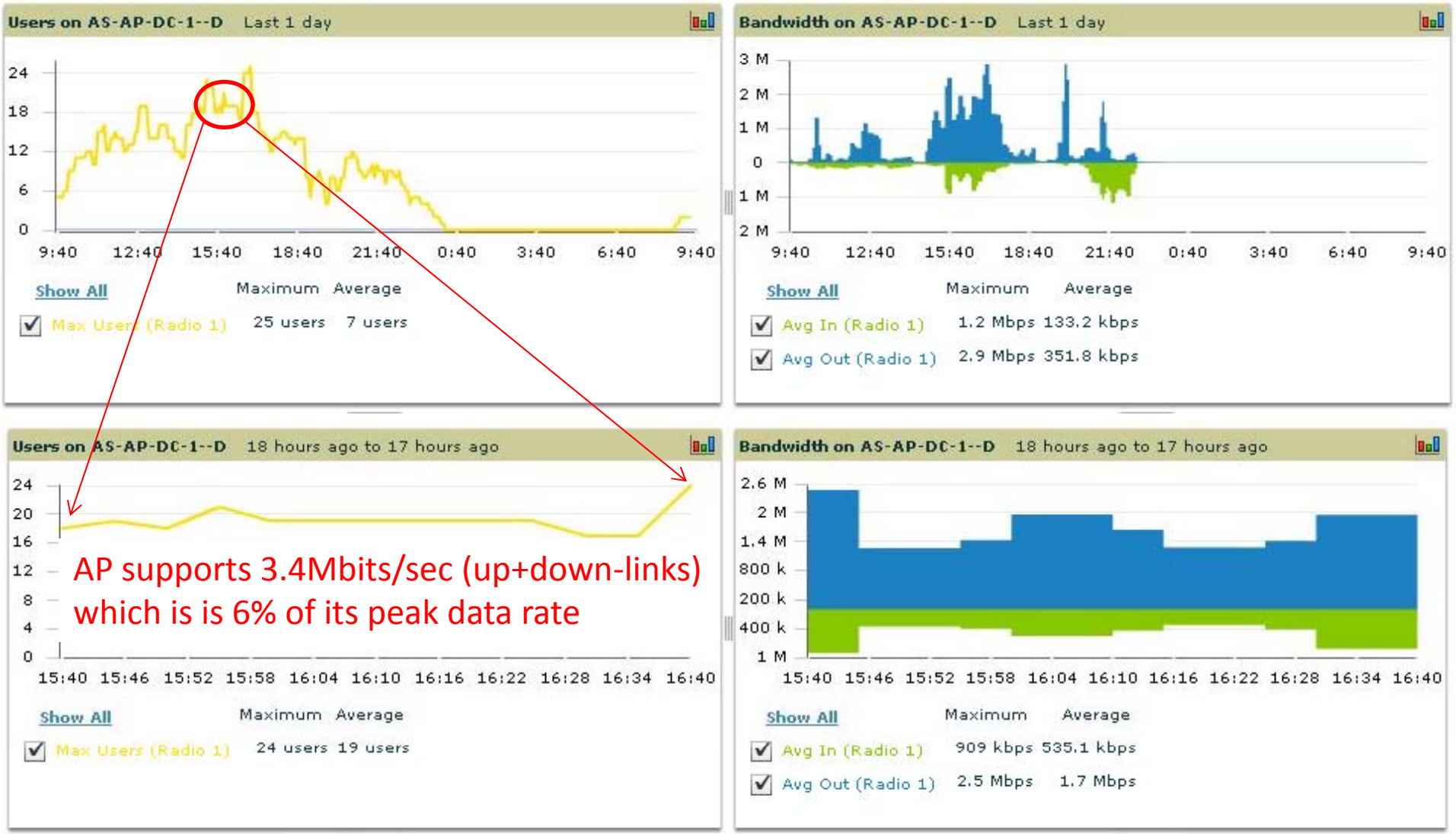
- UW Campus: Total of 1400 wireless APs across campus serving 4200 active wireless IP
  - In theory, each AP should support at least around 54Mbits/sec
  - They usually install an additional AP if the typical number of clients connecting to an AP exceeds 10 most of the time




Average=70Kbits/sec/user (up+down-links) Peak=80Kbits/sec/user (up+down-links)

# A Busy Access Point in the Library



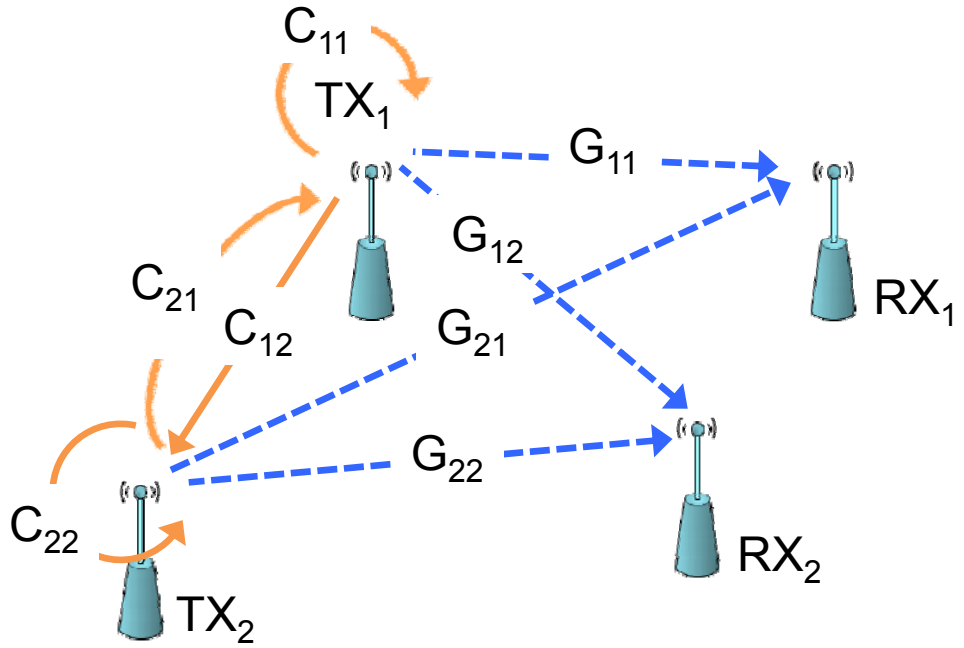
# A New Concept:
## Superimposed Networking for Control Signaling

- Control signaling, particularly signaling in uplink required to join the network, is a primary bottleneck.
- Methods described for handling asynchronous users enable superimposing a half-duplex, low bit rate, low power, easy to detect network for control signaling on top of the network of primary full-duplex data links.
- Features of superimposed links:
  - Separated from the primary full-duplex data links in code domain.
  - Use time multiplexing and CSMA among themselves, but conventional problems are avoided as these operate in parallel with the primary full-duplex data links.
  - Have a low spectral efficiency, but this is not an issue as control signaling has a minor load on the overall throughput.
  - PHY is designed such that full-duplex links can detect and cancel the interference caused by the superimposed control link.

# Highlight of Network Applications

- Possibility of supporting two-way asynchronous links with multiple clients solves many of MAC, resource allocation/QoS, scheduling issues in wireless networks.
- Two neighboring nodes, by listening to each other while transmitting, can form a distributed Alamouti code.
  - Useful in the design of MAC
  - Useful in multiple access scenarios, e.g., two clients send data to the same access point.
- Feedback link is useful in sending pilots, in ARQ, in adaptive transmission, etc.
  - Example: One node can broadcast a set of pilots to be used by all network nodes as reference.
- Nodes have an indication of the level of interference by listening while transmitting.

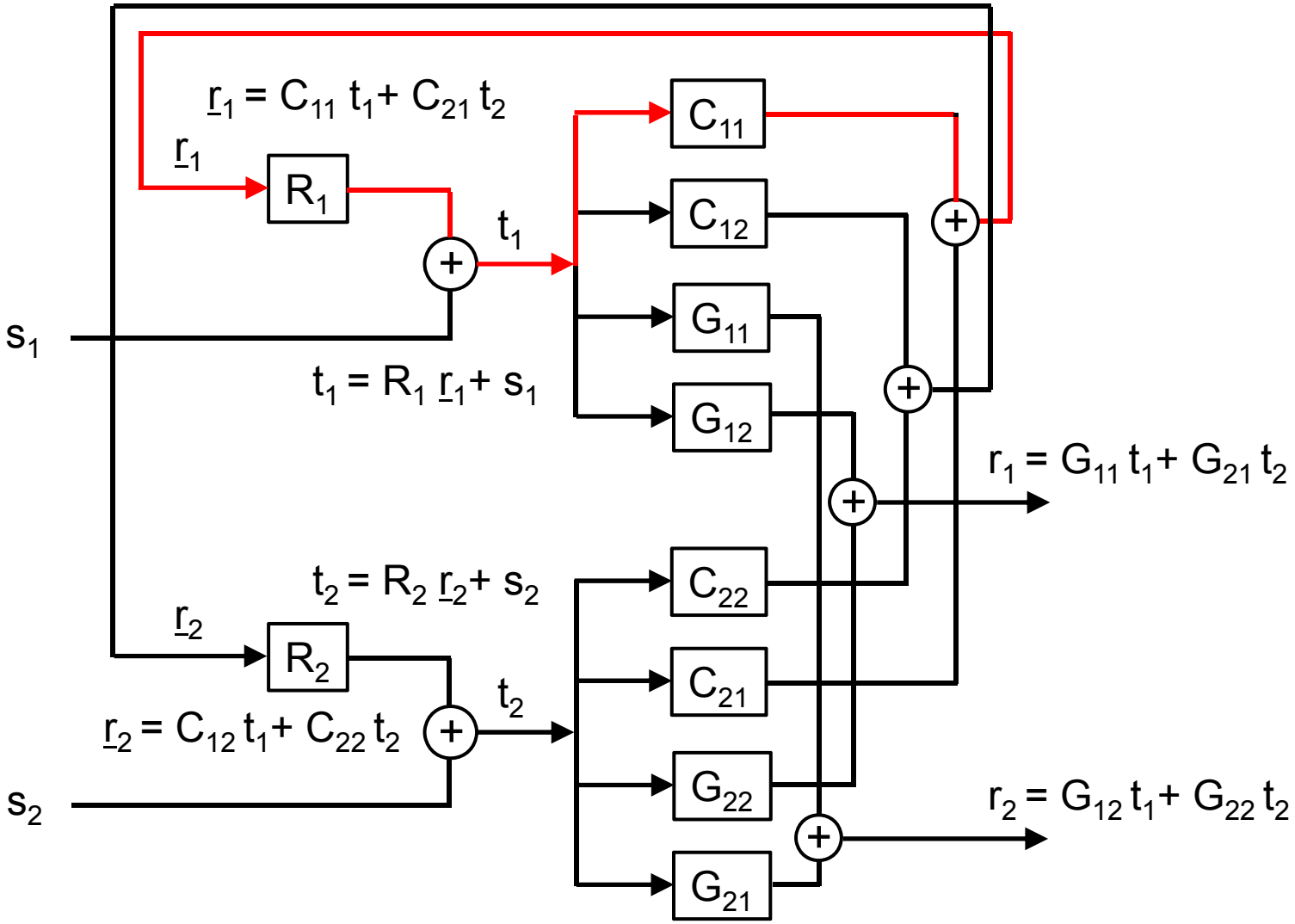
# Interference Channel




- $R_1$ and $R_2$ are filters at receivers of nodes $TX_1$ and $TX_2$, respectively.
- To cancel interference, we need:

$$R_1 = \frac{G_{21}}{G_{21}C_{11} - G_{11}C_{21}} \qquad R_2 = \frac{G_{12}}{G_{12}C_{22} - G_{22}C_{12}}$$

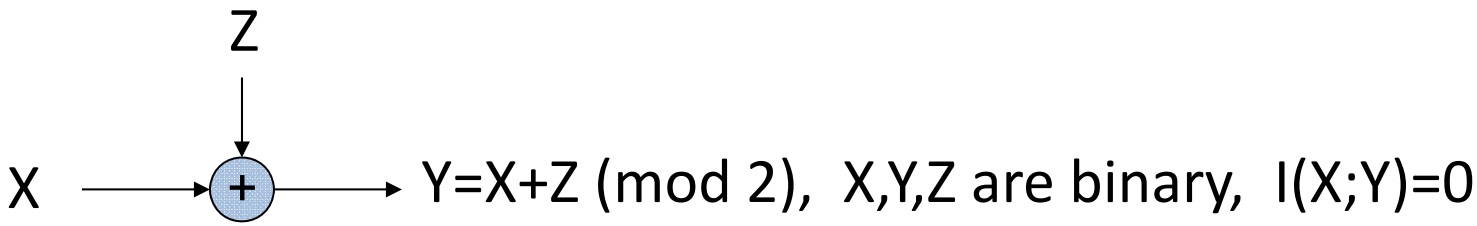
# Stability Condition: Satisfied by Adjusting TX/RX Gains



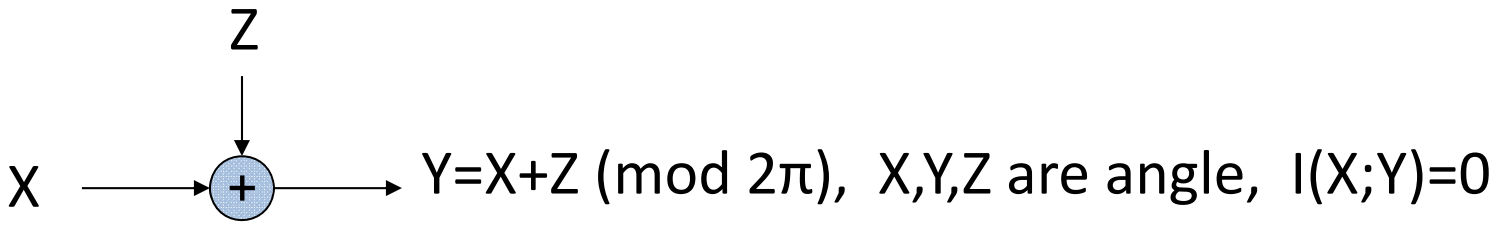
# Security Applications:
# One-time Pad (Vernam Cipher)

# Unbreakable Security: Vernam Cipher, One-time Pad

- Vernam Cipher, One-time Pad: Bit-wise XOR of a (non-reusable) mask with the message




- Generalization:

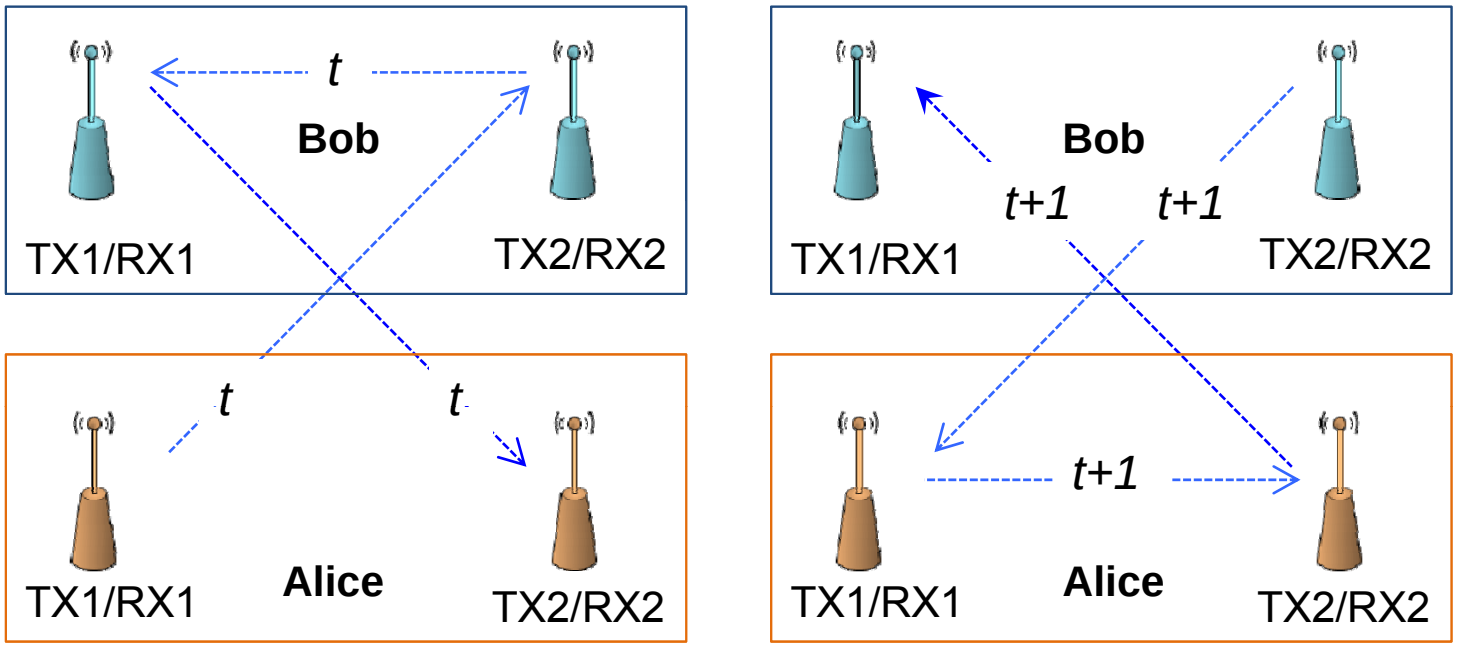



  - Happens naturally in wireless transmission
    - Need to change/track the channel and use PSK modulation.

# Unbreakable Security: One-time Pad using Channel Phase

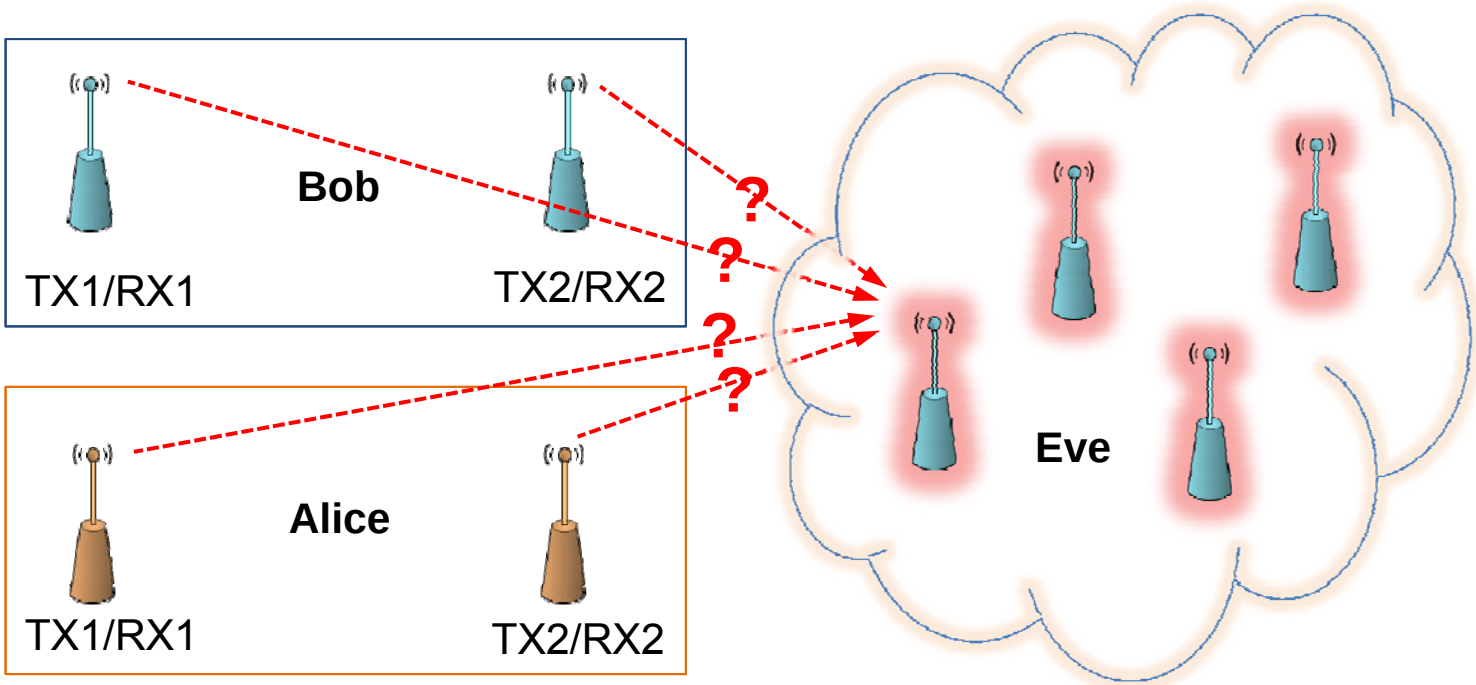
- Basic Idea:
  - Two parties use (common random) phase values to scramble each PSK transmission.
  - Errors in common phase values are corrected by the overall channel code.
- Challenges:
  - Synchronizing the two parties to agree on phase.
  - Providing a new common random phase for each PSK symbol.
- Two-way wireless solves both above challenges
  - Leakage (self interference) helps

# Key (common random phase) Generation




- At OFDM symbol *t-1*, Alice and Bob measure their loop-back channels from Bob/TX1 to Bob/RX2 and from Alice/TX2 to Alice/RX1 (send low power pilots after scrambling and loop back in each unit)
- At OFDM symbol *t*, Alice/TX1 sends pilots (after scrambling) to Bob/RX2, who (using Bob/TX1) forwards it to Alice/RX2.
- At OFDM symbol *t+1*, Bob/TX2 sends pilots (after scrambling) to Alice/RX1, who (using Alice/TX2) forwards it to Bob/RX1.
- The two units, knowing their loop-back channels and relying on reciprocity, compute the channel:(Alice/TX1→Bob/RX2)x(Bob-loop-back)x(Bob/TX1→Alice/RX2)x(Alice-loop-back) to be used a key. This is possible as up/down conversion at each unit is performed using the same carrier/clock.

# Sketch of Proof




- There are four legitimate antennas and four transmissions.
  - **Key point**: There is a single transmission from each legitimate antenna.
- Eve has a large number of distributed antennas with high SNR.
  - Each of Eve's antennas receives four signals, but each signal is through a channel with an unknown phase and conveys no useful information.

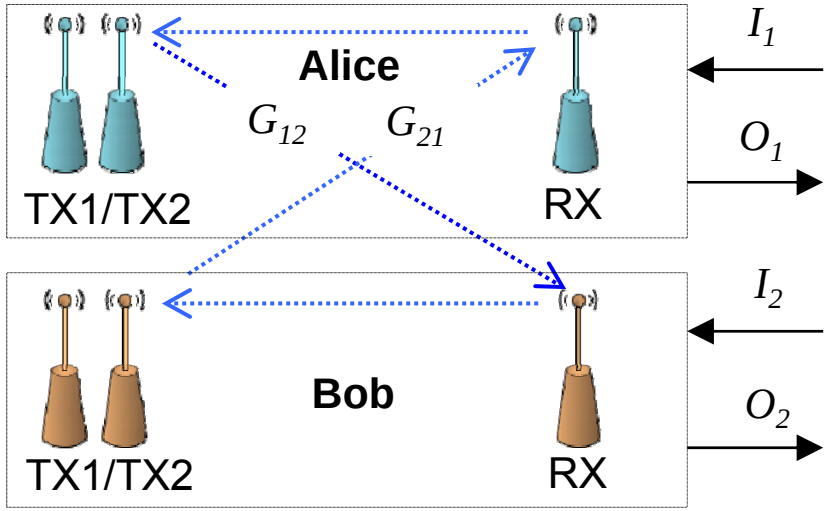
# Key Generation: A Simpler Approach

- TX1 & TX2 in each unit are used to create a null at their corresponding RX.
  - Beam-forming gains are measured (quietly) in each unit.
- Each unit transmits the sum of its received signal and its input, i.e., $I_1, I_2$.
  - $I_1, I_2, O_1, O_2$ (base-band signals) span a two-dimensional space.

$$\left.\frac{O_1}{I_2}\right|_{I_1=0} = \frac{G_{21}}{1-G_{12}G_{21}} \equiv \alpha \qquad \left.\frac{O_2}{I_1}\right|_{I_2=0} = \frac{G_{12}}{1-G_{12}G_{21}} \equiv \beta$$

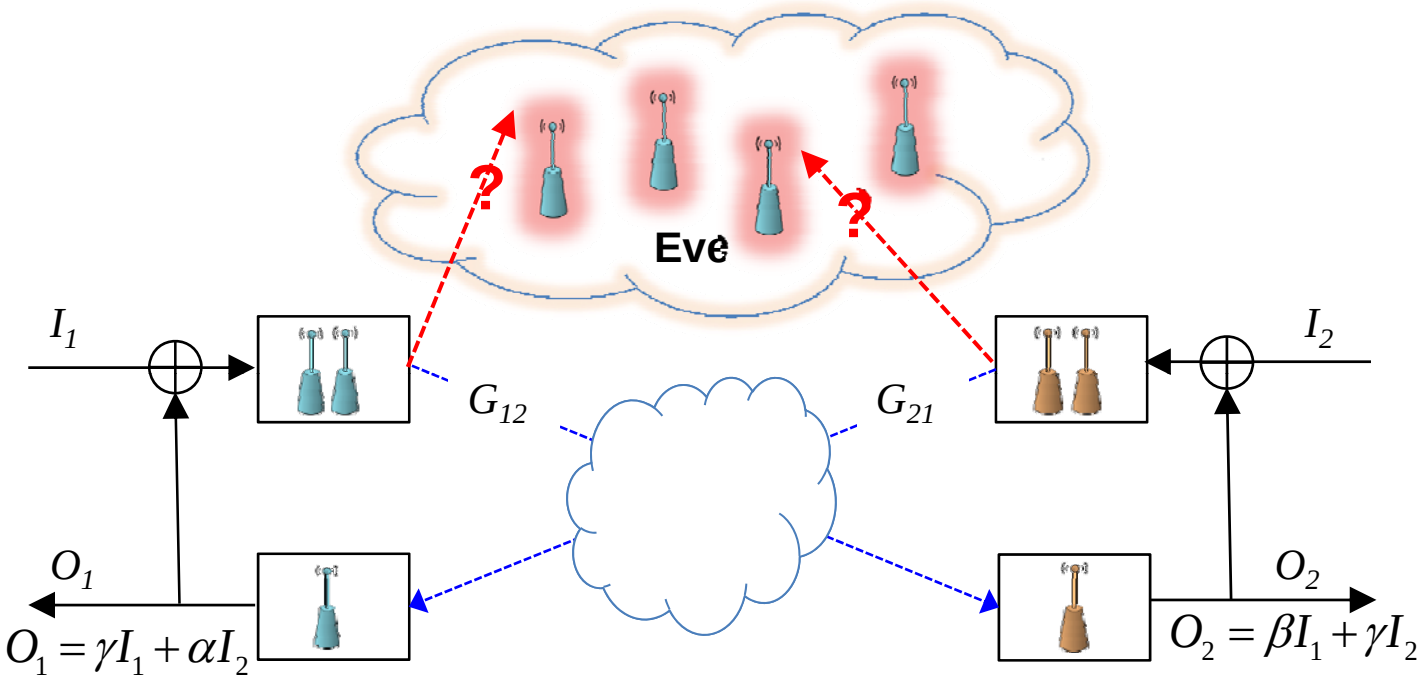
$$\left.\frac{O_1}{I_1}\right|_{I_2=0} = \left.\frac{O_2}{I_2}\right|_{I_1=0} = \frac{1}{1-G_{12}G_{21}} \equiv \gamma$$

$$O_1 = \gamma I_1 + \alpha I_2 \qquad O_2 = \beta I_1 + \gamma I_2$$




- Alice/Bob send (simultaneously) pilots *A/B*, followed by *–A/B,* respectively.
  - Each unit obtains two equations which are used to find phase values of $AG_{12}$ and $BG_{21}$.
  - For higher security, only one of the two phase values is used.
  - Channels are perturbed (at both units) prior to the next round.

# Key Generation: A Simpler Approach




$$\left.\frac{O_1}{I_2}\right|_{I_1=0} = \frac{G_{21}}{1-G_{12}G_{21}} \equiv \alpha \qquad \left.\frac{O_1}{I_1}\right|_{I_2=0} = \left.\frac{O_2}{I_2}\right|_{I_1=0} = \frac{1}{1-G_{12}G_{21}} \equiv \gamma \qquad \left.\frac{O_2}{I_1}\right|_{I_2=0} = \frac{G_{12}}{1-G_{12}G_{21}} \equiv \beta$$

- Key Point: Each eavesdropping antenna introduces a new unknown phase in listening to legitimate transmit units.

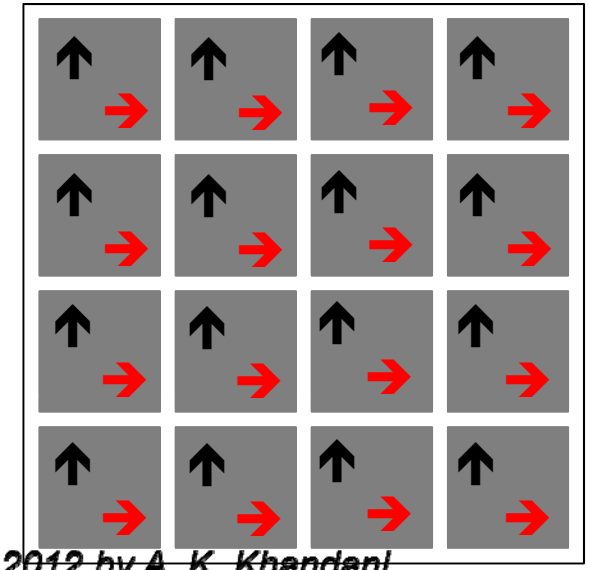
# Security Applications: Enhancing Capacity

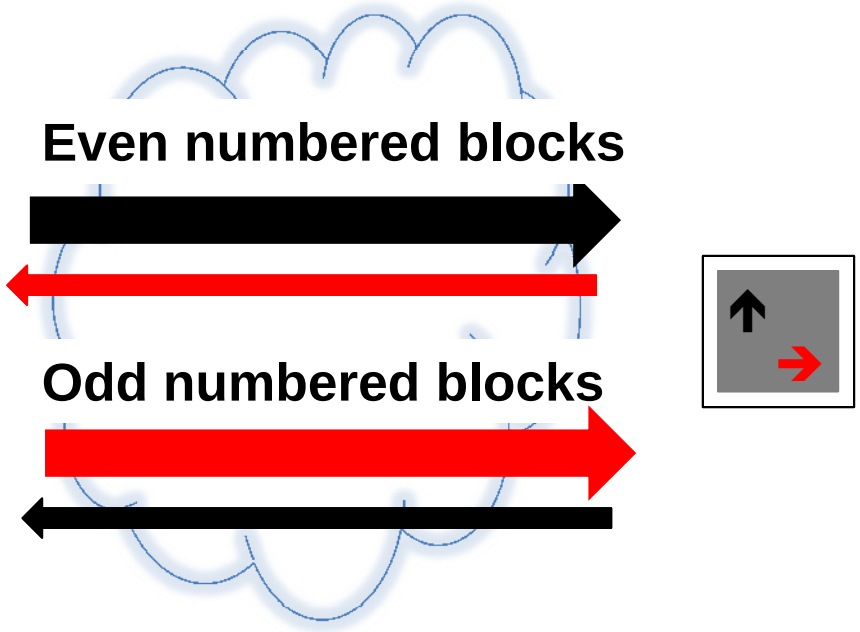
# Enhancing Security: **Increasing Confusion**

- Inherently more secure as Eve receives the sum of Alice's and Bob's signals.
- To further enhance security:
  - After the initial connection is established, Alice introduces a random offset in its carrier frequency for every new block of OFDM symbols.
  - Bob transmits the periodic preamble (used in OFDM for frequency synchronization) with high power and then transmits signal from a Gaussian code-book containing a secret key to be used by Alice in the next transmission block.

# Enhancing Security: **Improve Legitimate SNR**

- Transmitter side has N independent radios.
- Each radio has two antennas working either as TX or RX.
- The two sets in the main transmitter switch between transmit & training (receive) modes in subsequent blocks.
- Gain≈$\log_2(N)$, 20dB for N=100, and 10dB for N=10.





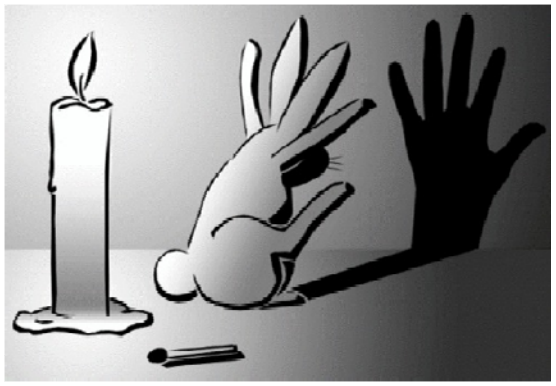
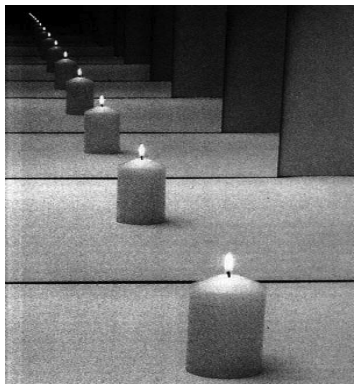
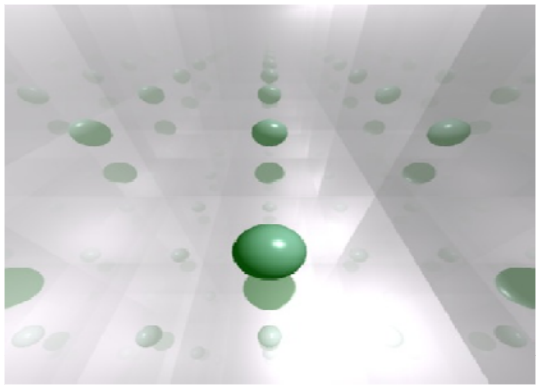
# A New Paradigm:
## Media-based
## vs.
## Source-based Wireless

# Source-based Wireless Communications

- Known methods for wireless transmission:
  - Source is varied to embed information and then passed through channel
    - Channel is a linear system with a Gaussian gain
    - Shannon capacity: $C \approx W \log(SNR)$
  - MIMO (most important breakthrough in wireless in last decade):
    - Using $N$ transmit and $M$ receive antenna results

$$C \approx \min(M, N) W \log(SNR)$$

# Media-based Wireless

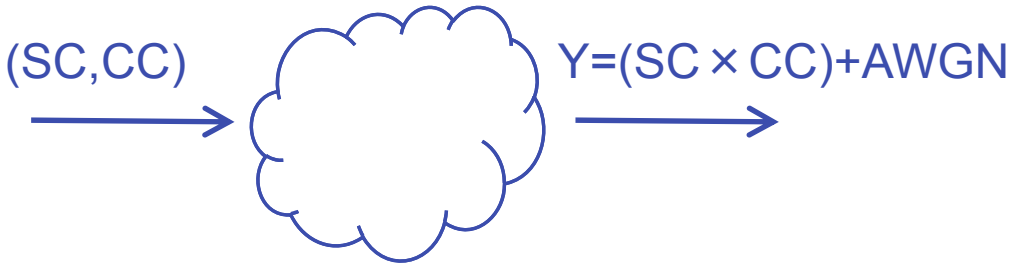
- Keep the source shining and change the media
- Enjoy rich variations with small changes in media
- Rich scattering environment: slightest perturbation in the environment causes independent outcomes.
- Variations of phase is critical and can be exploited with stable TX/RX synchronization using two-way link (continually sending back pilot from RX to TX).

# Media-based Wireless

- Solution for SISO:
  - Select the channel with the highest gain and use it with a Gaussian source. This results in a saving of energy scaling with log(|CC|).
- What about SIMO?
- $one$ transmit, $N$ receive antennas
- Unlike source-based case, signal received by different antennas will be linearly independent, resulting in a full rank constellation over the $N$ receive dimensions.
- Due to full rank property, rate embedded in the channel constellation grows linearly with $N$
  - Note that components of vector CC (gains to different RX antennas) are independent, but cannot be selected independently.

# Media-based Wireless: SIMO Case

- RF environment around transmitter, i.e., Channel State (phase, magnitude, polarization) can be selected (in each transmission) from a randomly generated set called Channel Code-book (CC).
- There is also a traditional code-book associated with the source called Source Code-book (SC).




Objective: Minimize P{outage}

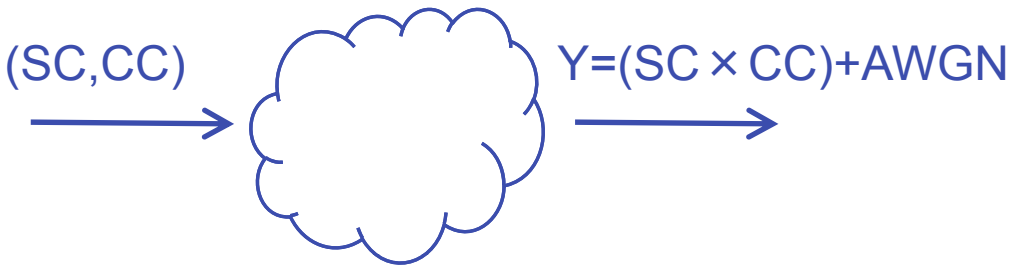
Min: $P\{I(CC,SC;Y)\leq\varepsilon\}$

Or Min: $P\{H(Y)\leq\delta\}$

s.t. $E(SC^2)\leq P$

- RX knows the elements of CC.
- TX does not know the elements of CC, but by using a simple feedback, TX and RX agree on a subset of CC to be used.
  - Consequence: CC is a discrete set (Constellation)
  - Due to Raleigh fading, distribution of CC has spherical symmetry.

# Media-based Wireless: SIMO Case




Objective: Minimize P{outage}

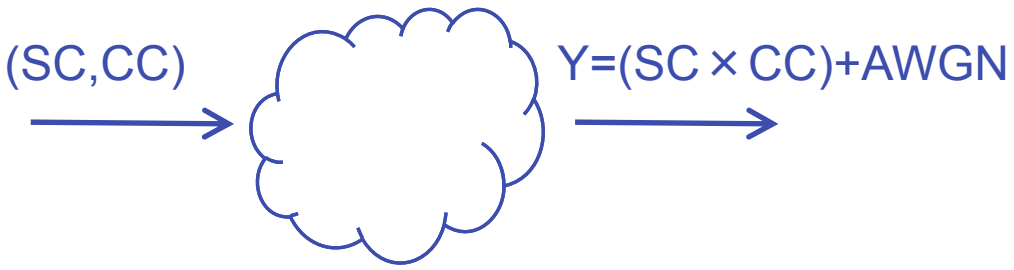
Min: $P\{I(CC,SC;Y)\leq\varepsilon\}$

Or Min: $P\{H(Y)\leq\delta\}$

s.t. $E(SC^2)\leq P$

- We assume cardinality of channel code-book is finite. Otherwise, the capacity would become infinity, which is unrealistic and reflects the fact that for large channel code-books, model of "rich scattering" will not be valid any longer.
- System is linear (superposition principle holds), but its impulse repose is changed prior to reaching to its steady state.

# Media-based Wireless: SIMO Case




Objective: Minimize P{outage}

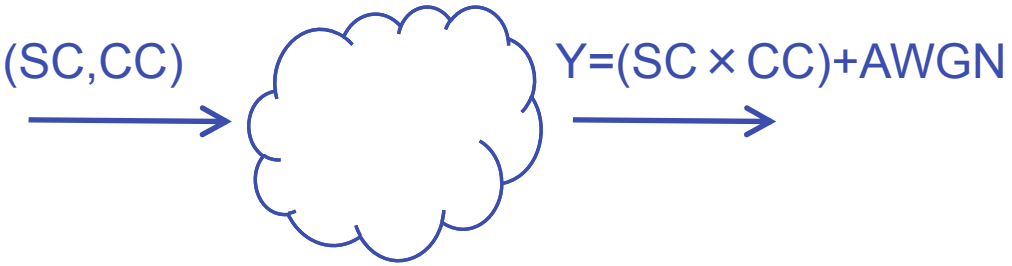
Min: $P\{I(CC,SC;Y)\leq\varepsilon\}$

Or Min: $P\{H(Y)\leq\delta\}$

s.t. $E(SC^2)\leq P$

- TX does not know the elements of CC, consequently:
  - TX selects the SC and the CC independently.
  - TX selects the elements of the CC with equal probability.
- At RX, SC spans a single complex dimension along received CC.
- Due to spherical symmetry in distribution of CC, optimization of SC involves only the distribution of the magnitude of CC.
- RX uses joint decoding to minimize P{outage}.

# Media-based Wireless




Objective: Minimize P{outage}

Min: $P\{I(CC,SC;Y)\leq\varepsilon\}$

Or Min: $P\{H(Y)\leq\delta\}$

s.t. $E(SC^2)\leq P$

- Consider $I(CC,SC;Y)=I(\angle SC;Y)+I(|SC|,CC;Y|\angle SC)$:
  - Due to spherical symmetry, optimum source codebook has a uniform phase. This can be verified noting that $P\{I(\angle SC;Y)\geq\boldsymbol{\theta}\}$ is maximized, for all **θ,** if $\angle SC$ is uniform and this choice affects neither energy, nor probabilistic behavior of $I(|SC|,CC;Y|\angle SC)$.
- We have: $I(|SC|,CC;Y|\angle SC)= I(CC;Y|\angle SC)+ I(|SC|;Y|\angle SC,CC)$.
  - As far as $I(|SC|;Y|\angle SC,CC)$ is concerned, $|SC|$ should be continuous.
  - As far as $I(CC;Y|\angle SC)$ is concerned, $|SC|^2$ should be constant , $|SC|^2=P$.
  - Sum is maximized using a discrete set of values for $|SC|$.
  - SC has a discrete set of circular shells used with different probabilities (to realize shaping gain), where points on each shell are equal likely.

# Power Spectrum

- Same old problem applies here: Signals cannot be both time and frequency limited.
- Received Power Spectrum:
  - Average of channels' spectrums times input spectrum
  - Input spectrum is shaped to limit the bandwidth.
  - Input source simply transmits the carrier, with modulation of SC, times the pulse shaping signal.

# Challenges and Solutions

- Challenge 1: Frequency synchronization between transmitter and receiver
  - Solution: Receiver is two-way and continually sends a pilot to the transmitter.
  - No restriction on spectrum of pilot as the media variations causing frequency expansion is done at the neighborhood of the transmitter.
- Challenge 2: Receiver needs to learn the channel code-book (channel constellation) and adopt to it.
  - Not too hard using a training phase (similar issues exist in MIMO).
  - RX can use correct frames to fine-tune its learning of constellation.

# Some General Remarks

- Equalization:
  - Channels with an impulse response of length $M$ provide $M$ extra dimensions per receive antenna (by inserting time gaps between subsequent transmissions).
- Constellation design:
  - Optimizing the tradeoff between “selection gain” and “rank gain”.
  - Method: Relying on two-way link, receiver helps in building the constellation.

# Some Remarks about SISO Case

- Let us consider a channel impulse response of length $LT$ where $T$ is symbol period.
- Base-TX signal is a sinusoid windowed in $[0,T]$ multiplied by a spectrum shaping signal $s(t)$ with spectrum $S(w)$.
- Base-RX signal is a Gaussian random process, time limited in $[0,LT]$, of auto-correlation $R(a)=1-|a|/T$, convolved with the inverse Fourier transform of $\{S(w)\}^2$

# SISO Case Revisited

- TX block is a train of $K$ consecutive base TX signals, followed by $L$-$1$ zeros prior to the next TX block.
- Channel in changed in each of $K$ time slots among $2^r$ possibilities, resulting in a linear system with a random impulse response.
  - Time shift in input results in the same time shift in the response.
  - Oversample RX signal (sum of time-shifted responses) by $L$.
    - $KL$ samples are full rank, yielding $LK^2/(L+K-1)$ dimensions per unit time.
    - Extra dimensions are correlated, degrading the performance.
    - Noise is correlated, improving the performance.
    - Iterative or Trellis decoding can be used for detection.
  - Source code-book is composed of a discrete set of shells (circular shells) with uniform phase.

# Perturbing the RF Channel

# How to Change the RF Channel?

- Changing channel phase is the key behind “security” applications.
- Changing channel state (phase, polarization, gain) is the key behind “media-based” applications.
- Tunable RF is a well established area of research.
  - Traditionally, focus in the RF literature has been on:
    - Changing and controlling direction/density of energy flow.
    - Changing of phase has been usually in the context of applying phase shift to the signal prior to transmission, or after reception, again motived by energy considerations in the context of beam-forming.
  - Interest here is to move from one random state (primarily channel phase) to another independent random state.
    - Neither interested in knowing the state, nor in controlling it.
    - Easier to accomplish as compared to traditional beam-forming.

# Conclusion

- Two-way wireless will have a profound impact on wireless networks in terms of cost, quality of service, efficiency and security.
  - Has more to offer than earlier breakthroughs in the last few decades.
- What is next:
  - Industry
    - Including two-way in new standards
    - Implementation is straightforward (mobile and/or base-station).
  - Academia
    - Materials and RF structures  for varying the channel
    - Network Information Theory of two-way wireless
    - Security and Key Exchange

# Frequently Asked Questions

- Q: Why most of discussion and reported implementation is based on using separate transmit and receive antennas?
- A: The sole reason has been to reduce complexity of hardware implementation based on the available platform which supports multiple antennas.
- Q: Why presentation is based on using corrective beam-forming (which requires two transmit antennas) rather than signal injection?
- A: Again, the reason has been to reduce complexity of hardware implementation, and also make it possible to study various signals involved in cancellation. It should be obvious to a person skilled in the area that similar results would be obtained using signal injection.
- Q: What is the size of A/D and D/A used in the implementation?
- A: A/D and D/A were limited to what is in the hardware of Lyrtech platform (14 bits A/D and 12 bits D/A). We did not have any indication that A/D or D/A would act as performance bottleneck even if the number of bits is significantly lower. Also, A/D and D/A of a decent size are readily available at sampling rates required in typical wireless applications. Requirement on D/A accuracy is less than A/D, as inaccuracies in D/A do not contradict linearity and will be subsequently canceled in the final stage in the base-band.
- Q: What would be an immediate application of full-duplex nodes?
- A: The primary benefit of full-duplex is in networking applications where a central node can transmit, while listening to new clients who want to join the network. This can be achieved by having full-duplex data links (using OFDMA) and half duplex superimposed control signaling. Also, the clients do not need to support full-duplex and central node can transmit data to one and receive data from another. This feature can be added to many of current OFDMA networks with small modifications.
- Q: How is the degradation in SNR (Residual self-Interference plus Noise divided by Noise, RINR) measured?
- A: Power of residual self-interference+noise is measured in non-zero OFDM tones. Power of noise is measured in both OFDM zero tones as well as when transmitter is off (no significant difference was observed). In the reported tests, AGC was disabled (LNA gain was once manually set) to have a better framework to compare different schemes in terms of RINR (AGC saves some A/D bits). Tests were performed over 802.11 channel 13 which is not used in North America (to reduce interference from neighboring nodes). RINR is averaged over several thousands OFDM frames. Measurements were also performed to measure the equivalent of RINR is a half-duplex link. This accounts for the degradation in SNR due to various mismatches which can be quite significant in half-duplex connection between distant nodes, while these are avoided in a full-duplex system due to having access to the same clock/carrier/timing in cancellation of self-interference. Results show that the degradation is generally higher than what is observed for RINR, and consequently the observed RINR due to adding the full duplex feature is even less significant. These results are not reported due to space limitations as well as the fact that the results would depend on the specific implementation (in our case, we have followed the conventional methods used in typical 802.11 receivers for carrier/time recovery and signal detection).
- Q: What is the setup for channel measurement in self-interference cancellation?
- A: We examined sending 3 consecutive pilots (long training sequence used in 802.11) with averaging to improve the channel measurement of the first phase, but the result was similar to the case of using a single pilot. In general, the system is very robust to such errors as the effect does not violate linearity and consequently subsequent stage of cancellation in base-band will account for such errors. For the second phase, number of pilots (again long training sequence of 802.11) used for averaging is adaptively adjusted depending on the conditions (to make sure second stage is always useful). The more effective is the first stage of active cancellation, the higher should be the accuracy of channel estimation in the second phase and two complementary adaptation rules are used to select the number of training sequences used in the second phase.



***PLEASE SEE THE SEPARATE FILE FOR UPDATES***. 

# Thank You

khandani@uwaterloo.ca
519-8851211 ext 35324


Ontario Centres of Excellence

Canada Foundation for Innovation
Fondation canadienne pour l'innovation

Canada Research Chairs

NSERC
CRSNG

UNIVERSITY OF
Waterloo