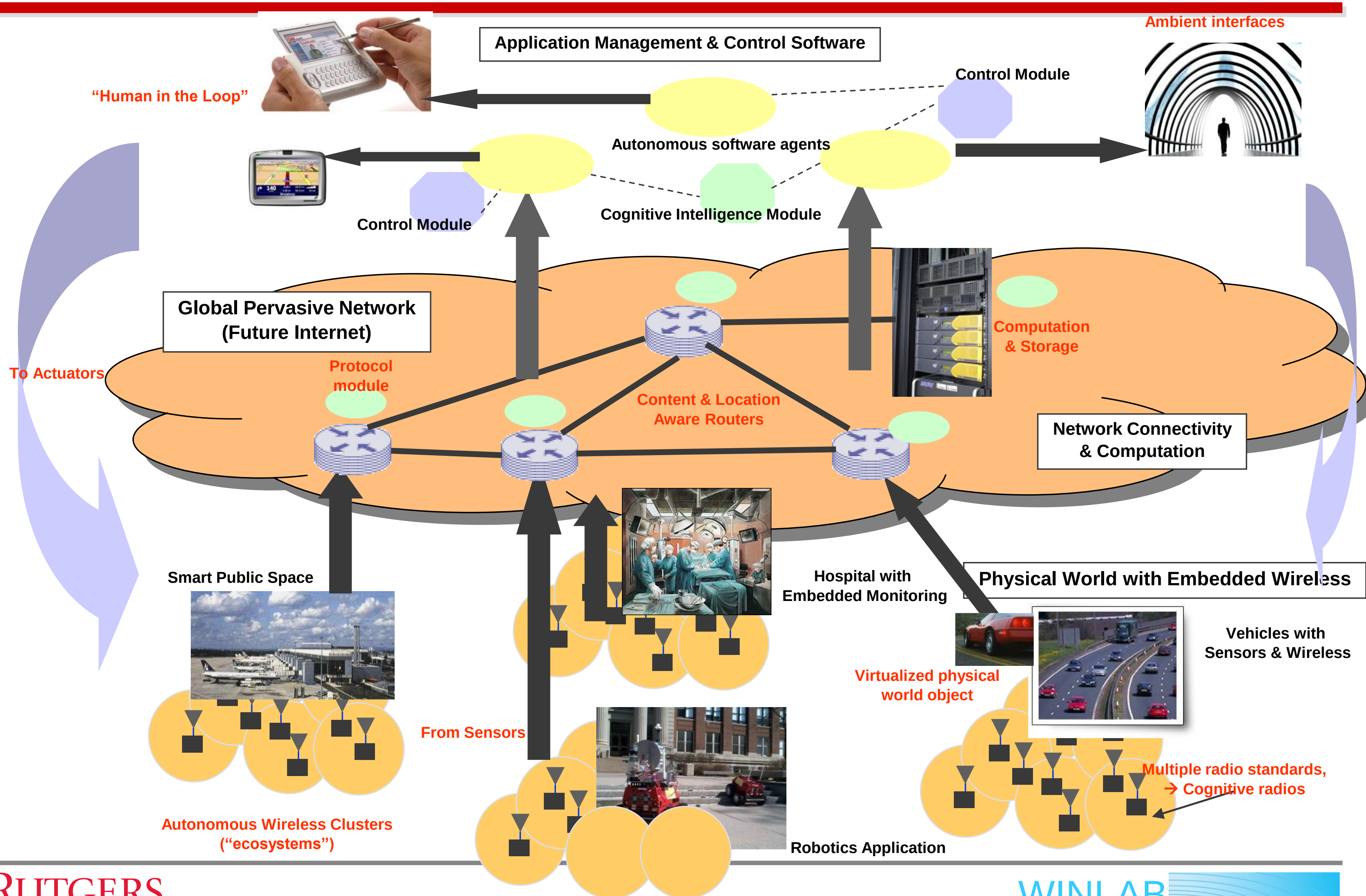
Putting Wireless Signal Security in a System Security Context

Wade Trappe

Opening Statement

- What is a system (or ecosystem)?
  – A system is a collection of interacting and possibly (but not necessarily) dependent parts that collectively form "a whole".
  – Systems are often characterized by their **boundaries**.
- Claim:
  – An examination of the world we live in reveals we are interacting in many new and varied ways.
  – But this is **tearing down** a variety of boundaries, which is exposing us to serious risks.

“Wireless Ecosystems” represents the next generation of pervasive computing systems



Hacking and Protecting the Wireless Ecosystem: Purpose of this Talk

- **Over-arching objective:** A call to action, wireless **signals** are everywhere, let's think about how we can use them for good and for evil…
- How we aim to do this:
  - High-level look at potential security/privacy services or attacks
  - **Attack:** Examine how easily the wireless ecosystem can be subverted…
  - **Try to arrive at a "system security perspective"**
    - ***Professional, pragmatic and researcher views***
  - **Defend:** Examine specific flavors of signal security services to protect the wireless ecosystem
- **Secondary objective:** Have fun! Get your hands dirty… leave your MATLAB at the door!
- **Tertiary objective:** Conclude with problems to look at, hurdles to overcome, etc…

Attacks… Really, we don't learn anything, do we? (aka, wireless everywhere, choose one to hack)

Subverting Wireless Automotive Sensors
Subverting Wireless Power Meters
Subverting Your Medical Privacy

This work appeared in various places

Thanks to our collaborators who suffered to bring these stories to you…

Case Study: Spoofing validation

- Tested on two equipments:
  - ATEQ VT55 validates packet structure.
  - A car using TPS-A validates ECU’s logic.
    - *40 packets per minute*

- Observations
  - No authentication;
  - No input validation and weak filtering
  - Warning lights only depend on the alarm flag, not the real pressure
  - Large range: 38 meters with a cheap antenna without any amplifier
  - Inter-Vehicle Spoofing is feasible; travel speed 55 km/h and 110 km/h

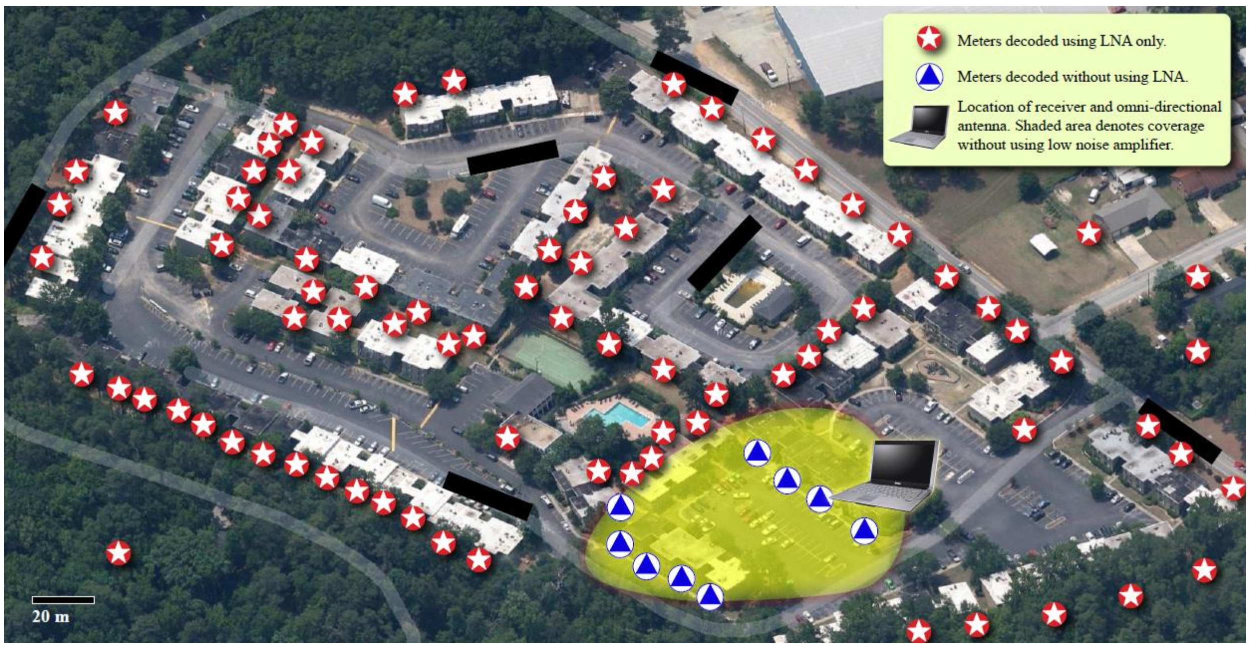
• TPMS-LPW Light

• Vehicle's warning light

Case Study 2: Smart Meter Privacy and Security

- Analyzed existing smart meters with USRP software radio

- Meters broadcast every 30s
- Able to spoof readings and eavesdrop on hundreds of meters



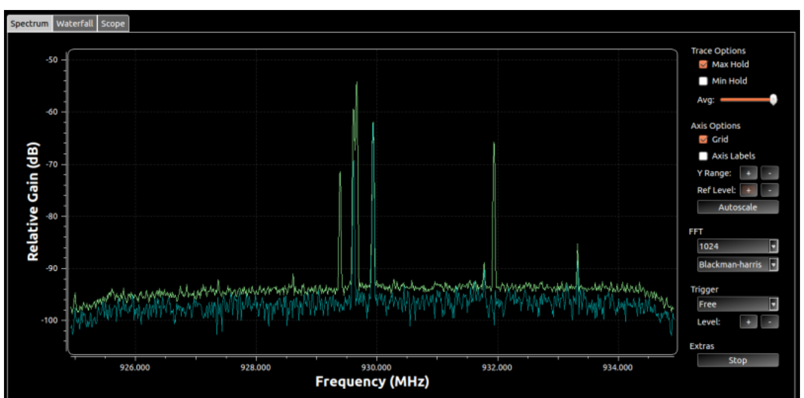
Case Study: The IoMT goes beyond the sensors themselves! To close the loop one must reach the doctors… and this is a potential weakpoint.

- What about the paging system?
- Many existing medical paging systems use the FLEX paging protocol
  - Paging protocol developed by Motorola used by many pagers
  - Main alternative to POCSAG
  - Operates in many common bands, such as the 929MHz and 931MHz paging bands
- Paging messages are "in the clear"

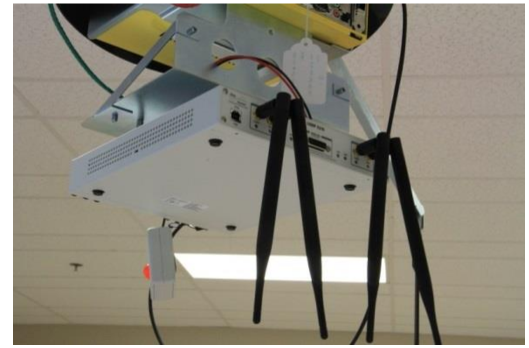
- We present the results of a quick "data collect" to show how bad this problem is and can be.
- Key take-away:
  - **This was EASY!!!**

The data collect…

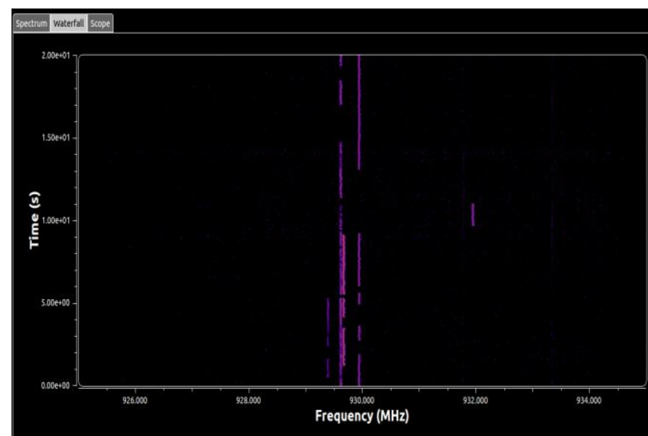
- We used:
  - COTS software defined radios
  - USRP X310 w/UBX RF daughterboard
  - Laptop (GNU Radio) w/usrp_flex python script
- Focused on 929 MHz band
  - Transportation services
  - Medical communication



- USRP X310



- Lots and lots of paging…



- Wonder what the talking is about?

What we observed: data is in the clear. Much of this data can be valuable to malicious parties.

- Full patient/physician names
- DOBs/potential SSNs
- Medical conditions/diagnoses
- Phone numbers/Room Numbers
- Snapshots of results have names, dates changed, and ***XXX*** to preserve patient privacy

Start ER ADULT to Dest DIALYSIS via Bed Patient Name **XXX** , Wilma DOB **XXX**/8/ **XXX** Routine **XXX** - **XXX** -03

Assign: Bed: 218W Available | M/S 6A Patient: SHERYL **XXX**, [Female] [DOB:**XXX**/12/**XXX**] PAIN, UNSPECIFIED| Phys: **XXX**, FRED

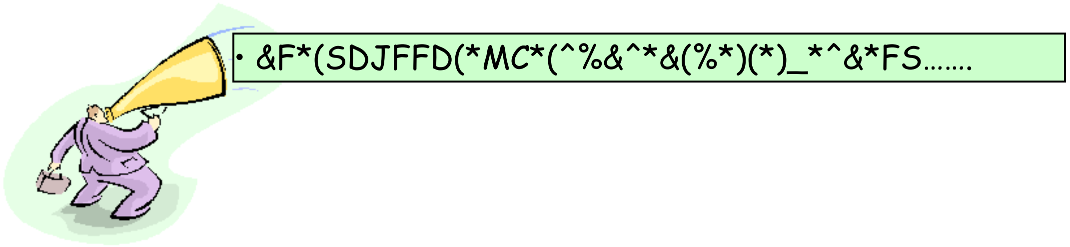
ASSGN RTM: **XXX**, JANE 48 Visit #: **XXX** F Isolation:None Dest Room-Bed: 10A 9B14 B Dest Bed Status: Clean Origin Unit: RH ED Admitting: **XXX**, PATEL MD Diagnosis: CHEST PAIN, OTHER

Subj:RETU.Msg:**XXX**, RINALDO, chf chest pain trop neg. EKG unchanged 231556. (ForwardMsg:187**XXX**697). Forwarded From: **XXX**@intellimsg.net

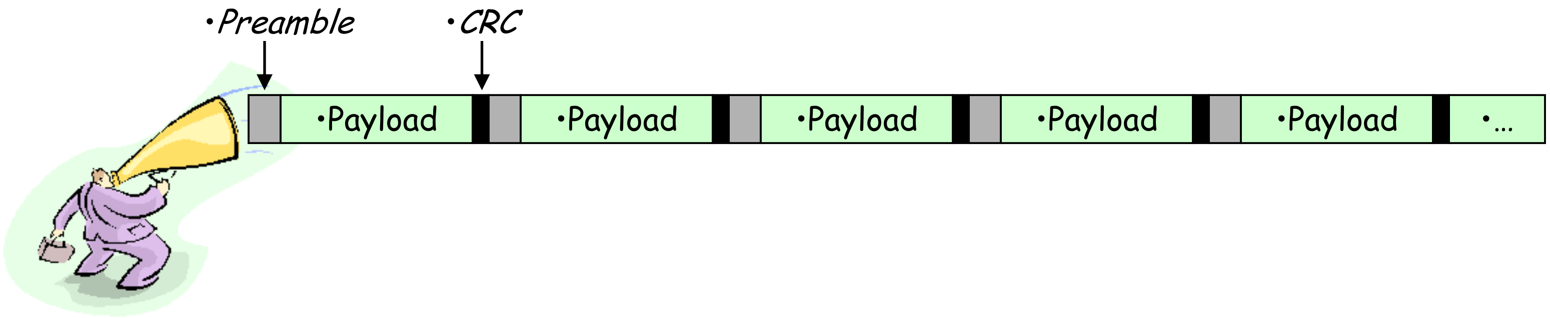
XXX, DAVID (AA01126**XXX**) checked in into ICU / 215. DOB: **XXX**/23/**XXX**. Complaints: ATRIAL FIBRILLATION.

CHARLENE ***XXX*** VIEW HOSPITAL `**XXX**-**XXX**-8112 * `**XXX** DEREK `JONATHAN `OUTPATIENT`BRAIN `ONLY RECIEVED PARTIAL ORDERS FOR THERAPY. NEEDS THE ORDERS. `

Jamming is Easy: Jammer Attack Models

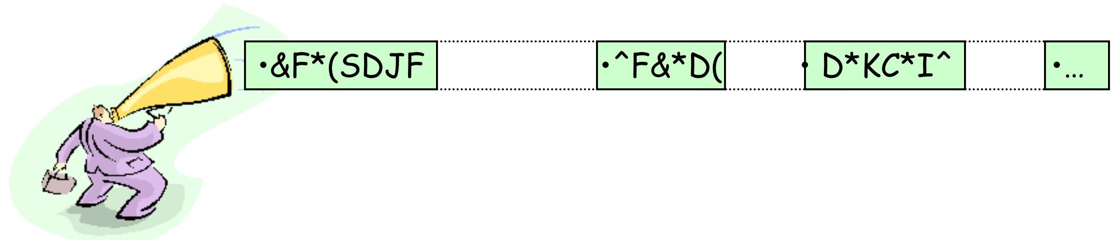


- Constant jammer:
  - Continuously emits a radio signal

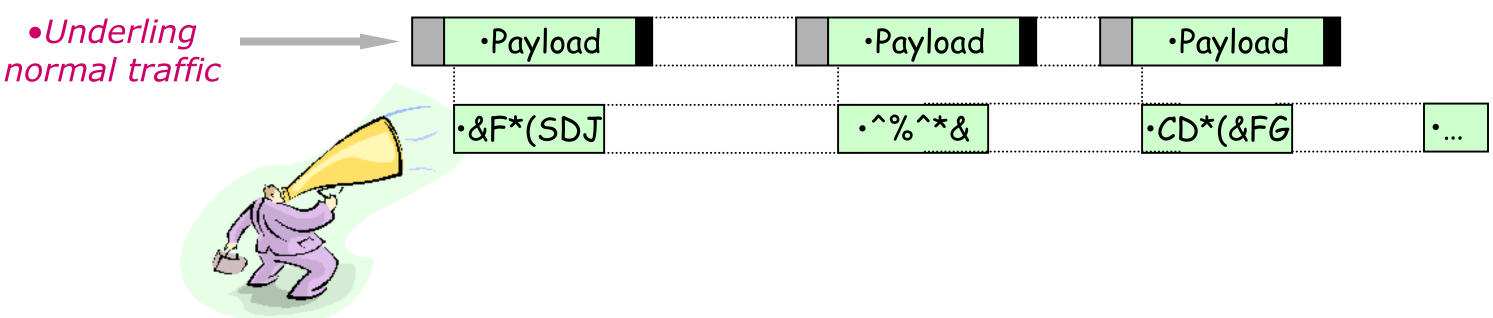


- Deceptive jammer:
  - Constantly injects regular packets to the channel without any gap between consecutive packet transmissions
  - A normal communicator will be deceived into the receive state

Jammer Attack Models



- Random jammer:
  - Alternates between sleeping and jamming
    - *Sleeping period: turn off the radio*
    - *Jamming period: either a constant jammer or deceptive jammer*



- Reactive jammer:
  - Stays quiet when the channel is idle, starts transmitting a radio signal as soon as it senses activity on the channel.
  - Targets the reception of a message

Experimental Results

- Involved three parties:
  - Normal nodes:
    - *Sender A*
    - *Receiver B*
  - Jammer X
- Parameters
  - Four jammer models
  - Distance
    - *Let* $d_{XB} = d_{XA}$
    - *Fix* d_{AB} *at 30 inches*
  - Power
    - $P_A = P_B = P_X = -4dBm$
  - MAC
    - *Fix MAC threshold*
    - *Adaptive MAC threshold (BMAC)*

Deceptive Jammer		
d_{xa} (inch)	PSR(%)	PDR(%)
38.6	0.00	0.00
54.0	0.00	0.00
72.0	0.00	0.00

Reactive Jammer			
d_{xa} (inch)		PSR(%)	PDR(%)
m = 7bytes	38.6	99.00	0.00
	54.0	100.0	99.24
m = 33bytes	38.6	99.00	0.00
	54.0	99.25	98.00

Back to the Systems Perspective…

Lead with a Systems Question

- What to do in a situation where wireless signals are everywhere and exploits are imminently possible?
- Answer: Break the problem into two parts…

The Professional Answer

Conduct a security audit

Identify stakeholders

– Label adversaries

Identification of potential security threats and risks

– Methods of intrusions

– Risks from a successful attack

Identification of potential services that could address threats and mitigate risks

The Research Answer

Analyze information flows

Find something that someone hasn’t done before, and look for “point” solutions

– If I develop a new XYZ then ABC will be protected

– Write paper and universe will be safe because people will read my work…

Unforutunately point solutions don’t add together well…

- Disclaimer: The rest of this talk is 10% Professional, 10% Pragmatic, and 80% “Researchy”

Professional Viewpoint: It is a daunting challenge, but start simple…

- In the past, every organization was a silo, but now many systems and data flows operate concurrently
  - Organizations are being pushed to deploy the latest technology
- IT staff must also bridge the gap between "the way things were" and "advancing the organization with the latest and greatest."
- Credos to consider:

1. Security challenge increases with the scale of the organization and the number of different technologies used;
2. Security/privacy is governed the security of the weakest technology;
3. Organizations typically carry many legacy technologies;
4. Technology is providing new tools to hackers.

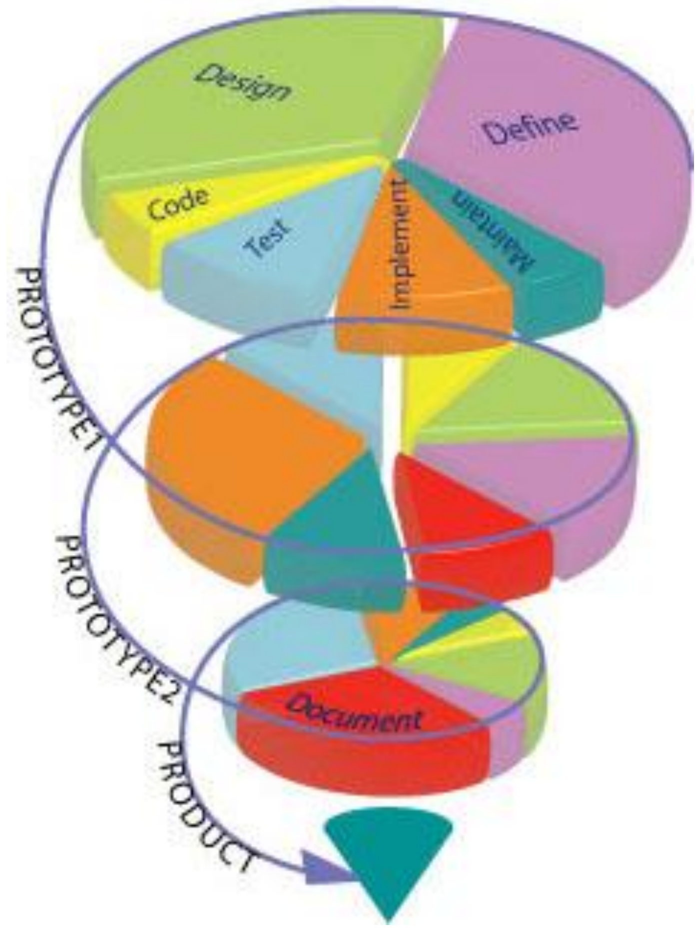
- Recommendation: An inventory of technologies that are being used by their employees— in particular, both the latest as well as legacy technologies. These should all have a quick sanity test done to see whether they have any form of security being used to protect them.

Pragmatic question: Do you know all of your wireless signals? And what data they are carrying?

- Consider the hospital
  - Wireless is embedded in everything, signals are everywhere
  - Medical sensors can be manipulated remotely through side-channels (EMI for manipulating cardiac monitors)
    - *Attack the measurement physics to remotely forged heartbeat signals*
  - Doctors/nurses accessing data
- Take Away:
  - Wireless is now prolific, often we aren’t even aware of how it is used
  - These systems/ecosystems have many parts, with data flowing everywhere
  - Wireless is just too convenient not to use!

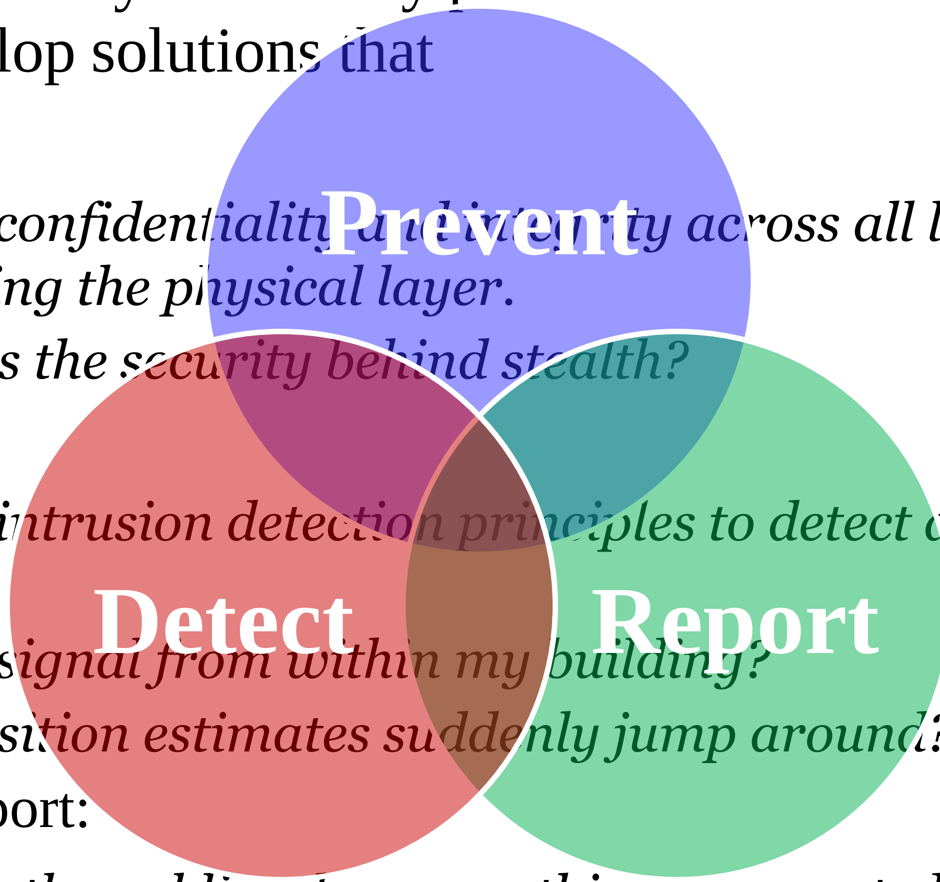
Pragmatic viewpoint: Do not be afraid to start somewhere!

- There are many frameworks out there for conducting a security analysis…
  - It really doesn't matter
  - Start somewhere
  - Make it fun, make it a team effort
- Engineers/IT staff should ask:
  - What could go wrong?
- Very important to stop 90% of the potential security risks "ASAP"
  - These threats and risks are not hard to stop ("SPIRAL-1")
  - Worry about sophisticated attacks second ("SPIRAL-2")
  - Patch, fix, refine ("SPIRAL-3")



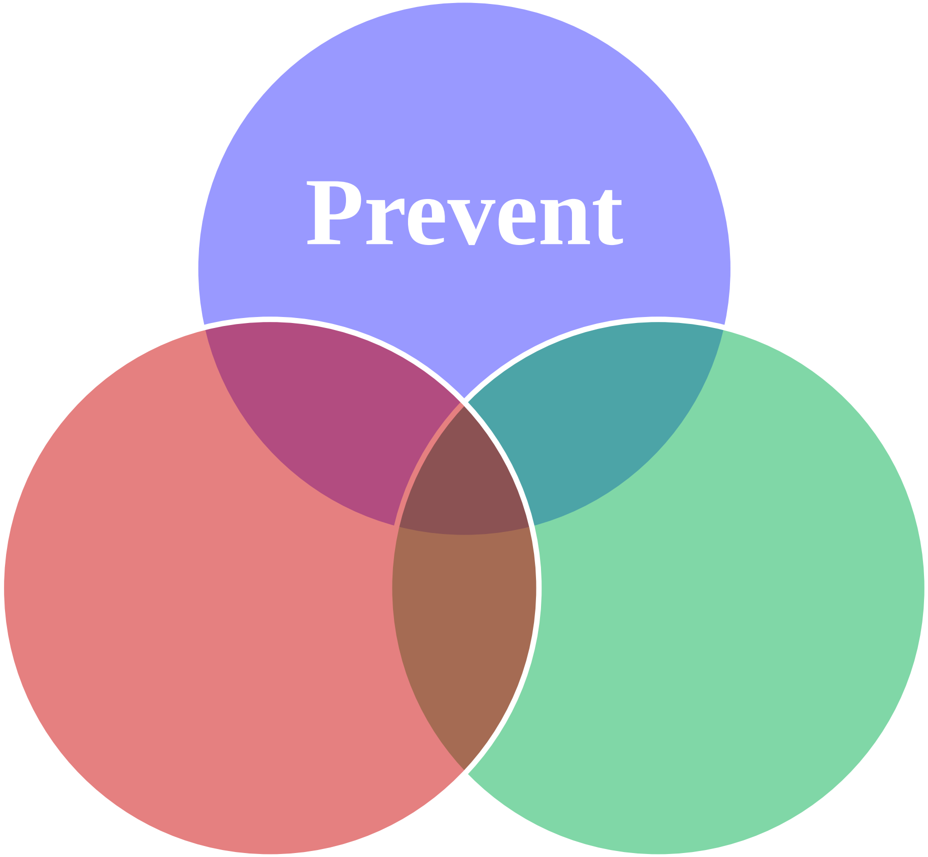
“Signal Security” has the same over-arching responsibilities as cybersecurity

- Our responsibility as security professionals/researchers is to deploy/develop solutions that
  - Prevent:
    - *Apply confidentiality and integrity across all layers– including the physical layer.*
    - *What is the security behind stealth?*
  - Detect
    - *Apply intrusion detection principles to detect anomalous events*
    - *Is this signal from within my building?*
    - *Did position estimates suddenly jump around?*
  - Audit/Report:
    - *Inform the public when something unexpected happens with production equipment*
    - *Post-process signal data to infer what happened!!!*



Signal Security:

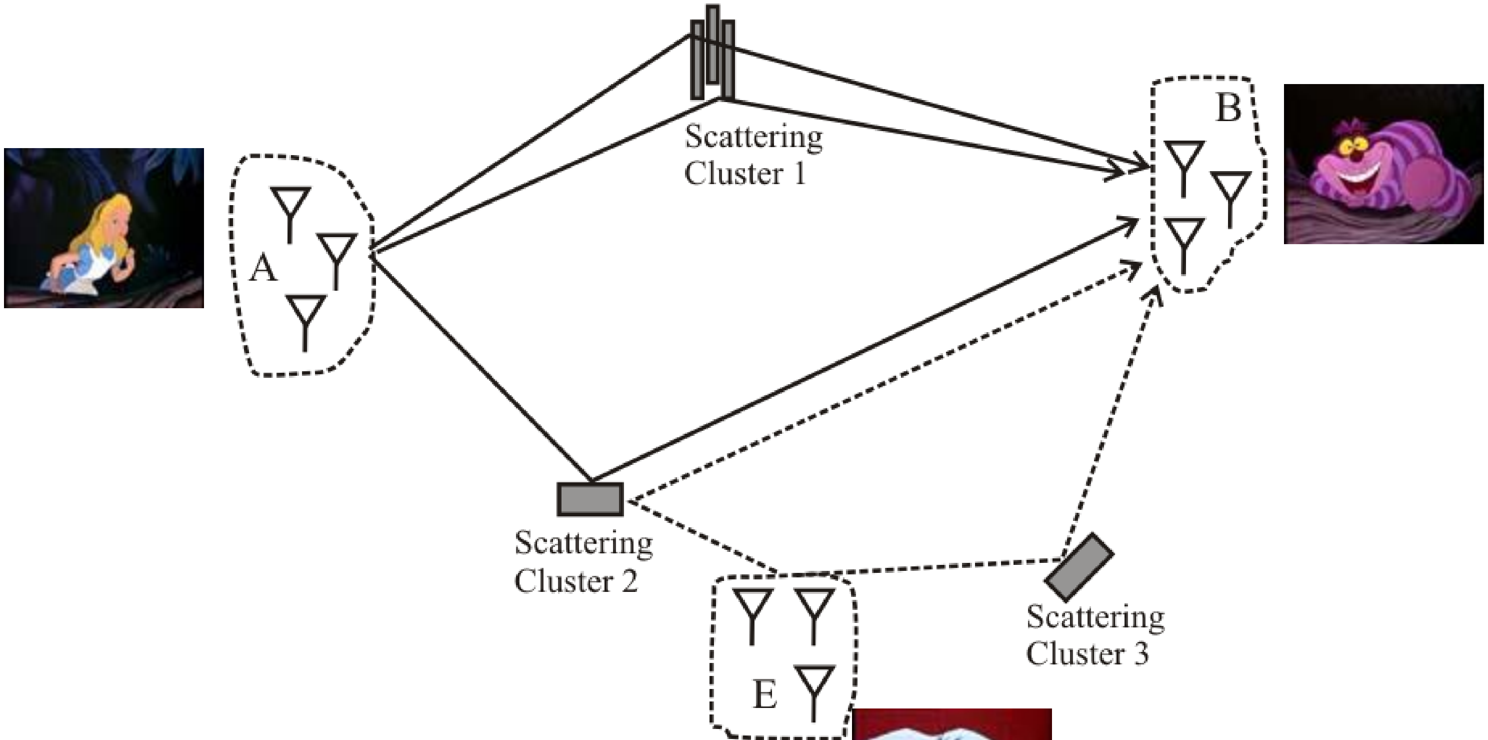
Prevent



Physical Layer Security: Pie in the Sky

- Although conventional cryptographic and network security techniques are essential to securing wireless networks, they are not a complete solution
- There is a belief that lower-layer information associated with the wireless channel can be used to enhance wireless security
  - The typical wireless multipath transmit-receive channel is *frequency-selective* (or in the time domain, *dispersive*) in a way that is *location-specific* with rapid *decorrelation* properties
  - The channel response between a transmitter and a receiver can be a unique, shared, non-predictable source of *secret* information
- This secret information might be a "fingerprint in the ether" to develop cross-layer *Authentication Services* and *Confidentiality Services*
- The wireless channel and its variability might be exploited to allow entities to communicate secretly in the presence of eavesdroppers
  - Capability further supported by the idea of other entities being able to help by injecting noise

Alice, Bob and Eve get Physical !!!



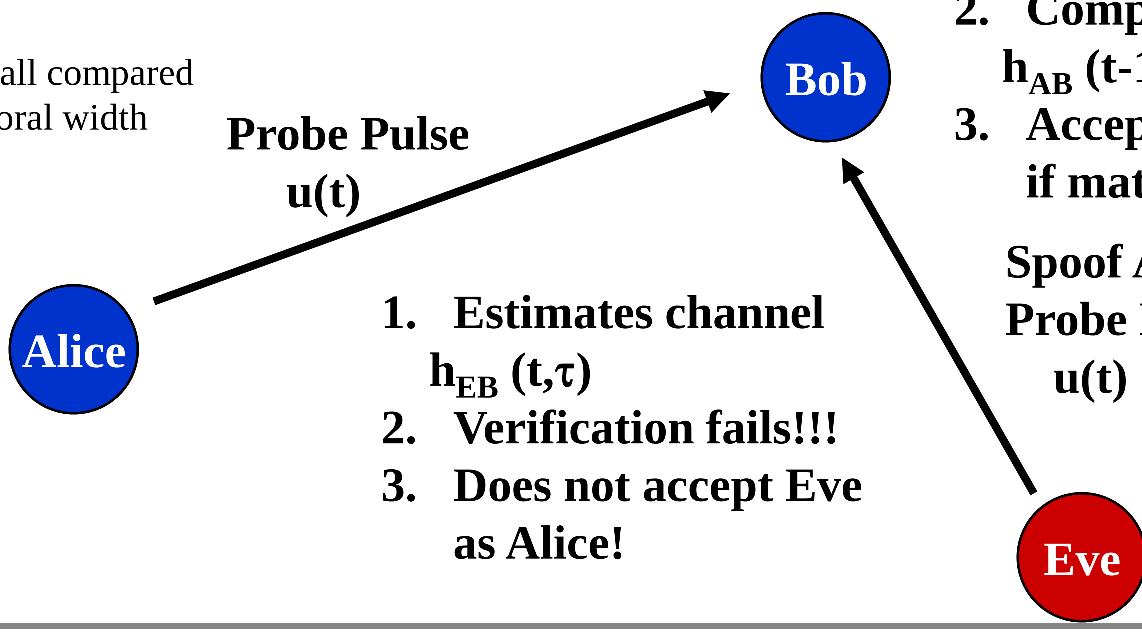
- All security problems need actors:
  - Alice (A): The transmitter
  - Bob (B): The receiver
  - Eve (E): The evil adversary
- Their roles depend on the type of security objective we have

Authentication: A Cartoon Version

- Authentication in the PHY-sense is about verifying a transmission came from a particular transmitter– useful for spoofing detection!!!
- Wireless devices can authenticate themselves based upon
  – Ability to produce an appropriate received signal/channel estimate at the recipient
  – Location information can be extracted to authenticate a transmitter relative to its previous location

Bandwidth W of Probe Pulse is critical!
1/W must be small compared to channel temporal width

Probe Pulse
u(t)



1. **Estimates channel $h_{AB}(t,\tau)$**
2. **Compares against $h_{AB}(t-1,\tau)$**
3. **Accepts transmission if match**

Spoof Alice:
Probe Pulse
u(t)

1. **Estimates channel $h_{EB}(t,\tau)$**
2. **Verification fails!!!**
3. **Does not accept Eve as Alice!**

PHY-Authentication: Spoofing Detection Via Significance Testing

- Sample frequency response at M frequencies, two complex frequency response vectors

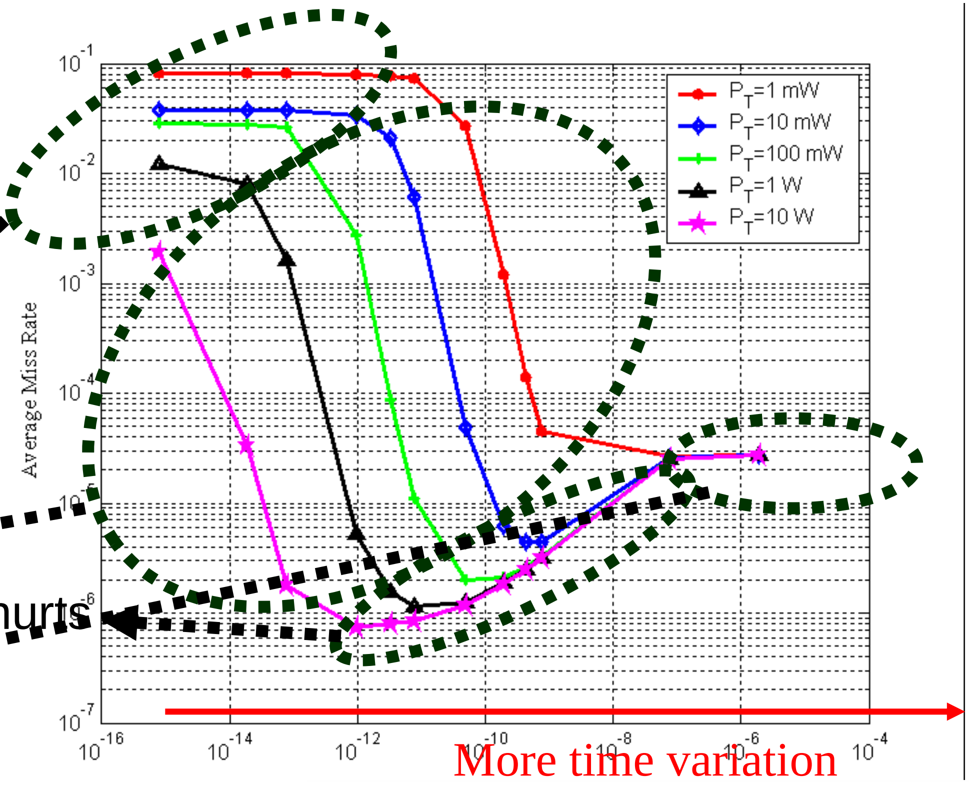
$$\underline{\hat{H}}_{AB} = [\hat{H}_{AB}(0, f_1), \hat{H}_{AB}(0, f_2), ..., \hat{H}_{AB}(0, f_M)]^T$$
$$\underline{\hat{H}}_{t} = [\hat{H}_{?}(t, f_1), \hat{H}_{?}(t, f_2), ..., \hat{H}_{?}(t, f_M)]^T$$

- Simple Hypothesis:

$$\mathcal{H}_0: \ \underline{H}_t = \underline{H}_{AB}$$
$$\mathcal{H}_1: \ \underline{H}_t \neq \underline{H}_{AB}$$

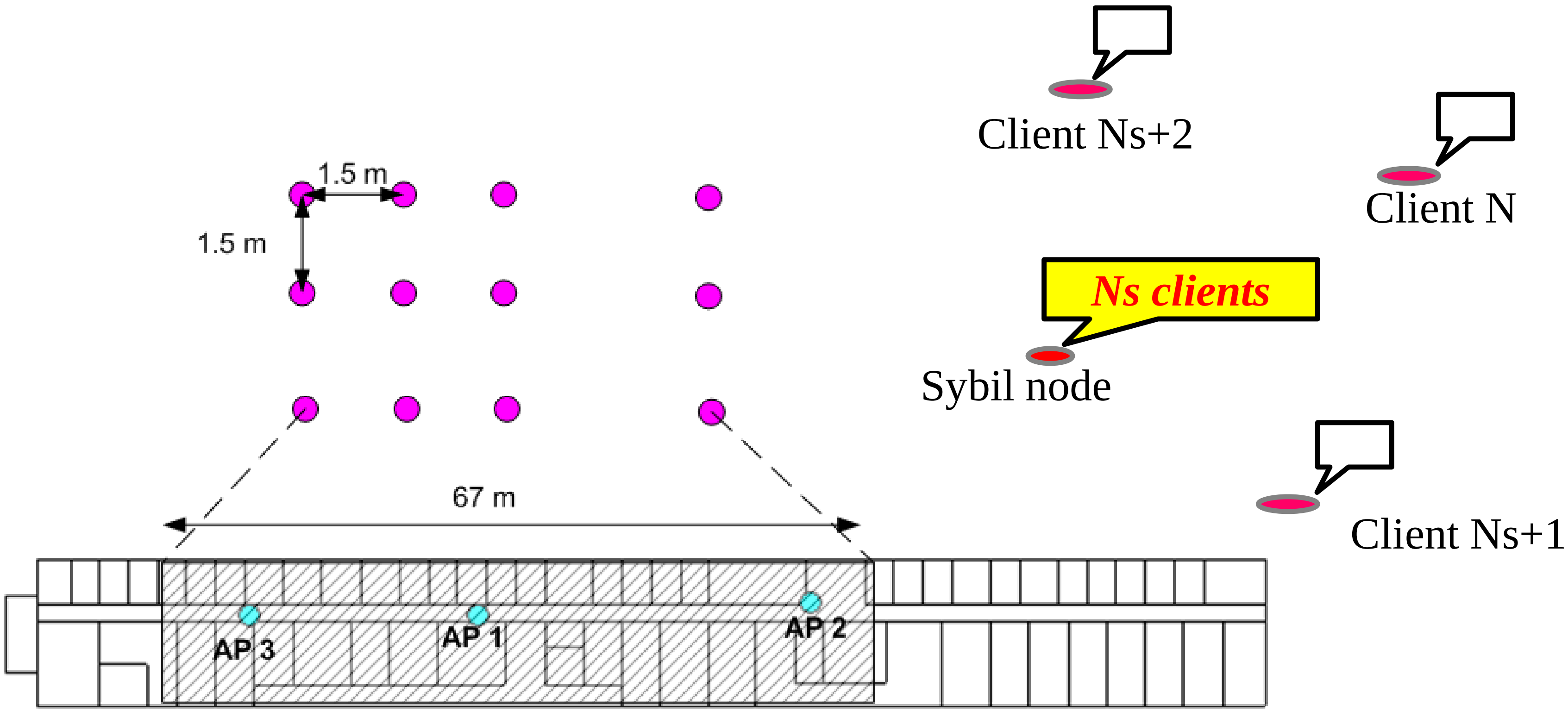
$$Z = \min_{\theta} \frac{1}{\sigma^2} \| \underline{\hat{H}}_A - \underline{\hat{H}}_t e^{j\theta} \|^2$$

Time variation is negligible
Time variation helps
Time variation is so big that it hurts
Thermal noise is negligible

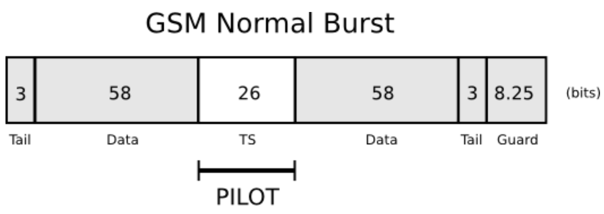


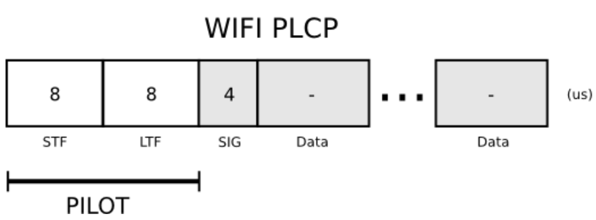
PHY-Authentication, a Variation: Sybil Detection

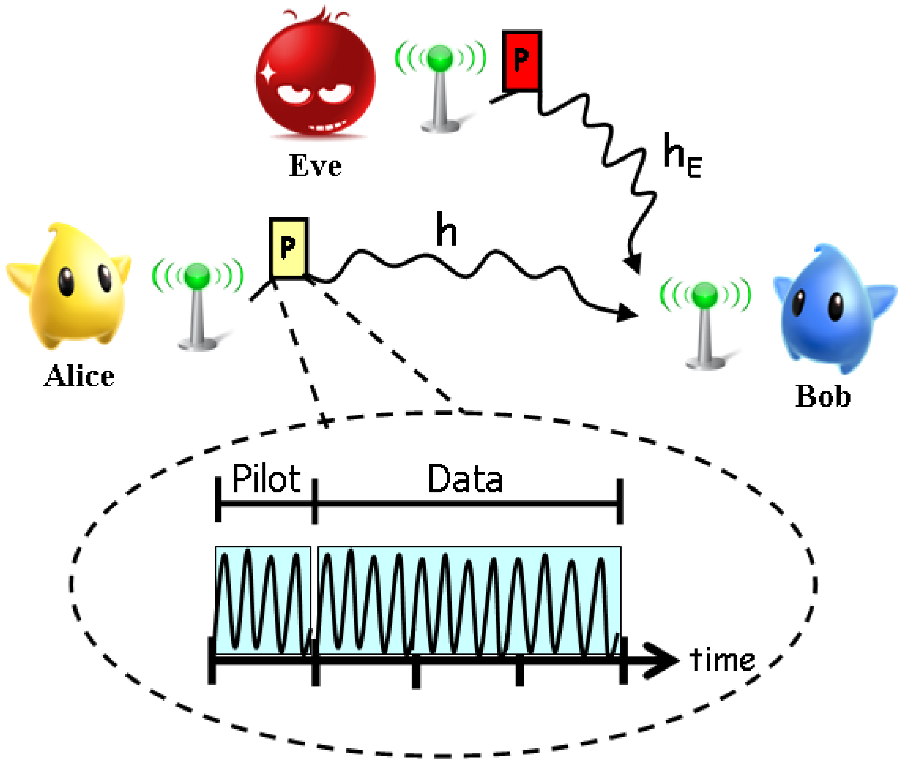
- The Sybil Attack: A node claims multiple identities
- The channel response serves as a fingerprint to detect multiple claimed identities
- Clever Adversary: Adapt power across subcarriers for each identity (but don't change "shape" or else decoding failure!)
- Issues to consider: System bandwidth, Number of APs and their synchronization



Rather than use the channel, we may use channel estimation (piloting) for message authentication



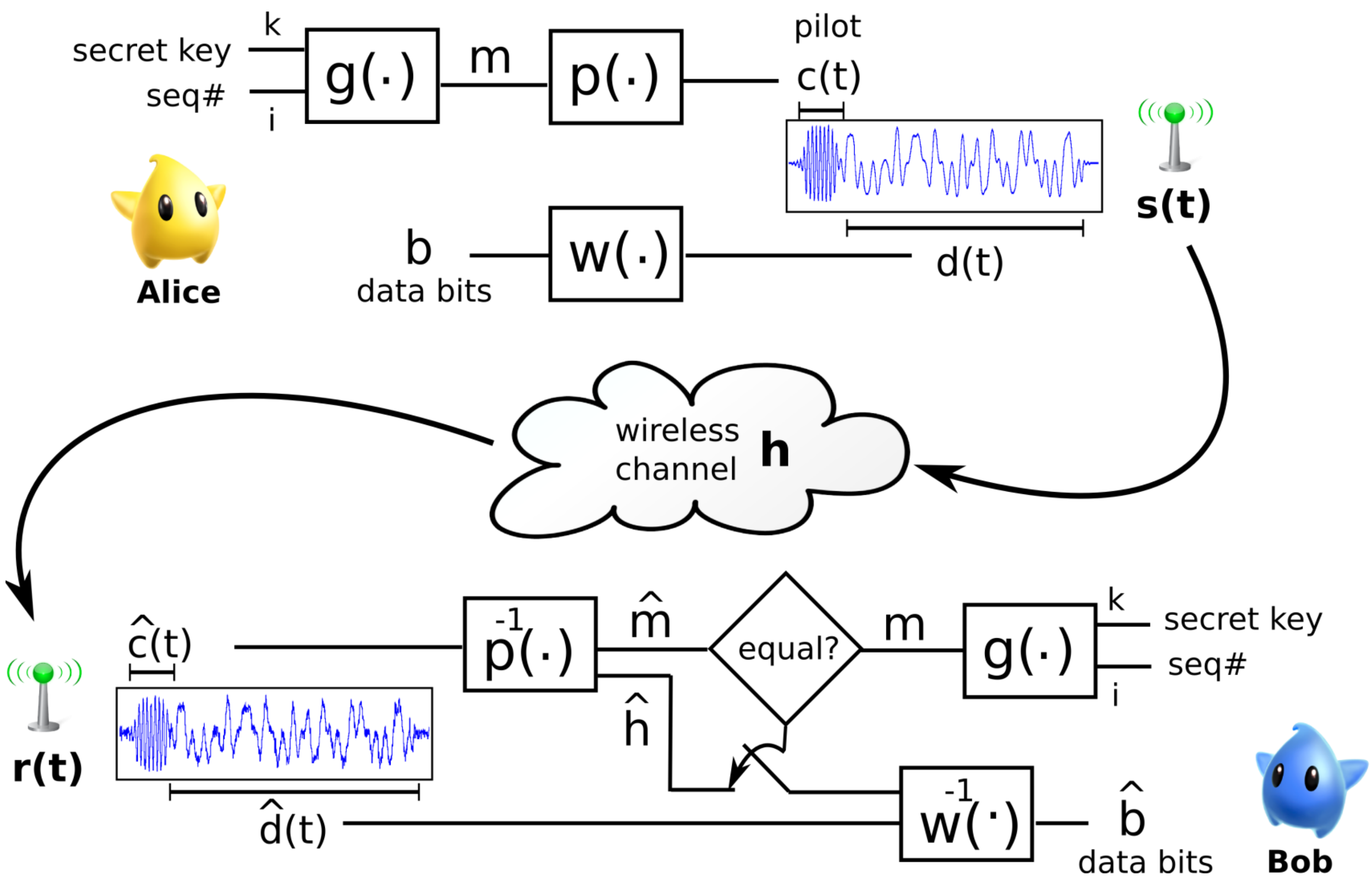




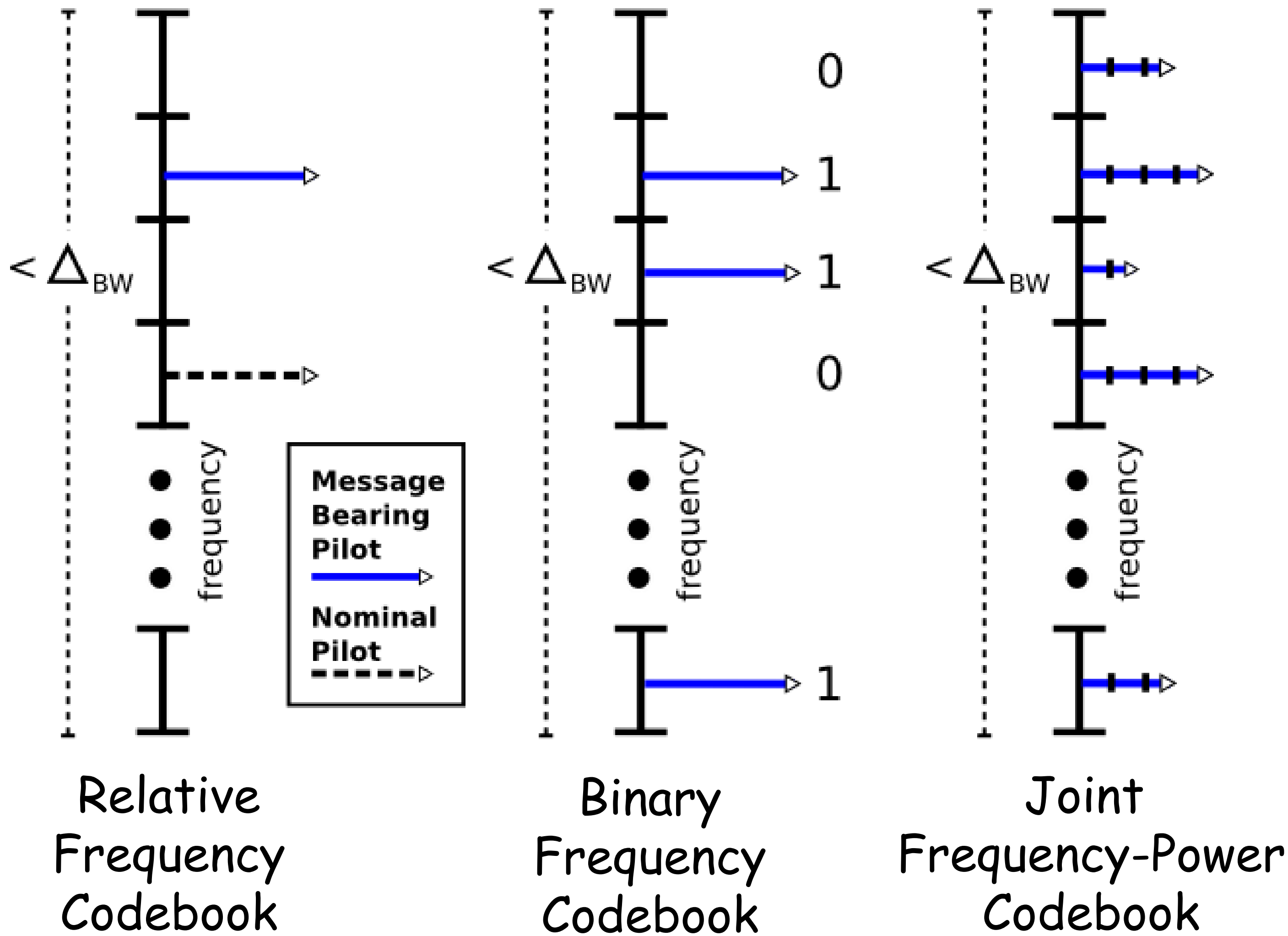
$$y(t) = h(t) * x(t) + n(t)$$

$$h(t) = \sum_{d=0}^{D-1} a_d e^{j\theta_d} \delta(t - \tau_d)$$

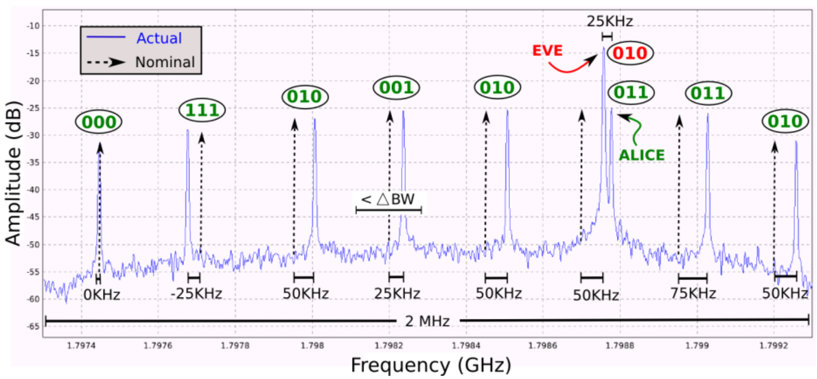
By embedding an authenticator in the CSI estimation phase, the communication is validated rapidly



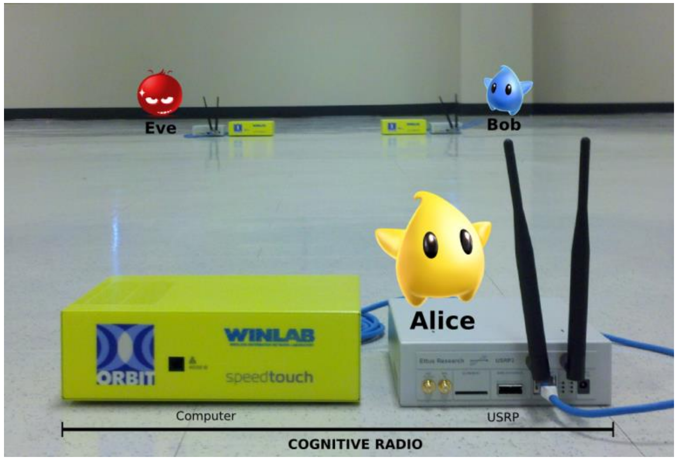
There are several strategies for embedding authenticator messages into pilot symbols



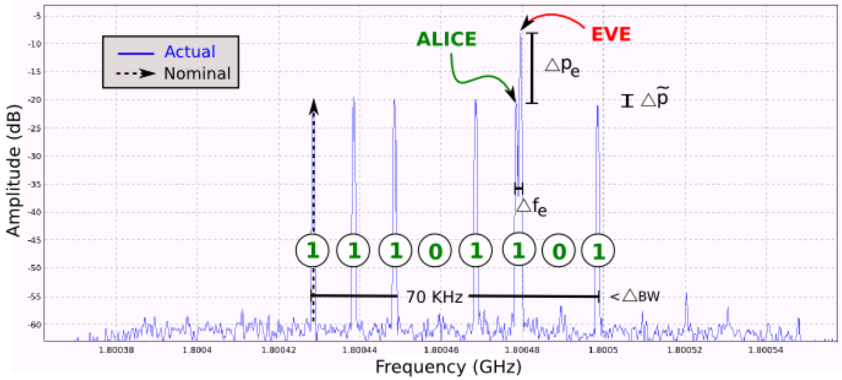
Prior experimental validation using current SDRs illustrates feasibility of CSI authentication in rejecting false communications



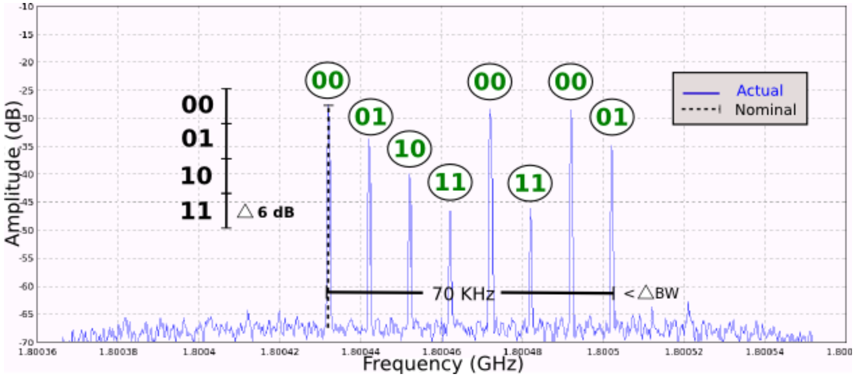
RFC Experiment



Experimental Setup



BFC Experiment



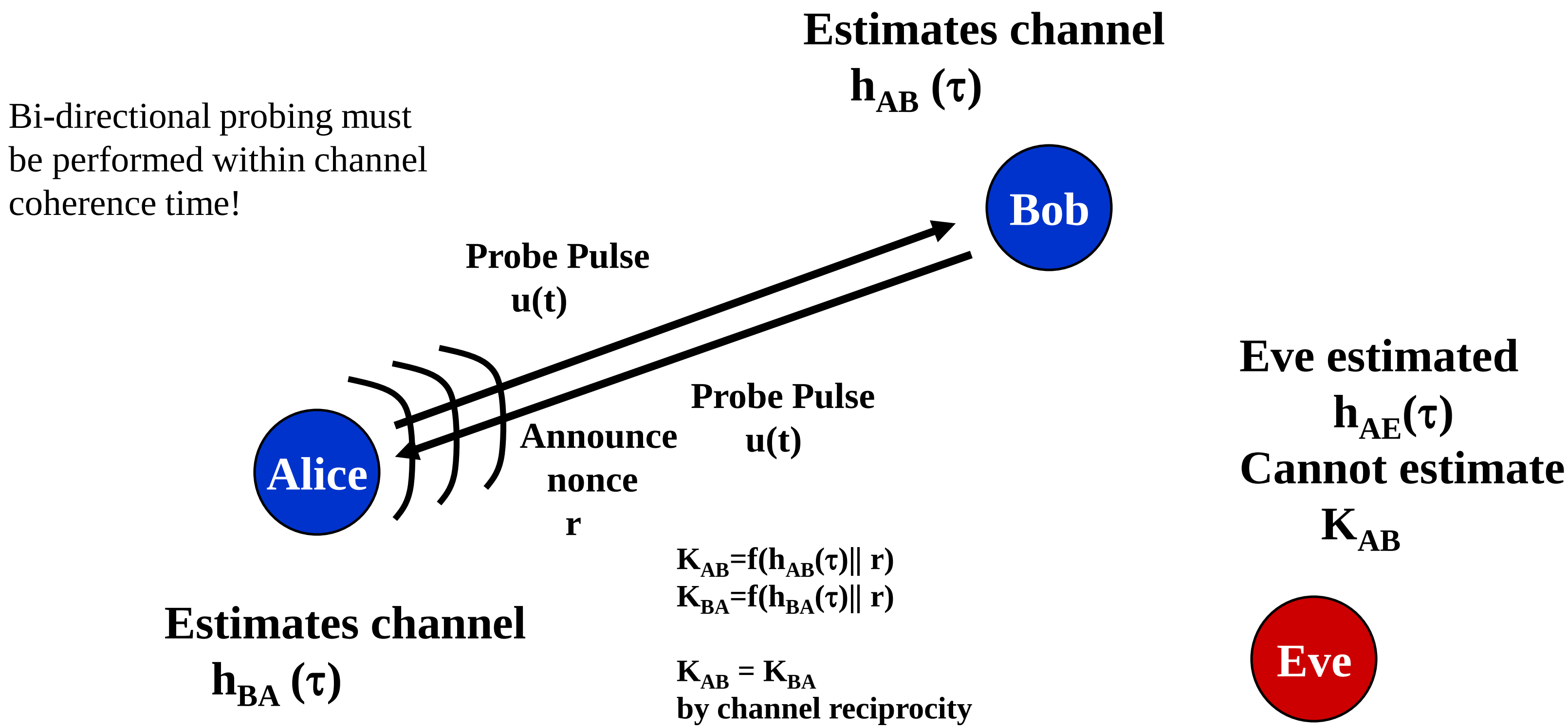
FPC Experiment

Confidentiality: Different Means to an End

- We also would like to use the PHY-Layer to support confidential communications
  - For higher-rate secret communications, we suggest that the PHY-layer be used to form higher-layer cryptographic keys
- There are two types of PHY-Layer Confidentiality Services:
  - *Extraction*: Use the channel estimate itself to form key bits
  - *Dissemination*: Use channel variations to opportunistically, and secretly convey communications/key bits…
- Note: There is a distinction between secret communication and LPI/LPD communications!
  - Question to think about: If Eve isn't even aware that you are communicating, then do you get secrecy by default?

Extraction: A Cartoon Version

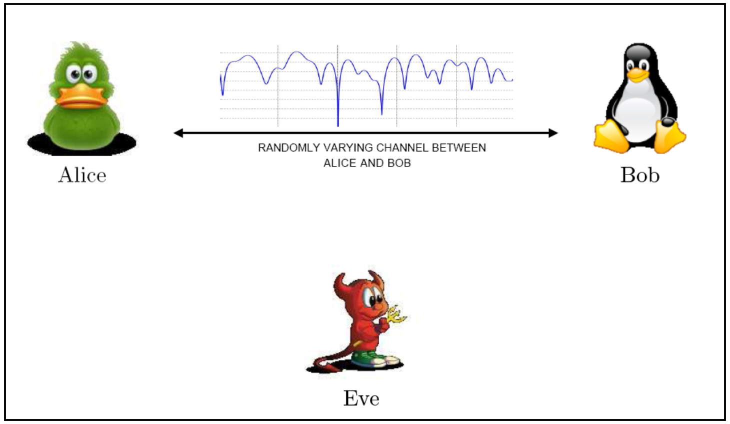
- The uniqueness and non-predictability of the channel can be used to establish a shared secret key for encryption services

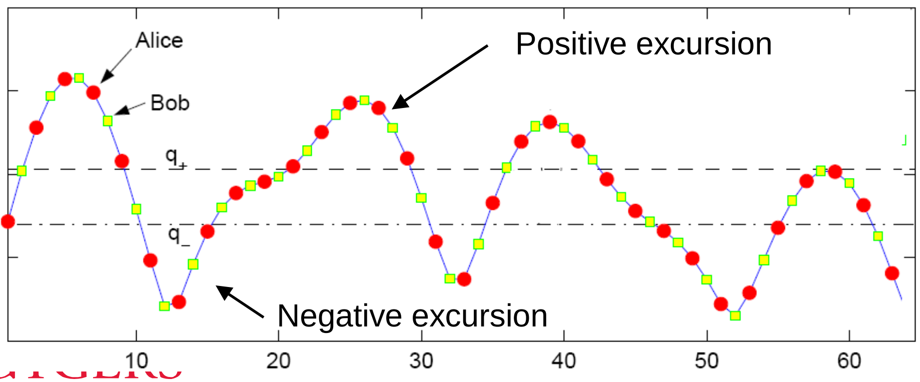


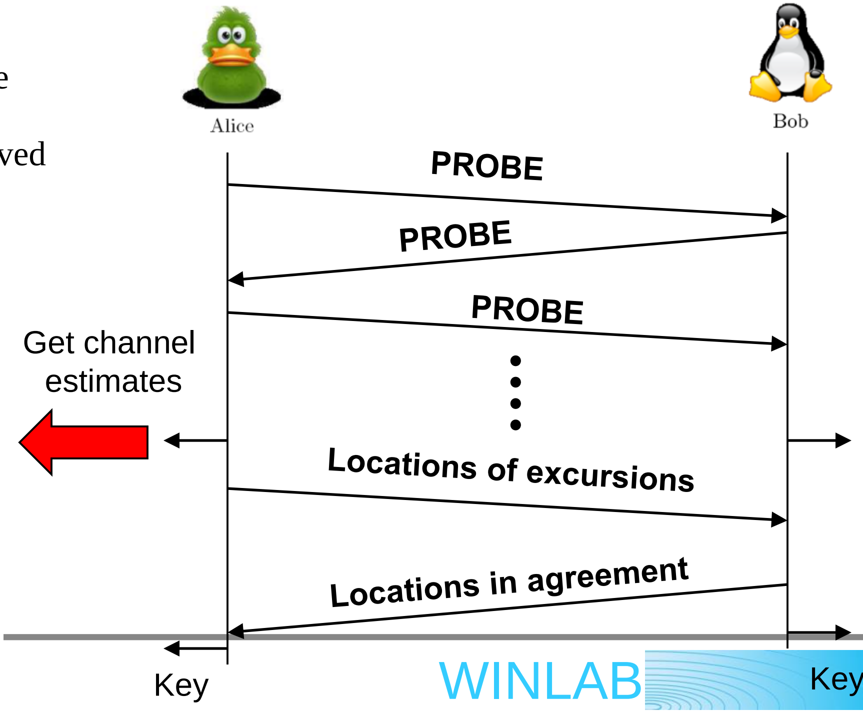
- Practical issues arise: quantization of channel estimates, channel reciprocity, temporal coherence, fast channel estimation.

PHY-Confidentiality: Secret key extraction from a wireless channel

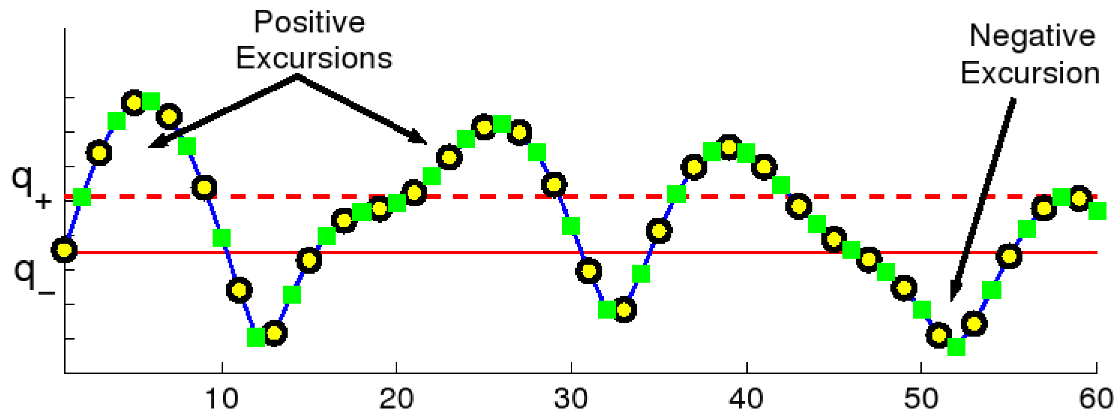
- Use channel reciprocity to build highly correlated data sets
  - Probe the channel in each direction
  - Estimate channel using recd. probe
- Eve receives only uncorrelated information as she is more than $\lambda/2$ away
- Level crossings are used to generate bits
- Alice and Bob must exchange msgs over public channel to create identical bits
- What if channel is not already authenticated?
  - Requires additional sophistry to prevent man-in-the-middle attack.
  - It is possible using the correlated data collected from received probes.







PHY-Confidentiality: Radio Telepathy, The Protocol



Find locations of excursions in X^n of size $\geq m$. e.g. $\{6, 27, 42, 52 \ldots\}$
Send a random subset to Bob
$L = \{6, 42, 52 \ldots\}$

$\xrightarrow{L}$

Find the set of indices $\tilde{L} \subseteq L$ where Y^n has excursions of size $\geq m - 1$

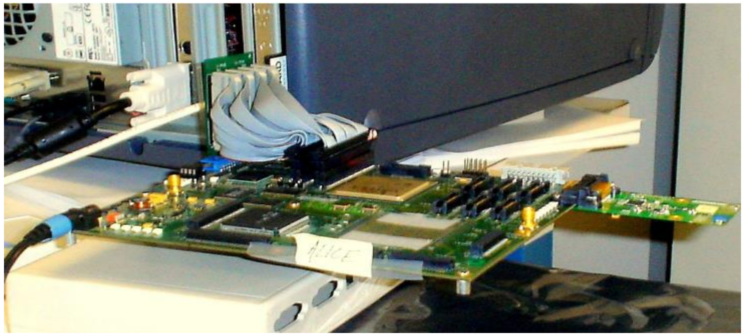
If $\frac{|\tilde{L}|}{|L|} < \frac{1}{2} + \epsilon$ for some $0 < \epsilon < \frac{1}{2}$, declare message not sent by Alice

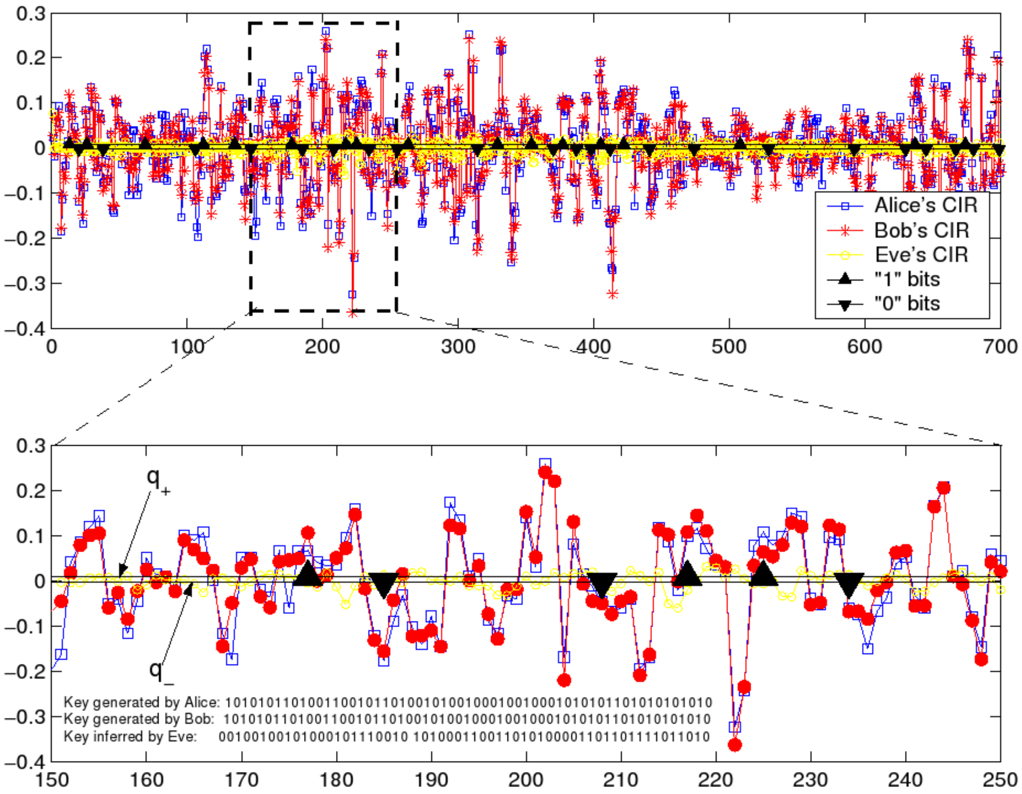
Compute $Q(Y^n(\tilde{L}))$.
The first N_{au} bits = auth-key K_{au}.
Remaining $N - N_{au}$ bits = secret key.
Send $\left\{\tilde{L}, MAC\left(K_{au}, \tilde{L}\right)\right\}$ to Alice.

$\xleftarrow{\tilde{L}, mac}$

Compute $Q(X^n(\tilde{L}))$. The first N_{au} bits = auth-key K_{au} to verify the MAC.

PHY-Confidentiality: Radio Telepathy Prototyping



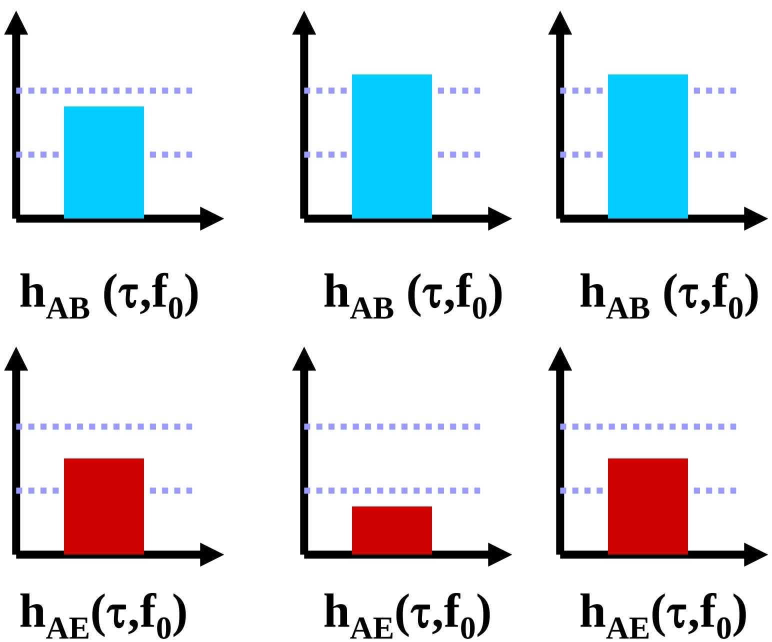


- 64 Point Channel Impulse Response from 802.11a Preamble
- Tallest Peak in CIR Extracted
- STA= Bob, AP =Alice
- Probing of channel: PROBE request and PROBE response
- New PROBE every 110msec

Dissemination: A Cartoon Version

- Idea: When Alice→Bob channel is good, and Alice→Eve channel is bad… transmit!!!

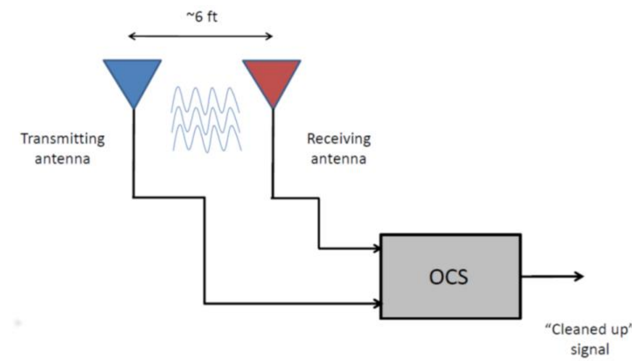
Assume everyone's channel conditions are known by Alice



- Question: Why would Alice know Eve's channel?

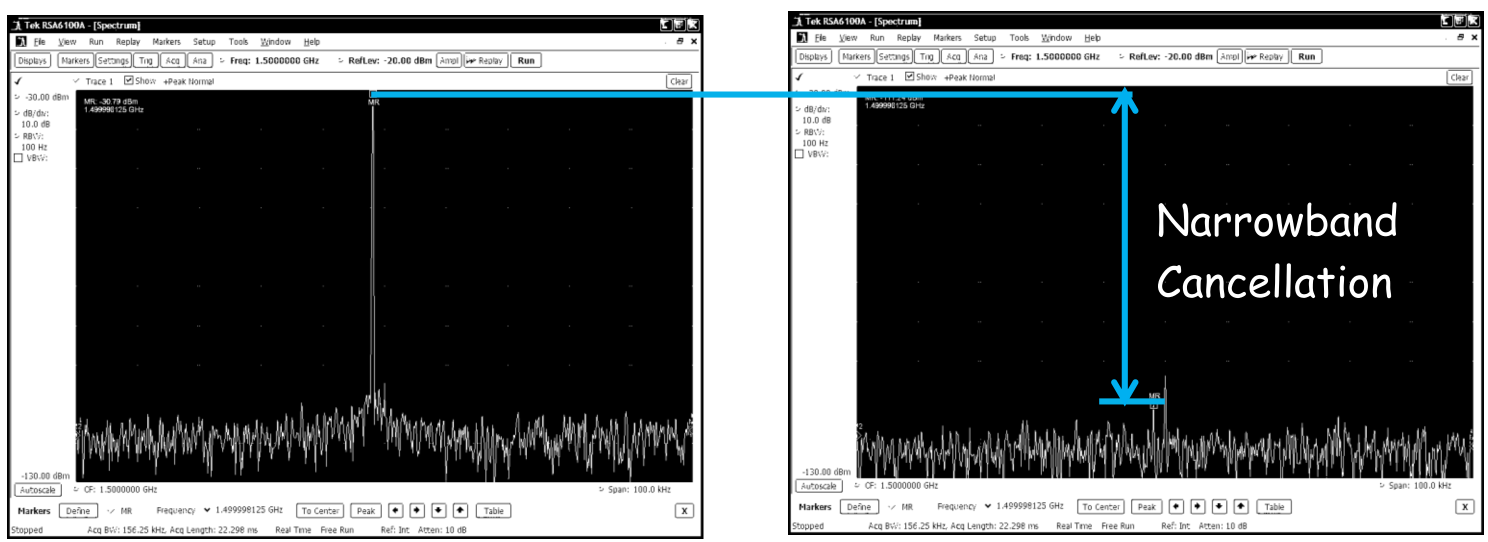
One approach for improving confidentiality rates is to transmit interference, but how?

- Artificial noise limits Eve's SNR even if Eve's channel gain is very large
  - *Corresponding secrecy improvement*
- Simultaneous transmit-and-receive system designs allows the receiver to transmit interference while subtracting off interference
  - Implementations: RF Photonics, circulators, etc.
  - Challenges: cancellation fidelity, self-multipath, bandwidth cancellation fidelity



Narrowband Measurement

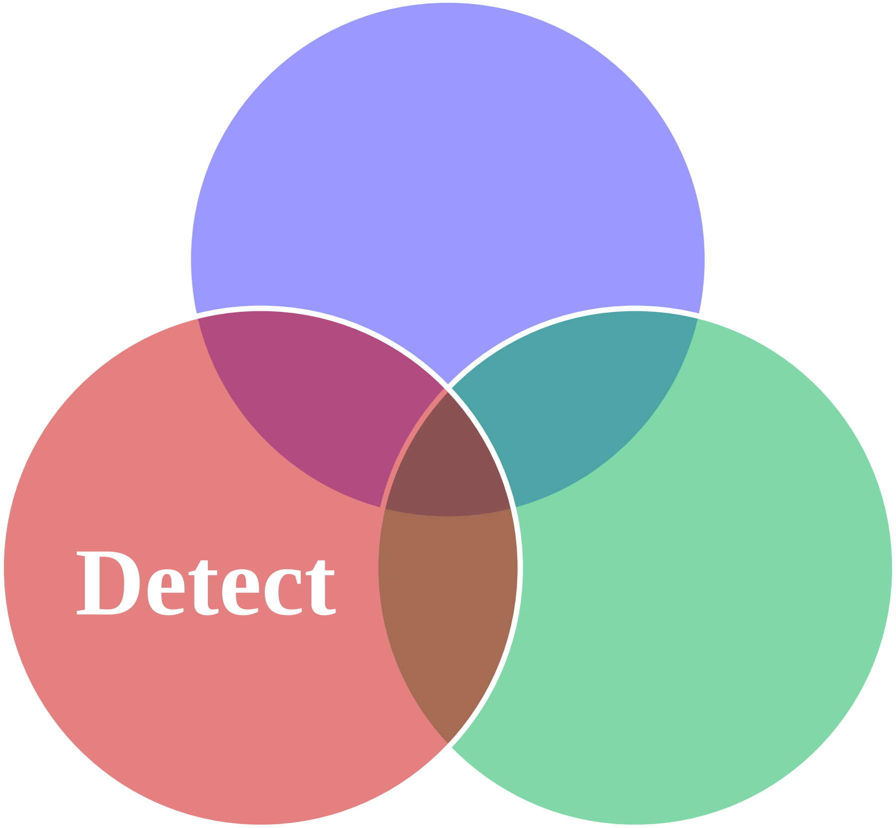
~80 dB cancellation



 Acknowldegement: Results from Princeton Lightwave Laboratory

Signal Security:

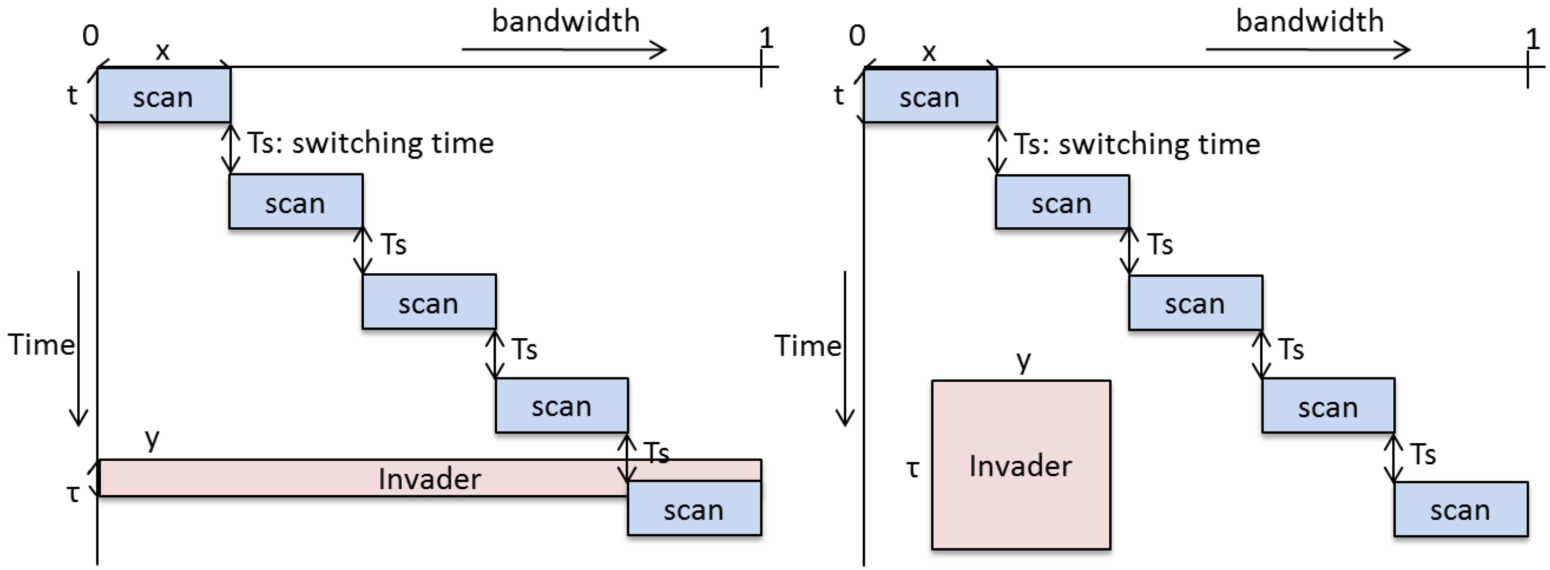
Detect



Spectrum forensics is not an easy task: there are many dimensions to explore

- *Discovering the Crime*: radio measurements can be used to detect rogue users. How to correctly detect violation based on potentially biased data?
  - Lots of spectrum to scan…
  - Why is the adversary trying to use the spectrum in the first place?
- *Identification*: identify individuals/radios associated with a crime
  - measure transmitter radio signatures based on unavoidable and random fabrication difference (see Signal Prints and NIST studies)
  - embed hard-to-alter (or mandatory) RF fingerprints within every transmission
- *Punishment policies formalize:* Most spectrum policy languages are NOT designed to specify what to do if spectrum abuse is detected
  - Extend XG policy language to include punishment definition.
  - If the punishment rule is selected and activated, then new punishing rules with certain expiration period will be generated based on the level and type of punishment, and be inserted into the existing spectrum polices for certain amount of time.

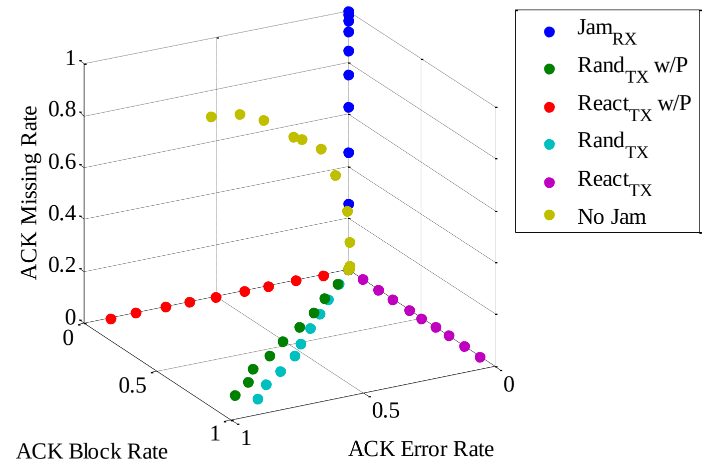
Practical matter: Finding the adversary isn't easy, there are many scenarios that yield comparable benefits

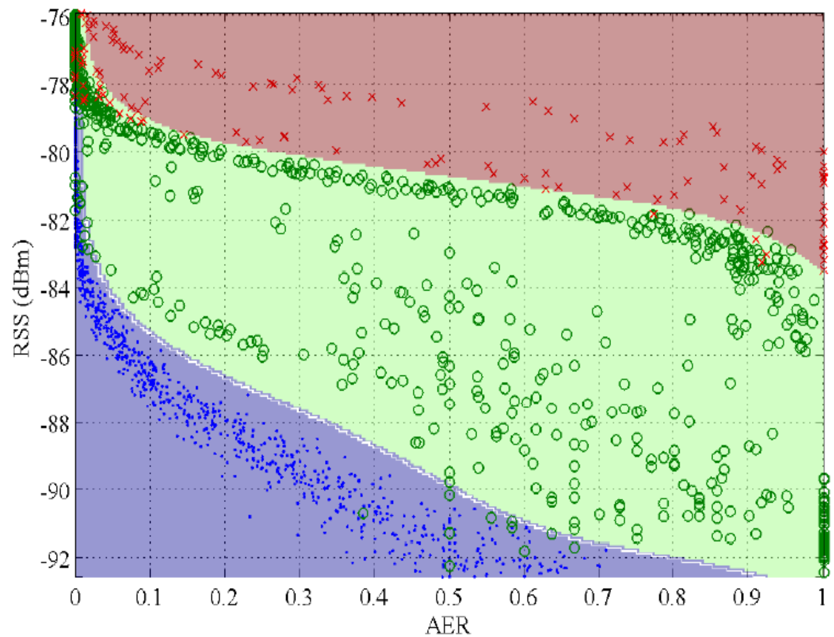


- There is an underlying geometric tradeoff that exists in the problem of scanning to find an adversary…
  - If the adversary's payoff is related to how much he managed to "sneak", then certain shapes of time-vs-bandwidth are more amenable to avoid detection
  - On the otherhand, certain shapes of time-vs-bandwidth by the scanner are also more supportive of detection
- There is a fundamental need to arrive at relationships between probability of detection versus the invader's time and bandwidth used, and versus scanning bandwidth, dwell time, and switching time for different scanning strategies.

Detecting jamming against the a wireless system is complicated by normal interference scenarios

- Normal Interference in Mobile Networks
  - Experiments have shown that the *hidden terminal* problem remains in spite of MAC-layer collision-avoidance (e.g. a transmitter outside of the physical carrier sensing range can still cause interference).
  - It is equivalent to a low-power jamming attack.
- Other jamming attacks, such as reactive attacks, require different detection mechanisms
- Sender-oriented detection of jamming can utilize network ACKs and signal levels to detect jamming
- AER-RSS signal space consists of three regions
  - Interference-free: no hidden terminal
  - Normal interference: caused by legitimate hidden terminals
  - Intentional interference: malicious jamming

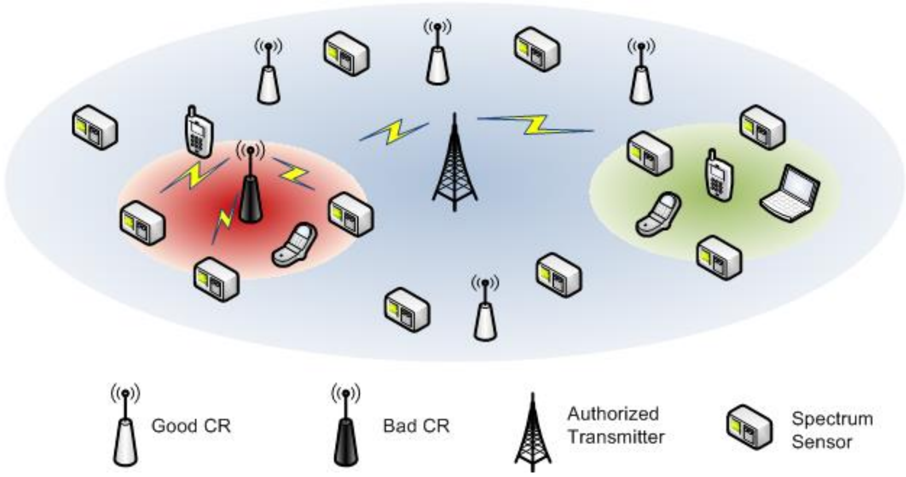


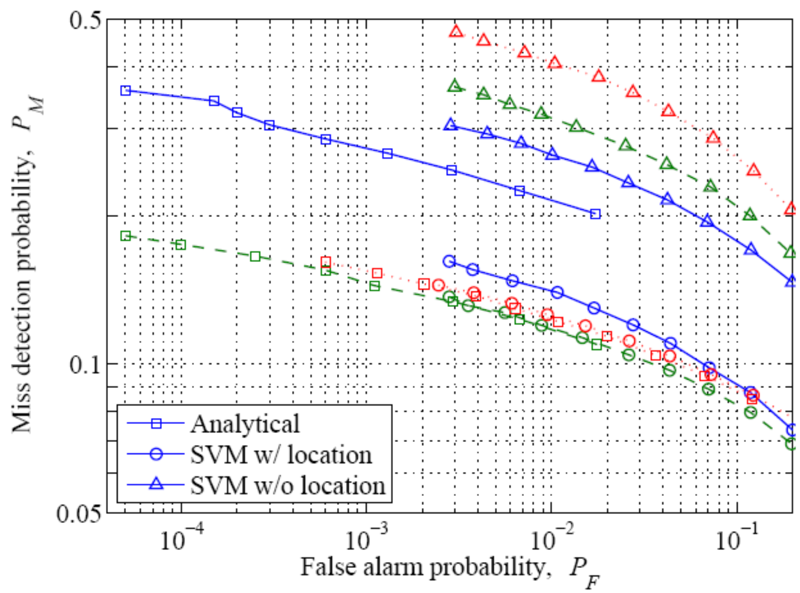


Sensor-assisted anomaly detection for detecting manipulation and exploitation

- Network Structure for Anomaly Detection
  - Primary (authorized) transmitter is stationary
  - Distributed detection by a network of sensors that collaborate locally.
- Significance Testing
  - Test statistic **T**: a measure of observed data
  - Acceptance Region Ω: we accept the null hypothesis if $\mathbf{T} \in \Omega$
  - Significance level α : probability of false alarm
- When a channel is dedicated to a single authorized user we can try to distinguish between single and multiple transmissions
  - Formulate a decision statistic that captures the characteristics of the received power in the normal case

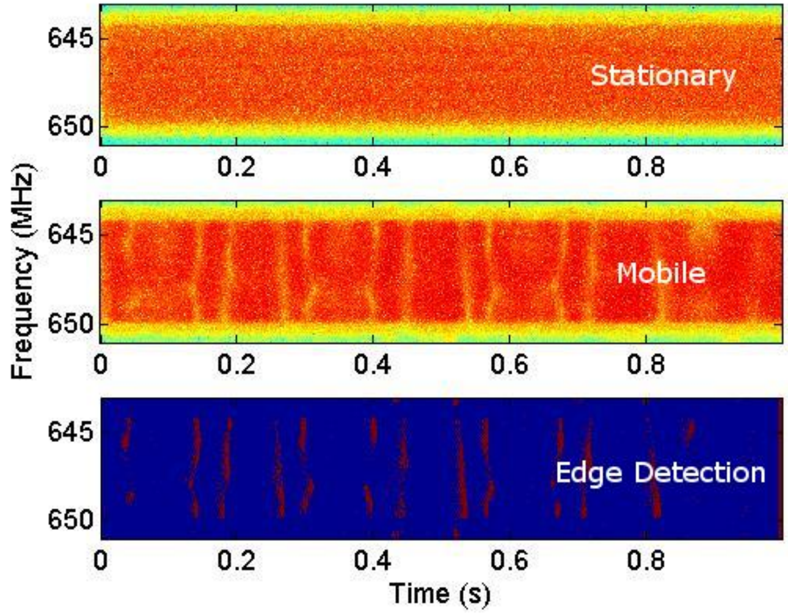
$$Y_n = Y_0 - 10\gamma \log_{10}(d_n/d_0) + Y_{R,n}$$

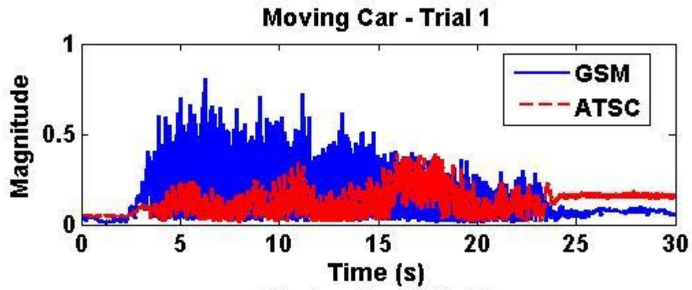


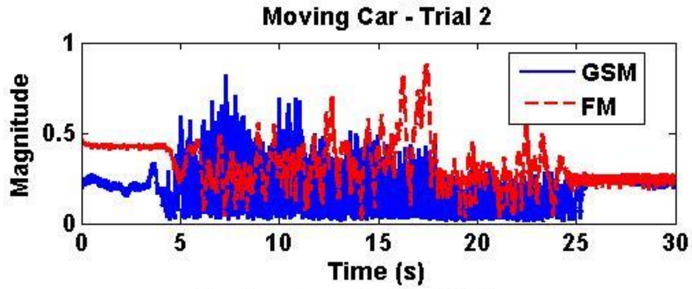


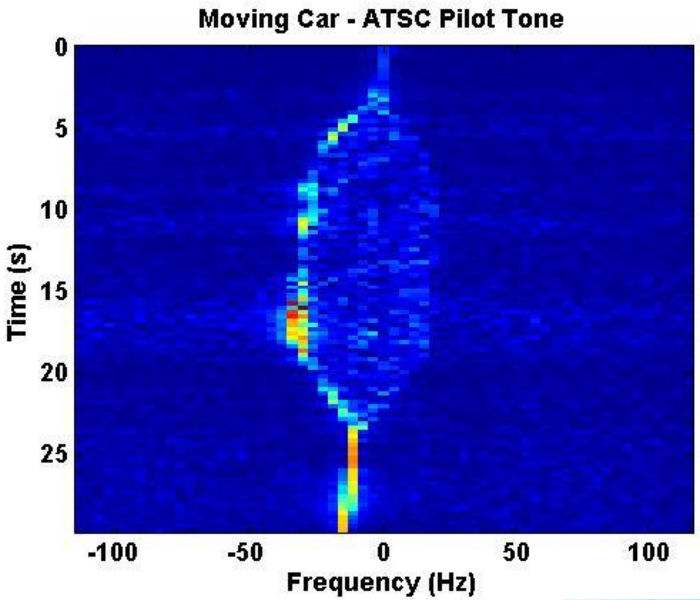
When intruders are mobile, we may analyze signals to look for device mobility

- Spectrogram Feature Extraction
  - Edge Detection predicts mobility
- Power Statistics
  - Variability indicates mobility
- Doppler Shift Tracking
  - Qualitative estimate of mobility





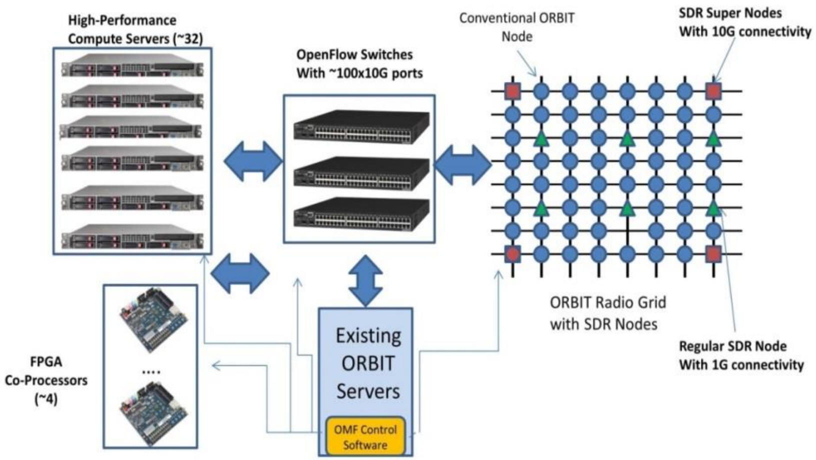


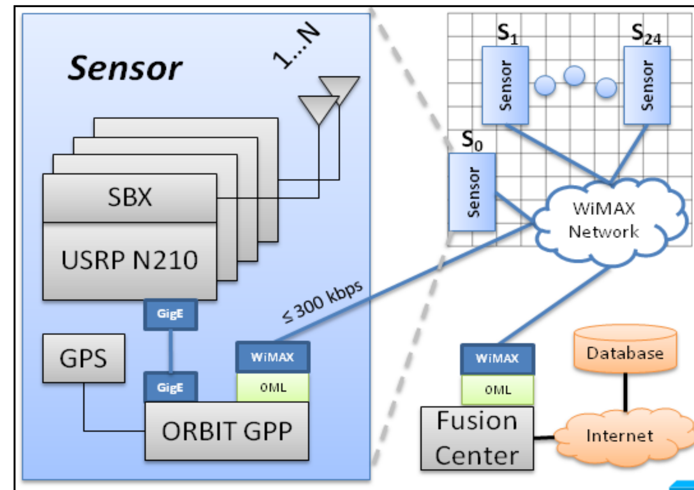


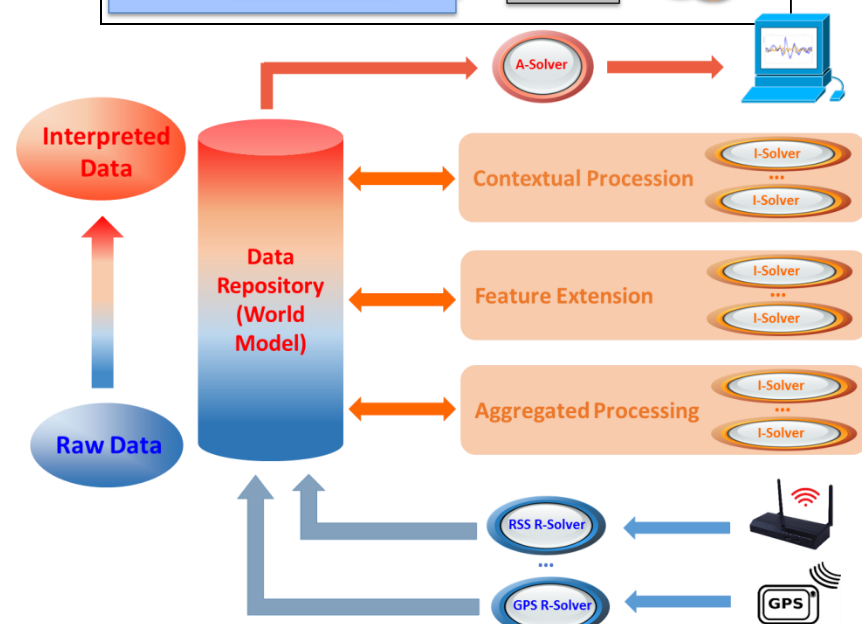
Signal Security:

Audit/Report

C-RAN technologies can facilitate spectrum forensics and wireless signal audit logging







- Storage is cheap, and computing is cheap
- We are developing tools for cloud-RAN's that can be dual-used for post-event analysis
- Example application: GPS interference detection

Wrapping Up: No Good Deed Goes Unpunished…
Where we need to go…

Some research ideas/questions

- What is the tradeoff between "confidentiality" and "covertness"?
  - If you have covert communications, do you get confidentiality for free?
- How does one build "solvers" that analyze raw signal data to write a transcript regarding what was seen?
  - The "IBM Watson" of wireless data
- Tradeoffs between throughput and secrecy and efficiency
  - Secrecy at the signal level requires long coding (LDPCs) → message expansion (akin to probabilistic encryption) could become prohibitive
- Is signal security "really security?" What value does "soft security" have in a whole system perspective?

The caveats: To be honest…

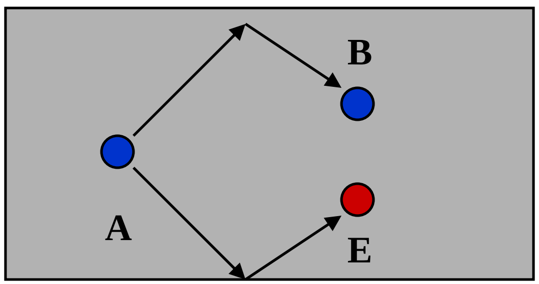
- Much of the new "wireless security" (particularly physical layer security) is being worked on by stand-alone communities:
  - Communication and information theorists without security training
    - *Very few security people actually work on physical layer security*
  - Security people without wireless and signal analysis skills
    - *Very little wireless systems knowledge*
- This translates into:
  - Toy problems
  - Signal analysis methods are primitive
    - *E.g. Take a Neural Network or SVM and apply blindly…*
  - People using "security" to mean "secrecy"
  - Lack of good adversary models
    - *What about Dolev-Yao?*
  - Why do people say "information-theoretic security is the best?"
    - *What about CPA, CCA, CCA2?*
    - *Perfect secrecy is far from perfect*

Putting Eve in a Nice Box

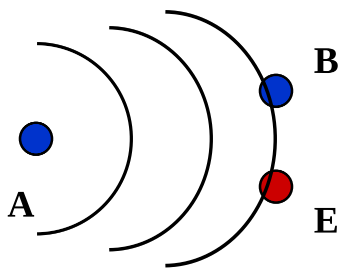
- Some of our standard Eve assumptions:
  - Adversaries are passive and dumb
  - Adversaries are randomly placed
  - Adversaries have the same antennas as Alice and Bob
  - Eve has omni-directional antennas (aka, no spatial filtering)
    - *How much gain can Eve buy for an additional $100? $100000?*
- In Dolev-Yao, Eve the adversary, can:
  - Obtain <u>any</u> message passing through the network
  - Act as a legitimate user of the network (i.e. can initiate a conversation with any other user)
  - Can become the receiver to any sender
  - Can send messages to any entity by impersonating any other entity

Symmetries: Weakness?

- The governing principle behind PHY-authentication is how multipaths combine
- It is possible to construct "benign" scenarios where
  - Alice → Bob phasor sum is the same as Alice→ Eve
  - Temporally, if there are no other entities, then Eve can move to Bob's location at a later time
- But are these really a problem?
  - No environment is such a simple ray-tracing environment
  - Eve moving changes the environment when she moves
- These are challenging fundamental questions to understand and quantify
  - What does it mean to quantify???



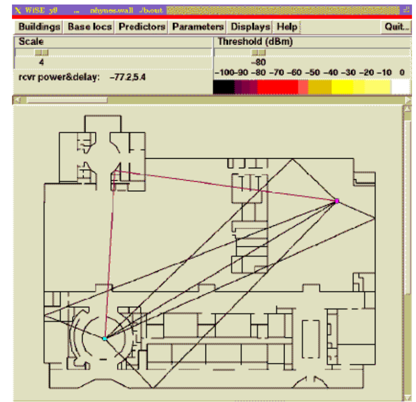
Rectangular rooms



Freespace

Ray-tracing, Complexity and Shadow Attacks

- Question 1: What if the adversary has ray-tracing?
  - Can predict keys? Can use probe knowledge to guess authenticator…
  - Complexity of the “description program”?
  - How accurate is enough?
- Question 2: What if the adversary follows Alice/Bob and uses their old position?
  - Eve can record and decode later
  - Half wavelength is still small…
  - Environments are dynamic
  - Storage requirements…



Many blueprints are public domain!

Common Materials:

Ground

8″ Concrete Cinderblock

Sheetrock

Lossy Sheet Rock

1″ Wood

1″ Wood on 8″ Concrete

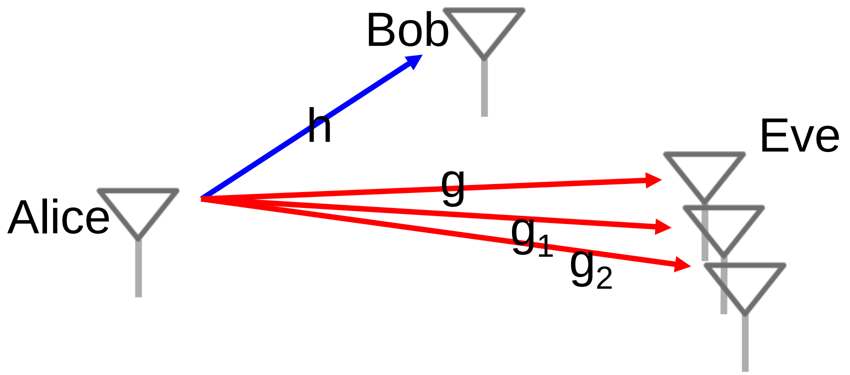
0.5″ Glass

Metallic Wall

Collusion: Weakness for Dissemination

- Dissemination protocols are, inherently, reliant on the fact that Alice→Bob has a better channel than Alice→ Eve (real or synthetically)
- If Eve gets multiple (N) independent observations then
  - At the least, the probability that one of these N is better than A→B goes up (no collaborative processing)
  - With collaborative processing, this probability goes up rapidly.

Nightmare: Collusion Hurts Dissemination



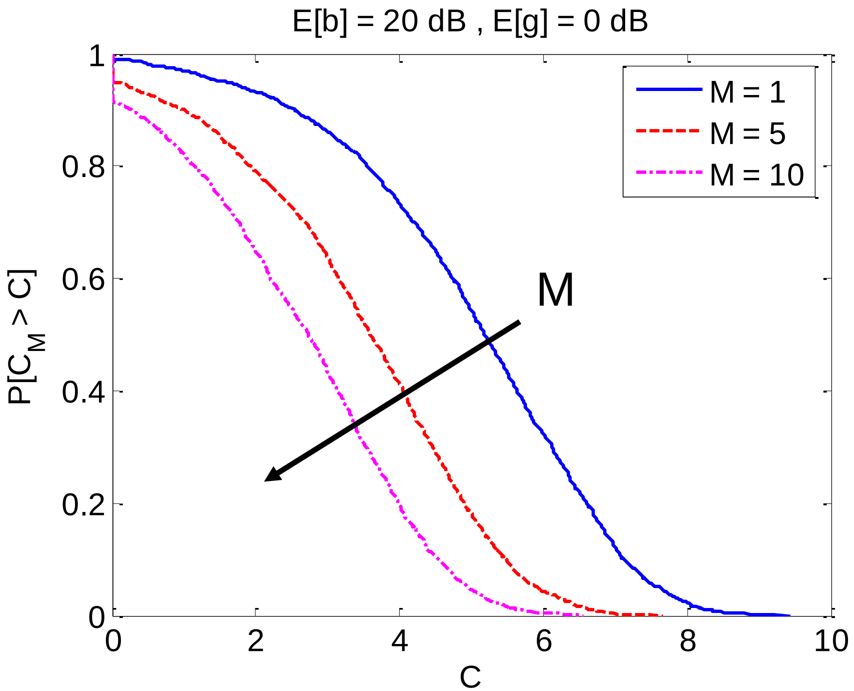
Single Channel Gain: $|g|^2$

New Channel Gain: $|g|^2 + |g_1|^2+|g_2|^2$

Multiple receiving antennas at Eve
- increases Eve's channel gain
- enhances his eavesdropping ability

Case Study:

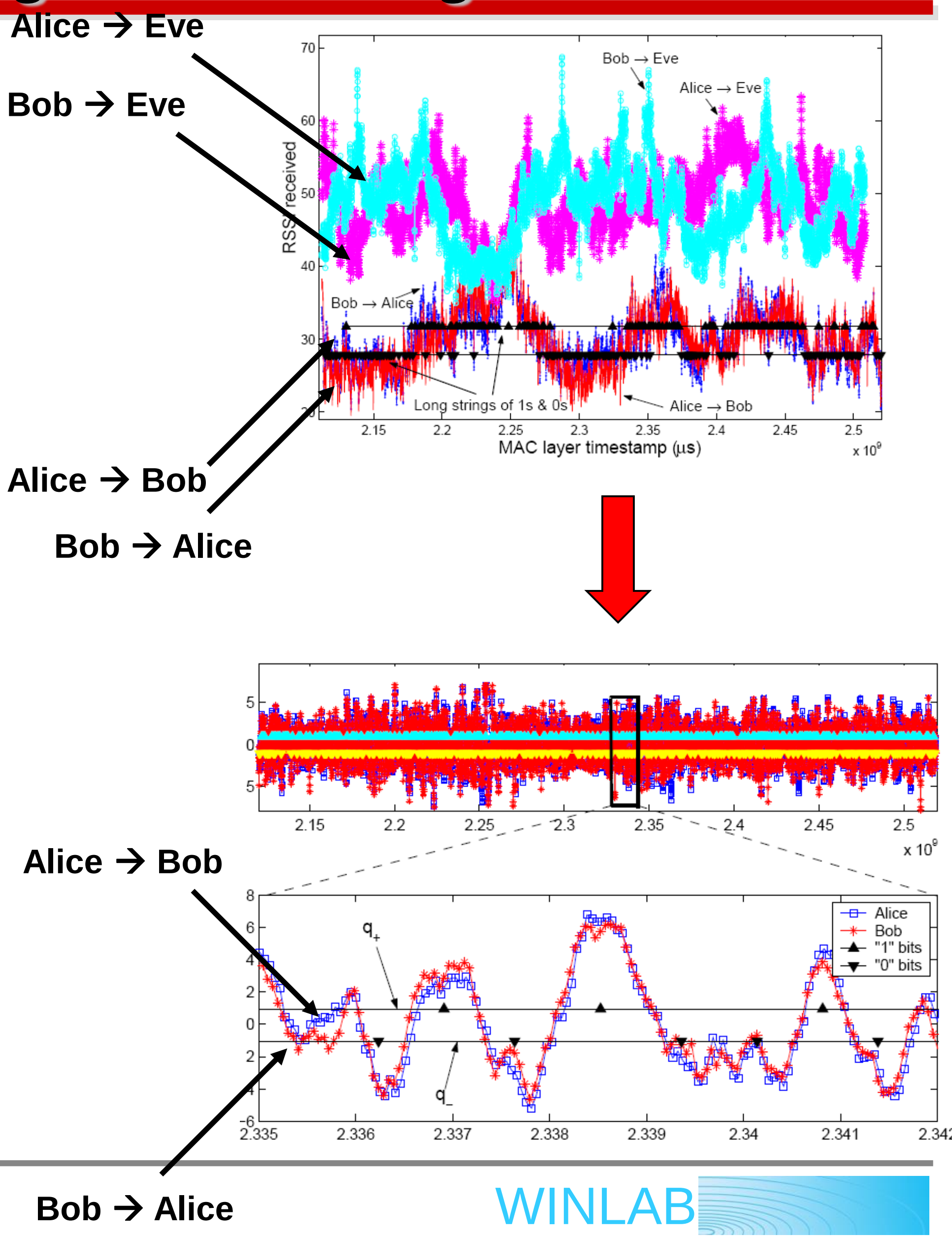
- •Suppose Alice and Bob are SISO, while Alice→Eve is SIMO
- •Eve's average channel gain increases linearly with the number of his receiving antennas
- •Complementary CDF of secrecy capacity



Moral to the Story: Sub-exponential resources for Eve thwarts Dissemination…

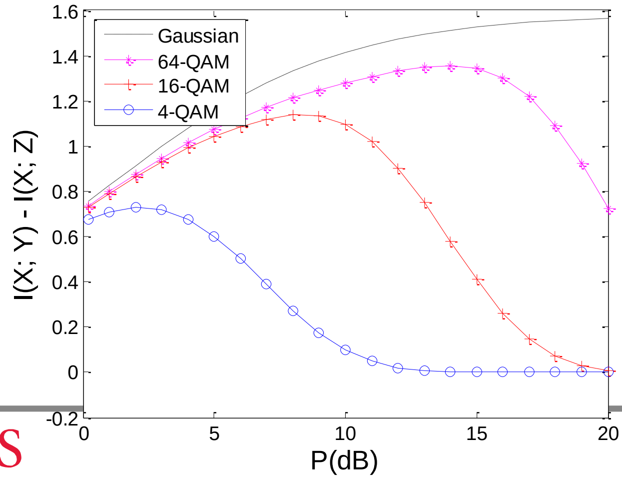
Sometimes you should listen to your hunches… System Validation using 802.11 RSSI goes bad

- Experimental setup:
  - Alice = AP
  - Bob = Client
  - Eve = Client on same channel
- Alice → Bob: **PING REQUEST** Bob → Alice: **PING REPLY**
- 20 packets per second
- Eve overhears packets from both legitimate users
- (RSSI, timestamp) from recd. packet headers are pulled out by each user
- Msg. exchange protocol uses the locations of excursions to distil identical bits
- ~1 bit/sec in typical indoor environments with no errors.
- **Problem: Eve can manipulate RSSI in a meaningful way**
  - **Eve cannot manipulate complex channel response**

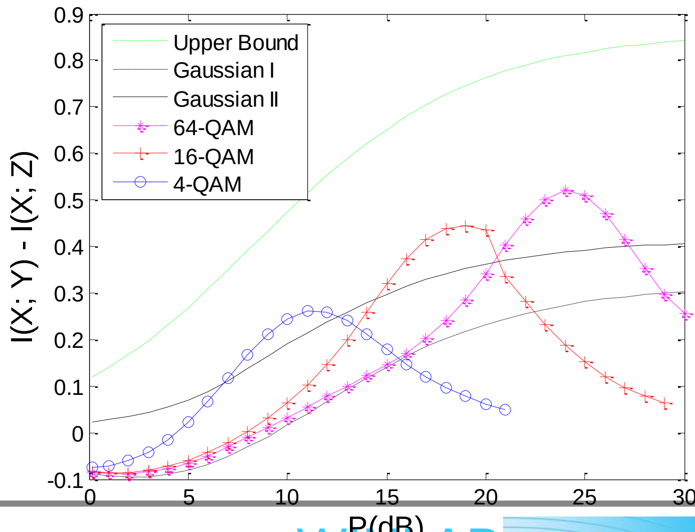


Some Non-Normal Concerns

- How Gaussian is "Gaussian" really in fading?
  - Without symmetry in the fading distribution, we have poor distillation
  - Gaussianity arises in fading from the sum of many independent non-resolvable multipaths
    - *As bandwidth increases, resolvability sets in and application of central limit theorem fails*
    - *Aka, what happens as we take this to the wideband regime?*



- Has anyone ever transmitted a "Gaussian" signal?
  - Results are very different for realistic discrete signaling
  - E.g. for fast fading QAM performs better than Gaussian schemes when Bob's channel is on average worse than Eve's channel – it effectively limits the information leakage when Eve's channel is better



Maybe its not so bad…Reality Check

- This field is new…
- Security community feedback:
  - Open to denial of service
  - Not associated with user identity
  - Man-in-the-middle attacks
  - Weak security models
- Every initial idea has weaknesses and takes time to mature…
- We would note two prior examples:
  - Classical Diffie-Hellman:
    - *Originally susceptible to man-in-the-middle and other authentication failures…*
    - *DH came out in 1976 while STS came out in 1987 (O'Higgins)*
  - Quantum Key Distribution:
    - *Trivially susceptible to DoS– Eve just observes the photons…*
- We need to place such new methods in a holistic cross-layer framework , and integrate with conventional security methods

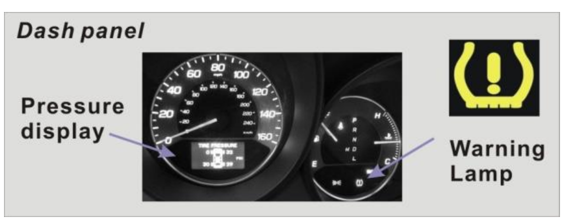
We can try for a holistic and new approach to addressing security issues in wireless systems at the "signal level"

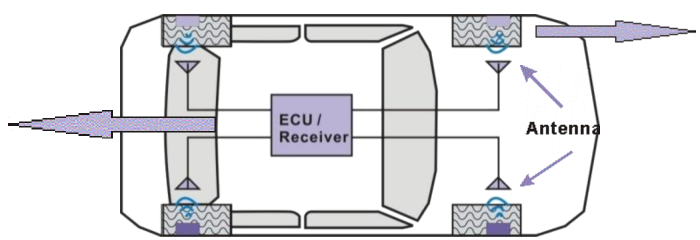
Confidentiality	Wireless is easy to sniff. We still need encryption services and key management. Signals can be made to be hard to decode.
Integrity	Signals should be verified that they originate from who/where they claim to come from, and should not be modified during transit.
Forensics	Wireless networks will be the platform of choice for attacks. Should there be signal recordings to keep track of forensic evidence?
Privacy	Perpetual connectivity can mean constant surveillance! With snooping one can monitor mobility and handoffs between networks.
Location	Location is a new form of information provided by wireless signals/systems that will facilitate new services.
Intrusion	The pervasiveness of the wireless networks should not mean that just anyone can participate! Example: Rogue APs
Availability	The value of a wireless network is its promise of ubiquitous connectivity. Unfortunately, wireless links are easy to "break" (e.g. jam, denial of service)
Non-repudiation	RF energy radiates, and wireless entities within the radio coverage pattern may serve as witnesses for the actions of the transmitter.

SUPPLEMENTAL MATERIAL

Case 1: TPMS — From the Public Domain

- Components of TPMS:
  - Tire pressure sensors
  - TPMS electric control unit (ECU)
  - Receiving antenna(s)
    - *Four or one antenna*
  - Dashboard
- Communication protocols
  - Link Sensor IDs with TPMS ECU
  - Sensors → ECU **315/433Mhz**
    - *ASK/FSK*
    - *ECU filters packets based on IDs*
  - Sensors can be waken up by
    - *ECU → sensors* ***125kHz***
    - *Travel at high speeds(>40 km/h)*





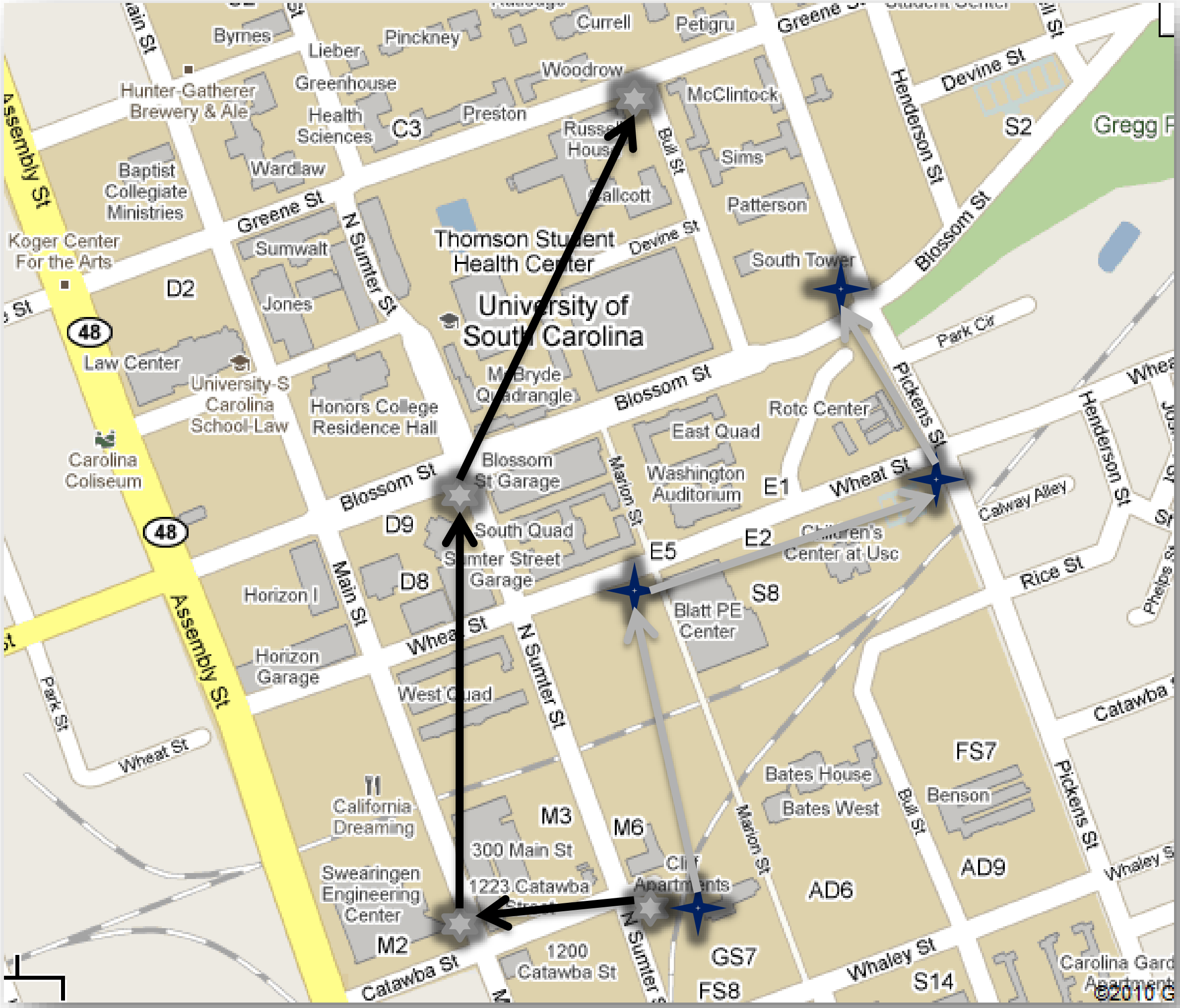
TPMS — To Be Discovered

- The details of communication protocols are proprietary
  - How difficult to reverse engineering?
  - Messages encrypted?
  - Messages authenticated?

- How likely to eavesdrop TPMS communication?
  - High speed, car's Metal body, message rate, transmission power

- How likely to spoof TPMS communication?
  - ECU filters/rejects suspicious packets?
  - How much damage can spoofing accomplish?

Misuse 1: car tracking



Misuse 2: trick the driver to stop

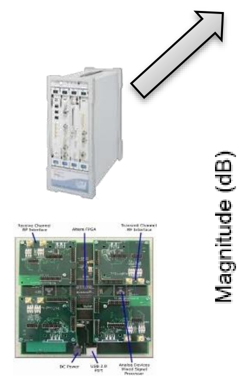
Security and Privacy Analysis step 1: Reverse-engineering

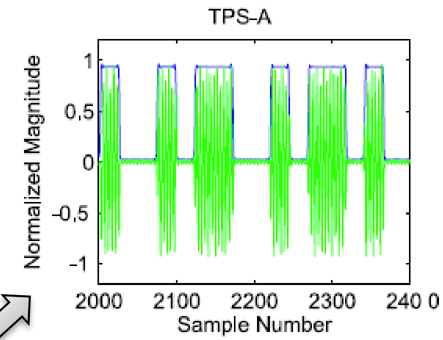
- Proprietary protocols
  - Security through obscurity?
- Goal
  - Modulation schemes
  - Encoding schemes
  - Message formats
  - Encrypted?

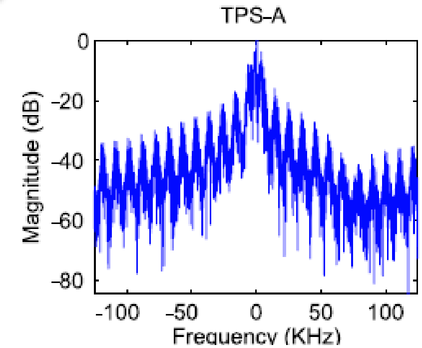
- Equipment
  - Sensors: TPS-A and TPS-B
  - ATEQ VT55
  - Agilent Vector Signal Analyzer (VSA)
  - Universal Software Radio Peripheral (USRP)

Reverse-Engineering Walk-Through

- Capture packet transmission
- Demodulate and decode data
- Determine packet format



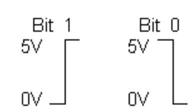




•Triggered sensors at 125 kHz → •Responded at 315 MHz → •Captured RF transmission at 315 MHz → •Determined Modulation ASK

↓

•Encoding Scheme Manchester → •Determined Message Format

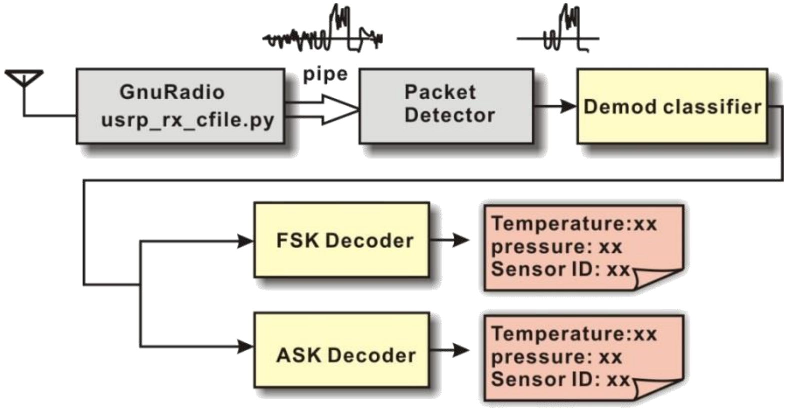


preamble	Sensor ID	Pressure	Temperature	Flags	Checksum

- **No encryption**
- **32-bit or 28-bit**

Security and Privacy Analysis step 2: Eavesdrop capability

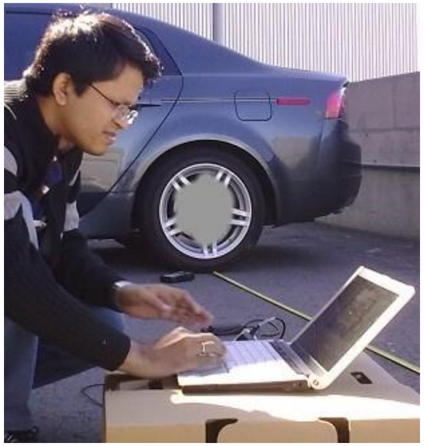
- How likely to eavesdrop?
  - Cars travel at high speeds.
  - Cars’ Metal bodies shield RF.
  - TPMS message rate (1 per 60s-90s)
  - Low transmission power (battery)
- Equipment
  - Sensors: TPS-A and TPS-B
  - A car with TPS-A sensor
  - ATEQ VT55
  - USRP (no VSA)
  - Low noise amplifier (LNA)
- Eavesdropping System
  - Reused decoders from RE
  - Developed a live decoder/eavesdropper

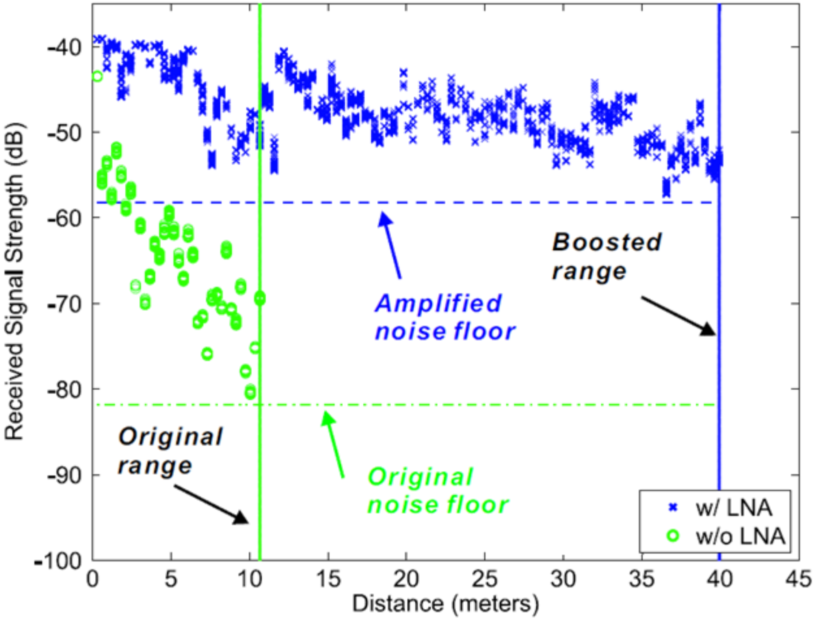


Exp. 1: Eavesdropping Distance

- Scenarios:
  - USRP + cheap antenna
  - USRP +LNA ($75) + cheap antenna

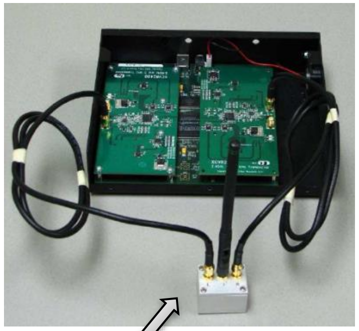
- Observations
  - Able to decode packets, if RSS (received signal strength) > Ambient noise floor
  - LNA boosts the decoding range from 10.7m to 40m





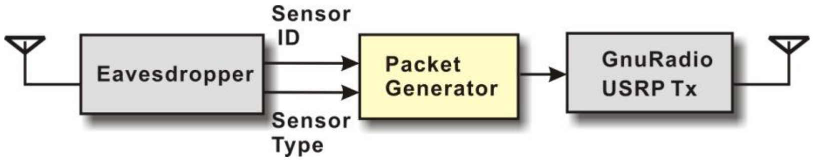
Security and Privacy Analysis : Packet Spoofing

- How likely to spoof TPMS communication?
  - Is the in-car radio able to pick up spoofing packets from outside the vehicle or a neighboring vehicle?
  - Security mechanisms in ECU?
    - *Will ECU filter/reject suspicious packets?*
    - *How long will ECU recover from the spoofing?*



- ***Frequency mixer***

- Equipment
  - ATEQ VT55; A car with TPS-A sensor; USRP
  - Frequency mixer



- Spoofing System
  - Reused eavesdropper from step 2
  - Developed a packet generator
    - *Include proper checksum*
    - *Contain the alarming flag*

Spoofing validation

- Tested on two equipment:
  - ATEQ VT55 validates packet structure.
  - A car using TPS-A validates ECU's logic.
    - *40 packets per minute*

- Observations
  - No authentication;
  - No input validation and weak filtering
  - Warning lights only depend on the alarm flag, not the real pressure
  - Large range: 38 meters with a cheap antenna without any amplifier
  - Inter-Vehicle Spoofing is feasible; travel speed 55 km/h and 110 km/h

• *TPMS-LPW Light*

• *Vehicle's warning light*

PHY-101

- RF Signals transmitted from Alice to Bob are affected by a variety of different factors: attenuation, large-scale and small-scale fading
- Fading arises as a signal's multipaths constructively & destructively combine at the receiver
- System Model: For input u(t), the received signal is

$$r(t) = \int_{-\infty}^{\infty} h(t,\tau)u(t-\tau)d\tau$$

- Under the wide-sense stationary uncorrelated scatter (WSSUS) model, the channel response becomes a tapped-delay line:

$$h(t,\tau) = \sum_{i=1}^{N} h_i(t)\delta(t-\tau_i)$$

- Under Rayleigh Fading assumptions $h_i(t)$ are zero-mean complex Gaussian

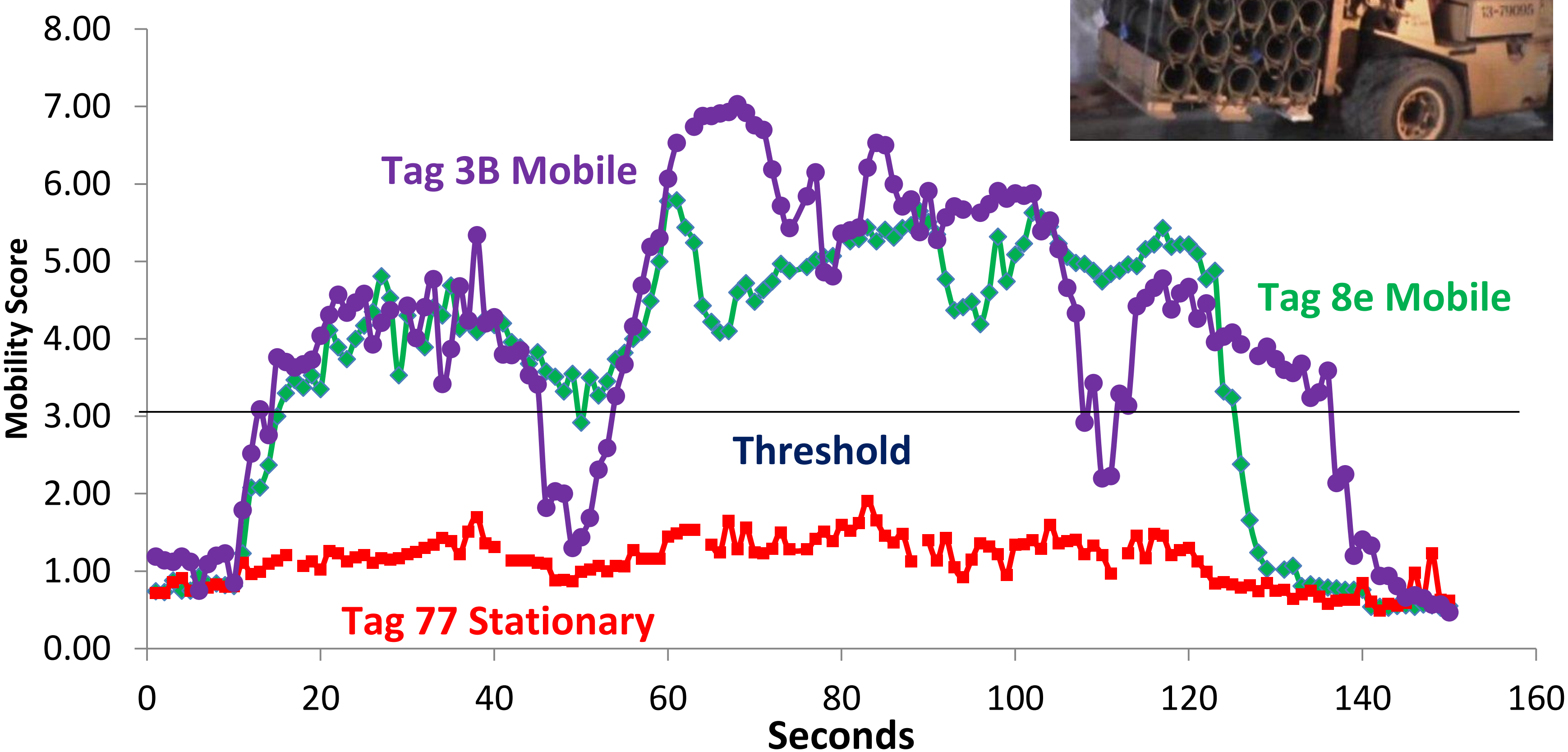
PHY-101

- The channel response is itself time-varying and stochastic
  - There is temporal, spectral and spatial variability of the channel response
  - *Coherence Time:* Difference in time needed for fading correlation to drop below a threshold
  - *Coherence Bandwidth:* Separation in frequency needed for fading correlation to drop below a threshold
- Additionally, we may examine the instantaneous fading correlation between locations
- Jakes showed under uniform scattering that the fading correlation (amplitude correlation in received signal) drops off rapidly over a distance of half a wavelength

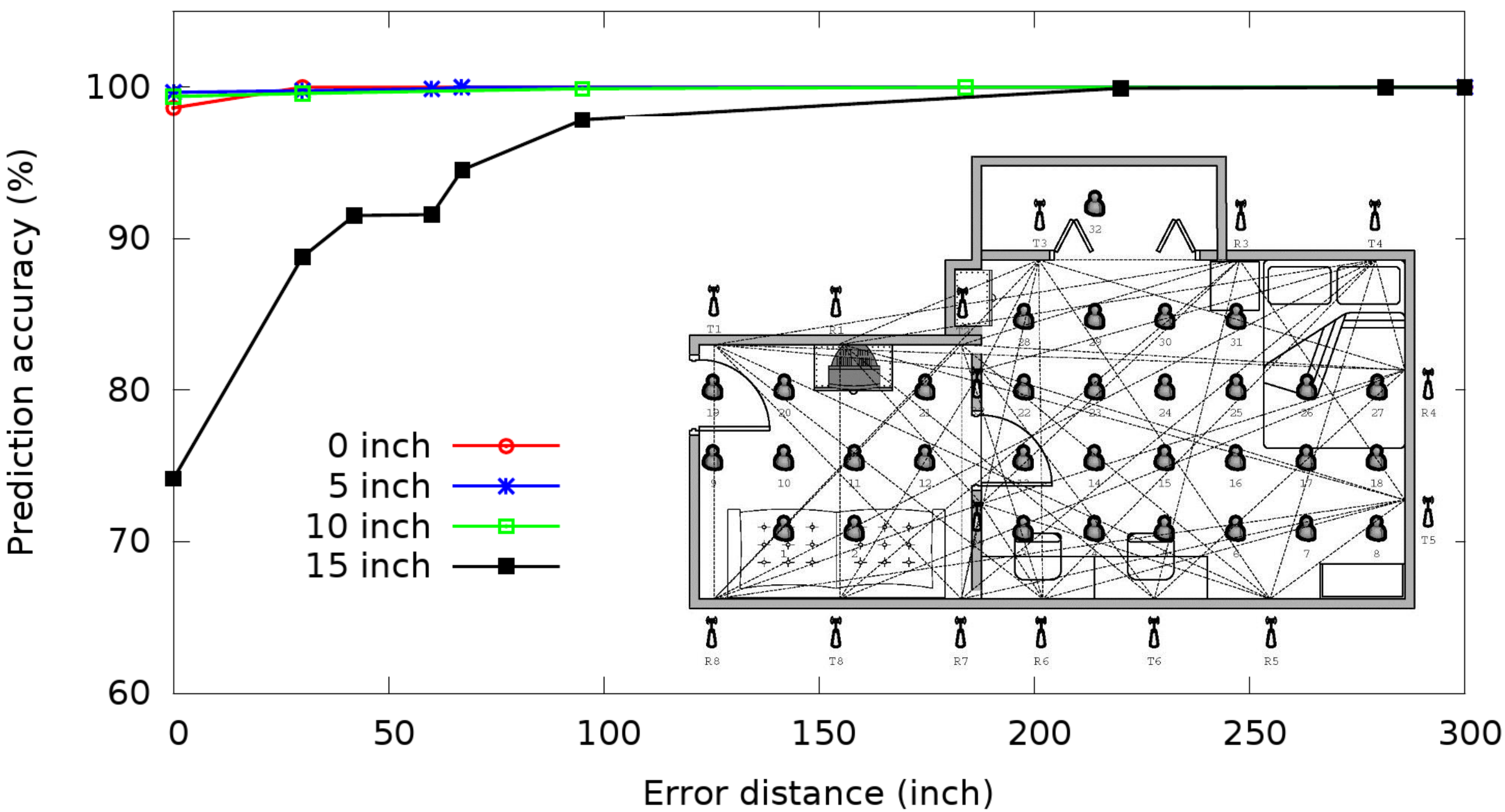
$$C(d) \approx J_0^2(2\pi d / \lambda)$$

- Separate by a wavelength and independence is a reasonable assumption (under Rayleigh WSSUS)

Mobility Detection is Possible by Monitoring Ambient RF



The wireless medium allows for forms of tomographic information extraction



"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov