2013 DHS S&T/DoD ASD (R&E)
CYBER SECURITY SBIR WORKSHOP

ASYNCHRONOUS NETWORK SIGNAL SENSING & AUTOMATED MODULATION CLASSIFICATION TECHNIQUES

ANDRO Computational Solutions, LLC
Andrew L. Drozd

23-24 July 2013

Homeland Security
Science and Technology

Asynchronous Network Signal Sensing & Automated Modulation Classification

- Andrew L. Drozd, President & Chief Scientist

- ANDRO Computational Solutions, LLC
  The Beeches Professional Campus
  One Beeches Place, Suite 2
  7980 Turin Road
  Rome, NY 13440-1998
  Email: *adrozd@androcs.com*
  (315) 334-1163, x1# (phone)
  (315) 334-1397 (fax)
  Web Site: *http://www.androcs.com*

Company Profile

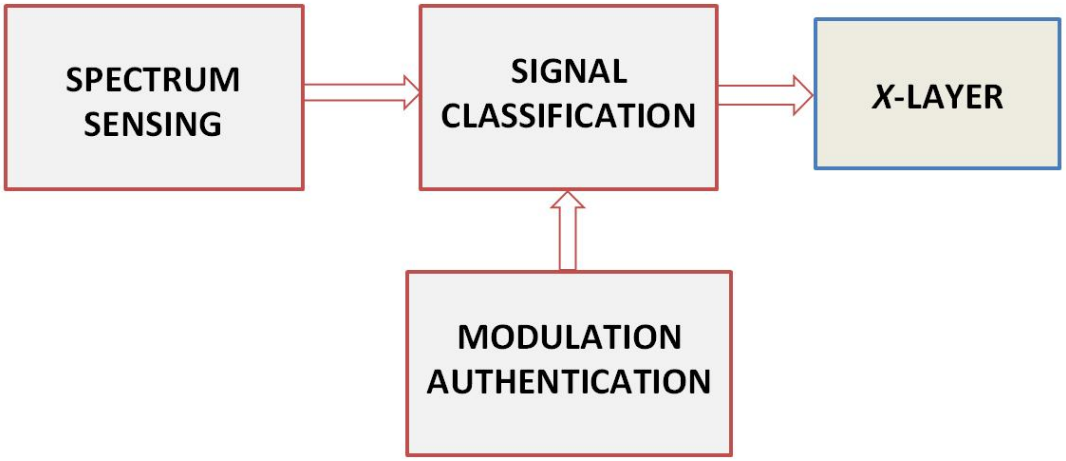
- *For profit* Small Business established 1994
  - ~20 staff at several locations (Rome/Syracuse, NY, Dayton, OH)
- Engineering R&D/core expertise
  - Software systems development and experimental hardware
    - Wireless security & cyber-domain spectrum exploitation
    - Cognitive radio networks
    - EM spectrum management & dynamic spectrum access
    - Electromagnetic environment effects (E^3) on large systems
    - Multisensor resource management and information fusion
- Tech staff with advanced degrees in EE, physics, math
- Nationally recognized expertise via IEEE (standards)
- Multiple university and industry partnerships

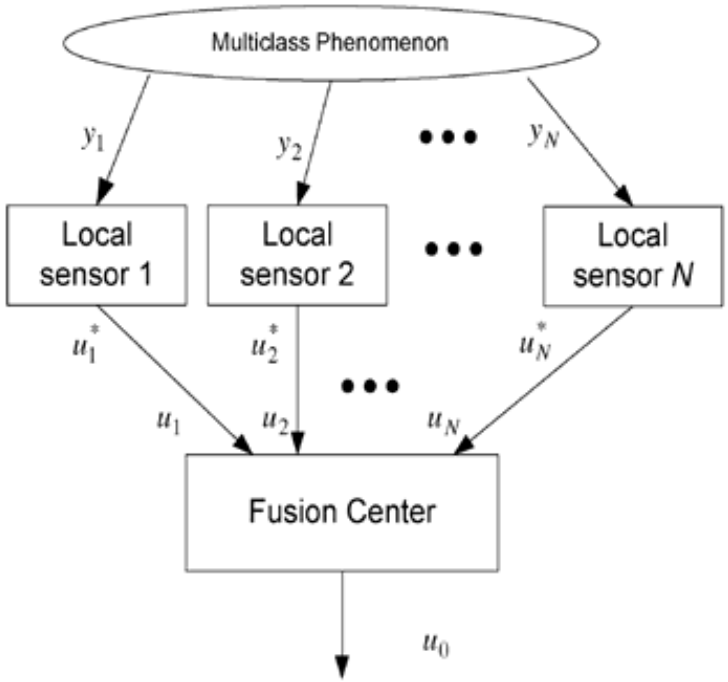
Customer Need – "Radio Mapping" for Assured Secure Comms Nets

- The problem -- non-cooperative transmission environment:
  - Multi-cast signals may emanate from both friendly and hostile sources.
  - RF interceptors sense/extract weak signals then blindly classify them.
  - Hostile wireless comms devices (eavesdroppers, infiltrators, exfiltrators, etc.) can transmit at low power to avoid detection and conduct cyber attack:
    - Covertly change their transmitting frequency
    - Modify modulation format on-the-fly
    - Blind the network and/or exfiltrate data.
- Our solution supports legacy receivers and SDR nets for SIGINT:
  - Leverage new/existing wireless sensor networks to achieve a technological breakthrough in signal sensing and AMC of weak signals not detectable via traditional single sensor methods to ID/classify malicious users, etc.
  - Link multiple sensors to a master FC and enhance ability for AMC under low SNR regimes as well as eliminate channel distortion.
  - Centralized and distributed data fusion techniques employed.

Approach

Physical Layer Robust Signal Sensing and Classification





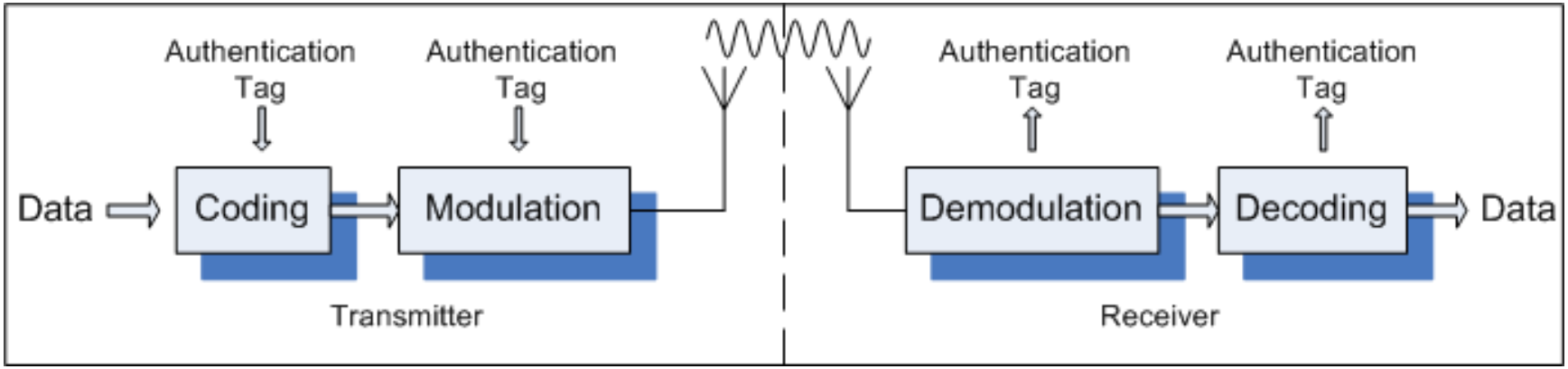
- Data fusion performed using input from N distributed sensors each observing the same signal received through different fading and noisy channels ($y_1 \ldots y_N$).

Modulation Authentication

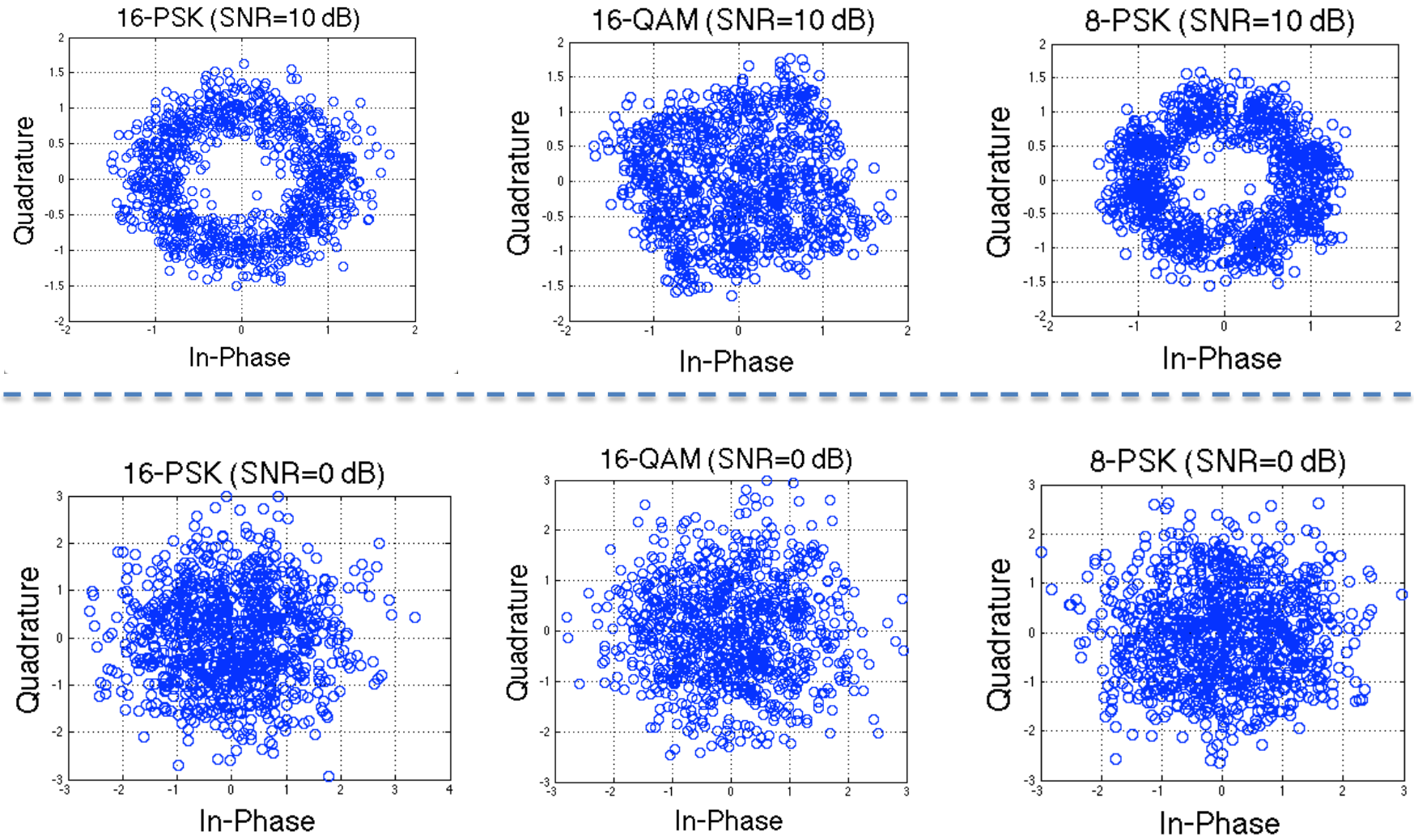
- PHY Layer Authentication
  - Requirements
    - Transparent to existing users
    - Conducted at the PHY layer with low overhead penalties (efficient and extra layer of robustness)
    - Based on well established crypto primitives and authentication tagging schemes.
  - Applications
    - Primary user’s signal can be proven authentic
    - Illegal use of spectrum can be detected.

Modulation Authentication

- We have a novel authentication schemes based on digital modulation
  - **Objective:** detect whether spectrum user legitimately owns the spectrum.
  - **Approach:** sender embeds an authentication tag in the signals with additive noise that improves security performance.



Robust Signal Classification: Linear Modulation Constellations – Signal Space Representations

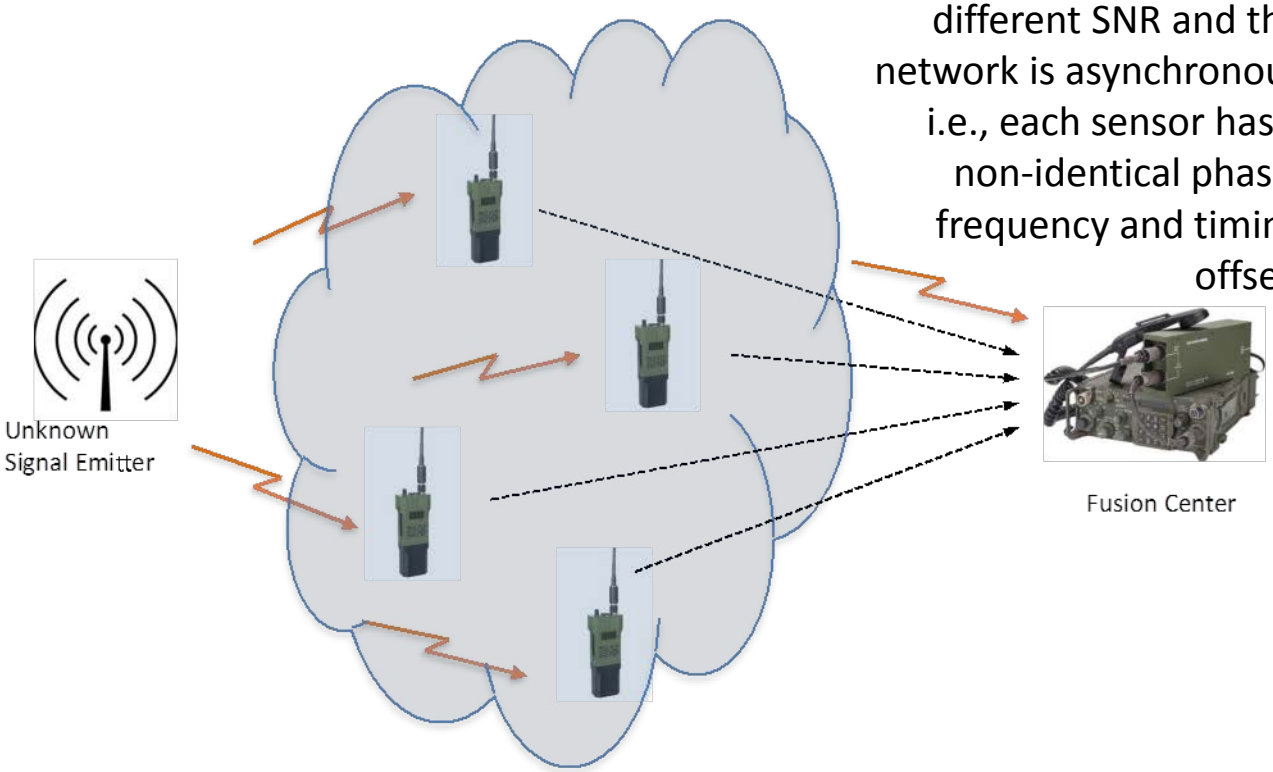


Data Fusion for AMC (*Foreign Network Discovery*)

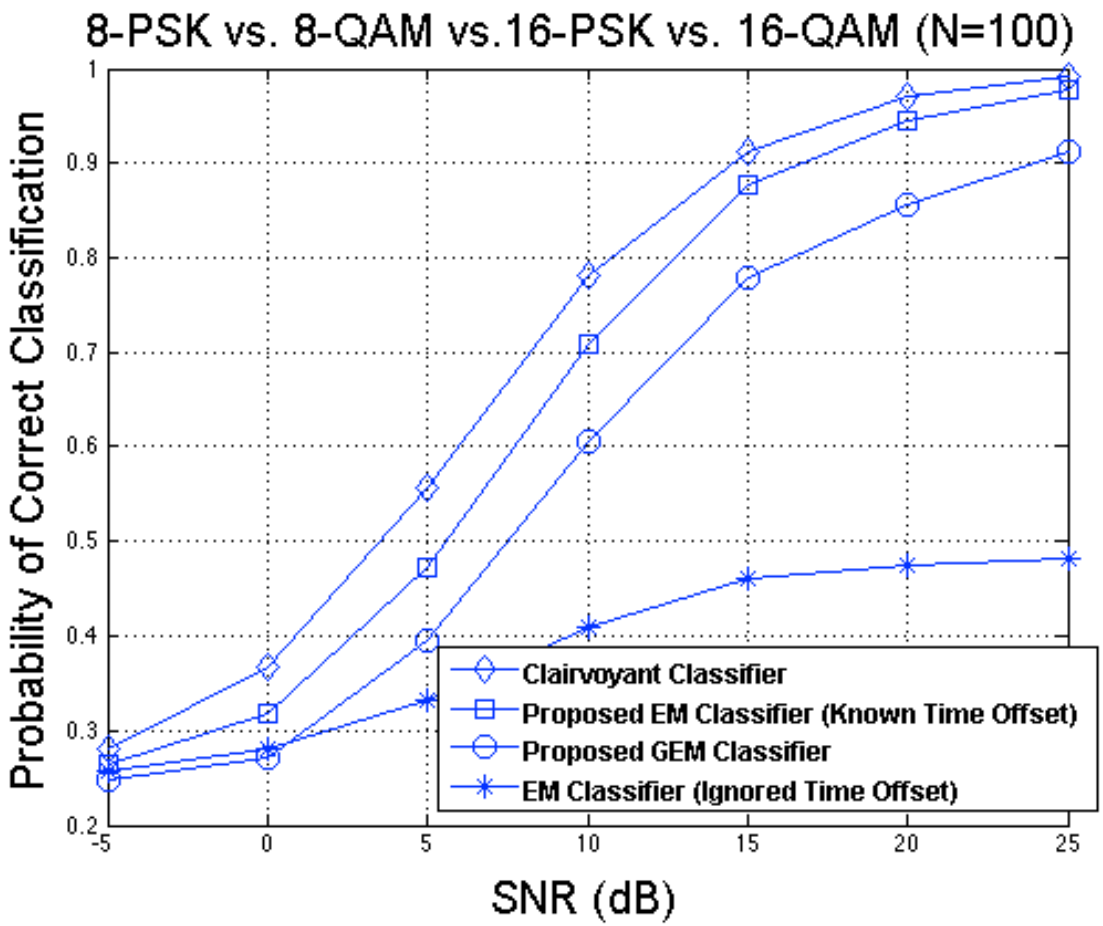
- We apply (probabilistic) data fusion with spatially distributed sensors to improve classification performance for weak signals in a multi-cast environment.

- 802.11/16 wireless network
- AIS
- Low bandwidth link
- Cellular; e.g., LTE network
- Military comms system
- Other (inexpensive receiver with spurious emissions)
  - ✓Eavesdropper
  - ✓Exfiltrator

Each sensor experiences a different SNR and the network is asynchronous i.e., each sensor has a non-identical phase, frequency and timing offset.



Numerical Results (1 of 2)

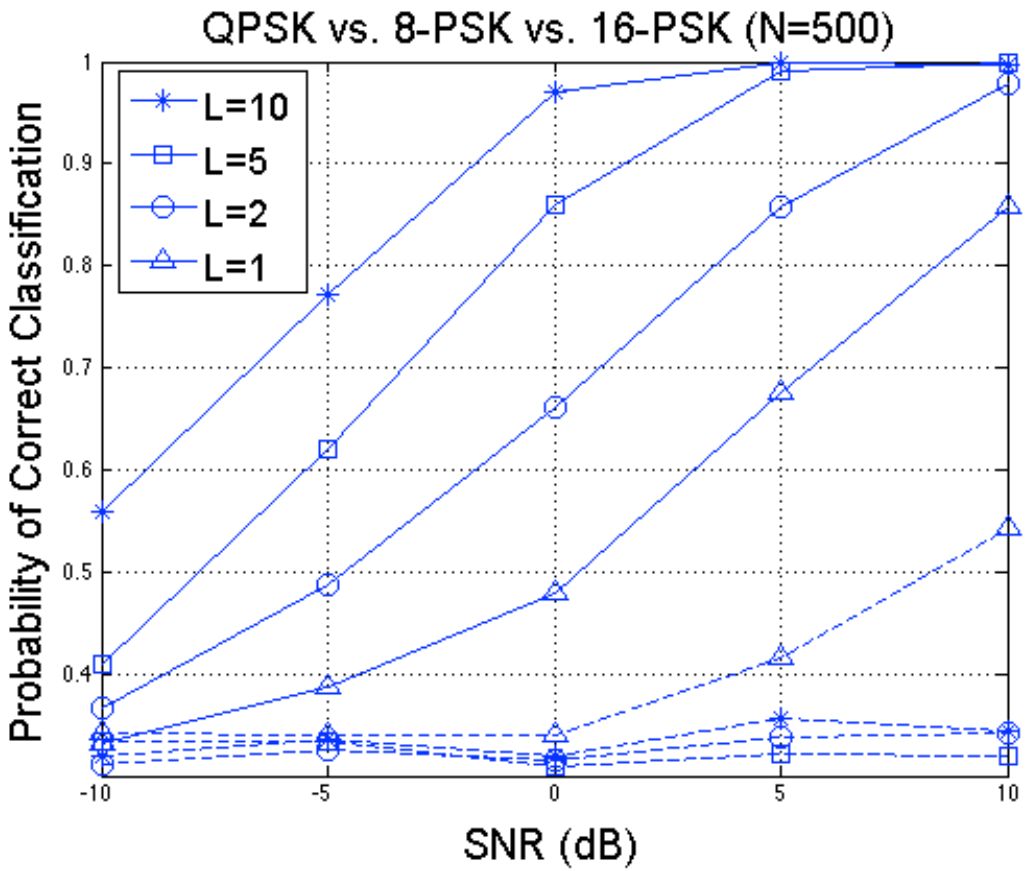


Our Proposed Approach: Maximum likelihood (**ML**) modulation classification using Expectation Maximization (**EM**)

Method of Moments Estimators require ~N=10^4 samples for acceptable performance*

* W. C. Headley and C. R. C. M. da Silva, "Asynchronous classification of digital amplitude-phase modulations in flat-fading channels," *IEEE Trans. Commun.*, vol. 59, no. 1, pp. 7–12, Jan. 2011.

Numerical Results (2 of 2)



Solid Lines: Proposed Approach

Dashed Lines: Method of Moments Estimators*

* F. Hameed, O. A. Dobre, and D. C. Popescu, "On the likelihood-based approach to modulation classification," *IEEE Trans. Wireless Commun.*, vol. 8, no. 12, pp. 5884–5892, Dec. 2009.

AMC for *Foreign Network Discovery*

- Designed to identify, recognize and discriminate within these network types:
  - IEEE standard 802.11/16 wireless networks
  - Automatic Identification System (AIS)
  - Low bandwidth links
  - SATCOM and/or cellular; e.g. Long Term Evolution (LTE) networks
  - Military communications systems (e.g., JTRS networks).
- Prototype algorithms are being developed, tested and will be expanded to recognize and determine friend or foe.
- Goal: localize and isolate foreign networks (~100% with minimal false alarms).
- Applicable to *cross-layer* wireless networks and employs multi-level security (MLS) approaches.

Benefits

- New AMC data fusion techniques expected to provide a min 10-fold improvement in performance under low SNR regimes to deny cyber attackers.
  - ~3 dB improvement w/10 sensors compared to single sensor
  - Additional improvement approaching → two-orders of magnitude when soft decision fusion or centralized data fusion approaches are used.
- Supports networks legacy radio receivers and SDRs for SIGINT apps.
- Enables commercial and public safety applications where opportunistic SDRs use dynamic spectrum access techniques to access the spectrum non-coop.
- Potential adopters include military radio-sensor providers.
- Supports multiple DoD programs:
  - Army: PM Prophet, PM Signals Warfare
  - Air Force: KESTREL system from AFRL's PROFORMA SIGDEV program.

Current Status

- Accomplishments
  - Significant results for multiple receivers (sensors, RF comms) using centralized fusion processes demonstrated.
  - Formulated ML-based centralized fusion scheme.
  - Formulated distributed decision fusion scheme (hard & soft decision fusion) and derived generalized rule for optimal multi-hypothesis classification.
  - Derived upper/lower bounds for probability of modulation classification error and used Monte Carlo sampling since closed form solutions are intractable.
- In process
  - Research to refine algorithms is continuing
  - Defining a dictionary for *template matching*
  - Experiments to test performance using USRP2/GNU radio suites

Next Steps

- We are working with potential radio-sensor hardware transition partners to insert AMC technologies and perform field tests.
- We are coordinating with Army Tech Transition Advocate (TAA) to identify PoR sponsorships for Commercialization Readiness Program (CRP) and follow-on funding.
- We are seeking to identify additional sponsorships and opportunities for extending and fielding the AMC technologies for military, federal and public sector applications.

Additional Contact Information

- Carmen Luvera, Director of Business Development

  cluvera@androcs.com

  (315) 723-5373 (mobile)
- Rick Lawrence, Assistant Dir. of Business Development / Technology Transition Specialist

  rlawrence@androcs.com

  (315) 726-1219 (mobile)
- Irina Kasperovich, CTO

  ikasperovich@androcs.com

  (315) 334-1163 (office)