



NAVAL
POSTGRADUATE
SCHOOL

Software Defined Radios for Cyberspace Operations

Frank Kragh

Assistant Professor of Electrical and Computer Engineering

NPS Cyber Summit

October 29, 2009

GL-109

Monterey, California

WWW.NPS.EDU



- Why SDRs are important to cyberspace operations.
- Past NPS research in SDR
- Current NPS research in SDR
- Looking ahead: Possibilities for future NPS research in SDR

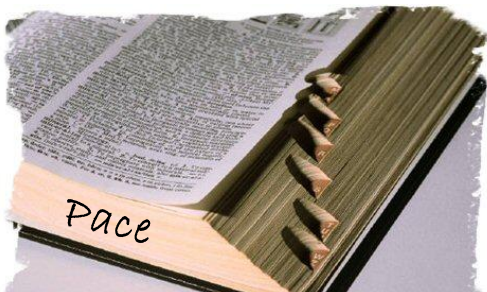


“Cyberspace is defined as:

A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data in networked systems and associated physical infrastructures.”

the wireless part is important!

- The National Military Strategy for Cyberspace Operations, Dec 2006





Importance of Wireless to Cyberspace operations

- The enemy uses wireless.
- wireless comms can be vulnerable to exploitation
 - detection
 - geolocation
 - eavesdropping
- ... and we have distinct advantages over the enemy





What is a Software Defined Radio?

- *A software-defined radio (SDR) can receive any modulation across a large frequency spectrum by means of programmable hardware which is controlled by software*
- strong analogy with computers.
 - A computer can be a word processor, a financial tool, or an analysis tool by running the appropriate software.
 - A SDR can be a cell phone, a wireless LAN transceiver, or a SINCGARS by running the appropriate software.
- Examples: Joint Tactical Radio System, Digital Modular Radio, FlexRadio systems, Universal Software Radio Peripheral*, High Performance SDR, Vanu's Anywave® Base Station, and some collection tools are SDRs.
- SDRs can be Cognitive Radios with the appropriate software





Why is SDR better than hardware radios for cyber operations?

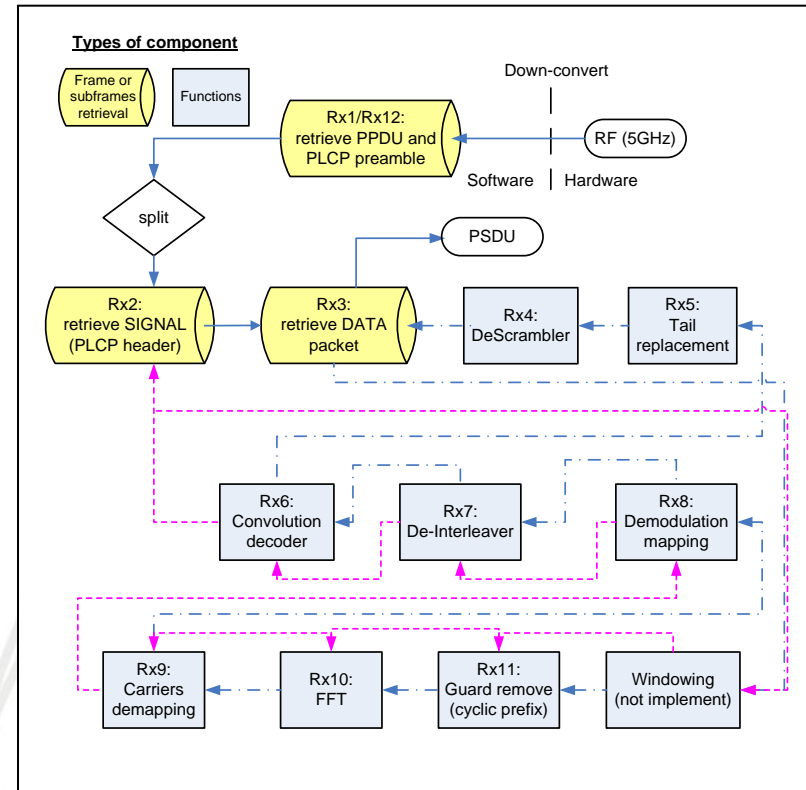
- multimode
 - 802.11, 802.16, 802.20, 802.22, IS-95, GSM, GSM Edge, cdma2000, W-CDMA, HIPERMAN, LTE, ...
- updatable (future-proof, in a sense)
 - many DoD systems are in place for a long time.
 - software updates for future wireless standards.
 - over the air (OTA) software updates
- scalable
 - many waveforms, many simultaneous signals
- real time or non-real time
- software is portable
 - can be used in complex baseband systems and simpler systems in the field



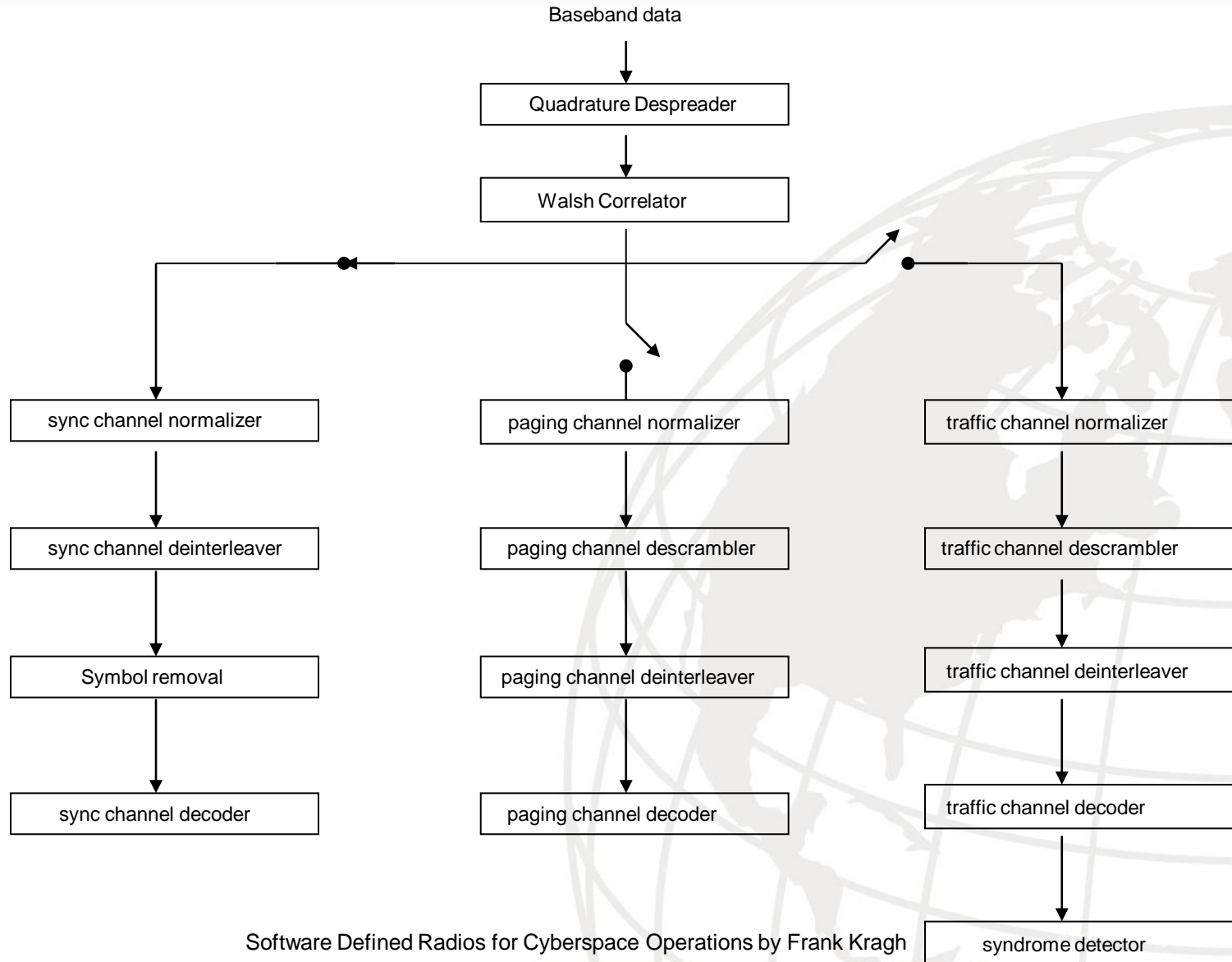
- Why SDRs are important to cyberspace operations.
- **Past NPS research in SDR**
- Current NPS research in SDR
- Looking ahead: Possibilities for future NPS research in SDR

- 802.11a transceiver
- 802.16 transceiver
- IS95B transceiver
- GSM mobile phone locator
- Design of FPGA-based compression algorithm
- frequency shift keying transceiver
- Signal parser (separates overlapping unrelated signals)

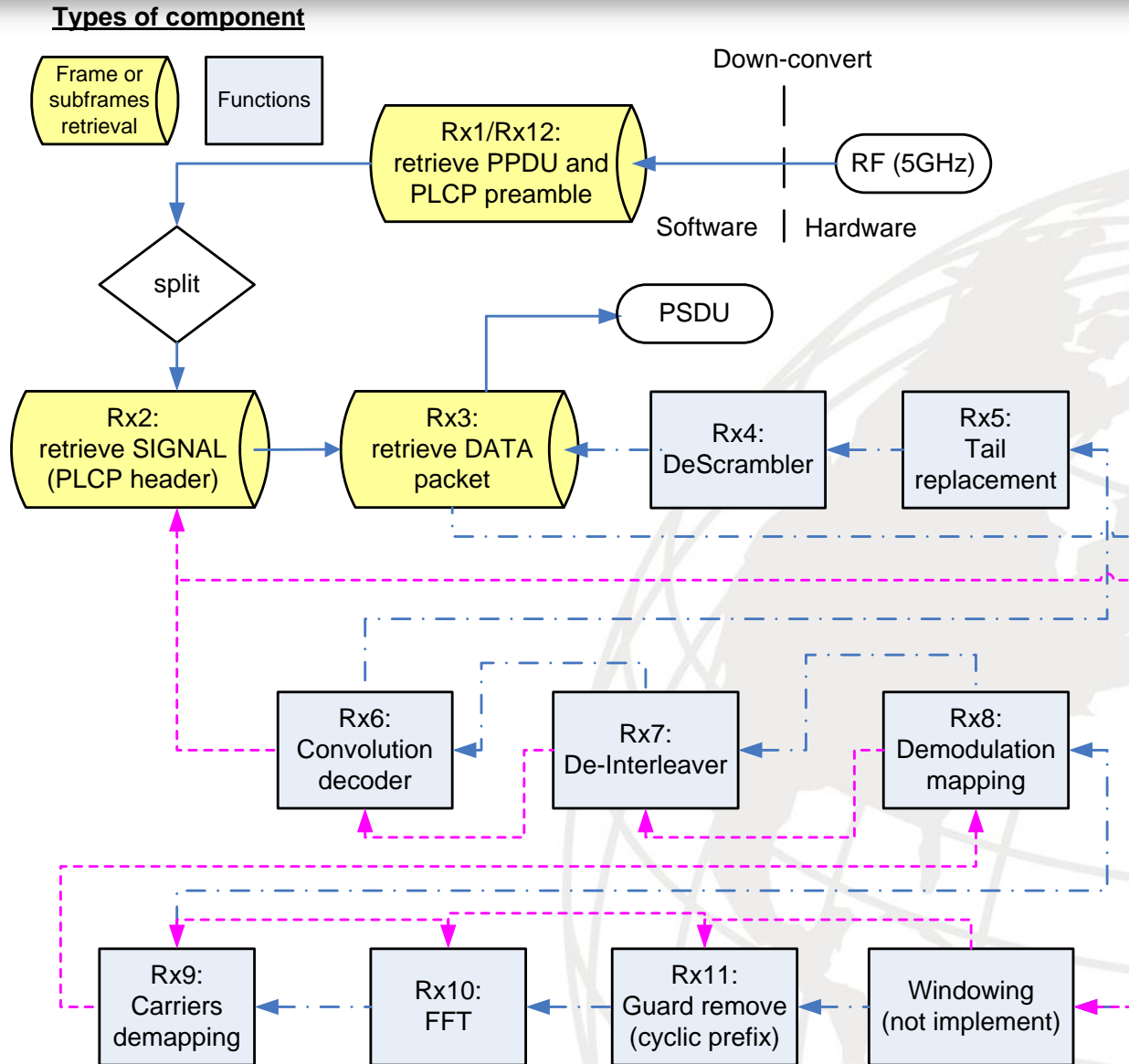
SCA compliant



IS95B receiver waveform

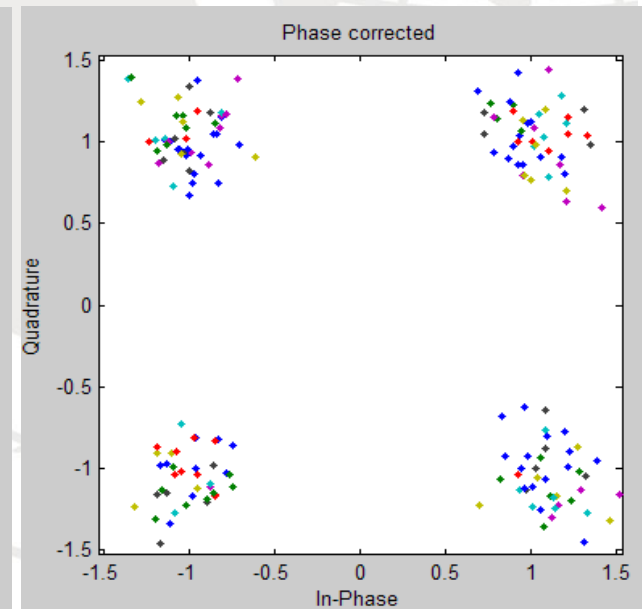
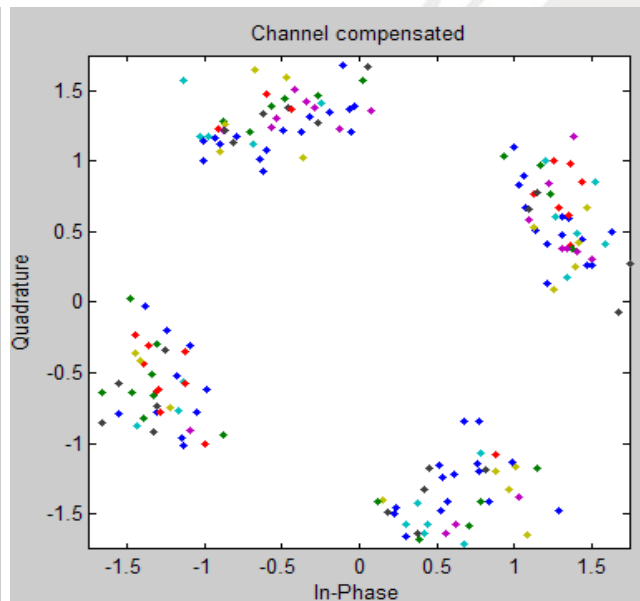
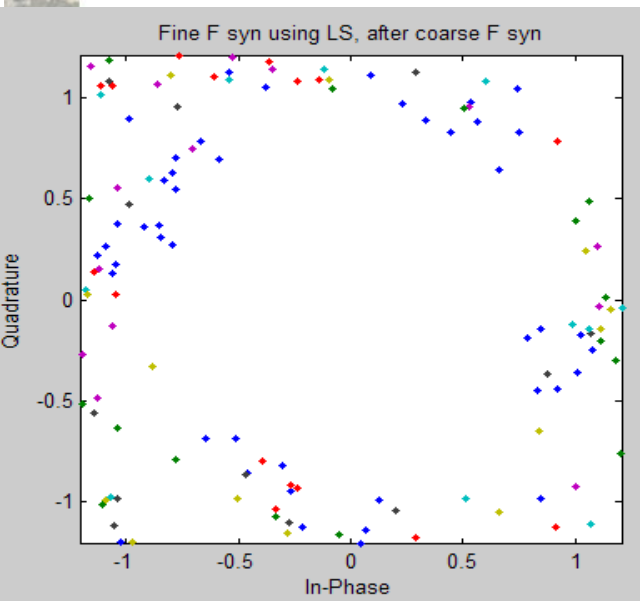
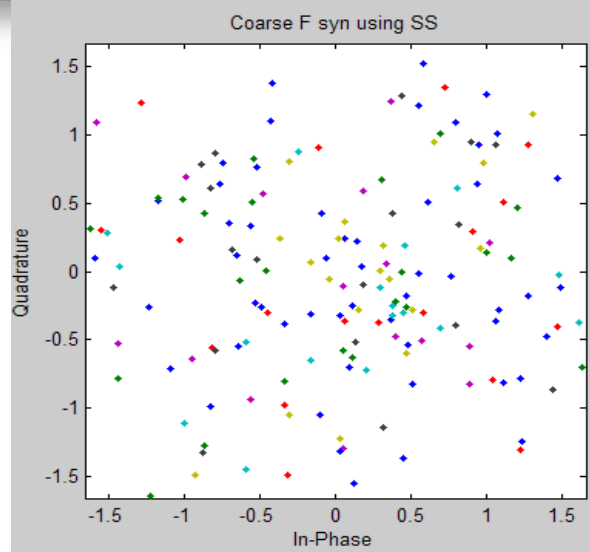
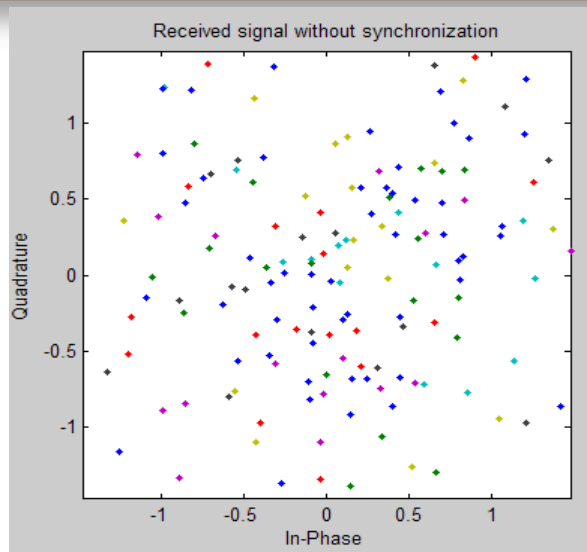


802.11a receiver waveform





802.11a receiver synchronization

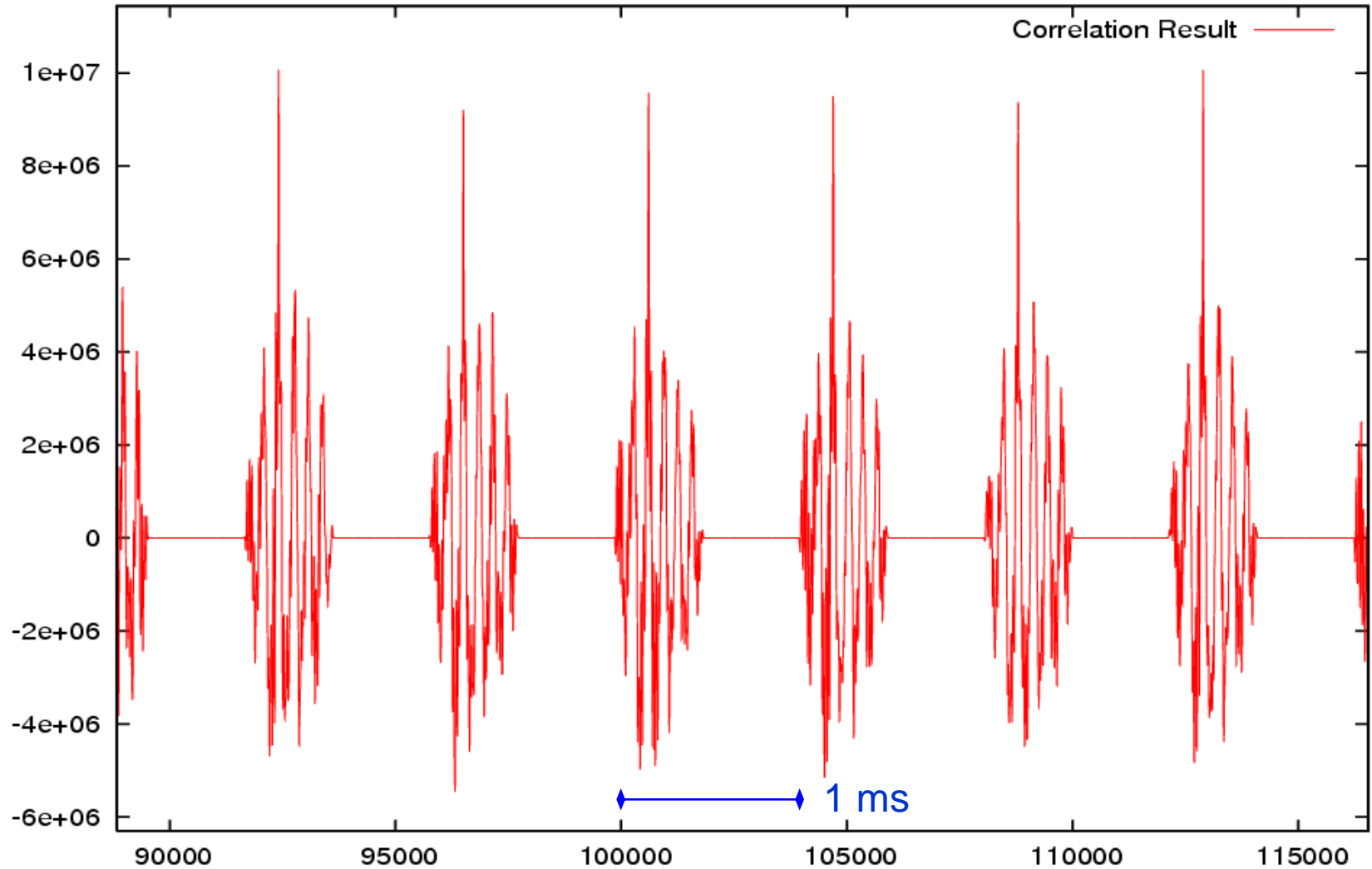


2009.10.15

Software Defined Radios for Cyberspace Operations by Frank Krahn

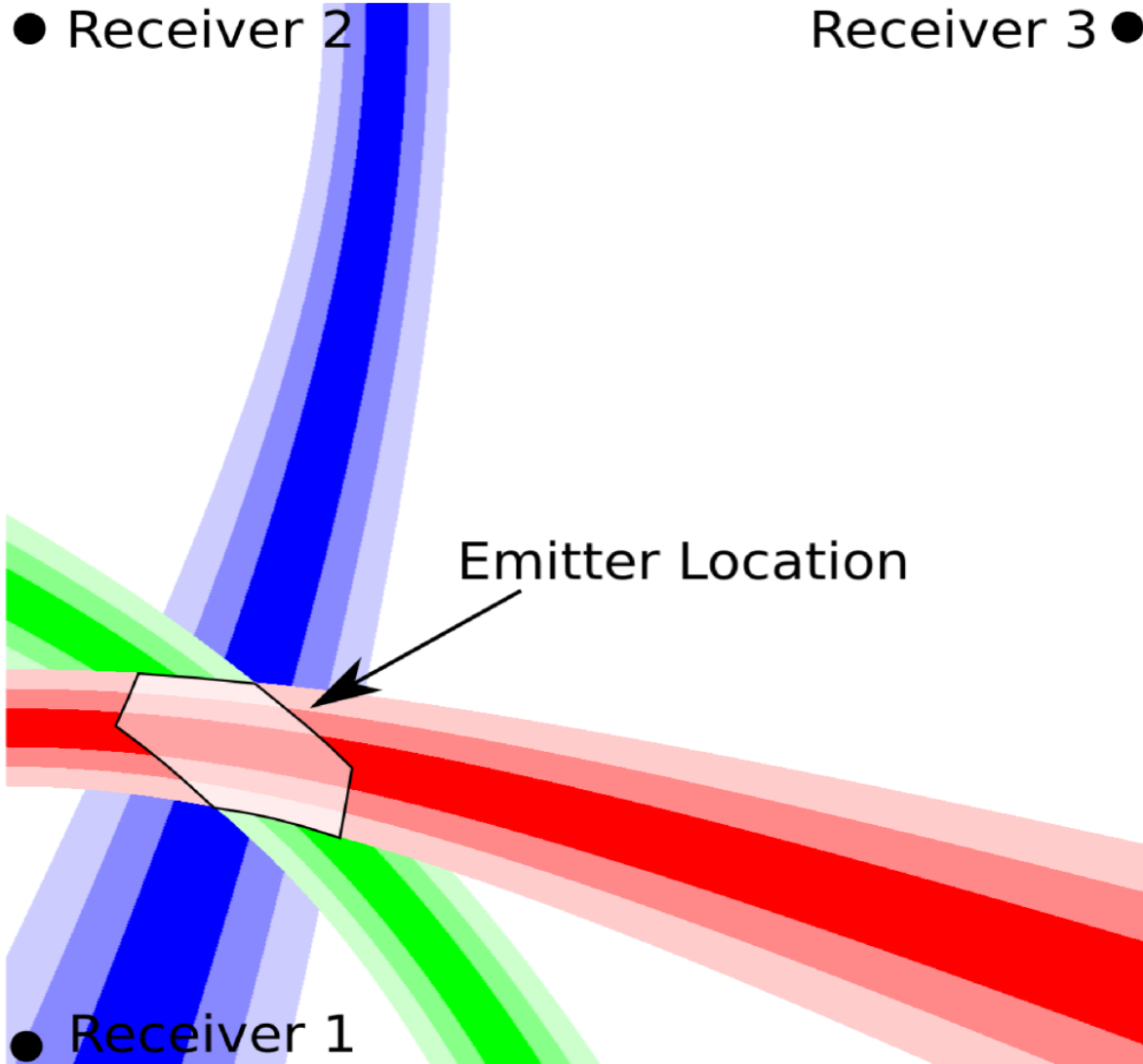


GSM Correlation Result





Simulation – GSM mobile phone location





SIGINT Applications of Software Defined & Cognitive Radio Technology (SASDCRT) Conference



- Hosted by NPS
- TS/SCI
- September 2006&2007
- two days
- ~40 presentations
- government, industry and academia represented
- rolling this into Classified Advanced Technology Update (CATU) for 2010

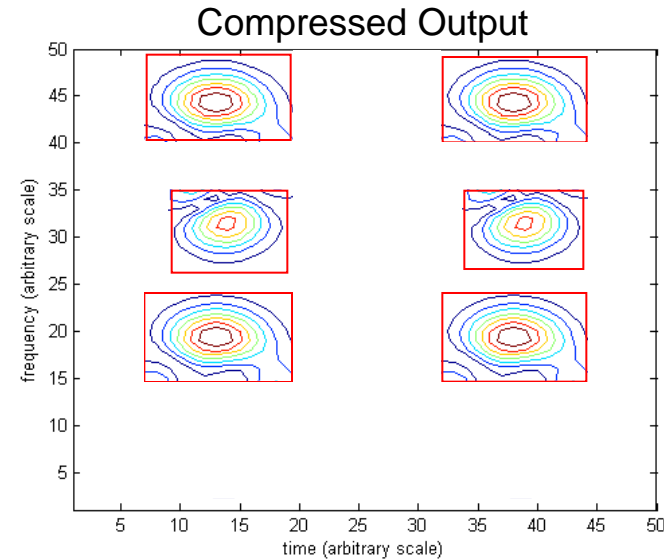
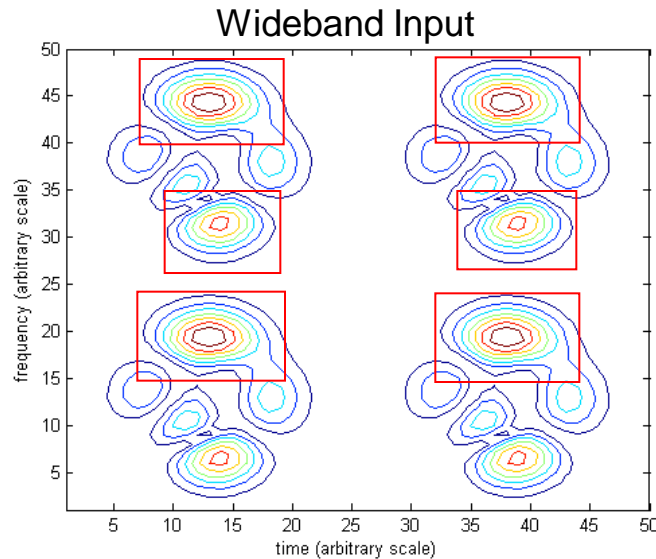


- Why SDRs are important to cyberspace operations.
- Past NPS research in SDR
- **Current NPS research in SDR**
- Looking ahead: Possibilities for future NPS research in SDR



- FPGAs are software definable hardware signal processors
 - allows for faster processing of more complex signals
 - FPGAs contain programmable logic blocks, and a hierarchy of reconfigurable interconnects.
- *Design for fault tolerant FPGA-based SDR*
- *Design of FPGA-based transceiver for 802.16 signaling.*

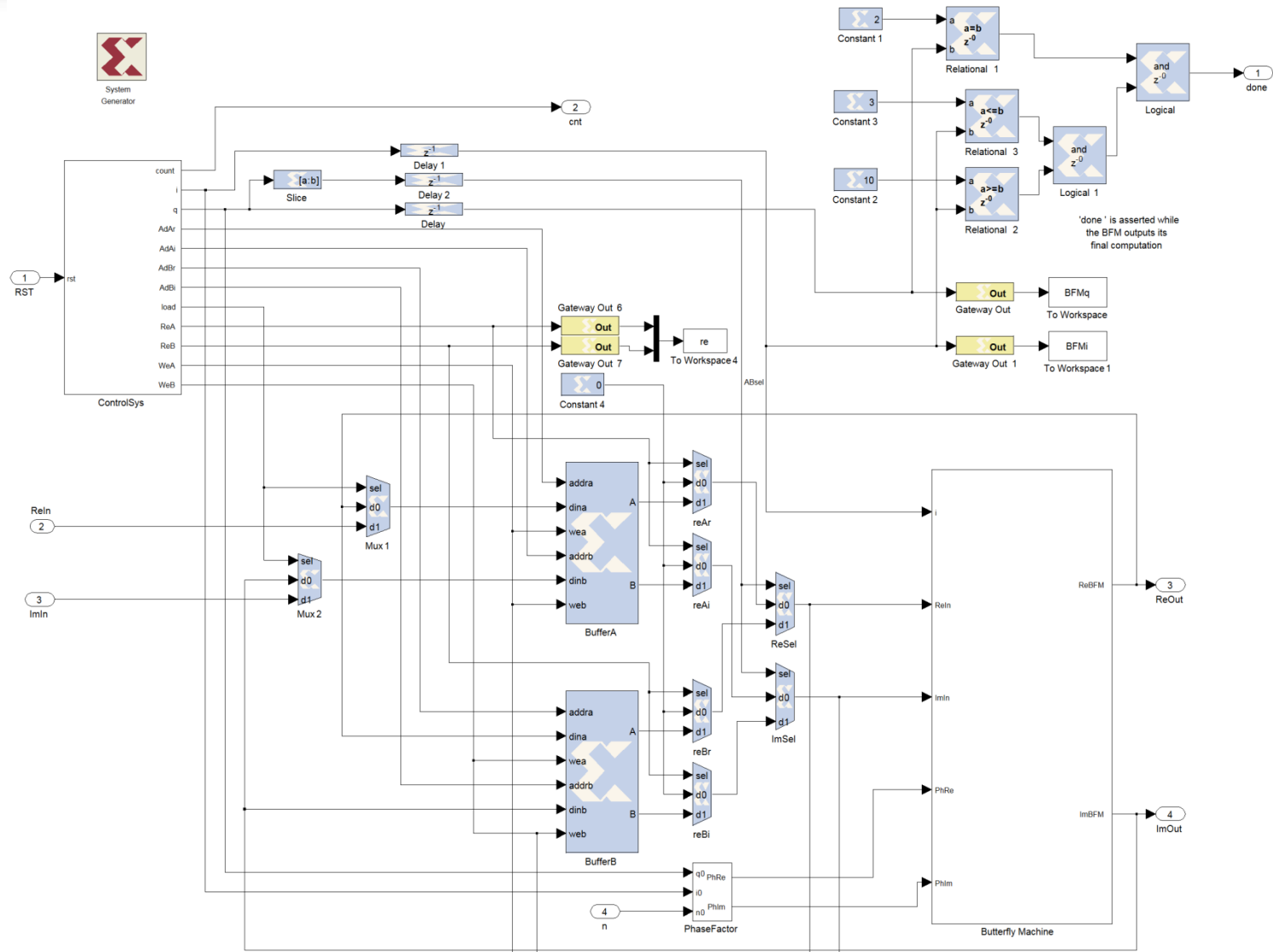




- Input RF energy distributed in time and frequency
- Operator determines “high energy” thresholds for various portions of the time-frequency distribution
- Maximize utility of the output bandwidth
 - Only pass high energy components to output channel
 - Filter noise, interferers, and signals known to be insignificant



Cooley – Tukey FFT Algorithm





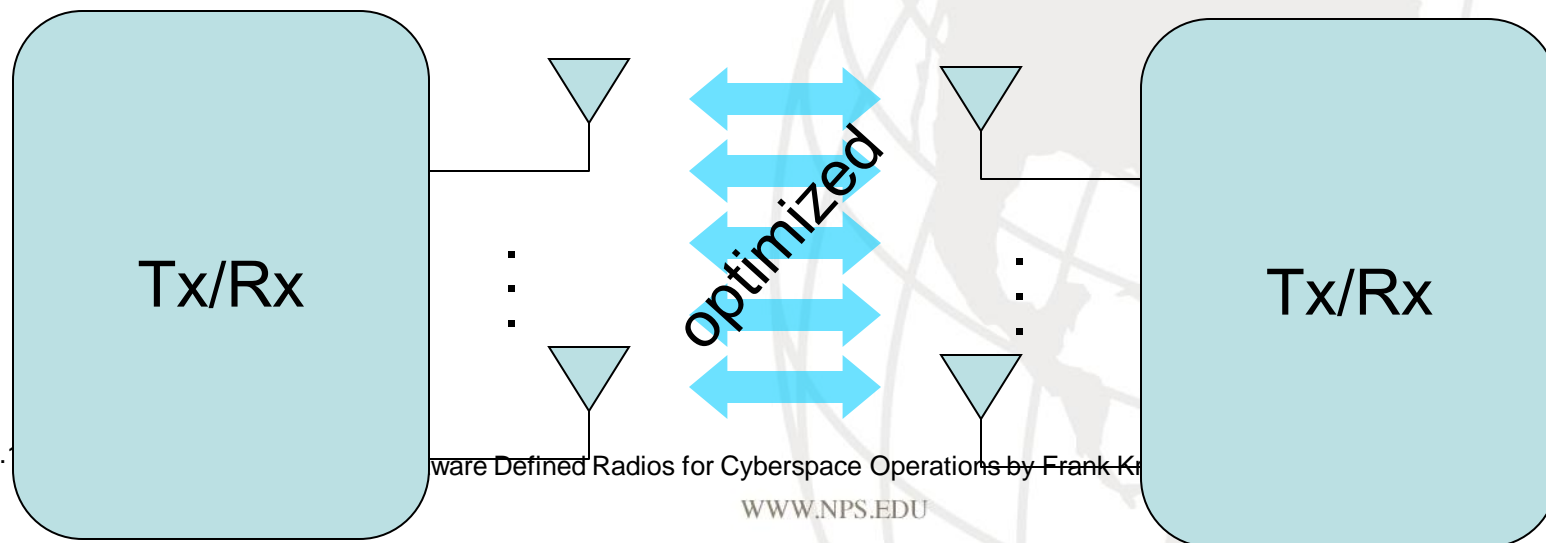
- Why SDRs are important to cyberspace operations.
- Past NPS research in SDR
- Current NPS research in SDR
- **Looking ahead: Possibilities for future NPS research in SDR**



- To an unprecedented degree, most of 4G will converge on two physical layer technologies,
- Multiple input multiple output (MIMO) systems involve encoding information over multiple transmit antennas and receiving them at multiple receive antennas
- Orthogonal Frequency Division Multiplexing (OFDM) uses many densely packed subcarriers
- These technologies are winners (often used together) because they offer high data rates and robustness to channel fades,
 - can trade between high data rates and robustness to adapt to current channel conditions

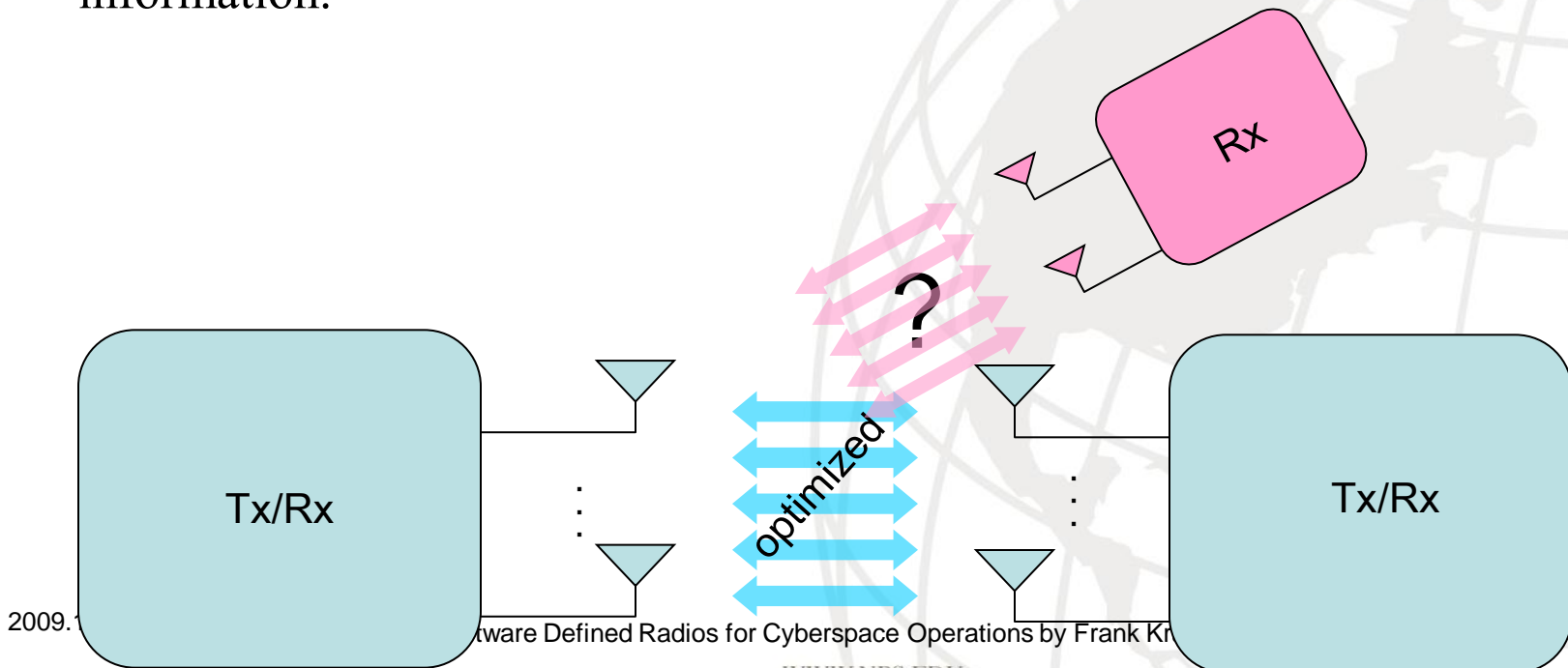
MIMO is the challenge to us

- In MIMO, the **receiver measures** the strength of the $N_{tx} \times N_{rx}$ SISO **channels** and feeds this information back to the transmitter. The **transmitter then encodes** the information such that more information is carried on the stronger SISO channels and less on the weaker SISO channels.
- The result is a transmission optimized for the intended receiver's current location



MIMO is the challenge to us

- Problem: Unintended receiver does not have this cooperation from the transmitter. This implies information encoding not well suited for channel conditions and more interference between the N_{tx} transmitted signals.
- **More gain does not solve the problem. This is very unlike past challenges.**
- Solution: Unintended receiver can measure its channel conditions and partially compensate. More advanced (but more computationally complex) receiver algorithms may be sufficient to demodulate and decode the information.





+

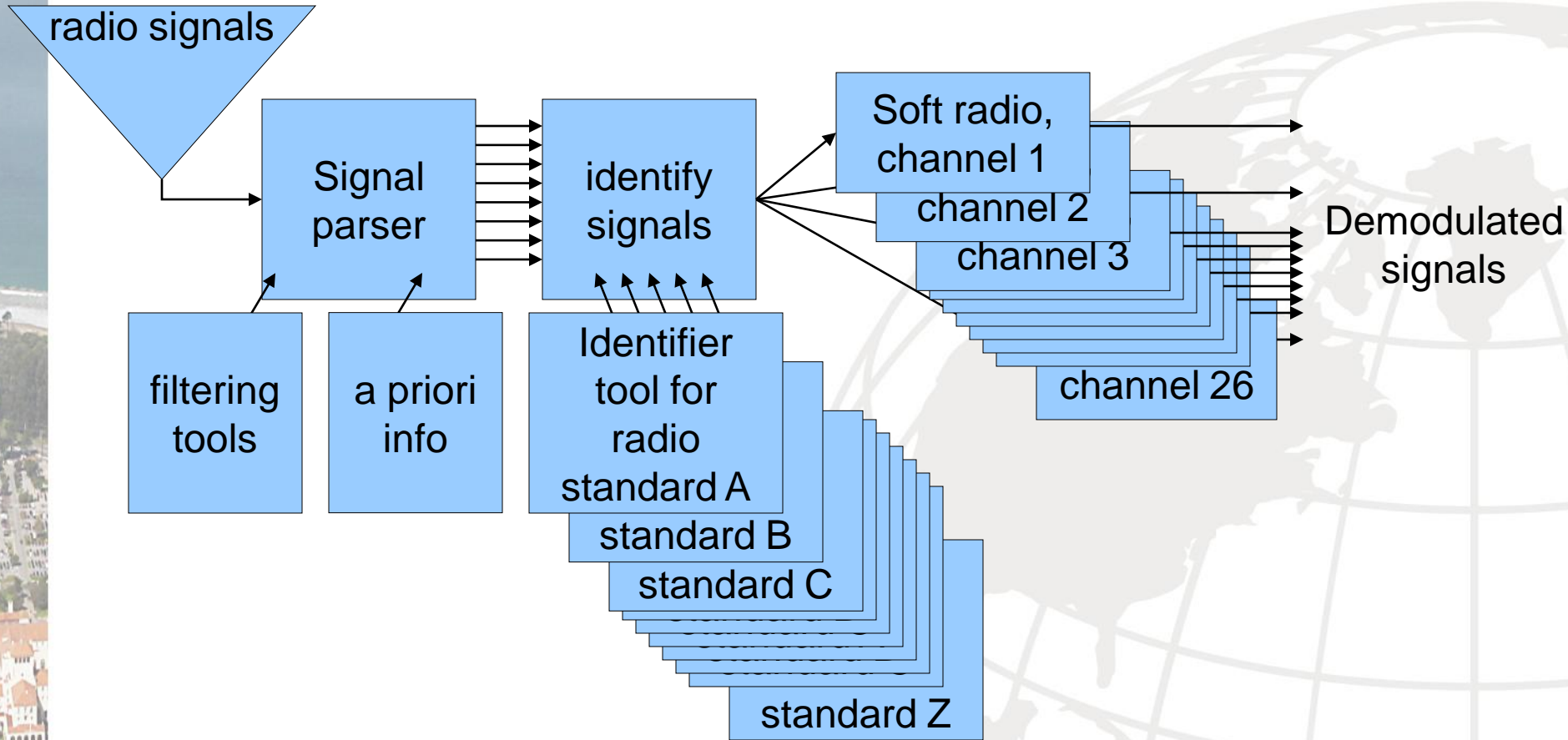


cognitive radios

- Cognitive radios are SDRs that adapt to communicate more effectively. The transmitter and receiver sense their environment, past usage, perhaps location, etc. and modify the transmission and reception parameters accordingly.
- Example: IEEE 802.22 is the standard for Wireless Regional Area Networks (WRANs)
 - will use white spaces in the TV frequency spectrum.
 - WRAN radios will be CRs that operate in the TV broadcast bands while assuring that no harmful interference is caused to any TV broadcasting (by sensing, analyzing, and predicting)
- Most of the current research in cognitive radios focuses on cognitive transmitters.



Vision: Cognitive Receiver



Automated reception capabilities.



- Puts collection into a scalable and automated architecture.
 - Good software engineering discipline required (i.e. a good architecture).
 - Automation mitigates information overload.
- Can Incorporate signal “value” information
 - can prioritize signals



NAVAL
POSTGRADUATE
SCHOOL

discussion?



Monterey, California

WWW.NPS.EDU



NAVAL
POSTGRADUATE
SCHOOL

backup slides

Monterey, California

WWW.NPS.EDU

- “Software communications architecture (SCA) compliant software defined radio design for IEEE 802.16 wirelessMAN-OFDM™ transceiver”
 - By Major John Low, Singapore Air Force
- design of transmitter and receiver 802.16 waveforms (single mode operation)





- Software defined radio design for synchronization of an IEEE 802.11a receiver
- LCDR Juan SanFuentes, Chilean Navy
- Built upon much of the work in
 - “Extending the range of the IEEE 802.11g WLAN through improved synchronization techniques” by LCDR Vikram Sardana, USN



- “Software defined radio design for an IEEE 802.11a transceiver using open source software communications architecture (SCA) implementation:: embedded (OSSIE)”
 - By Major Chris Leong, Singapore Air Force
- design of transmitter and receiver 802.11a waveforms





- Software Defined Radio Design for a GSM Receiver
- geolocation of GSM transmitter
- Tools
 - GNU Radio and
 - Universal Software Radio Peripheral
- LT Ian Larsen, USN





- “Software communications architecture (SCA) compliant software radio design for interim standard 95B (IS-95B) transceiver”
 - By LT Rami Ramdat, USN
- Design of IS95B transmitter and receiver waveforms





- Receive and process wideband RF signals
- Compress IF signals and preserve relevant information
- Driven by remotely parameterized criteria
- Automated output (Parameters & Signal Properties)
- Interface with existing systems



- Why SDRs are important to cyberspace operations.
- Past NPS research in SDR
- Current NPS research in SDR
- Looking ahead: Possibilities for future NPS research in SDR
- **SDR in the NPS curriculum**



NPS Curriculum includes SDR

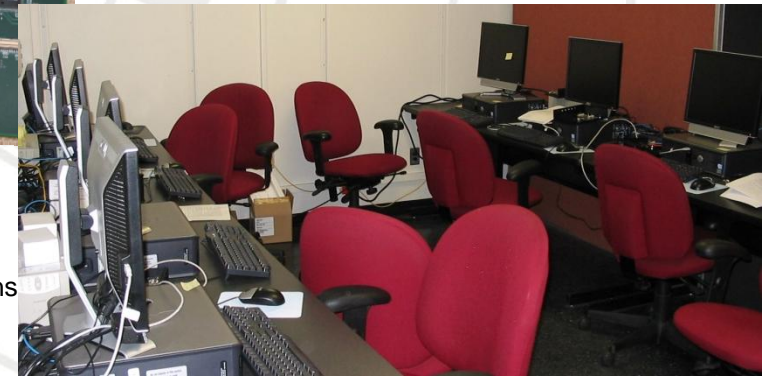
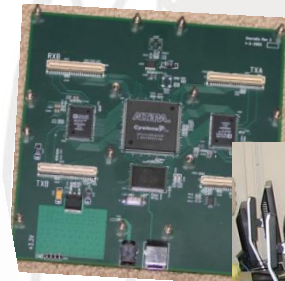
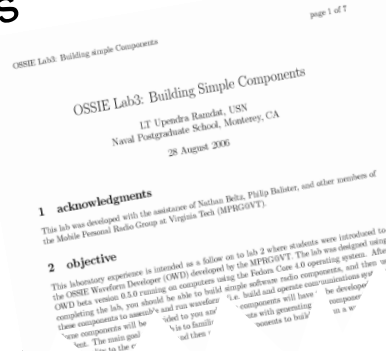
EC4530 Soft Radio (3-2) Summer

An introduction to soft radios, devices that generate (transmitter) and/or process (receiver) digital communications signals in software and in reconfigurable hardware. The course covers basic radio frequency (RF) design principles, soft radio architectures, analysis of receiver operation, and existing soft radio efforts. Prerequisite: EC3510 or consent of instructor.

Emphasis on DoD relevant engineering aspects including JTRS JPEO's Software Communications Architecture

designing SCA-compliant SDRs in projects

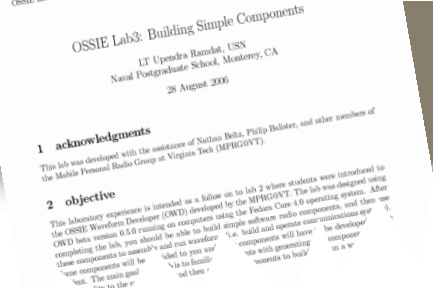
Building SCA-compliant AM radio receiver in labs



2009.10.15



- (1) RF front end (hardware) issues: dynamic range, RF components, noise, transmitter architectures, distortion
- (2) Multi-rate signal processing: decimation, interpolation, filtering, timing recovery
- (3) Generation of signals using digital hardware: direct digital synthesis (DDS), spurious signals, jitter, bandpass signal generation, performance of DDS systems
- (4) Analog to digital and digital to analog conversion: ideal vs. practical data converters, architectures
- (5) Relevant digital hardware: DSP hardware, FPGAs, ASICs, power management
- (6) Software Communications Architecture (SCA) and Object-oriented representations: networks, object-oriented programming, classes, inheritance, object brokers, standardized application programming interfaces (APIs), Common Object Broker Request Architecture (CORBA),
- (7) Case study: Joint Tactical Radio System (JTRS) and/or Digital Modular Radio (DMR).



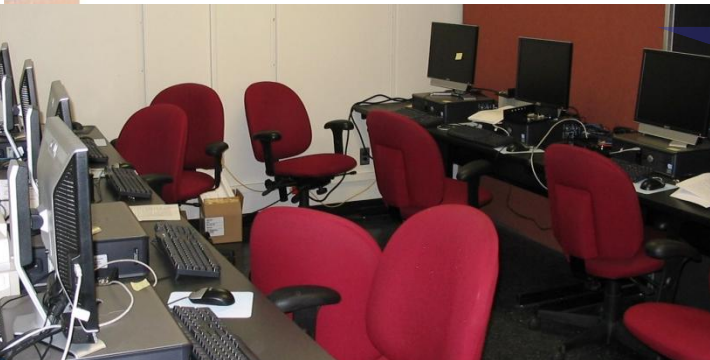
I. SCA Design tool Introduction.
Assemble & run first waveform

II. Modifying properties for a QPSK waveform

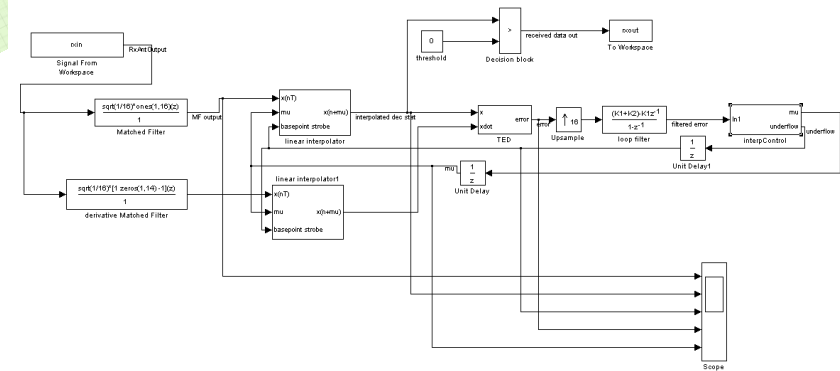
III. Designing components.
Designing a waveform

IV. Interfacing with hardware

V. Build an SCA-compliant AM SDR



- Analysis
- Simulation
- Design

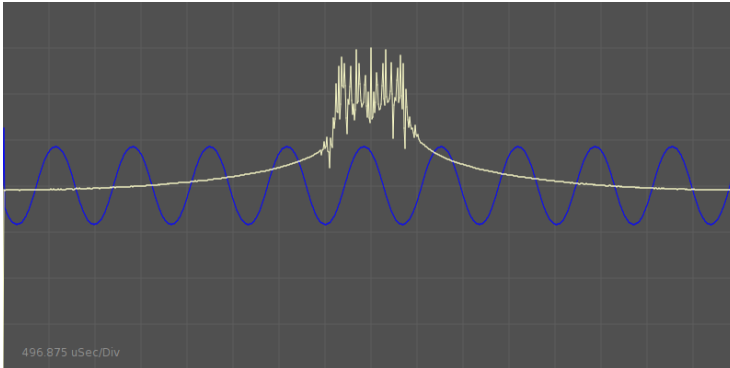


```

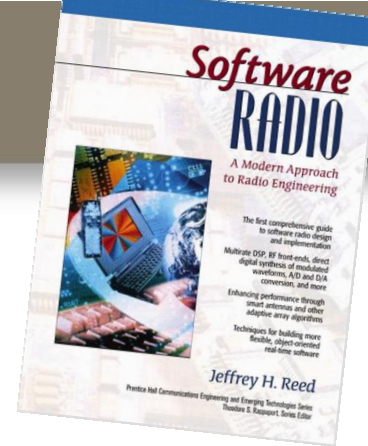
36
37
38 // Form the line for m_list
39     ina.S_un.S_addr = pipHeader->sourceIP;
40     pSource = inet_ntoa(ina);
41     strcpy(szSource, pSource);
42     ina.S_un.S_addr = pipHeader->destIP;
43     pDest = inet_ntoa(ina);
44     strcpy(szDest, pDest);
45     CString str;
46     if(pipHeader->sourceIP == (pDig->m_ipcheckedhost)
47         str.Format("%s > %s len = %d ttl=%d",
48             ilen, pipHeader->ttl, get_proto_name(
49             else
50             str.Format("%s < %s len = %d ttl=%d",
51             ilen, pipHeader->ttl, get_proto_name(
52             pDig->m_list.AddString(str);
53     )

```





- Oscilloscope & spectrum analyzer
 - C++, gnu, USRP
- Oscilloscope & spectrum analyzer
 - OSSIE, USRP
- FM receiver
 - OSSIE, USRP
- QPSK transceiver
 - OSSIE, USRP



- Lectures
 - Help from Jeff Reed of VT
- Labs
 - Labs started at NPS
 - Help from Donna Miller, Rami Ramdat, Juan SanFuentes, and Nathan Beltz of NPS
 - Labs shared with VT
 - Updated and extended by Jeff Reed, Carl Dietrich, and VT OSSIE team
- Tutorial
 - Carl Dietrich and Donna Miller
 - at VT Wireless Symposium
 - 2007, '08, '09
 - at SDR Forum
 - '07, '08, '09 (come see us in DC in December)
- Papers
 - “Open-Source SCA-Based Core Framework and Rapid Development Tools Enable Software-Defined Radio Education and Research”, by Carlos R. Aguayo Gonzalez, Carl B. Dietrich, Frank E. Kragh, Shereef Sayed, Haris I. Volos, Joseph D. Gaeddert, P. Max Robert, and Jeffrey H. Reed, *IEEE Communications Magazine*, October 2009.
 - F. Kragh, J. Reed, C. Dietrich, and D. Miller, “Education in Software Defined Radio Design Engineering”, *Proceedings of the American Society for Engineering Education Conference 2008*, June 2008.



A key aspect to exploiting the enemy's use of cyberspace is to detect, locate, and intercept his communications in cyberspace. The wireless portion of cyberspace offers an excellent opportunity to do this. Software defined radio (SDR) technology allows us to field multimode receivers that are scalable, software updatable, flexible, and maintainable. The Naval Postgraduate School has conducted substantial research in software defined radio, to include the design of SDRs for interception of some of today's common wireless transmissions, geolocation of emitters, and automatic parsing of overlapping signals. Future research efforts will address emerging wireless technologies that pose tough new challenges to detection, location, and interception of radio signals.



- importance of wireless to cyberspace operations
- what is a SDR?
- past
 - waveforms developed
 - geolocation techniques developed
 - FPGA based SDRs. DSP & microprocessor based SDRs
 - SASDCRT
- future
 - The 4G challenge, more advanced receivers
 - cognitive radios
 - cognitive sigint receiver
- Lab and curriculum