UMassAmherst

# Physical Layer Security and Privacy with Ultra-wideband

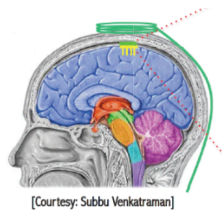

Prof. Wayne Burleson

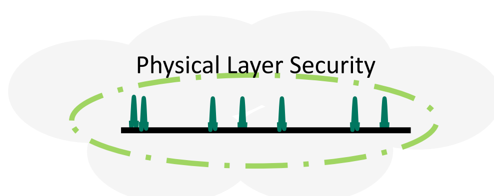
Department of Electrical and Computer Engineering

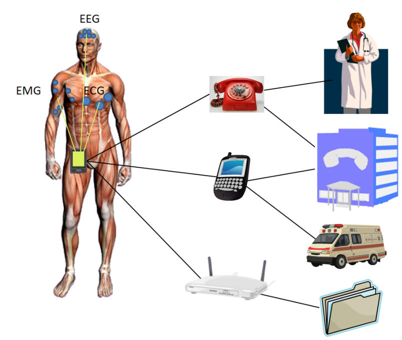
University of Massachusetts Amherst

burleson@ecs.umass.edu

(visiting EPFL 2010-2011)


Supported by NSF 0831133 CT-ER: Ultra-wideband Radio for Low-Power Security

# Disclaimer

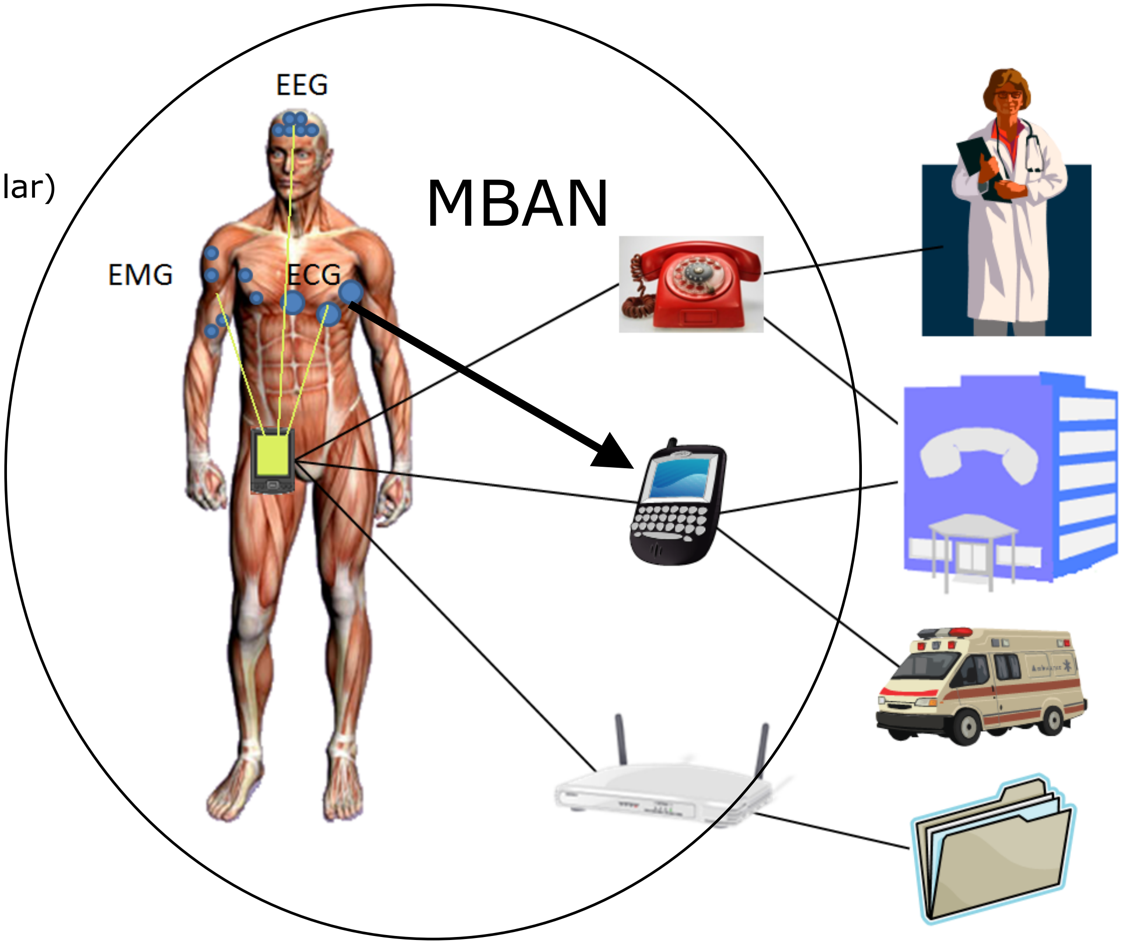
- This presentation is a survey of some recent work in the UWB area applied to implantable medical devices.
- My contribution is largely speculative, namely, that physical layer UWB provides a good match for the low-level security/ privacy requirements of a class of implantable medical devices.
- There is still much work to be done…

# Outline

- Motivations
  - Requirements of IMD communication
    - Security and Privacy
    - Data-rate (>100kbps)
    - Range/Channel : BAN
    - Asymmetric channel: ie lightweight device, heavy reader ( Active RFID)
  - Challenges
    - Threat: Physical Layer Detection and Identification,
    - Threat: Eavesdropping
    - Power (battery-powered, harvested, or remote-powered device)
- A Possible UWB Solution (Ko and Goeckel, 2010)
- Related Work (timedomain.com, ETHZ, BWRC)
- Future Directions

# Wearable Medical BAN applications

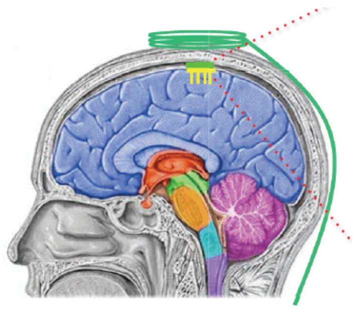
- **Bio-Medical**
  - EEG Electroencephalography
  - ECG Electrocardiogram
  - EMG Electromyography (muscular)
  - Blood pressure
  - Blood SpO2
  - Blood pH
  - Glucose sensor
  - Respiration
  - Temperature
  - Fall detection
  - Ocular/cochlear prosthesis
  - Digestive tract tracking
  - Digestive tract imaging
- **Sports performance**
  - Distance
  - Speed
  - Posture (Body Position)
  - Sports training aid



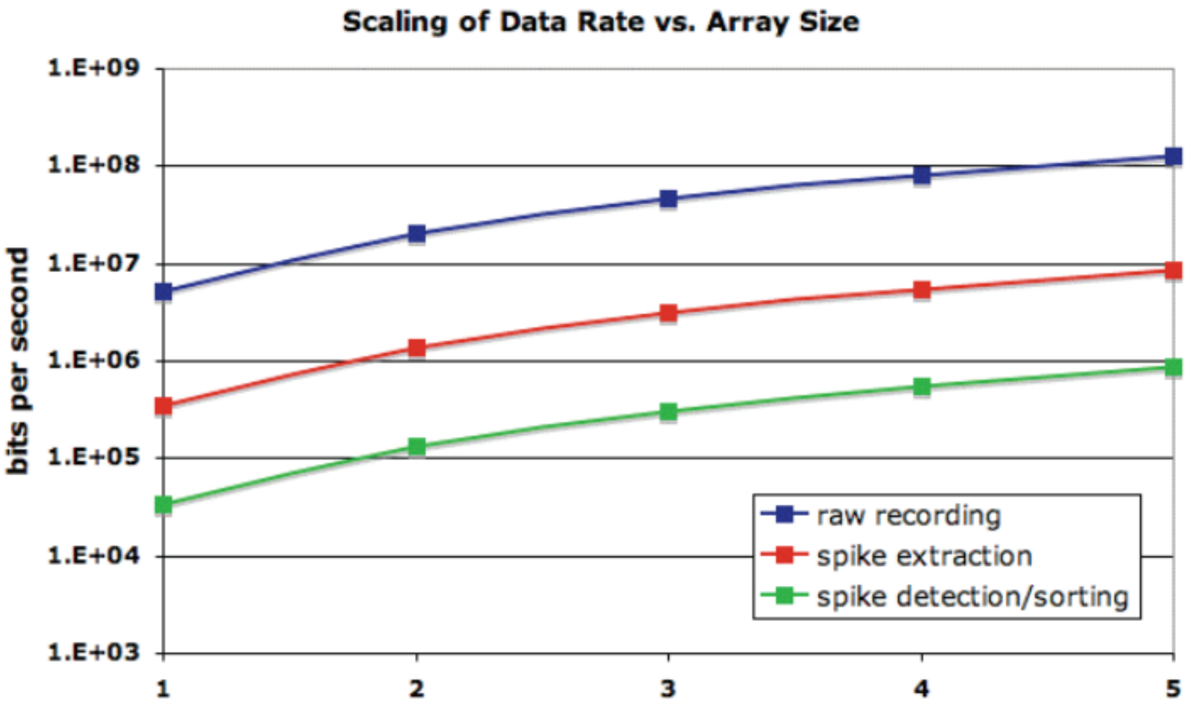

Images courtesy CSEM , 2009

# Increasing data rates in IMDs

Example:
Brain Implant,
Berkeley Wireless
Research Center



[Courtesy: Subbu Venkatraman]




[Rizk 07 and Harrison 06]

# Conflicting Design Goals in IMDs

## Safety/Utility goals

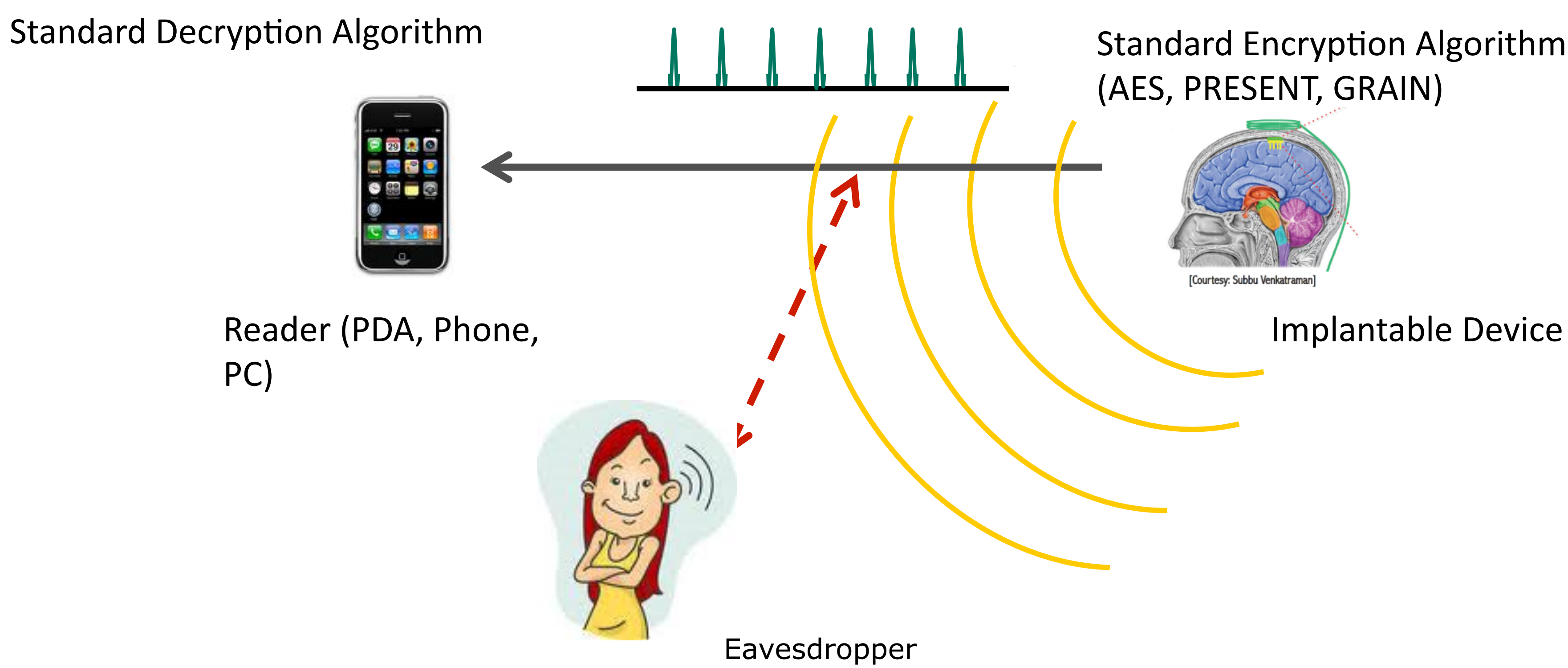
- Data access
- Data accuracy
- Device identification
- Configurability
- Updatable software
- Multi-device coordination
- Auditable
- Resource efficient

## Security/Privacy goals

- Authorization (personal, role-based, IMD selection)
- Availability
- Device software and settings
- Device-existence privacy
- Device-type privacy
- Specific-device ID privacy
- Measurement and Log Privacy
- Bearer privacy
- Data integrity

From D. Halperin et al, "Security and Privacy for Implantable Medical Devices", IEEE Pervasive Computing, 2008

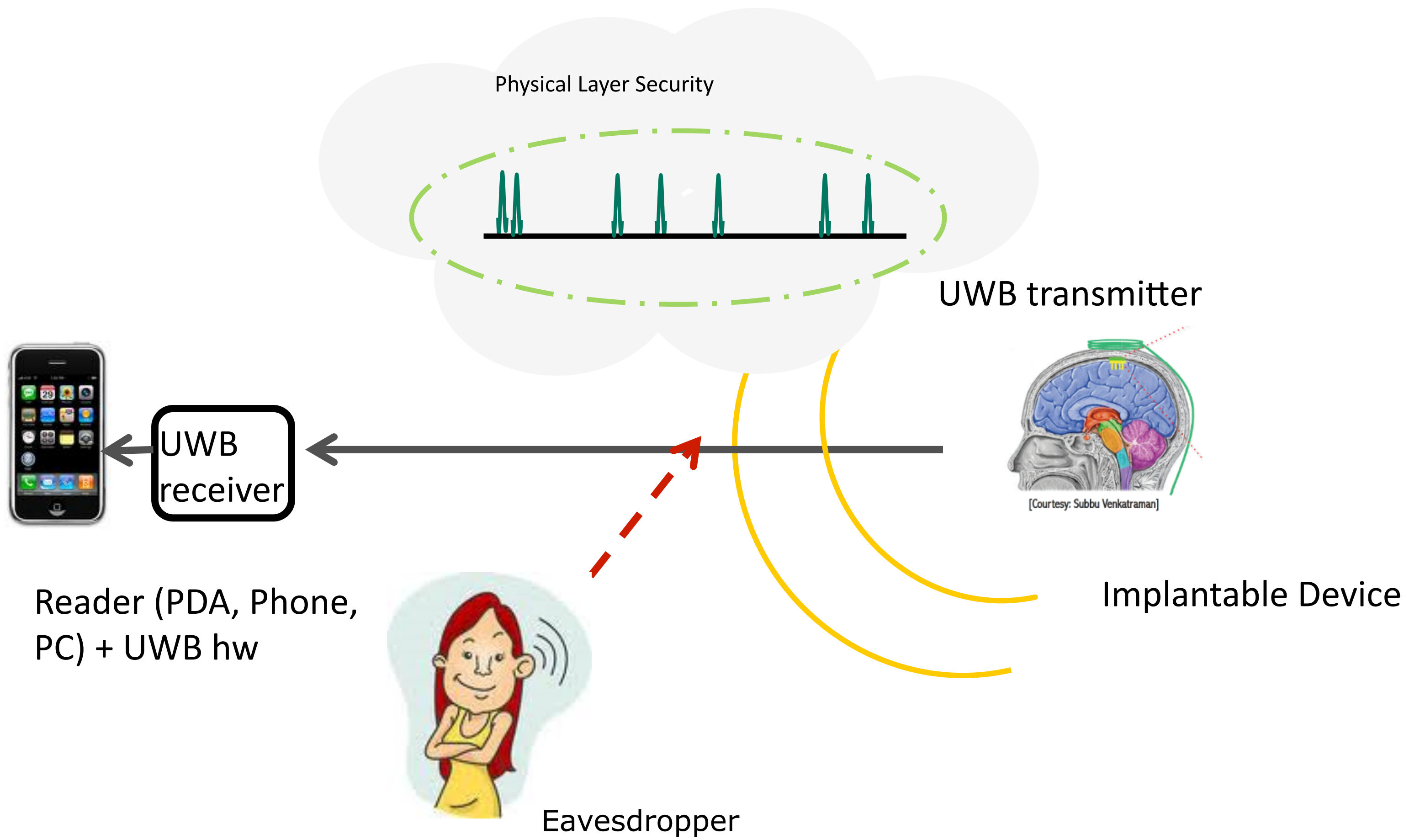
# Encrypt the high data-rate uplink to prevent eavesdropping





7

# Idea: Use UWB to achieve physical layer security





8

# Ultra-wideband Radio for Low Power Security

**Original Motivation:** Standard crypto algorithms (AES, etc.) can be too power/energy consuming for RFID tags, especially passive tags.

**Idea:** Can we save power by pushing some part of the cryptography to the Physical Layer? Employ impulse-radio ultra-wideband to "hide" the signal in the time-domain.

- Desired receiver (knows the key) can aggregate energy to perform channel estimation (and eventually decode). (D. Goeckel)
- Eavesdropper suffers from (asymptotically infinite,) noncoherent combining loss.

**Questions**:

1. Can we formulate a "hard" problem for the eavesdropper to solve?
   (Ari Juels – RSA Labs, Dan Boneh – Stanford)
2. How does the power consumption compare to all-digital schemes?
   (W. Burleson– digital, R. Jackson – analog/RF).
3. Is the scheme more side-channel tolerant? (W. Burleson and C. Paar).

Supported by NSF 0831133 CT-ER: Ultra-wideband Radio for Low-Power Security

# Experiment with UWB schemes to optimize BER metrics

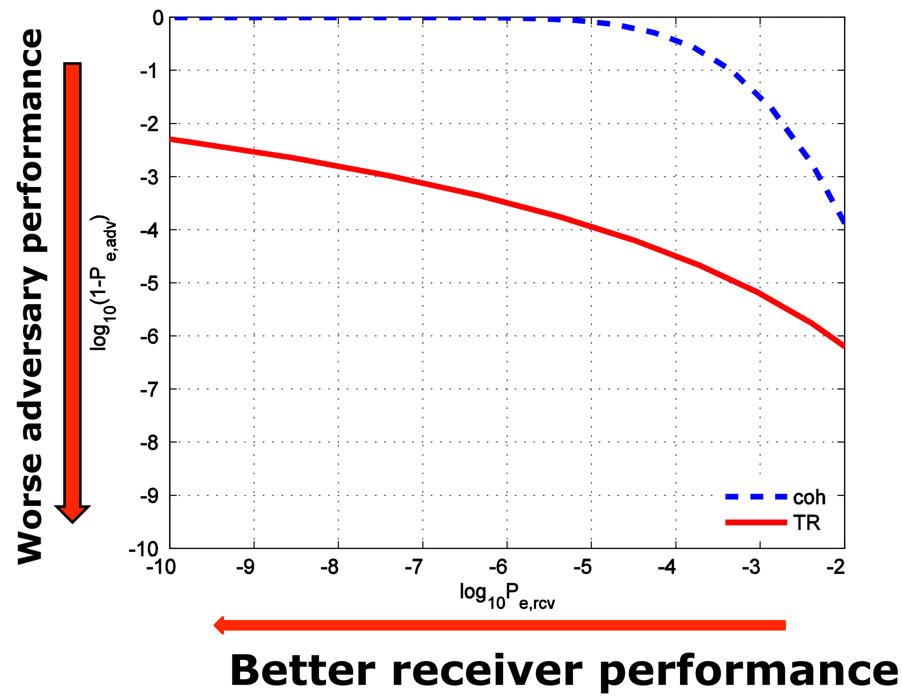
**Goal (big picture):**

Position UWB pulses with a key so that receiver has advantage over eavesdropping adversary

**Choices:**

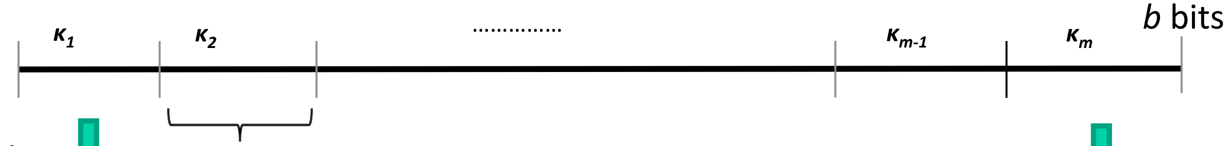
Coherent vs. Transmitted Reference

Framed vs. Frameless



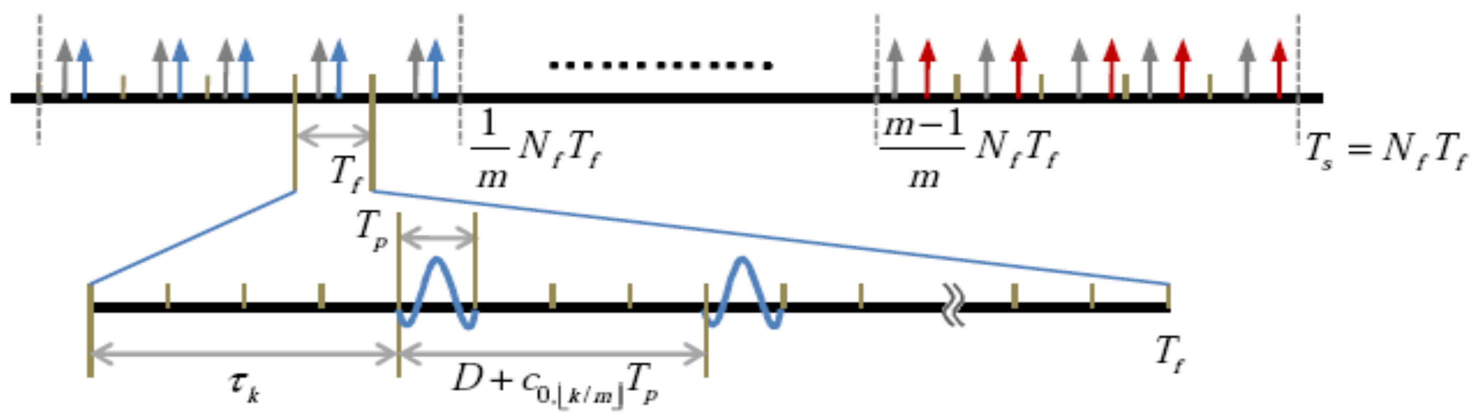
# Keyed Time-referenced Impulse Radio UWB

*b*-bit secret key K

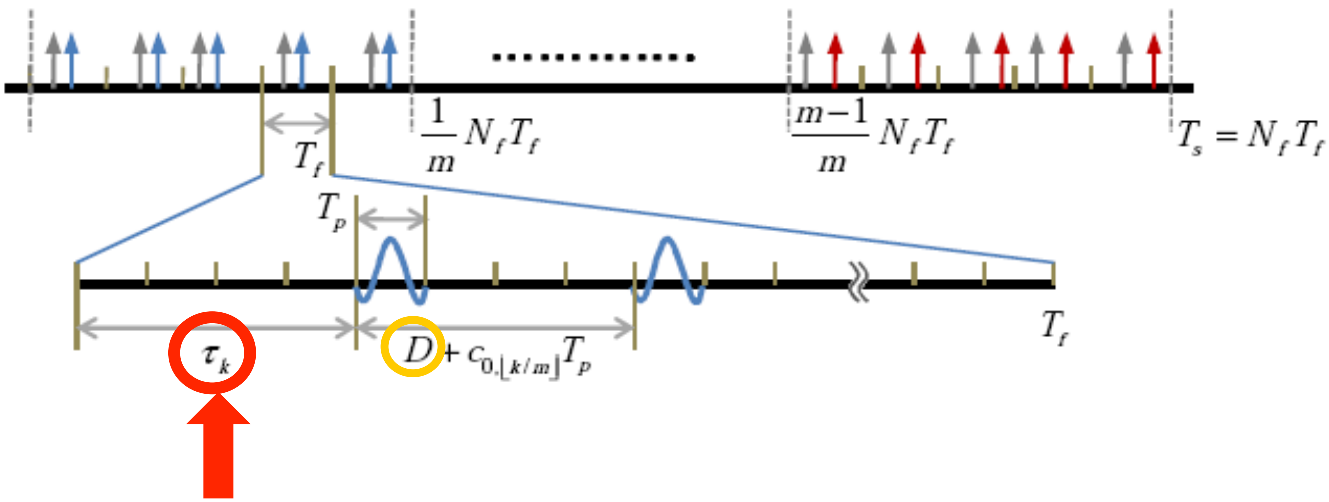



*Determine the time delay between the reference and data pulses in the initial $N_f/m$ frames*

*Determine the time delay between the reference and data pulses in the final $N_f/m$ frames*



# Lightweight TRNG needed to confuse adversary.

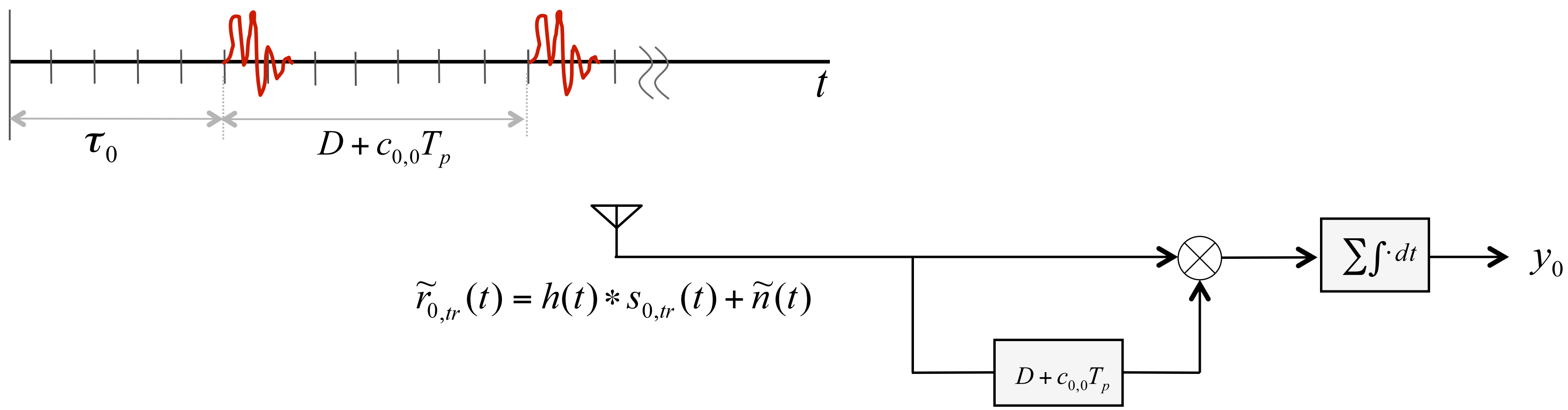



- Random offsets employed to prevent the adversary from detecting the transmitted signal coherently
- Generated by a very fast and light True Random Number Generator (TRNG)
  - S. Srinivasan, et al (Intel) "A 4Gbps 0.57pJ/bit Process-Voltage-Temperature Variation Tolerant All-Digital True Random Number Generator in 45nm CMOS", in Intl. Conf. on VLSI Design, 2009,
  with secure calibration enhancements by V. Suresh and W. Burleson, HOST 2010.
- Intended receiver only knows key but does not need to know TRNGs

M. Ko and D. Goeckel, "*Wireless Physical-Layer Security Performance of UWB systems*", MILCOMM, 2010

# Performance for Transmited Reference (TR) Reception

## *Intended Receiver*



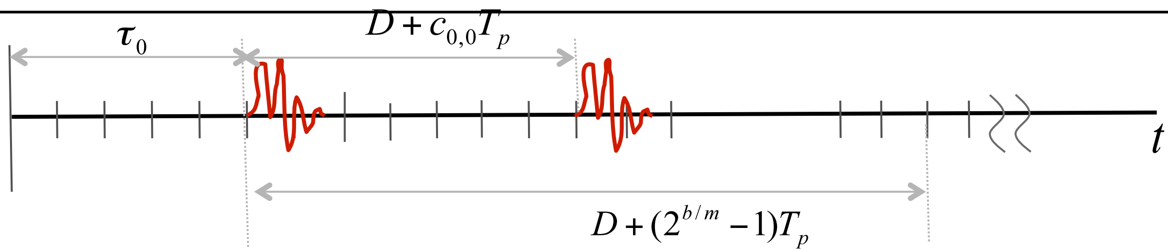

*Thus, the decoding error probability of the receiver*

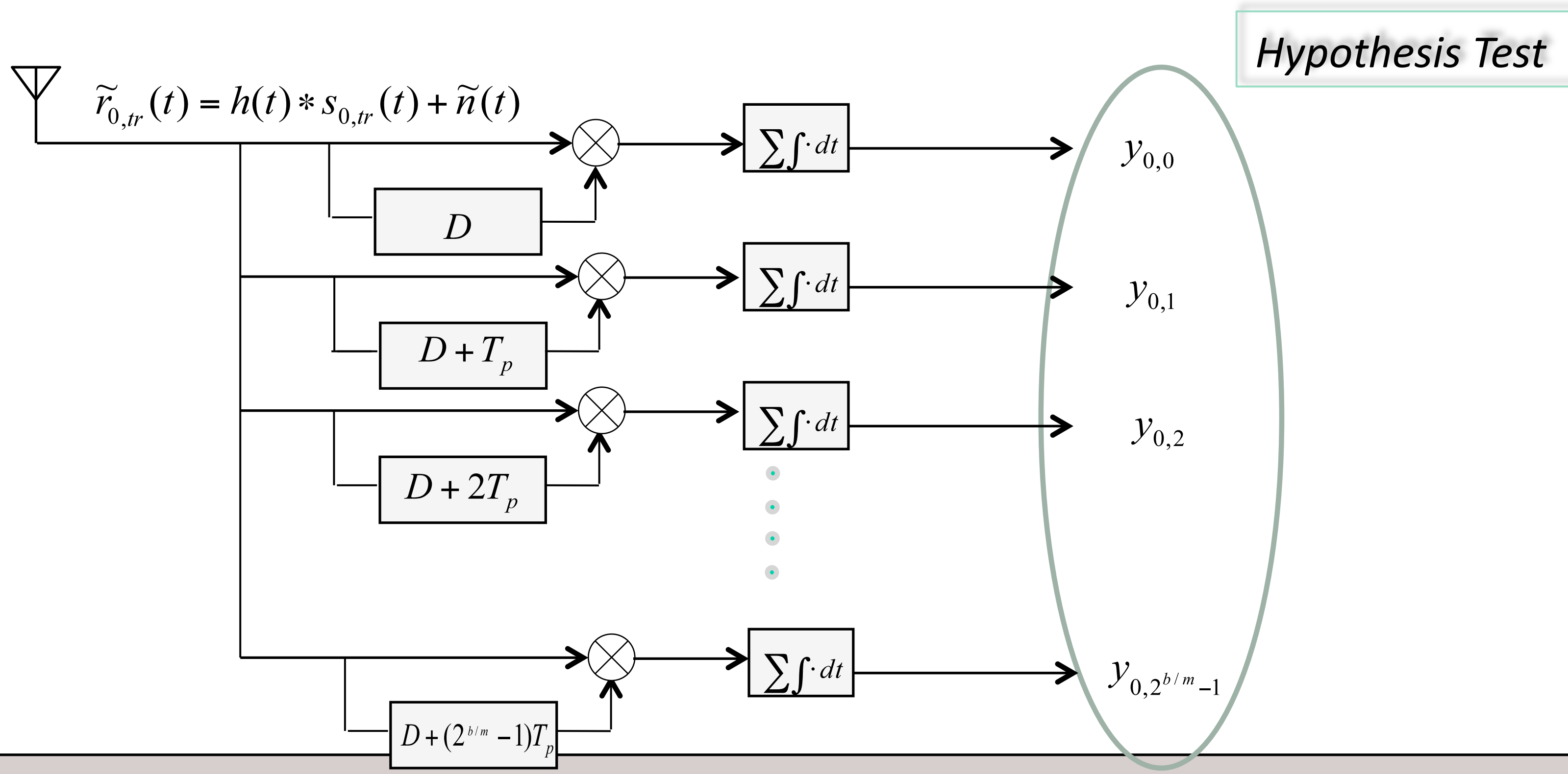
$$P_{e,\,TR-rcv} = E_{\underline{h_l}}\left[Q\left(\frac{E_s \sum_{l=0}^{L-1} h_l^2}{\sqrt{4E_s N_0 \sum_{l=0}^{L-1} h_l^2 + 2T_s N_0^2 W}}\right)\right]$$

M. Ko and D. Goeckel, "*Wireless Physical-Layer Security Performance of UWB systems*", MILCOMM, 2010

# Performance for TR Reception

***Adversary***




M. Ko and D. Goeckel, "*Wireless Physical-Layer Security Performance of UWB systems*", MILCOMM, 2010

UMassAmherst

# Performance for TR Reception

**Adversary**

*Hypothesis Test*

$y_{0,c_{0,0}} \sim N(\mu_0, \sigma^2)$ *when finding the signal*

$y_{0,i} \sim N(\mu_i, \sigma^2), \quad i \neq c_{0,0}$ *when missing the signal*

*where*

$$\mu_0 = \frac{E_s}{2m} \sum_{l=0}^{L-1} h_l^2$$

$$\mu_i = \begin{cases} \frac{E_s}{2m} \sum_{l=0}^{L-|i-c_{0,0}|-1} h_l h_{l+|i-c_{0,0}|}, & c_{0,0} - L < i < c_{0,0} + L \\ 0, & \text{otherwise} \end{cases}$$

$$\sigma^2 = \frac{E_s N_0}{m} \sum_{l=0}^{L-1} h_l^2 + \frac{T_s {N_0}^2 W}{2}$$

M. Ko and D. Goeckel, "*Wireless Physical-Layer Security Performance of UWB systems*", MILCOMM, 2010

# Performance for TR Reception

## *Adversary*

*The probability of finding the correct pulse positions in each group of $N_f$/m frames*

$$P_{c,\ TR-adv,\ 0|\underline{h}}$$
$$= \int_{-\infty}^{\infty} \prod_{i=0, i \neq c_{0,0}}^{2^{b/m}-1} \left(1 - Q\left(\frac{r-\mu_i}{\sigma}\right)\right) \cdot \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(r-\mu_0)^2}{2\sigma^2}}\ dr$$

*Thus, the probability of error for the adversary finding the entire key*

$$P_{e,\ TR-adv} = 1 - E_{\underline{h_l}}\left[\left(P_{c,\ tr-adv,\ 0|\underline{h_l}}\right)^m\right]$$

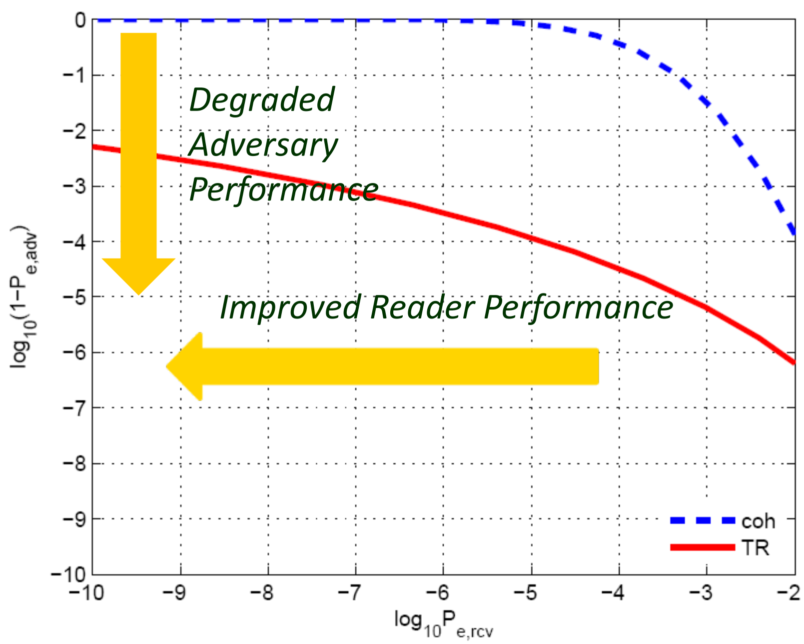
M. Ko and D. Goeckel, "*Wireless Physical-Layer Security Performance of UWB systems*", MILCOMM, 2010

# Simulation assumptions

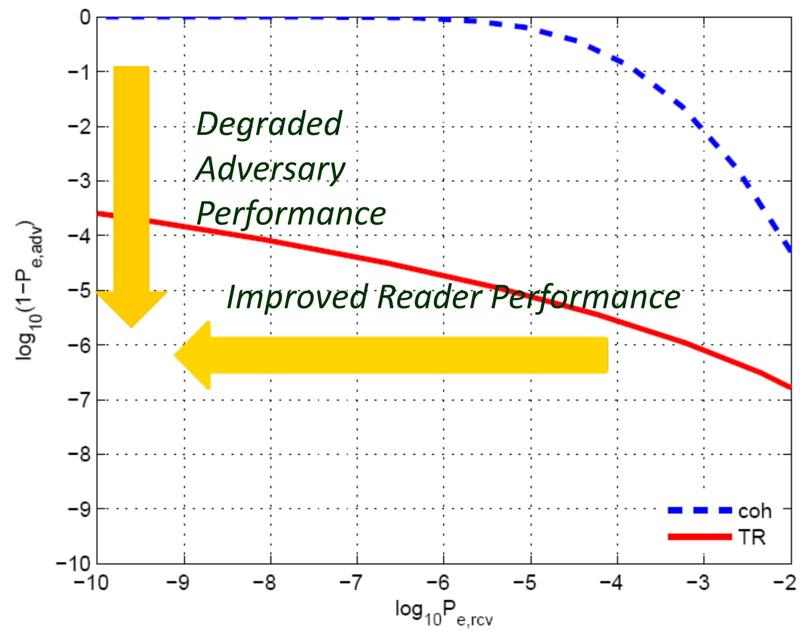
- Tested security performance of the intended receiver and the adversary for both coherent and TR reception
- Considered two different environments, i.e., IEEE 802.15.4a LOS office and LOS outdoor environments
- Assumed the received SNR is the same at both the intended receivers and the adversaries (ignoring near-far problem)
- Used a *30-bit* secret key by dividing it into 5 parts ($m$=5)
- Considered a low-data rate application of 100 *k*bps

UMassAmherst

# Comparison of Security Performance




*Comparison of security performance of UWB systems intended for coherent reception and TR reception in IEEE 802.15.4a **LOS office** environments*



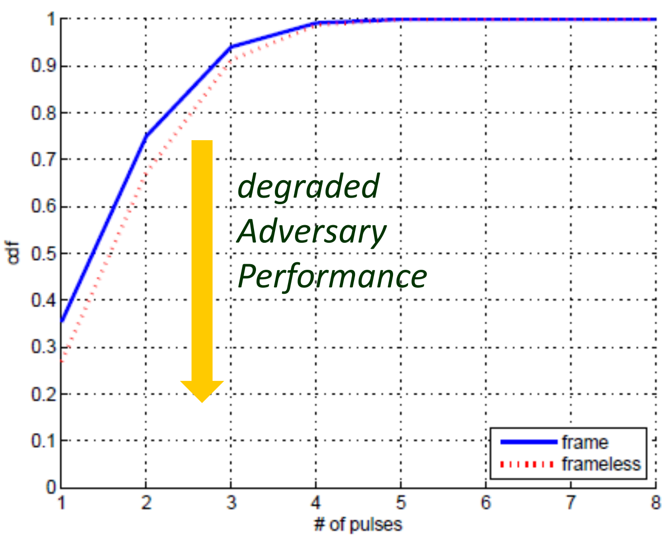

*Comparison of security performance of UWB systems intended for coherent reception and TR reception in IEEE 802.15.4a **LOS outdoor** environments*

M. Ko and D. Goeckel, "*Wireless Physical-Layer Security Performance of UWB systems*", MILCOMM, 2010

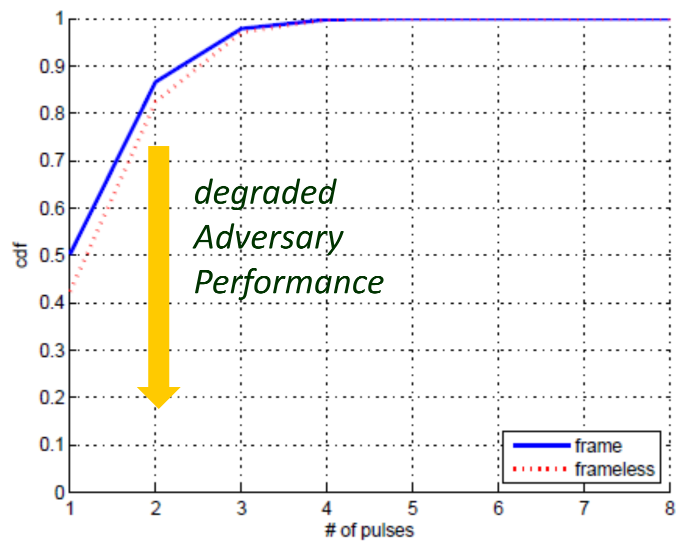
# Performance Comparison: Framed vs. Frameless

## No limitation on key bits

*Given sufficient secret key bits, assume* $N_f = N_p = \frac{b}{k}$ *and consider integers satisfying these relationships.*




*CDFs of the number of pulses that the adversary detects.*
*B=128, k=16, and* $N_f = N_p = 8$
*Frameless is better*




*CDFs of the number of pulses that the adversary detects.*
*B=64, k=8, and* $N_f = N_p = 8$
*Frameless is better*

M. Ko and D. Goeckel, "*Wireless Physical-Layer Security Performance of UWB systems*", MILCOMM, 2010



19

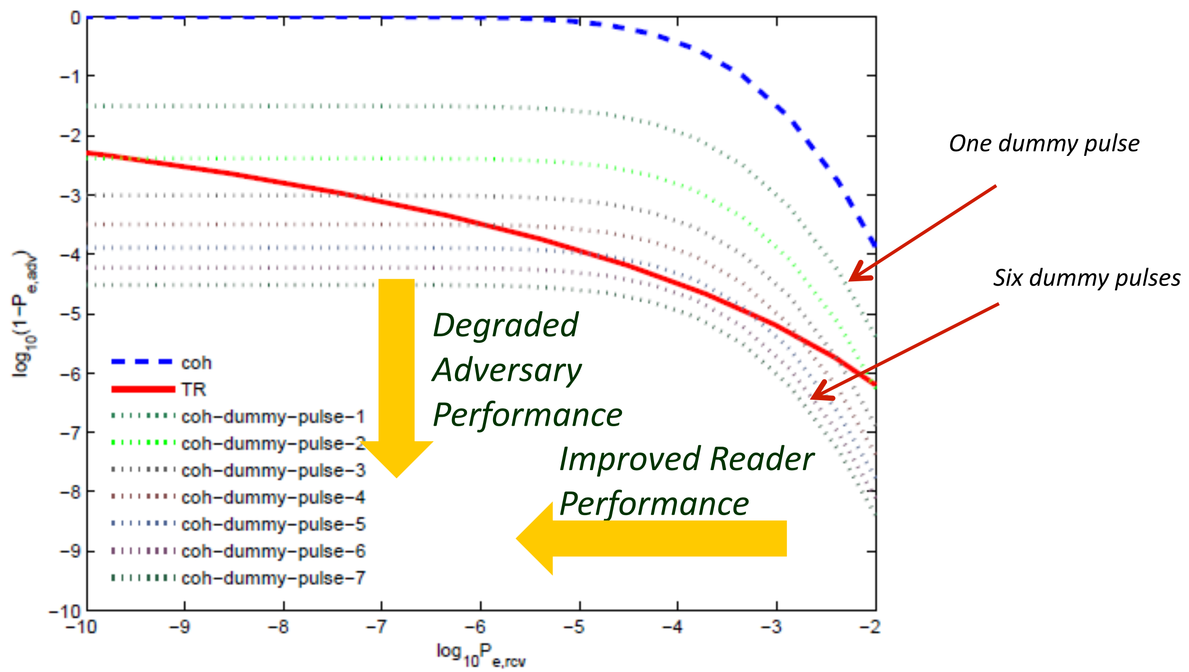
# Results from simulations

- Proposed low-power UWB signaling schemes to provide some level of encryption at the physical layer when the transmission of signals is intended for coherent reception and TR reception
- Suggested that the UWB TR systems outperform the coherent UWB systems in terms of performance of the desired receiver versus that of the adversary
- Proposed a frameless signaling scheme when the transmission is intended for coherent reception to offer enhanced physical layer security
- Suggested that frameless signaling schemes outperform framed signaling schemes if there are the same number of pulses in one symbol period


20

# Comparison of UWB TR and coherent with dummy pulses.

*Use excess power to produce dummy pulses in the coherent system*




*Comparison of security performance of UWB system intended for coherent reception generating dummy pulses and TR system in IEEE 802.15.4a LOS office environments*

# Additional Benefits of UWB

- Harder to detect (timedomain.com)
- Harder to physically fingerprint (Danev et al (ETHZ), Usenix 2009)
- Can be implemented as backscatter in a purely passive tag by modulating reflected pulse train (Berkeley Wireless Research Center)

# Low probability of detection

- Time Domain Corporation (TDC) proposes using an Ultra-wideband (UWB) communication system to provide a reliable 30 km RF link between an unmanned aerial vehicle and a ground station. Pseudo random flipped and time hopped codes provide a whitened pulse train with very low power spectral density (PSD). The **PSD looks like Gaussian distributed noise to most narrowband low noise detection systems and would be very difficult to detect with wideband systems.**

  Timedomain.com

# Physical layer identification of wireless devices

- Signal processing and pattern recognition methods allow very accurate identification of wireless devices from analog radio behavior
- Power-up transient and other discriminants
- We conjecture that IR-UWB reduces these vulnerabilities.

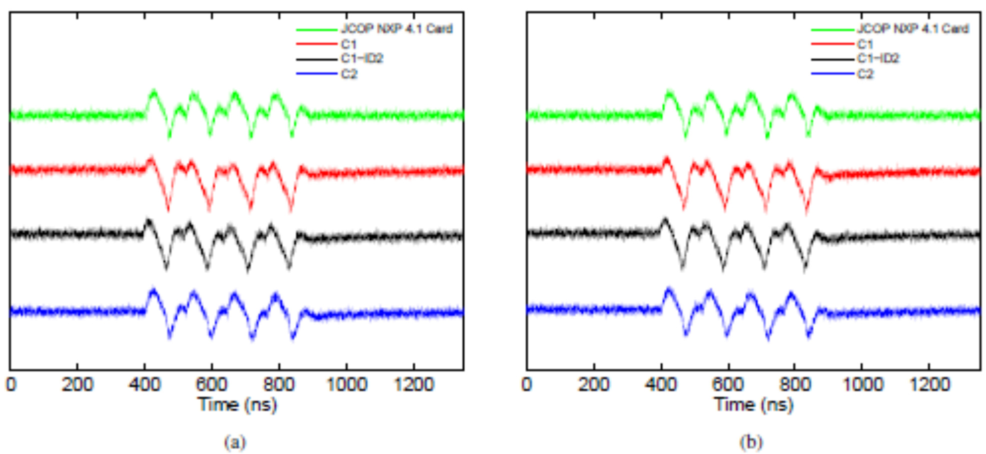
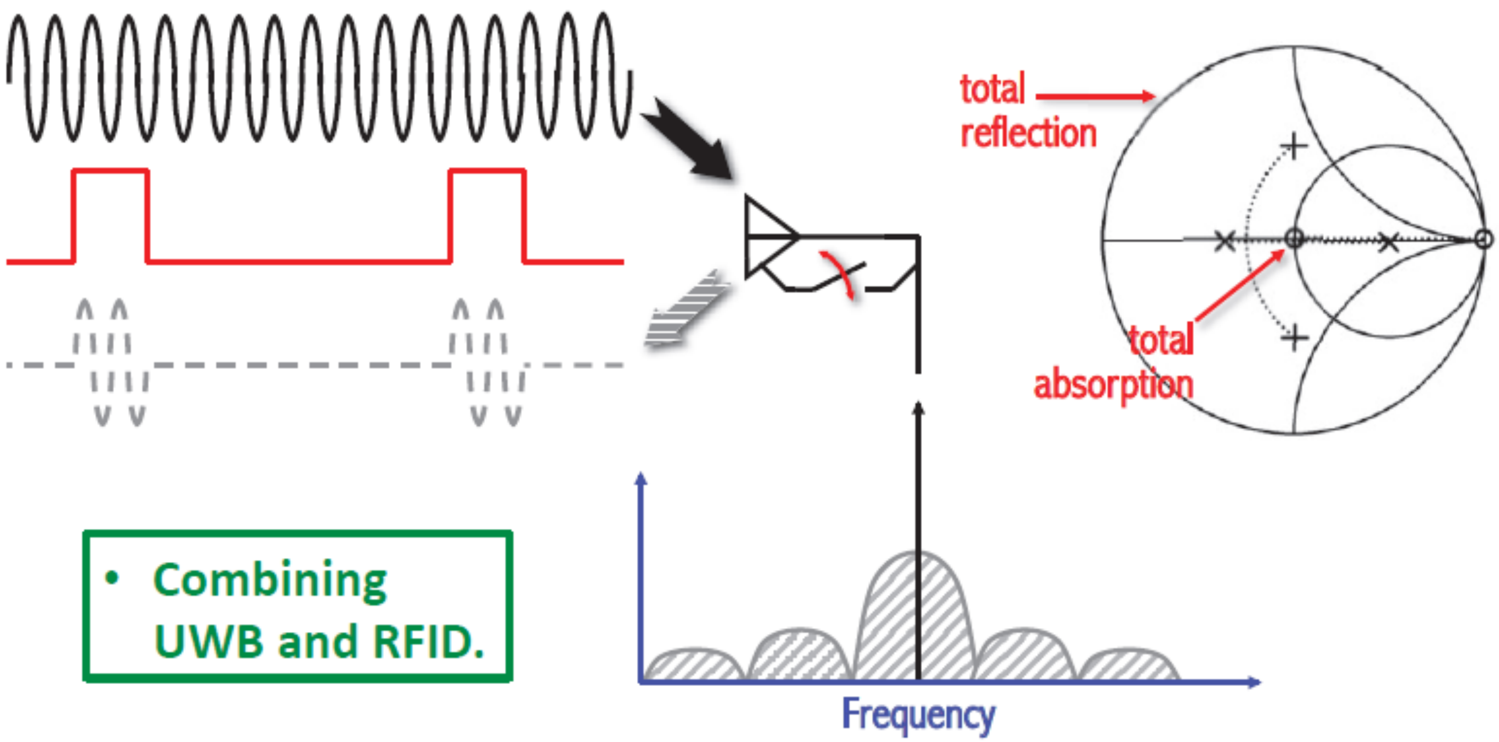



Figure 6: Modulation shape of the responses of 4 different classes (C1),(C1-ID2),(C2),(JCOP): a) first run b) second run. In each run, the sample transponders were freshly placed in the fingerprinting setup. These plots show the stability of the collected modulation-shape features across different runs.

B. Danev, T. Heydt-Benjamin, S. Capkun., Physical-layer Identification of RFID Devices , USENIX Security Symposium, 2009.

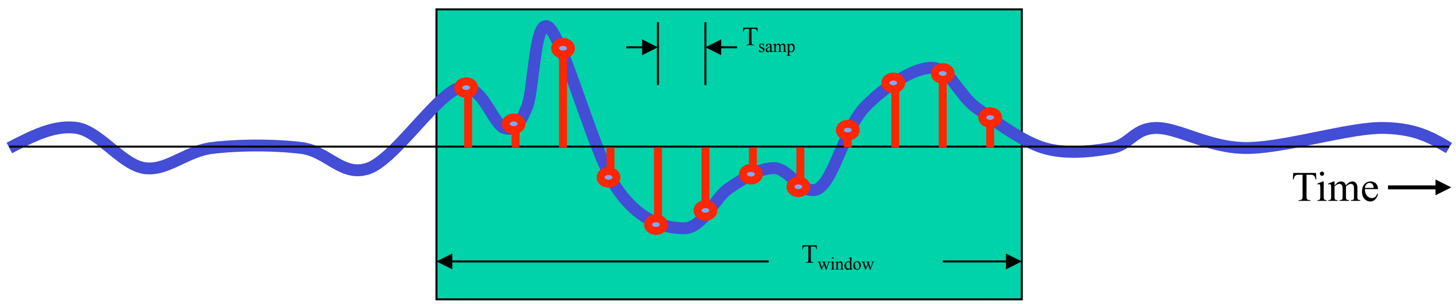
# Reflective Impulse Radios (RIR)




- Combining UWB and RFID.

# UWB Receiver Implementation Issues

Energy of Pulse is Contained in Small Time Window




Only Need Limited Amount of Fast Sampling

Use Parallel Sampling Blocks

Have Rest of Time in Cycle to Process Samples

Do Digital Correlation

Minimum of Analog Blocks Run at Speed

# Conclusions

- Security can be implemented at the physical layer through impulse-based UWB providing low-power protection against:
  - Eavesdropping
  - Device detection
  - Device identification
- UWB schemes transmitted reference vs. coherent and framed vs. frameless were evaluated for different scenarios
- Future Directions:
  - Implementation of UWB radio in small form factor and low energy
  - Experiments on realistic MBAN channel
  - More thorough security analysis including RF fingerprinting
  - Extensions to allow passive back-scatter (RIR) tags

# Upcoming Event!

Speakers:

- Kevin Fu, UMass Amherst, USA
- Srdjan Capkun, ETHZ, CH
- Jos Huiskens, IMEC, NL
- Ahmad Sadeghi, Darmstadt, DE
- Ian Brown, Oxford, GB
- F. Valgimigli, Metarini, IT
- A. Guiseppi-Elie, Clemson, USA
- Q. Tan, Shanghai, China

Panel : How real and urgent are the security/privacy threats for IMDs? Which IMDs?

(just following IEEE ISMICT in nearby Montreux, Switzerland, www.ismict2011.org)


**http://si.epfl.ch/SPIMD**

# Is this too novel, too late? Aren't standards in place?

"Medical marches to a different cadence than most of the electronics industry. Design cycles can stretch from three to five years and cost $10-15 million, thanks to the lengthy regulatory process. The product lifecycles can also extend over a 20 year time span."

*Jon Knight, Boston Scientific*