

IAI Capabilities for IARPA SCISRS



Intelligent Automation, Inc. (IAI)
15400 Calhoun Drive, Suite 190
Rockville, MD 20855

Contact: Edward Colbert ecolbert@i-a-i.com 301-294-4763

1. Company Overview

Intelligent Automation, Incorporated (IAI), a research organization of over 240 scientists and engineers, brings to this effort extensive expertise in RF and wireless signals analysis using both classical signal-processing and AI-based approaches. Our company is headquartered in Rockville, Maryland and conducts the majority of its work with the US government. We have been listed as a top 5 small federal R&D business for the last 10 years. We have over 60,000 sq. ft of state-of-the-art facilities including cleared spaces, R&D labs, and product manufacturing facilities. We have a TS facility clearance.

IAI has successfully conducted a large number of SBIR, STTR and BAA projects in which we developed intelligent algorithms for RF signal processing and characterization. Customers include: Army, AFRL, DARPA, AFLCMC, DCERDEC, ARL, and ONR. IAI has developed machine learning-based signal localization, waveform classification, protocol identification, and authentication techniques, and implemented them on embedded platforms and regularly analyzes complex RF signals in our Rockville MD labs for algorithm and sensor development. IAI also has extensive expertise developing customized SDR platforms with a variety of form factors. Additional detail on our analytic capabilities is provided later in this document.

Many of the innovative algorithms that we have developed are instantiated in R&D products (see <https://www.i-a-i.com/products-and-services>), which are sold commercially, or further customized for special applications. Of particular relevance to IARPA SCISRS is our DeepRadio platform (see Figure 1), which is a stand-alone deep learning-based MIMO SDR for signal detection, waveform classification, and protocol identification. It utilizes FPGA implementations of AI-based deep neural-network algorithms and provides low-latency and low-



Figure 1: Deep Radio Platform with Smartphone Application as a User Interface.

power spectrum operation for RF spectrum characterization, to include standard OFDM, 5G, and custom modulated waveforms. DeepRadio provides configurable deployment of the full network protocol stack for effective interference management, spectrum adaptation, high data rate communications, and general signal-processing analytics of RF signals using on-board ARM Linux software tools.

Our wireless RadioLab facility (shown in Figure 2) in Rockville MD is well suited for RF signal experimentation using a wide variety of SDR types. We utilize IAI's RFnest™ network channel emulator (shown in Figure 3), which provides a repeatable, controllable, and scalable test wireless network environment, allowing a full mesh of RF signals to be emulated with realistic channels effects for signal processing, detection and characterization. RFnest currently operates in the 0-15 GHz range, with 40 GHz option, and has an IBW of 450MHz (upgradable to 2GHz). RFnest allows development of new wireless network technologies that are at the test and evaluation phase without the need for a lengthy frequency allocation process. It is an ideal tool for the testing of emerging technologies using cognitive and SDRs which are otherwise difficult to test due to regulatory issues. Environmental effects (including antenna directionality) experienced by transmitted RF signals are emulated, allowing high fidelity T&E in a lab environment, thus reducing development cost and time.

2. Analytic Capabilities

IAI has significant experience in original research and practical laboratory experimentation in detection and characterization of all of the signal types for the SCISRS program: standard overt RF signals, anomalous RF signals with LPI, RF signals mimicking standard overt signal types, altered overt RF signals carrying additional information, and unintended emissions from microprocessors and other electronics. Some publications from past work are listed at the end of this document and sample results are described below.

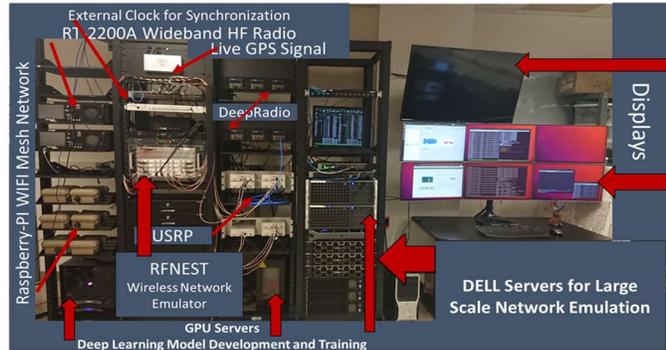


Figure 2: IAI RadioLab facility



Figure 3: RFnest Multi-use Channel Emulator

Overt Signals

Many IAI SBIR programs for tactical wireless networking have included development efforts for innovative deep-learning based RF signal localization, waveform classification, and protocol identification algorithms. Our capabilities can be summarized as:

- Machine learning and conventional estimation techniques for detection of 5G, LTE, WiFi, and other commercial and tactical waveforms;
- Detection and classification of emitters of RF signal through RF fingerprinting;
- Continual learning when signal types change over time (mitigating catastrophic forgetting);
- Hardware/Front end-agnostic implementation of ML/DL-based RF classifiers on FPGA, ARM and embedded GPU.

For example, in [10], we report on a general methodology we employ for utilizing deep neural network classifiers for overt signals (e.g. 5G, LTE, WiFi, and other commercial and tactical waveforms) that run directly on the FPGA fabric of an embedded SDR and classify signals through the RF front end in real time. Techniques using continual learning for deep learning algorithms further extend this capability by continuously updating deployed classifiers as the radios experience new waveforms. This capability is presented in [9] with impressive performance results. For interference-dominated cases where multiple signals overlap in time and frequency, performance of the deployed algorithms typically drop as classifiers are not trained for this condition. To address this realistic problem, we developed blind source separation techniques such as Independent Component Analysis and unsupervised learning approaches such that individual “cleaned” signals are input to the classifiers. IAI has demonstrated these innovative techniques for a variety of fixed and dynamically varying waveforms in wireless networks.

Anomalous (LPI, Mimicked, Altered) Signals

Anomalous transmissions cause serious issues for both statistical and deep learning algorithms. IAI has developed and applied several outlier detection algorithms from statistical methods such as Minimum Covariance Determinant and k-means clustering to semi-supervised or unsupervised learning algorithms that use neural networks to detect and characterize novel and anomalous waveforms. We summarize our capabilities related to anomalous signals as follows:

- Statistical (anomaly) detection of unknown signals for which there is no training data;
- Adversarial ML-based signal hiding below noise floor for LPI/LPD;
- Blind source separation to detect different signal types that may be superimposed due to interference from concurrent transmissions;
- Generation and detection of spoofed signals with generative adversarial networks;
- Generation and mitigation/detection of adversarial perturbations that aim to fool receivers;
- Detection of Trojan triggers (backdoors) in RF signals;
- Inference of RF signal memberships (in form of membership inference attack to identify emitters, channel conditions, waveforms, for example); and
- RF fingerprinting to detect signals that may be spoofed such as smart jammers replaying other signal types.

Advanced attacks using spoofed RF signals generated by jointly capturing waveform, channel and radio hardware effects using Generative Adversarial Networks (GANs) were demonstrated in [1] and [11]. Generation of LPI wireless communications using a cooperative jammer to carefully craft adversarial perturbations to mimic the overt signal as noise is demonstrated in [5]. Various deep learning techniques described in [9] are demonstrated to be effective in detection and classification of these signals. Very high accuracy for classification of 17 types of signals are demonstrated in [9]. Radio hardware imperfections such as I/Q imbalance, time/frequency drift, and power amplifier effects can be used as a “radio fingerprint” for detection and characterization RF signals. Deep learning approaches using such RF fingerprinting techniques are shown to be very effective in labeling multiple signals in wireless channels [3]. Many of these and other ML-based and classical signal processing techniques developed by IAI can be used for detecting and characterizing the types of anomalous signals of interest for IARPA SCISRS.

Unintended Emissions

Utilizing our experience with results from the DARPA LADS program for which technologies were developed to associate running state of microprocessors with unintended emission, we have performed additional laboratory experiments in-house at IAI that demonstrate that the precise state of the microprocessor can be identified with significantly increased fidelity using a variety of signal processing techniques in the time and frequency domain. Specific features of the unintended emission in the time and frequency domain can be estimated reliability and used to detect, characterize, and track the unintended emission using classical signal processing and/or machine learning techniques.

3. RF Data Collection and Analysis

IAI has extensive, practical experience collecting and analyzing Big Data across multiple domains including RF. IAI has the software, services, and infrastructure to support continuous collection, analysis, and model development to enable continuous integration and deployment (CI/CD) of SCISRS capability. IAI provides an on-premise cloud for IAI’s AI researchers with 100GbE switching network, over 100TB of high speed SSD/NVMe storage, and 30+ GPU resources, including the latest NVIDIA V100s and NVIDIA GeForce RTX GPUs. As part of the CI/CD process, the models and algorithms developed in the AI on-premise cloud servers are then optimized and targeted for deployment at multiple scales including commercial Cloud providers down to a variety of FPGA and NVIDIA embedded platforms, such as Jetson and Xavier.

4. Sample IAI Publications

- [1]. Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, "Generative Adversarial Network in the Air: Deep Adversarial Learning for Wireless Signal Spoofing," *IEEE Transactions on Cognitive Communications and Networking*, (Early Access), 2020.
- [2]. Y. E. Sagduyu, Y. Shi, and T. Erpek, "Adversarial Deep Learning for Over-the-Air Spectrum Poisoning Attacks," *IEEE Transactions on Mobile Computing* (Early Access), 2020.
- [3]. K. Davaslioglu, S. Soltani, T. Erpek, and Y. E. Sagduyu, "DeepWiFi: Cognitive WiFi with Deep Learning," *IEEE Transactions on Mobile Computing* (Early Access), 2019.
- [4]. T. Erpek, Y. E. Sagduyu, and Y. Shi, "Deep Learning for Launching and Mitigating Wireless Jamming Attacks," *IEEE Transactions on Cognitive Communications and Networking*, Mar. 2019.
- [5]. B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "How to Make 5G Communications "Invisible": Adversarial Machine Learning for Wireless Privacy," *Asilomar Conference on Signals, Systems, and Computers*, 2020.
- [6]. Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, "Over-the-Air Membership Inference Attacks as Privacy Threats for Deep Learning-based Wireless Signal Classifiers," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2020.
- [7]. B. Kim, Y. E. Sagduyu, K. Davaslioglu, T. Erpek, and S. Ulukus, "Over-the-Air Adversarial Attacks on Deep Learning Based Modulation Classifier over Wireless Channels," *Conference on Information Sciences and Systems (CISS)*, 2020.
- [8]. K. Davaslioglu and Y. E. Sagduyu, "Trojan Attacks on Wireless Signal Classification with Adversarial Machine Learning," *IEEE Workshop on Data-Driven Dynamic Spectrum Sharing of IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2019.
- [9]. Y. Shi, K. Davaslioglu, Y. E. Sagduyu, W. C. Headley, M. Fowler, and G. Green, "Deep Learning for Signal Classification in Unknown and Dynamic Spectrum Environments," *IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, 2019.
- [10]. S. Soltani, Y. E. Sagduyu, R. Hasan, K. Davaslioglu, H. Deng, and T. Erpek, "Real-Time and Embedded Deep Learning on FPGA for RF Signal Classification," *IEEE Military Communications Conference (MILCOM)*, 2019.
- [11]. Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, "Generative Adversarial Network for Wireless Signal Spoofing," *ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) Workshop on Wireless Security and Machine Learning (WiseML)*, 2019.