RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: **MBS-R05**

What IT Professionals Need to Know about Sniffing Wireless Traffic in 2016

Dr. Avril Salter, CCNP-W

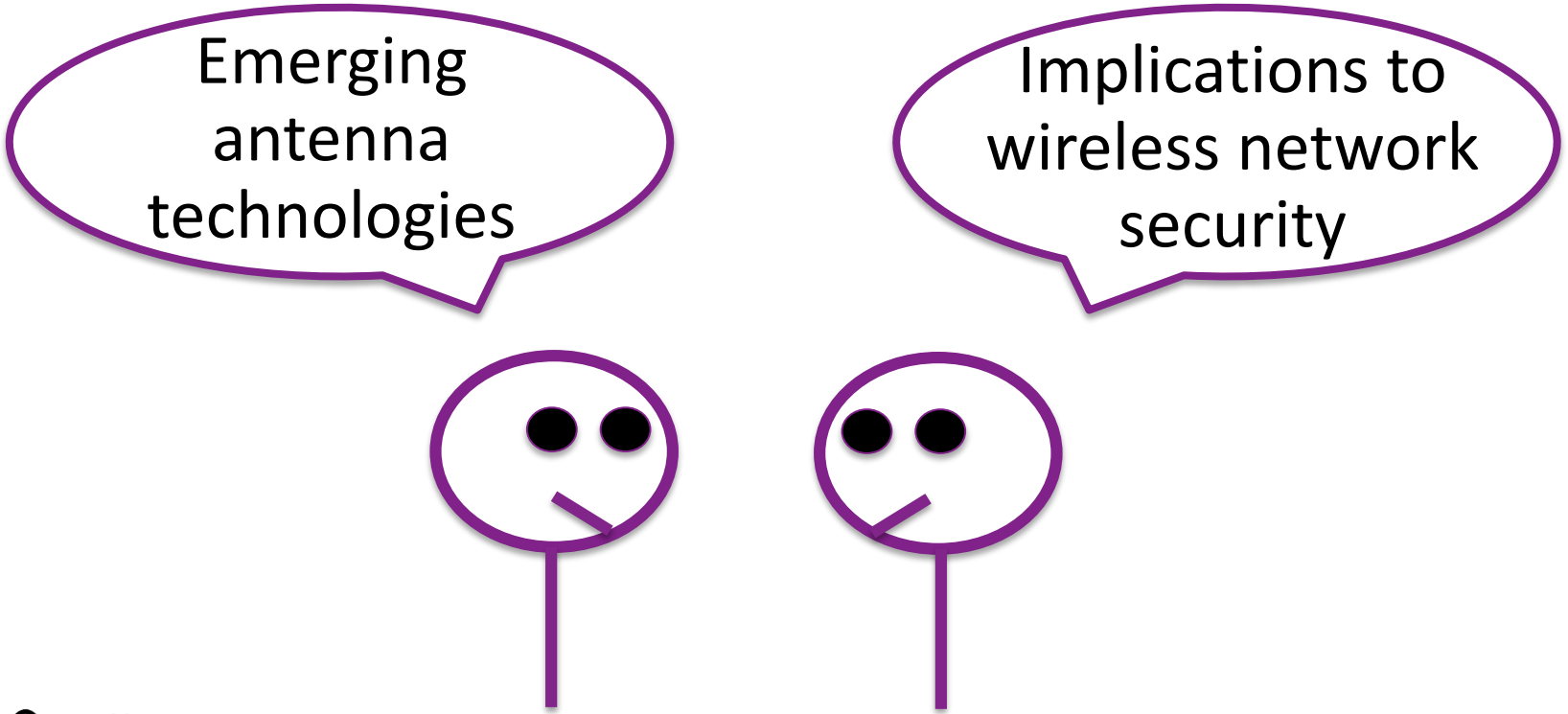
Wireless Implementation Architect

Salter & Associates

@avrilsalterUSA

#RSAC

What We Are Discussing



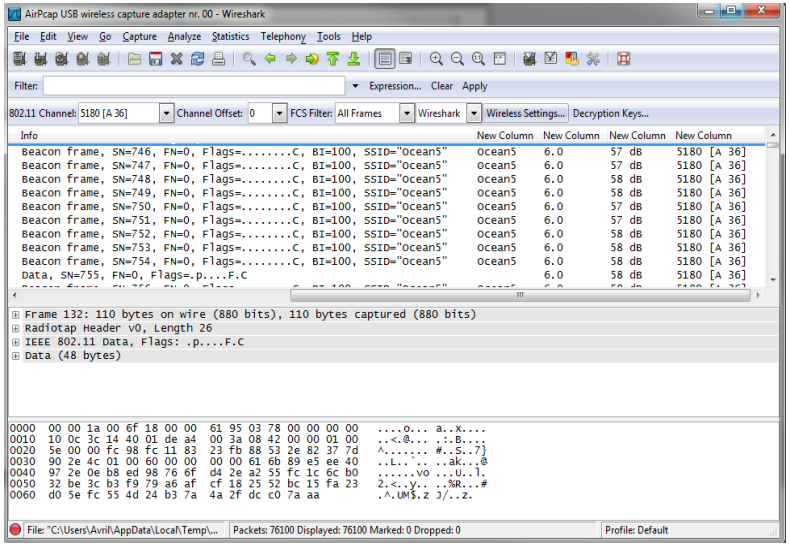
Privacy Rights

- Electronic Communications Privacy Act (ECPA)
  - Protects e-mail messages from interception and disclosure to third parties
- Wiretap Act
  - Federal law protecting privacy of communications
  - Intercept, disclose, or use the contents of any
    - Wire
    - Oral
    - Electronic communication

- Exceptions allows employers to monitor communications in the ordinary course of business

Protocol and Spectrum Analyzers

Protocol Analyzer



Spectrum Analyzer

Which Networks Can You Sniff?

Technology

- Wi-Fi
- Cellular
- Bluetooth
- ZigBee

Influencing Factors

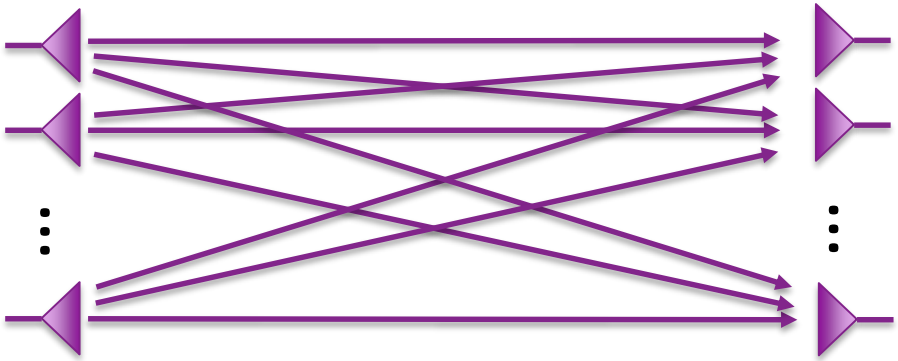
- Different network adapter
- Range depends on
  - Transmit power
  - Receiver antenna gain
  - Frequency bands

Defining MIMO

Input into the RF medium

Output from the RF medium

n transmit antennas



m receive antennas

Multiple Input antennas + Multiple Output antennas

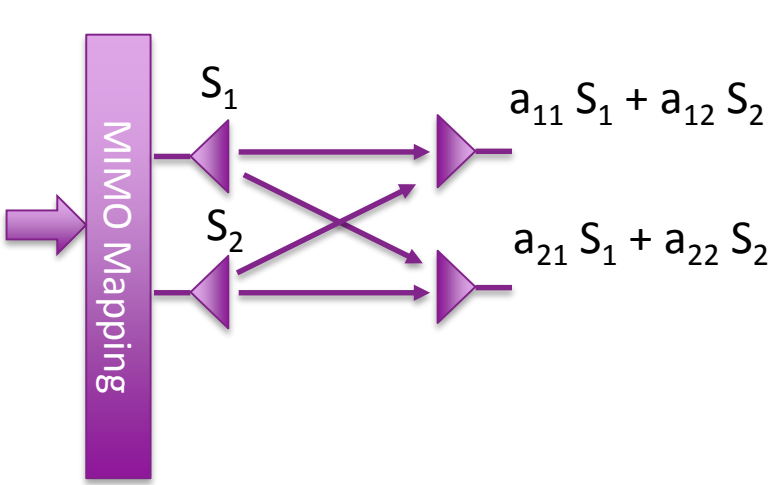
= n x m MIMO

Multi-Antenna Technologies

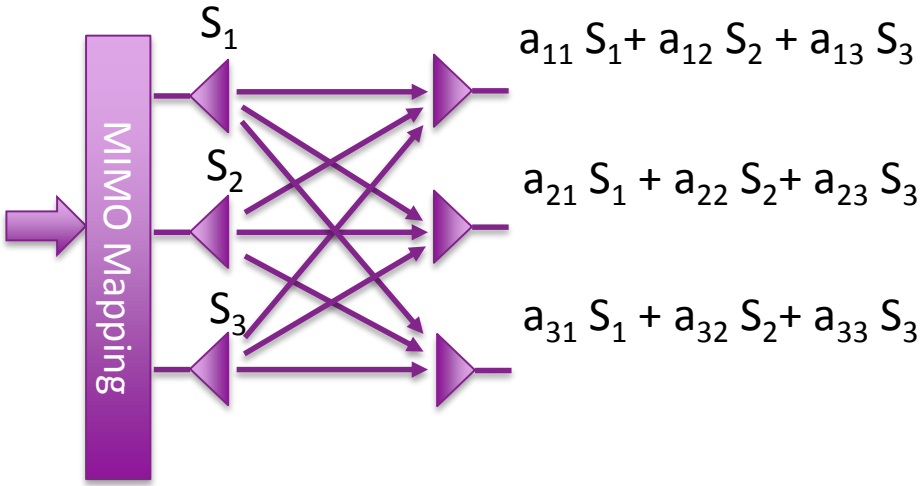
Mechanism	Performance advantage
Spatial Multiplexing	Higher user data rates
Space Time Coding	Improves SNR - Coverage
Beamforming	Extends the range where higher data rates can be attained
Multi-User MIMO	Increases throughput

Spatial Multiplexing

- 2x2 MIMO



- 3x3 MIMO



Spatial Multiplexing

Number of receive antennas ≥ Transmit antennas

Implications

1x1 MIMO

1x3 MIMO

2x2 MIMO

2x3 MIMO

3x3 MIMO

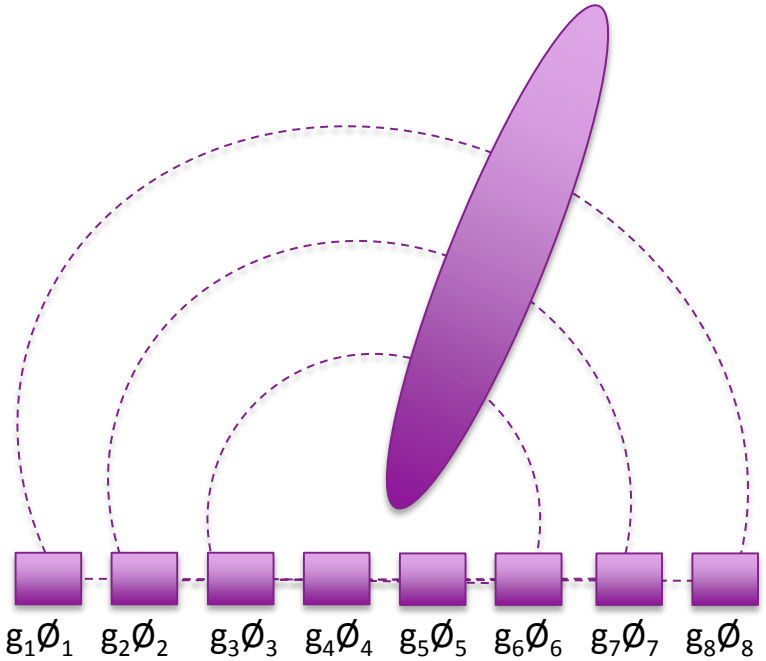
3x3 MIMO

Are you capturing all the wireless traffic?

Beamforming

Creating Radiation Patterns

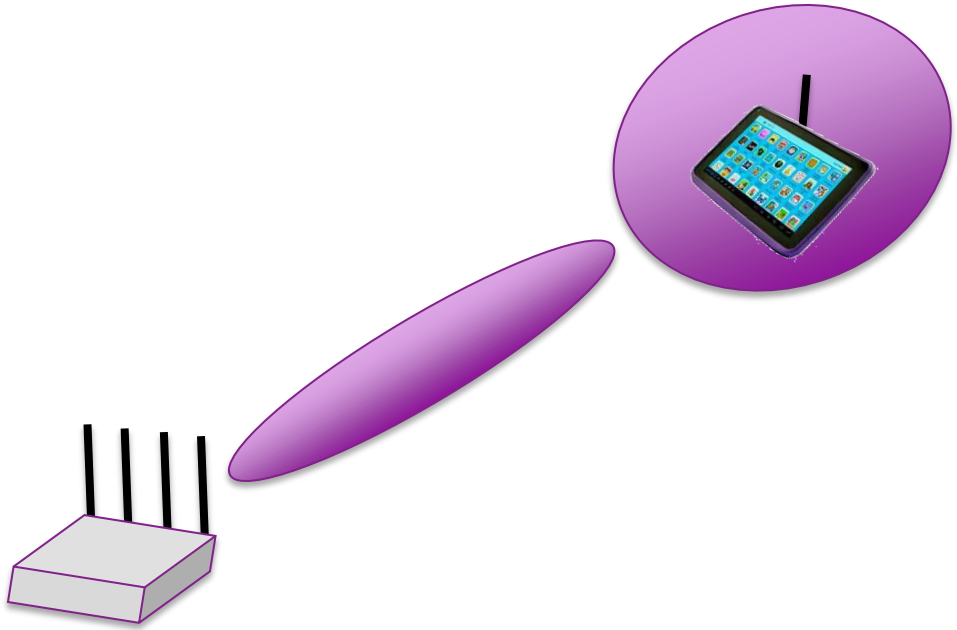
- In theory
  - N * (N - 1) beams
  - N - 1 nulls



Antenna Reciprocity

It is common practice to describe antenna characteristics from the perspective of the transmitter

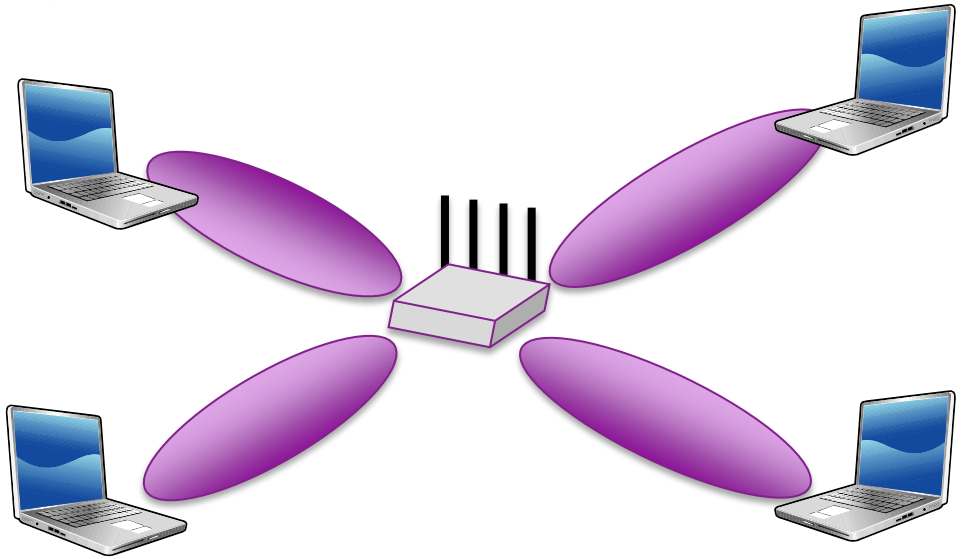
Implications



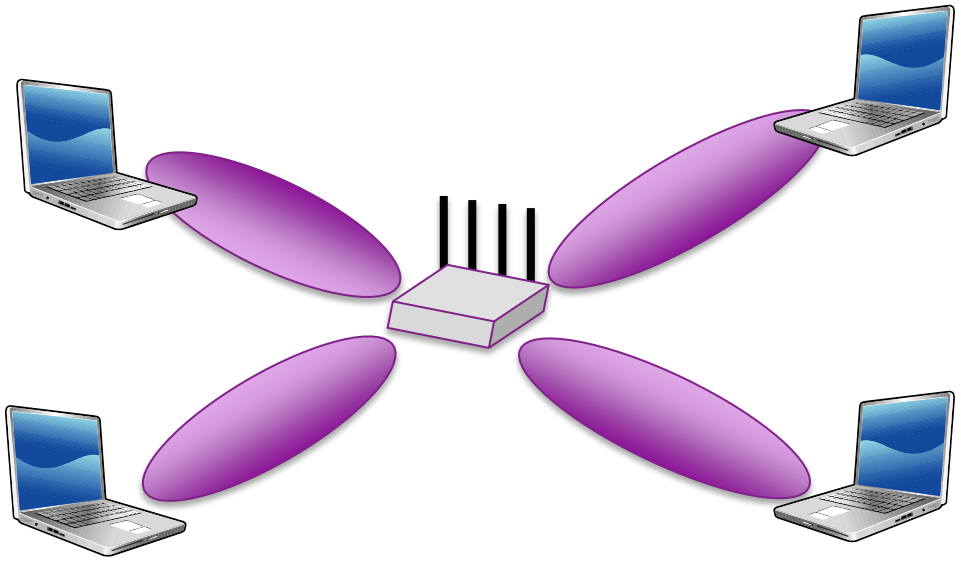
Are you capturing all the wireless traffic?

Multi-User MIMO

- Transmit to multiple users
- On same frequency channel
- At the same time



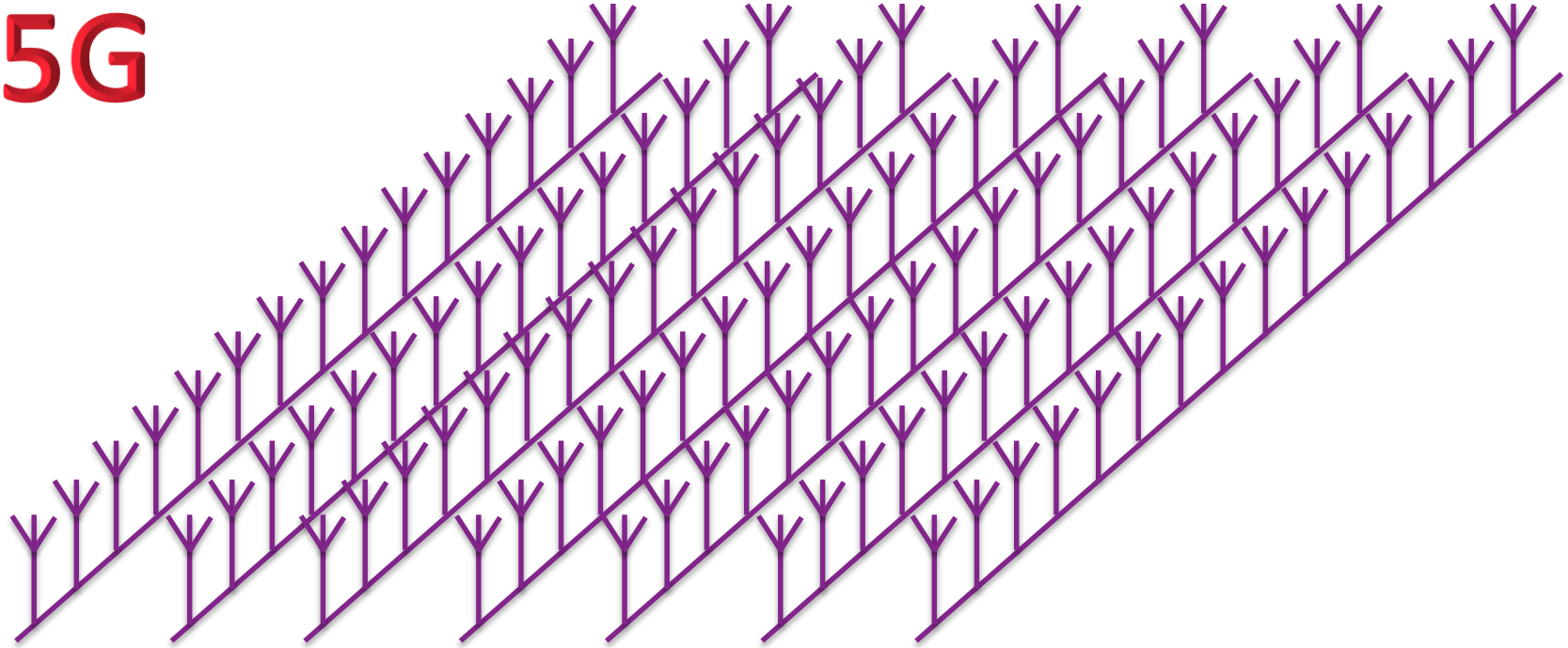
Multi-User MIMO



Are you capturing all the wireless traffic?

Massive MIMO

5G



What You Need To Know

MU-MIMO

- Mobile networks
  - LTE Advanced
- Wi-Fi networks
  - 802.11ac
- 5G

Omni-directional antennas

- IoT networks
  - ZigBee
  - WirelessHart
  - ISA100-11a
  - Wi-SUN
  - Bluetooth Low Energy

What About IoT Networks

- Requires explicit feedback
- Size and power performance limitations
- Multi-hop mesh for reliability

Implications

- Over-the-air captures are significantly more complex
  - Arguably some wireless networks are more secure
- Hackers would need techniques that minimize use of MU-MIMO
  - E.g. Disruptive interference

What You Should Do Now

- Know the limitations of the antenna technologies you are using for analyzing over-the-air traffic
- Understand disruptive techniques and how to identify them

Thank you for listening ☺

www.**linkedin**.com/in/**avrilsalter**
@avrilsalterUSA