Raytheon BBN Technologies
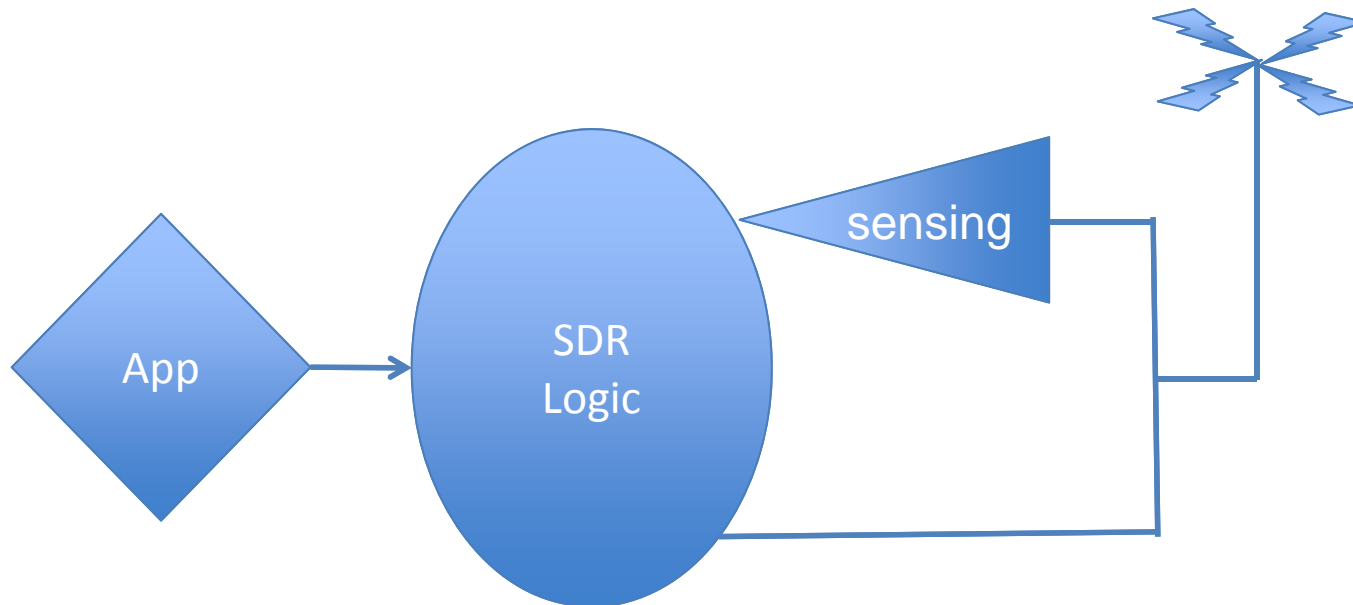
Network Measurement in a World of Software Defined Radios

Dr. Craig Partridge
Chief Scientist – Network Research
AIMS Workshop

Raytheon
BBN Technologies

SDRs are Chameleons

- They change frequencies and protocols as applications and local RF conditions require
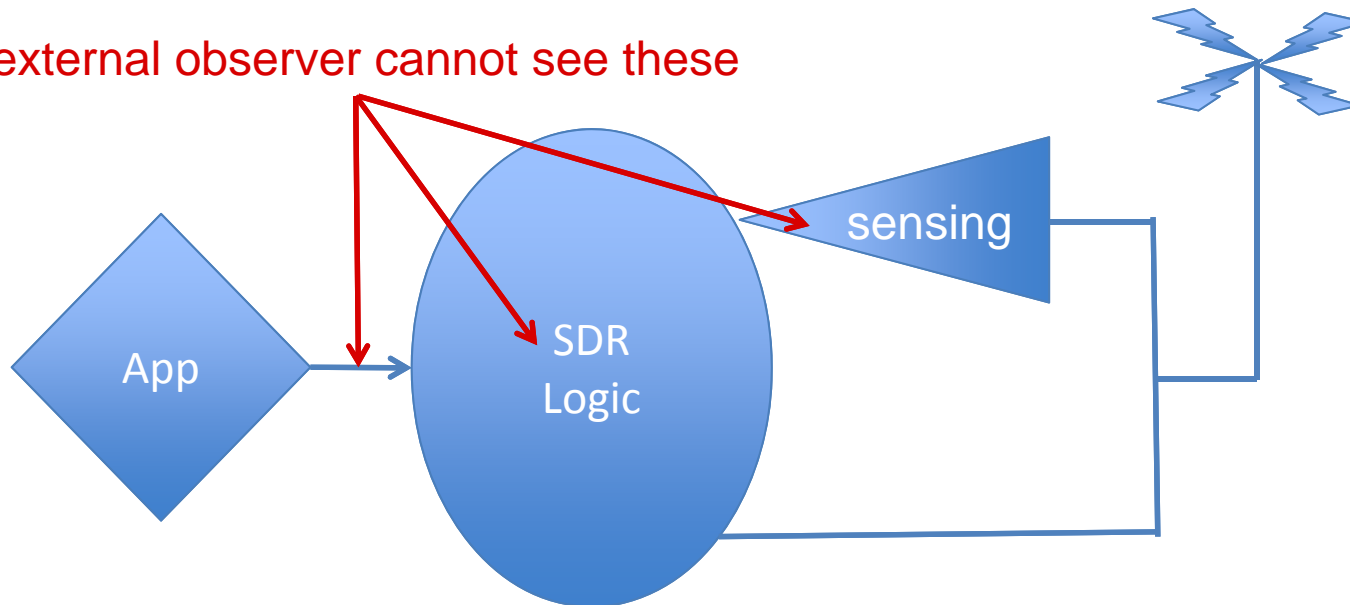

- Many measurement challenges
- Many things to measure (black box SDR net's performance, protocol stack performance, SDR decision making, etc…)

SDRs are Chameleons

- They change frequencies and protocols as applications and local RF conditions require

An external observer cannot see these

App → SDR Logic → sensing

- Many measurement challenges
- Many things to measure (black box SDR net's performance, protocol stack performance, SDR decision making, etc…)

SDRs are Chameleons

- They change frequencies and protocols as applications and local RF conditions require
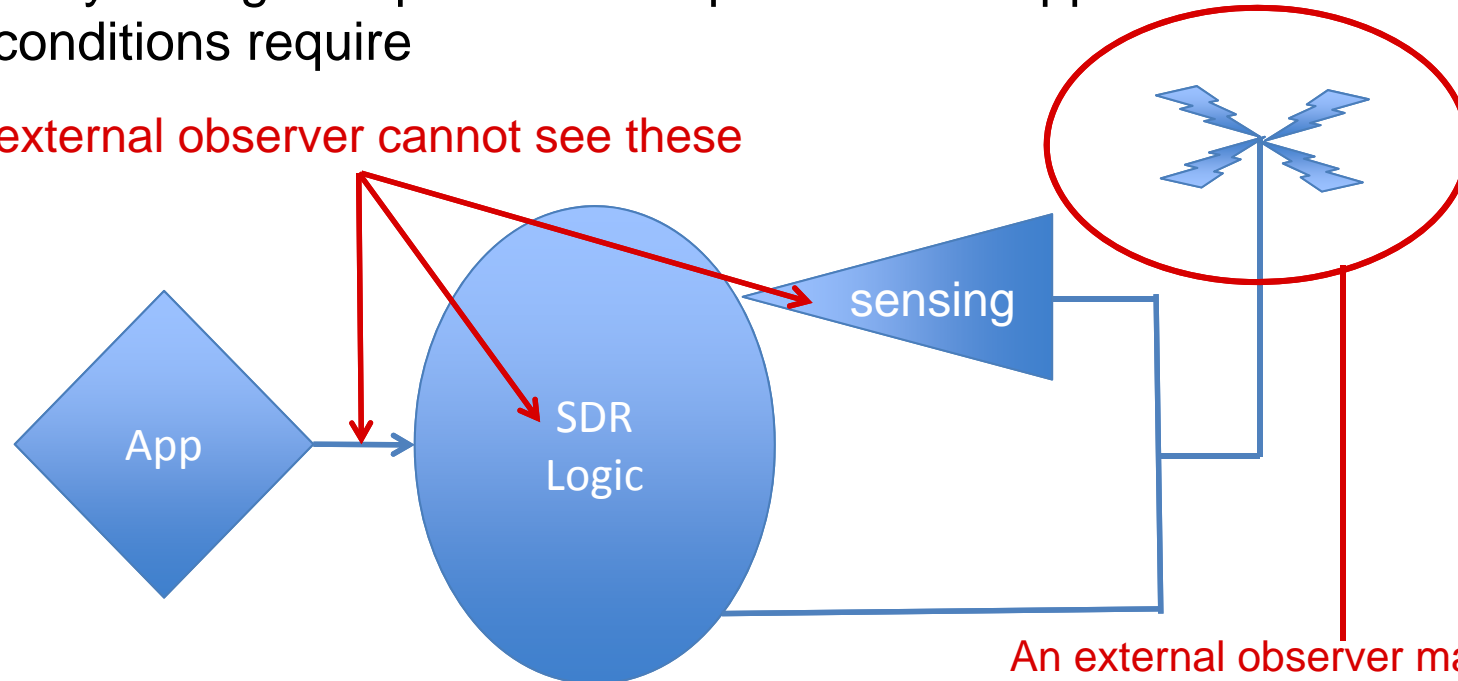
An external observer cannot see these

App

SDR Logic

sensing

- Many measurement challenges
- Many things to measure (black box SDR net's performance, protocol stack performance, SDR decision making, etc…)

An external observer may see only part of the radio transmissions (in and out) and does not know which frequencies the SDR was listening for…

What Might An Outside Observer Do?

- Use sophisticated spectrum capture devices that…
  - Can identify emitters
  - Can infer protocols
  - Blanket the measurement area with these devices to catch all signals
- Listen to the control/coordination channel
  - Many spectrum agile systems have them (e.g. P1900)
  - Tells you what the radios plan to do
- Unfortunately
  - Not clear such a spectrum capture device exists or is affordable or meets most needs
    - Wide spectrum to see everything limits sensitivity, due to noise
    - Narrow spectrum sensing with fast scanning limits what you can see at any one time
    - Also if you don't know channel being used, you may only capture part of the band.
  - Not all spectrum agile systems use control channels (e.g. white space)

Radios Observing Themselves?

- If you can't do the measurement from the outside, may need to measure from the inside

- Each radio logs what it does
  - This is what we do in the WNAN radio
  - Modern radios tend to have memory available for logging some classes of information
    - There are limits: can't retain all IQ samples for long

- Obviously questions about what to log
  - Measurement issues (what to collect to answer key measurement questions)
  - Catching everything across all radios in a network is a LOT of data to analyze
  - Privacy issues (how to retain user's privacy)
    - location is often THE most useful thing to know and also the most sensitive

- Also some practical issues
  - Radio is a real-time system and don't want to perturb its performance during measurement

Additional Comments

- Not all collection problems follow this pattern
  - Cf. Kone et al, "On the Feasibility of Effective Open Spectrum Access" at IMC 2010 (capture fine grain spectrum presence measurements, then run various algorithms to see what capacity can be achieved)

- What data to collect?
  - I'm a minimalist – there's a lot to be learned from very little
  - Cf. Cousins et al, "Understanding encrypted networks through signal and systems analysis of traffic timing", Aerospace 2003 (timestamp + emitter ID reveals a lot of info about traffic streams and apps)