Information Institute®

Visiting Faculty Research Program

Summer Faculty Fellowship Program

Research Fellowship Program

2025

Research

Topics

Version 1.1

Approved for Public Release; Distribution Unlimited: Case No.: AFRL-2024-4061,
Dated: 25 July 2024

Visiting Faculty Research Program
Summer Faculty Fellowship Program
Research Fellowship Program

2025 Research Topics
Version 1.0

Table of Contents

Topics by Division

Topic Advisor by Division

Information Systems (AFRL/RIS)

Multi-agent Approaches for Planning Air Cargo Pickup and Delivery

Andre Beckus
(315) 330-2734
andre.beckus@us.af.mil

Efforts to improve air logistics planning have been ongoing for decades, helping drive the development of critical techniques such as the simplex method for solving linear programs. The classic air cargo pickup and delivery problem can be broadly defined in the following way [1]: the air network consists of a graph, where nodes are capacity-constrained airports, and edges are routes with an associated cost and time-of-flight. Each cargo item is stored at a node, and must be picked up by agents (airplanes) and delivered to a target node. The primary objective is to deliver cargo on time, with a secondary objective to minimize cost.

We seek to explore the following topic areas:

1) **New techniques for solving the air cargo problem**. Recently, there has been success in using machine learning to solve related problems such as the Vehicle Routing Problem [2] or Pickup and Delivery Problem [3]. Graph Neural Networks have also showed potential for solving planning problems [4]. Meanwhile, operations research continues to provide promising results, e.g. in the area of Multi-Agent Path Finding for robot and train routing [5]. We seek application of these or other techniques to improve over existing methods in terms of optimality, computational cost, and scalability.
2) **Extensions to address stochastic events**. Disruptions may render a plan obsolete. For example, routes (edges) or airplanes (agents) may become unavailable due to storms or maintenance issues. Even minor local delays can propagate through the system and lead to long-lasting consequences. New delivery needs may also arise, e.g., a new cargo item may appear at one of the nodes with an urgent deadline. We seek techniques to update an existing plan without requiring the problem to be completely re-solved.

[1] “The Airlift Planning Problem" **https://dl.acm.org/doi/abs/10.1287/trsc.2018.0847**

[2] “Reinforcement Learning for Solving the Vehicle Routing Problem”:
https://papers.nips.cc/paper/8190-reinforcement-learning-for-solving-the-vehicle-routing-problem

[3] "Heterogeneous Attentions for Solving Pickup and Delivery Problem via Deep Reinforcement Learning": **https://arxiv.org/pdf/2110.02634**

[4] “Graph Neural Networks for Decentralized Multi-Robot Path Planning “:
https://arxiv.org/abs/1912.06095

[5] “Multi-Agent Pathfinding: Definitions, Variants, and Benchmarks”:
https://www.aaai.org/ocs/index.php/SOCS/SOCS19/paper/view/18341/17457

Distributed Workflow Execution and Dynamic Routing

Andre Beckus
(315) 330-2734
andre.beckus@us.af.mil

The ability to coordinate distributed teams and weapon systems in a contested fight has become a major concern for the Air Force. Current Air Force operations rely on centralized command and control (C2) nodes to conduct planning and orchestration for execution. Future operations will require the use of Agile Combat Employment (ACE) to shift operations from centralized physical infrastructures to a network of smaller, dispersed locations. Inherent in ACE doctrine is the idea of centralized command, distributed control, and decentralized execution (CC-DC-DE). This allows for efficiently utilizing the distributed resources at the proper time, to maximize the capacity of each function, while minimizing the process execution time.

We seek to develop a capability to continuously orchestrate C2 processes in an ACE operational environment through distributed workflow execution. Potential research directions include (but are not limited to):

- Orchestrating human and machine executable processes that are resource constrained. Algorithms should address varying "intent" of a mission thread and change how the C2 processes utilize distributed functions and resources in execution.
- Managing the complexity of shared resources across distributed C2 nodes and distributed C2 processes that are continuously executing. Algorithms should address the deconfliction of shared resources and continuously manage when "intent" of mission threads is used to influence priority of process execution.
- Tracking conditions-based authorities of specific processes to delegate tasking through lower tier C2 nodes. Algorithms should update the conditions-based authority of each function as "intent" of the mission threads is used to influence priority of process execution at alternate nodes.

Robust Logistics and Cargo Transport

Andre Beckus
(315)330-2734
andre.beckus@us.af.mil

The military requires the timely distribution of various movement of cargo, supplies and/or personnel often within strict time limits. This is hampered by a multitude factors ranging from weather disruptions to limited space at airports and depots. We seek new techniques for resilient logistics that can overcome these challenges. Potential topic areas include, but are not limited to:

- Optimization techniques for pickup and delivery of cargo.
- Vehicle routing to avoid congestion and reduce risk.
- Identification/mitigation of critical nodes and edges within the transport network.
- Multi-agent planning under limited communications.

Solutions may draw on a variety of approaches, for example using linear programming, multi-agent path finding, domain independent automated planners, or machine learning.

Dynamic Task Allocation for Distributed Workflow Execution

Andre Beckus
(315) 330-2734
andre.beckus@us.af.mil

The ability to coordinate distributed teams and weapon systems in a contested fight has become a major concern for the Air Force. Current Air Force operations rely on centralized command and control to conduct planning and orchestration for execution. Future operations will shift operations from centralized physical infrastructures to a network of smaller, dispersed locations. This will require a capability to execute distributed workflows across multiple locations while factoring in changing states, resources, and mission objectives.

We seek techniques to facilitate dynamic task allocation for distributed workflow execution among geographically distributed worker nodes. Techniques could draw from diverse discipline areas, including Internet of Things (IoT) task allocation on energy-constrained edge devices, or software defined network routing. Solutions may exploit a variety of approaches, for example using linear programming, constraint programming, domain independent automated planners, or machine learning. This topic may also cover techniques for sharing state information and reasoning over knowledge, in support of optimization and distributed decision-making.

Mathematical Theory for Advances in Machine Learning

Ashley Prater-Bennette
(315) 330-2033
Ashley.Prater-Bennette@us.af.mil

To alleviate the effects of the so-called ‘curse of dimensionality’, researchers have developed sparse, hierarchical and distributed computing techniques to allow timely and meaningful decisions based on large amounts of structured or unstructured data. As the amount of data available to analysts continues to grow, a strong mathematical foundation for new techniques is required. This research topic is focused on the development of theoretical mathematics with applications to machine learning and decision making with a special emphasis on techniques that admit sparse, low-rank, overcomplete, or hierarchical methods on multimodal data. Proposals with a strong mathematical foundation will receive special consideration.

Multi-Unit, Multi-Action Adversarial Planning

Brayden Hollis
(315) 330-2331
Brayden.Hollis.1@us.af.mil

Planning is a critical component for any command and control enterprise. While there have been impressive breakthroughs with domain independent heuristics and Monte Carlo tree search, in adversarial settings with multiple units, further work is still required to deal with the enormous state and action space to find quality actions that progress towards the goal and are robust to adversarial actions. We seek to develop new adversarial, domain-independent heuristics that exploit interactions between adversaries’ components. In addition to developing new heuristics, we are also interested in more intelligent and efficient search

techniques that will allow planning over multiple units. Areas of interest include Automated Planning, Heuristic Search, Planning over Simulators, and Game Theory.

Modeling Mission Impact in System-Of-Systems. A Dynamical Approach

Marco Gamarra
(315) 330 2640
Marco.Gamarra@us.af.mil

Dependency relationships between systems are critical in mission impact analysis defined in networked systems-of-systems (SOS); several models have been proposed to capture, quantify, and analyze the dependency relationship between systems under the system's administrator and user's perspectives. However, few efforts have been made in models that capture the dynamic behavior of dependencies between system components. This research topic will explore:

- Rigorous mathematical models for the analysis and simulation of the interdependencies in networks of system-of-systems.
- Models based on actual measurement of time-variant dependency variables.
- Models for the analysis and simulation of cascading failures in networks with switching topology.
- Optimal control on networks of SOS.

Some research areas of interest in this topic includes but are not limited to dynamical systems, dynamic graphs, network of multi-agent systems, and optimal control.

Resilient Distributed Optimization and Learning

Marco Gamarra
(315) 330 2640
Marco.Gamarra@us.af.mil

In many military applications, large volumes of heterogeneous streaming data are needed to be collected by a team of autonomous agents which then collaboratively explore a complex and cluttered environment to accomplish various types of missions, including decision making, optimization and learning. In order to successfully and reliably perform these operations in uncertain and unfriendly environments, novel concepts and methodologies are needed to 1) analyze the resiliency of algorithms, and 2) maintain the capability to reliably deliver information and perform desired operations. This research topic will develop resilient distributed optimization and learning algorithms in the presence of

- Abrupt changes in the inter-agent communication network,
- Asynchronous communications and computations,
- Adversarial cyber-attacks capable of introducing untrustworthy information into the communication network.

Some distributed methods of interest in this topic include, but are not limited to weighted-averaging, push-sum, push-pull, stochastic gradient descent, and multi-armed bandits.

Distributed Optimization and Learning with Limited Information

Marco Gamarra
(315) 330 2640
Marco.Gamarra@us.af.mil

Modern optimization and learning problems are often with very high-dimensional states, especially when deep neural networks are involved. In the corresponding distributed optimization and learning algorithms, relevant local information shared among neighboring agents is thus frequently high-dimensional, which leads to expensive communication costs and vulnerable information transmissions. This research topic will develop distributed optimization and learning algorithms with limited information transfer between agents for the purposes of

- Communication efficiency,
- Privacy preserving,
- Information security.

Some distributed problems of interest in this topic include, but are not limited to convex and nonconvex optimization, online optimization, reinforcement learning, and neural network optimization.

ML-Aided Autonomous UAV Network Connectivity and Data Dissemination

Norman Ahmed
(315) 330-2283
Norman.Ahmed@us.af.mil

Networked UAV-based communications hold tremendous potential across a wide range of applications, offering swift, adaptive deployment, and robust line-of-sight communication capabilities. These networked nodes typically operate on variable application-level network protocols such as Mobile Ad-hoc Networks (MANET) or Flying Ad-hoc Networks (FANET), and LoRaWAN, over heterogeneous underlying communication channels powered by a combination of Terrestrial and Non-Terrestrial Networks (NTN). This variability coupled with their mobility poses significant challenges on achieving reliable network connectivity and guaranteed information/data dissemination among the UAVs and NTN nodes. This research areas of interest include but not limited to:

- Bio-inspired autonomous UAV swarming techniques resilient to disruptions, specifically, aerial P2P overlay network topology construction algorithms with strong theoretical foundation.
- Light-weight secure messaging middleware for autonomous networked UAVs.
- Advanced Machine Learning (ML)-based for:
    - Application-layer network protocol stack selection prediction techniques. For instance, switching between Named Data Networking (NDN) and Delay-Tolerant Network (DTN) protocols over MANET/FANET.
    - Network-layer channel prediction techniques that can facilitate effective beamforming and, consequently, higher throughput under conditions with substantial channel jittering.

Efficient spectrum selection and dynamic sensing techniques to aid continuous data dissemination

Optimal Routing for Dynamic Demand in Networks with Limited Capacity

Chad Salisbury
(315) 823-8997
chad.salisbury@us.af.mil

Mission planning across operational and tactical echelons requires development of complex logistics plans in support of all AF missions. The size of the force, distances to be traveled, fragility of our supply networks, and the ability of the adversary to hold our forces at risk all confound the DoD's ability to project and sustain the force. The objective is to facilitate the construction of a dynamic multigraph that represents the spatio-temporal logistics information and connections to mission objectives, defines the characteristics of those resultant multigraph properties that contribute to a contested state, and apply multivariate, critical node analysis techniques to provide a valuation of robustness of the logistics plan, and predict how an adversary may target critical logistics nodes so the Air Force may develop strategies to be resilient and robust to these attacks in order to optimize mission success. Ultimately, what is sought is how this newfound intuition into logistics plans can be leveraged to design them to be robust in the first place (not just to measure their fragility), and then how to address their resiliency on the fly when events happen dynamically in the middle of execution.

Enhanced Explainable Reinforcement Learning (XRL) Integrated with Topological Data Analysis (TDA)

Simon Khan
(315) 330-4554
simon.khan@us.af.mil

The need for Reinforcement Learning (RL) has surged because of its potential to address complex problems effectively. However, RL faces significant challenges such as balancing execution complexity with transparency, sequential decision-making, starving for data. As RL models become more intricate, understanding the rationale behind their decisions becomes more difficult. Since RL models learn autonomously, understanding the reasons behind their decisions is crucial for establishing trust between the user and the agent, which is influenced by the model's success or failure. On the other hand, Topological Data Analysis (TDA) has been a powerful tool to understand valuable insights into the structures and patterns within complex datasets. Therefore, when incorporated into XRL, TDA can enhance explainability of the learned policies and the decision-making process of the RL agents significantly. However, TDA has problems with scalability and computational efficiency. Therefore, this topic seeks proposal to utilize TDA integrated into XRL (but not only limited to) as follows:

1) Develop a novel method to better understand of the state space (simplification) for explainability
2) Develop a novel algorithm to apply TDA into the policy representation to identify key regions where policy changes drastically (policy and value function analysis)
3) Develop robust explainability algorithms/methods by identifying topological features in the state space that correlate to certain actions/decisions made by the agents

Criticality Determination for Explainable Reinforcement Learning (XRL)

Simon Khan
(315) 330-4554
simon.khan@us.af.mil

The current utilization of RL models within the USAF/USSF lacks a focus on trusted AI/Explainable RL (XRL) techniques, which are crucial for fostering trust between operators and RL models. This absence hampers the enhancement of mission intelligence, hindering optimized decision-making and the provision of evidence for mission assurance. For example, operators need to mitigate potential errors from multi-agent systems (e.g., RL agents/UAVs) to ensure mission success. Presently, operational debugging tools to clarify, measure, contrast, and instill operator trust in ML-based decisions, particularly in UAV tasks, are lacking in the USAF/USSF. Trusted AI, identified as a critical technology focus by the OUSD R&D based on the 2030 ST strategy, includes XRL, an emerging field dedicated to providing clear and understandable explanations for RL model decision-making processes. Given the increasing use of RL in multi-agent systems throughout the DoD, there is a pressing need to provide explanations for decisions made by RL-trained agents, fostering transparency between agents and human operators. State-of-the-art RL methods face challenges such as encountering unsafe situations for unknown reasons, posing risks to live missions, such as catastrophic collisions. This topic aims to develop a novel XRL framework to mitigate these situations by identifying opportunities, both in post-hoc and real-time deployment scenarios, where human overseer intervention can take place in mission critical scenarios.

Specifically, the researchers will develop a criticality framework to measure the impact of bad decisions while ensuring that the framework offers explainability. Existing work attempts to assess the criticality of decisions at various time points, but their effectiveness remains uncertain due to a lack of definitive benchmarks. Additionally, these assessments are not crafted for straightforward explanations that are interpretable by the end users. To address this need, the researchers may introduce true criticality as the expected drop in reward when an agent deviates from its policy for n consecutive random actions. They also may introduce the concept of proxy criticality, a low-overhead metric that has a statistically monotonic relationship to true criticality. Safety margins is another concept combining true and proxy criticality for better explanation and interpretability. It is defined as the number of random actions for which performance loss will not exceed some tolerance with high confidence. The criticality framework will measure the potential impacts of bad decisions, even before those decisions are made, allowing for more effective debugging and oversight of autonomous agents utilized by DoD agencies. The researchers are free to contact the advisor for further clarification.

Compositional Optimization

Matthew Klawonn
315-330-2420
matthew.klawonn.2@us.af.mil

Automating Air Force planning often involves formulating an optimization problem, choosing/developing an appropriate solver, and feeding data of the initial conditions for a specific problem instance to the resulting system. In this project we will explore how to define mathematically and implement in software the composition of such systems. The goal of this work is to create a library for the creation of highly complicated and sophisticated planners using smaller atomic components. We will leverage techniques from applied category theory and mathematical programming to do so. In addition to extensions to existing work [1,2,3] that could include the

study of properties of composite optimization problems, or the incorporation of more sophisticated solution algorithms, applicants can propose to study novel applications well suited to compositional approaches.

1) Hanks, T., Klawonn, M., Patterson, E., Hale, M., & Fairbanks, J. (2024). A Compositional Framework for First-Order Optimization. arXiv preprint arXiv:2403.05711.
2) Hanks, T., Klawonn, M., & Fairbanks, J. (2024). Generalized Gradient Descent is a Hypergraph Functor. arXiv preprint arXiv:2403.19845.
3) Hanks, T., She, B., Hale, M., Patterson, E., Klawonn, M., & Fairbanks, J. (2023). A compositional framework for convex model predictive control. *arXiv preprint arXiv:2305.03820*.

Relevance Realization for Distributed Information Systems

C. Tyler Diggans
(315) 330-2102
christopher.diggans@us.af.mil

Synchronization is a key concept in the functional execution of many tasks within a distributed system. In order for a collection of agents (e.g., the I/O layers of sensors or databases) to retain a shared world view (information state), the agents must be able to pass sufficient information about their own states in a way so that enough information diffuses throughout the system and all agents can update their internal states to avoid stale or inaccurate data. As the information states of such agents becomes high dimensional or temporally dynamic, a constraint on the bandwidth available for information sharing may prevent the maintenance of an essential synchronization backbone of the available network and thus prohibit full synchronization. Depending on the particular context of an application, e.g., sensor network anomaly detection, we wish to automate a process for identifying what portion of the state is most relevant to the application at hand, so that a collection of agents might synchronize only the relevant information when bandwidth is limited. Additional interest may be found in the hierarchical dissemination of designated relevance by an intelligent agent with redundancy and subsequent reporting back to authority.

Smart Grid Synchronization Perturbation Analysis

C. Tyler Diggans
(315) 330-2102
christopher.diggans@us.af.mil

Although the synchronization of phases and voltage can often be assumed in more traditional power grid transmission networks due to the large amounts of inertia inherent in industrial generators, as power systems move toward more decentralized prosumer-oriented generation, which lack this physical inertia, the problem of maintaining synchronization under perturbations becomes more central to consistent operations. The concept of an Essential Synchronization Backbone (ESB) can indicate what minimal network lines are required for infinitesimal

perturbations from the synchronous state, but the size of the basin of stability for synchronizing systems is not easily obtained. We wish to use information theory tools, such as those based on transfer entropy, to quantify the robustness of a given synchronous state of a powergrid system to larger, but bounded finite perturbations, ideally linking a network model and the predicted effects to real world PMU data.

Geography-Informed Network Generation for Robust Multi-layer Cyber-Physical Systems

C. Tyler Diggans
(315) 330-2102
christopher.diggans@us.af.mil

Modern military operations increasingly rely on integrated systems of systems, which can be modeled as multi-layer networks with interlayer dependencies. The structure or network topology of many of the subsystems (layers), including communications, the power grid, or sensor networks, may be dependent on the topography of a region. We seek realistic generative models for a specific layer or multiple layers with associated interconnections. A model that is relevant to AF operations might include network layers representing the physical structure of: the power grid, communications, sensor networks (e.g., radar), command and control, and firepower; however, generalizations that include other layers will be of interest as well. Furthermore, many of these subnetworks will inevitably include a cyber aspect and/or artificial intelligence in their operations. Finally, some network layers may even be mobile, but temporary operating locations would be generated in this case. More generally, generative models for realistic networks that incorporate geographic features and or other parameters are sought for the creation of either a detailed model of single layers of interest or generative models for how to combine several layers in a way that provides robust operations and resiliency in the face of targeted attacks.

Computing & Communications (AFRL/RIT)

Dynamic Resource Allocation in Airborne Networks

Elizabeth Serena Bentley
(315) 330-2371
Elizabeth.Bentley.3@us.af.mil

From the Air Force perspective, a new research and development paradigm supporting dynamic airborne networking parameter selection is of paramount importance to the next-generation warfighter. Constraints related to platform velocity, rapidly-changing topologies, mission priorities, power, bandwidth, latency, security, and covertness must be considered. By developing a dynamically reconfigurable network communications fabric that allocates and manages communications system resources, airborne networks can better satisfy and assure multiple, often conflicting, mission-dependent design constraints. Special consideration will be given to topics that address cross-layer optimization methods that focus on improving the performance at the application layer (i.e. video or audio), spectral-aware and/or priority-aware routing and scheduling, and spectral utilization problems in cognitive networks.

Discovering Structure in Nonconvex Optimization

Gwen McDonald
315-330-2248
gwendolyn.mcdonald@us.af.mil

Optimization problems arising from applications are often inherently nonconvex and nonsmooth. However the tools used to study and solve these problems are typically adopted from the classical domain, not adequately addressing the challenges posed by nonconvex problems. The purpose of this research is to develop accurate models and efficient algorithms which take advantage of useful structure or knowledge derived from the application in question. Examples of this structure include sparsity, generalizations of convexity, and metric regularity. Some areas of interest are sparse optimization, image and signal processing, variational analysis, and mathematical foundations of machine learning.

Millimeter Wave Propagation

George Brost
(315) 330-7669
George.Brost@us.af.mil

This effort addresses millimeter wave propagation over air-to-air; air-to-ground; and Earth-space paths to support development of new communication capabilities. The objective is to develop prediction methods that account for atmospheric effects that give rise to fading and distortion of the wanted signal. Predictions may range from near term to statistical distribution of propagation loss. Research topics of interest are those that will provide information, techniques and models that advance the prediction methodologies.

Optical Communications

John Malowicki
(315) 330-3634
John.Malowicki@us.af.mil

Quantum communications research involves theoretical and experimental work from diverse fields such as physics, electrical engineering and computer science, and from pure and applied mathematics. Objectives include investigations into integrating quantum data encryption with a QKD protocol, such as BB84, and characterizing its performance over a free space stationary link. The analysis of the secrecy of the data is extremely important. Quantum-based encryption systems that use the phase of the signal as the information carrier impose aggressive requirements on the accuracy of the measurements when an unauthorized party attempts intercepting the data stream.

Free Space Optical Communication Links: Laser beams propagating through the atmosphere are affected by turbulence. The resulting wave front distortions lead to performance degradation in the form of reduced signal power and increased bit-error-rates (BER), even in short links. Objectives include the development of the relationship between expected system performance and specific factors responsible for wave front distortions, which are typically linked to some weather variables, such as the air temperature, pressure, wind speed, etc. Additional goals are an assessment of potential vulnerability of the quantum data encryption.

Associated with the foregoing interests are the design and analysis of simple to complex quantum optical circuitry for quantum operations. Characterization of entanglement in states propagating through such circuits in terms of measures such as PPT, CSHS inequalities, and entropic techniques are of interest.

Secure Processing Systems

John Rooks
(315) 330-2618
John.Rooks@us.af.mil

The objective of the Secure Processing Systems topic is to develop hardware that supports maintaining control of our computing systems. Currently most commercial computing systems are built with the requirement to quickly and easily pick up new functionality. This also leaves the systems very vulnerable to picking up unwanted functionality. By adding specific features to microprocessors and limiting the software initially installed on the system we can obtain the needed functionality yet not be vulnerable to attacks which push new code to our system. The focus of this topic is selecting techniques and demonstrating them through the fabrication of a secure processor. Areas of interest include: 1) design, layout, timing and noise analysis of digital integrated circuits, 2) Implementing a trusted processor design and verifying that design, 3) Selection of security features for a microprocessor design, 4) verifying manufactured parts, and 5) demonstrations of the resulting hardware.

Nanocomputing

Joseph Van Nostrand
(315) 330-4920
Joseph.VanNostrand@us.af.mil

Advances in nanoscience and technology show great promise in the bottom-up development of smaller, faster, and reduced power computing systems. Nanotechnology research in this group is focused on

leveraging novel emerging nanoelectroic devices and circuits for neruromorphic spike processing on temporal data. Of particular interest is biologically inspired approaches to neuromorphic computing which utilize existing nanotechnologies including nanowires, memristors, coated nanoshells, and carbon nanotubes. We have a particular interest in the modeling and simulation of architectures that exploit the unique properties of these new and novel nanotechnologies. This includes development of analog/nonlinear sub-circuit models that accurately represent sub-circuit performance with subsequent CMOS integration. Also of interest are the use of nanoelectronics as a neural biological interface for enhanced warfighter functionality.

Quantum Networking with Atom-based Quantum Repeaters

David Hucul
(315) 330-2221
david.hucul@us.af.mil

A key step towards realizing a quantum network is the demonstration of long distance quantum communication. Thus far, using photons for long distance communication has proven challenging due to the absorption and other losses encountered when transmitting photons through optical fibers over long distances. An alternative, promising approach is to use atom-based quantum repeaters combined with purification/distillation techniques to transmit information over longer distances. This in-house research program will focus on trapped-ion based quantum repeaters featuring small arrays of trapped-ion qubits connected through photonic qubits. These techniques can be used to either transmit information between a single beginning and end point, or extended to create small networks with many users.

Trapped Ion Quantum Networking and Heterogeneous Quantum Networks

David Hucul
(315) 330-2221
David.hucul@us.af.mil

Quantum networking may offer disruptive new capabilities for quantum communication, such as being able to teleport information over a quantum channel. This project focuses on the memory nodes and interconnects within a quantum network. Trapped ions offer a near-ideal platform for quantum memory within a quantum network due to the ability to hold information within the long-lived ground states and the exquisite control possible over both the internal and external degrees of freedom. This in-house research program focuses on building quantum memory nodes based on trapped ions, operating a multi-node network with both photon-based connections to communicate between the network nodes and phonon-based operations for quantum information processing within individual network nodes. In addition, the work focuses on interfaces to other qubit technologies (superconducting qubits, integrated photonic circuits, etc.) for heterogeneous network operation, quantum frequency transduction, and software-layer control. This work will be performed both in the in-house research laboratories at AFRL and the nearby Innovare Advancement Center.

Wireless Sensor Networks in Contested Environments

Lauren Huie
(315) 330-3187
Lauren.Huie-Seversky@us.af.mil

Sensor networks are particularly versatile for a wide variety of detection and estimation tasks. Due to the nature of communication in a shared wireless medium, these sensors must operate in the presence of other co-located networks which may have competing, conflicting, and even adversarial objectives. This effort focuses on the development of the fundamental mathematics necessary to analyze the behavior of networks in contested environments. Security, fault tolerance, and methods for handling corrupted data in dynamically changing networks are of interest.

Research areas include but are not limited to optimization theory, information theory, detection/estimation theory, quickest detection, and game theory.

Development of new cryptographic techniques is not of interest under this research opportunity.

Superconducting and Hybrid Quantum Systems

Matthew LaHaye
(315) 330-2419
Matthew.LaHaye@us.af.mil

The Superconducting and Hybrid Quantum Systems group focuses on the development of heterogeneous quantum information platforms and the exploration of related fundamental physics in support of the quantum networking and computing missions of AFRL's Quantum Information Science and Technology Branch. A central theme of the group's work is to develop quantum interfaces between leading qubit modalities to utilize the respective advantages of each of these modalities for versatility and efficiency in the operation of quantum network nodes. Towards this end, the group's research is composed of several main thrusts: the development of novel superconducting systems for generating and distributing multi-partite entanglement; the development of interconnects for encoding and decoding multiplexed quantum information on a superconducting quantum bus; the investigation of hybrid superconducting and photonic platforms for transduction of quantum information between microwave and telecom domains; and exploration of quantum interface hardware for bridging trapped-ion and superconducting qubit modalities.

Optical Interconnects

Matthew Smith
(315) 330-7417
Amos.Smith.6@us.af.mil

Our main area of interest is the design, modeling, and building of interconnect devices for advance high performance computing architectures with an emphasis on interconnects for quantum computing. Current research focuses on interconnects for quantum computing including switching of entangled photons for time-bin entanglement.

Quantum computing is currently searching for a way to make meaningful progress without requiring a single computer with a very large number of qubits. The idea of quantum cluster computing, which consists of interconnected modules each consisting of a more manageable smaller number of qubits is attractive for

this reason. The qubits and quantum memory may be fashioned using dissimilar technologies and interconnecting such clusters will require pioneering work in the area of quantum interconnects. The communication abilities of optics as well as the ability of optics to determine the current state of many material systems makes optics a prime candidate for these quantum interconnects.

Integrated Photonic Element Design

Christopher C. Tison
(315) 330-3799
Christopher.Tison.2@us.af.mil

The maturation of quantum technologies from table-top experiments to the field will require the miniaturization and implementation of functional elements which may or may not currently have free-space optical equipment analogs. With the growth of CMOS fabrication technologies that are specialized in optical circuit design, there will be a push from proof-of-concept components to ones which implement the operational requirements needed for scaling quantum computing and networking efforts with high fidelity, yield, and density while reducing the loss and overhead of operation.

The focus of this effort is the development of integrated optical components for tasks relevant in a quantum platform. Examples include high extinction-ratio filtering of closely placed optical frequencies; reduction of loss in integrated optical components; and the design and characterization of components which are compatible with quantum memory technologies (e.g. visible wavelengths or for cryogenic environments).

This is both a theoretical (e.g. simulation or analytic approximations) or experimental (device fabrication and/or measurement) effort.

Airborne Networking and Communications Links

Elizabeth Serena Bentley
(315) 330-2371
Elizabeth.Bentley.3@us.af.mil

This research effort focuses on the examination of enabling techniques supporting potential and future highly mobile Airborne Networking and Communications Link capabilities and high-data-rate requirements as well as the exploration of research challenges therein. Special consideration will be given to topics that address the potential impact of cross-layer design and optimization among the physical, data link, and networking layers, to support heterogeneous information flows and differentiated quality of service over wireless networks including, but not limited to:

- Physical and MAC layer design considerations for efficient networking of airborne, terrestrial, and space platforms;
- Methods by which nodes will communicate across dynamic heterogeneous sub-networks with rapidly changing topologies and signaling environments, e.g., friendly/hostile links/nodes entering/leaving the grid;
- Techniques to optimize the use of limited physical resources under rigorous Quality of Service (QoS) and data prioritization constraints;
- Mechanisms to handle the security and information assurance problems associated with using new high-bandwidth, high-quality, communications links; and

- Antenna designs and advanced coding for improved performance on airborne platforms.

Wireless Innovations at Spectrum Edge: mm-Waves, THz Band and Beyond

Ngwe Thawdar
(315) 330-2951
Ngwe.Thawdar@us.af.mil

Today's increasing demand for higher data rates and congestion in conventional RF spectrum have motivated research and development in higher frequency bands such as millimeter-wave, terahertz band and beyond. In higher frequency bands such as millimeter wave and terahertz, where channel properties are affected by mobility and atmospheric conditions, an agile system with a flexible, resilient architecture and the ability to adapt to the changing environment is required. To that end, we are interested in both foundational and applications-focused research to meet the demands of next generation wireless systems.

For foundational research for wireless communications at spectrum edge, we would like to address the technical challenges in both accessing the spectrum and exploiting the spectrum. We are interested in advanced technologies in architecture, waveform and signal processing that enable access to the emerging spectrum bands that are not traditionally widely used for wireless communications. We are also interested in the radio architecture, system design, waveform, algorithm and protocols that will let us exploit the abundant bandwidth that the spectrum edge for future AF wireless applications. Examples include but are not limited to:

- Novel waveform designs that are robust to the high atmospheric absorption loss.
- Use of novel relay architectures such as reconfigurable intelligent surfaces to solve the blockage problem at higher frequency bands.
- Use of data science tools in machine learning to construct meaningful datasets from few RF data collected at these frequency bands.

We are also interested in applications-focused research that specifically calls for the use of frequency bands at spectrum edge in the proposed applications. Examples include but not limited to high bandwidth links for next-generation mobile communication systems, Air Force and commercial applications that consider converged sensing and communications systems, etc.

Quantum networking infrastructure: Techniques and hardware development

James Schneeloch
(315) 330-4036
james.schneeloch.1@us.af.mil

While quantum computing (QC) and networking have matured rapidly over the last decade, there are threshold capabilities, tools, and technologies that still need development before a large-scale quantum internet can be fully realized and utilized for real-world applications. Accomplishing this requires expertise from diverse fields including quantum optics/photonics, AMO physics, solid-state physics, materials science/engineering, computer science/engineering, and pure/applied mathematics.

Toward that end, the objectives of AFRL's Quantum Information Science (QIS) group include emphases on: developing tools from quantum information theory to benchmark and verify the

integrity of quantum networks and the resources employed therein; developing quantum computing algorithms achieving an advantage over conventional computing toward practical challenges; and in developing the physical hardware needed to carry out operations on these networks.

Among these emphases, topics of special interest include developing/characterizing quantum transducers between disparate species of qubits (e.g., microwave/optical transducers to connect distant superconducting-circuit qubits over fiber optics); developing quantum algorithms targeted to speed the solution of optimization and machine learning problems, and in developing efficient techniques to characterize quantum resources at a large scale.

Robust Adversarial Resilience

Ryan Luley
(315) 330-3848
Ryan.Luley@us.af.mil

Nathan Inkawhich
(315) 330-2117
nathan.inkawhich@us.af.mil

In recent literature, deep learning classification models have shown vulnerability to a variety of attacks. Recent studies describe techniques employed to defend against such attacks, e.g. adversarial training, mitigating unwanted bias, and increasing local stability via robust optimization. Further studies, however, demonstrate that these defenses can be circumvented through adapted attack interfaces. Given the relative ease by which most defenses are circumvented with new attacks, we will explore adversarial resilience from two angles. The first will be to improve the resistance of models against attacks in a robust fashion such that one-off attacks won't circumvent defensive measures. The second will be to attempt to classify subversion attacks by training a separate model to identify them. In order to accomplish both tasks, we will seek to understand the fundamental theory of deep learning architectures and attacks. We hypothesize that a mathematical analysis of attacks will show similarity between attacks that can be exploited by a classifier. We also hypothesize that a mathematical analysis of deep learned models will identify algorithmic weaknesses that are easily exploited by attacks. Understanding how attacks are generated, and how to identify the resultant adversarial examples, is necessary for generalizing countermeasures. Attacks may prey on measures used by the classifier, allowing for targeted deception or misclassification. These attacks often are designed for transferability; even classifiers employing typical countermeasures remain vulnerable. Other attacks prey on the linearity of the underlying model – these adversarial attacks require minimal modification to the data. Considering a nonlinear basis, such as radial basis functions, may improve resilience against such attacks. Exploring this design space will provide insight into methods we can employ to reduce adversarial impact.

Formal Methods for Complex Systems

Steve Drager
(315) 330-2735
steven.drager@us.af.mil

Formal methods are based on areas of mathematics that support reasoning about systems. They have been successful in supporting the design and analysis of systems of moderate complexity. Today's formal methods, however, cannot address the complexity of the computing infrastructure needed for our defense.

This area supports investigation on new powerful formal methods covering a range of activities throughout the lifecycle of a system: specification, design, modeling, and evolution. New mathematical notions are needed: to address the state-explosion problem, new powerful forms of abstraction, and composition. Furthermore, novel semantically sound integration of formal methods is also of interest. The goal is to develop tools that are based on rigorous mathematical notions, and provide useful, powerful, formal support in the development and evolution of complex systems.

Foundations of Resilient and Trusted Systems

Steve Drager
(315) 330-2735
steven.drager@us.af.mil

Research opportunities are available for model-based design, development and demonstration of foundations of resilient and trustworthy computing. Research includes technology, components and methods supporting a wide range of requirements for improving the resiliency and trustworthiness of computing systems via multiple resilience and trust anchors throughout the system life cycle including design, specification and verification of cyber-physical systems. Research supports security, resiliency, reliability, privacy and usability leading to high levels of availability, dependability, confidentiality and manageability. Thrusts include hardware, middleware and software theories, methodologies, techniques and tools for resilient and trusted, correct-by-construction, composable software and system development. Specific areas of interest include: Automated discovery of relationships between computations and the resources they utilize along with techniques to safely and dynamically incorporate optimized, tailored algorithms and implementations constructed in response to ecosystem changes; Theories and application of scalable formal models, automated abstraction, reachability analysis, and synthesis; Perpetual model validation (both of the system interacting with the environment and the model itself); Trusted resiliency and evolvability; Compositional verification techniques for resilience and adaptation to evolving ecosystem conditions; Reduced complexity of autonomous systems; Effective resilient and trusted real-time multi-core exploitation; Architectural security, resiliency and trust; Provably correct complex software and systems; Composability and predictability of complex real-time systems; Resiliency and trustworthiness of open source software; Scalable formal methods for verification and validation to prove trust in complex systems; Novel methodologies and techniques which overcome the expense of current evidence generation/collection techniques for certification and accreditation; and A calculus of resilience and trust allowing resilient and trusted systems to be composed from untrusted components.

Towards Data Communication using Neutrinos

Vijit Bedi
(315) 330-4871
Vijit.Bedi.1@us.af.mil

Existing beyond line of sight (BLOS) data communications relies on electromagnetic radiation for transmission and detection of information. This topic involves investigating a non-electromagnetic data communications approach using neutrinos.

Technical challenges to address include:

- *Transmission*: Particle accelerations are limited in transmit power and data modulation bandwidth. Perform analysis of the state-of-the-art particle accelerators and optimize particle accelerator designs primarily for digital communications.
- *Propagation*: Measuring the absorption coefficient and beam divergence of neutrino beams is key to distant neutrino communications. Propose techniques to measure and additionally perform data analysis of experimental data from ongoing experiments measuring both cosmic and accelerator neutrinos such as CERN.
- *Detection*: To achieve a practical bit error rate in data communications, increasing detector sensitivity or neutrinos detected per bit is crucial. Investigate neutrino detection methods to increase receiver sensitivity and optimize for digital communications.

Modular Machine Learning via Hyperdimensional Computing (HDC)

Nathan McDonald
(315) 330-3804
Nathan.McDonald.6@us.af.mil

Modular components can be independently optimized and arbitrarily arranged. Biological brains can compute across multiple data modalities because biological sensors convert diverse environmental stimuli to a consistent information representation, viz. high-dimensional spike time patterns. In contrast, traditional deep neural networks (DNN) can be independently trained but then not are not trivially cascadable: the output of one DNN as input to another DNN. Alternatively, DNNs may be assembled but must be trained monolithically, with exponentially increasing training resource costs. Consequently, there is growing interest in information representations to unify these algorithms, with the larger goal of designing ML modules that may be arbitrarily arranged to solve larger-scale ML problems, analogous to digital circuit design today. One promising information representation is that of a "symbol" expressed as a high-dimensional vector, thousands of elements long. Hyperdimensional computing (HDC), or vector symbolic architectures (VSA) is an algebra for the creation, manipulation, and measurement of correlations among "symbols" expressed as hypervectors. This research topic includes work towards implementing HDC in DNNs and spiking neural networks (SNN), sensor fusion via HDC symbolic reasoning, robotic perception and control, on-line/ continual/ life-long learning, and natively modular neural networks (e.g. external plexiform layer).

Neuromorphic Computing

Jack Lombardi
(315) 330-2627
Jack.Lombardi.2@us.af.mil
Qing Wu
(315) 330-3129
Qing.Wu.2@us.af.mi

The current high-profile demonstrations of machine learning/Artificial Intelligence (ML/AI), while impressive, are a) not suitable for Size, Weight, and Power (SWaP) limited systems and b) not operational without access to "the cloud" via high bandwidth communications. Neuromorphic computing is one of the most promising approaches for low-power, non-cloud-tethered ML/AI, capable of implementing a complete, high level intelligence at the level of a sensor platform, by

imitating aspects of biological brains, such as trainable networks of neurons and synapses, in non-traditional, highly parallelizable, reconfigurable hardware , in contrast to typical ML approaches today, which utilize commodity hardware and digital algorithms for ML/AI. This research aims for alignment of "the physics of the device" with ML algorithms to intrinsically and efficiently perform the computations in reconfigurable hardware the same way biological systems do so well. This research effort encompasses mathematical models, hardware emulation and characterization, computing architecture design, and algorithm development for neuromorphic computing. We are particularly interested in approaches that exploit the characteristic behavior of physical systems to perform computation, such as the complex behaviors provided from optics/photonics, memristors/ReRAM, superconductors, and metamaterials, among others. Again, special emphasis will be placed on imaginative technologies and solutions to satisfy future Air Force and Space Force needs for non-cloud-tethered ML on SWaP limited assets.

Game-Changing Technologies for Future Neuromorphic Computing

Kang Jun Bai
(315) 330-2425
Kang.Jun.Bai@us.af.mil

As a powerful component of future computing systems, deep neural networks (DNNs) are the next generation of artificial intelligence (AI) that intently emulate the neural structure and operation of the biological nervous system, representing the integration of neuroscience, computational architecture, circuitry, and algorithms. However, DNNs still have significant architectural limitations: (1) an inefficient processing pipeline for large-scale networks, (2) computationally expensive training methods that cannot keep up with increasing data density, and (3) improper network behavior and decreased accuracy due to anomalous or malicious agents. The scope of this effort is to formulate the fundamental research to advance the understanding of neuroscience, facilitate the development of neuromorphic computing hardware and algorithms, and accelerate neuromorphic computing to an extreme efficiency. Specifically, this research focuses on: (1) building an efficient DNN with a modular framework on embedded development platforms to support edge-enable applications, (2) improving learning algorithms to discover unknow objects with confidence, and (3) developing a working prototype of neuromorphic hardware with emerging circuitry and/or materials. Additional interest includes exploring robotic applications with respect to multimodal sensory information processed by DNNs and neuromorphic hardware.

Phased Array Control, Characterization, and Sensing for Directional Communications

William Stevers
(315) 330-2252
William.Stevers.1@us.af.mil

There is an immediate need for enabling RF spectrum agility and resilient communications in contested environments. Modern analog active electronically steered arrays (AESAs) enable highly directional communication systems that are inherently resilient to interference. However, the current state-of-the-practice for AESA control results in firmware-based controllers that often integrate a specific, singular radio architecture with a single, specific AESA panel. This system design paradigm increases system development time, SWaP, and cost while greatly reducing the spectrum agility and flexibility that the inherent modularity of the AESA panel itself enables.

We are interested in expanding the state-of-the-art in analog AESA-based communication systems by developing control architectures that preserve system flexibility while still allowing for adequate RF sensing and beamforming capabilities with multiple low-cost, modular AESAs from a variety of vendors. This involves foundational research in the following areas:

- Decoupling existing datalink sensing methods from specific hardware implementations so that they can be used with multiple AESA hardware configurations.
- Modelling and simulating pre-defined nulling techniques for AESAs and then implementing and characterizing these techniques.
- Identifying data-optimization techniques that balance the control latency and the desired RF performance of the AESA panel.
- Identifying traditional (non-adaptive, non-parametric) sensing techniques that can be modernized using the unique capabilities of analog AESAs.

We are also interested in applications-focused research on the use of highly directional, communication focused AESAs in contested environments. Examples include but are not limited to link discovery, high-capacity communications, directional communications for autonomous and semi-autonomous platforms, etc.

Software Assurance

William McKeever
(315) 330-2987
William.McKeever.1@us.af.mil

Software Assurance (SwA) is the justified confidence that the software functions as intended, and is guaranteed robust and secure. Currently, most SwA activities are labor-intensive and error-prone tasks that require a high level of expertise to use. SwA can and should be conducted across the lifecycle to increase the robustness and security of the software. While this topic is primarily concerned with testing and analysis phase, research directed over any phase of the lifecycle will be considered.

This topic is interested in advancing the state-of-the-art in SwA through approaches that will identify flaws in the software. The research can address SwA on source code, executables only or a hybrid (white box, black box, or grey box). Particular attention should be given to minimizing false positives and staying within an acceptable range, as this will assist in transition.

Areas of interest include: 1. Automation of SwA activities; 2. Lowering the expertise required to use SwA tools (e.g., augmenting SwA tools with AI technologies such as machine learning or Large Language models); 3. Automating the creation of static analysis checks; 4. Automated smart combination of SwA tools; 5. Prioritization of software bugs or alerts; 6. Metrics for SwA.

Information Warfare (AFRL/RIG)

Event Detection and Predictive Assessment in Near-real Time Complex Systems

Alfredo Vega Irizarry
(315) 330-2382
Alfredo.Vegairizarry.1@us.af.mil

The goal is to make best use of multi-point observations and sensor information for event detection and predictive assessment applicable to complex, near real time systems which are found in many military domains.

The first step in tackling these challenges is to analyze the data, remove any non-relevant information and concentrate efforts in understanding correlations between variables and events. The analysis is followed by designing and developing signal processing techniques that strengthen these correlations. The selected approach would end up transforming data that does not make much sense into a meaningful event prediction. This step is not an easy task because sensor readings and operator logs are sometimes inconsistent, unreliable, provide perishable data, generate outliers due to some catastrophic failure, or evolve in time in such way that data is almost impossible to predict.

Searching for strong correlations between data and events leads to choosing a model which can best assess the current conditions and then predict the possible outcomes for several possible scenarios. Scientists need to understand why a proposed method can be a potential solution.

Perhaps deterministic or statistical models can be simplified and solved; maybe a preprocessing stage can map data into a space where patterns are easily identified; it can be possible that solutions applied to other problems can be translated into the proposed problem, or there is an untested technique that can be applied to a dynamic model.

This is an opportunity for researchers to investigate event detection scenarios in the areas of telecommunications, radars, audio, imagery and video and support AFRL projects in sensor exploitation. An important element of this topic is brainstorming, testing ideas and to gain a general understanding of input data and output events.

Cyber Defense through Dynamic Analyses

Andrew Karam
(315) 330-2639
Andrew.Karam@us.af.mil

Modern systems are generally a tailored and complex integration of software, firmware and hardware. Additional complexity arises when these systems are further characterized by machine learning algorithms, with recent emphasis on deep learning methods. Couple this with the limited but “sufficient” testing in the development phases of the system and the end result is all too often an incompletely characterized set of system response to stimuli not of concern in the original tests.

We are interested in new approaches to system testing for security and vulnerabilities that would otherwise go undetected. In particular, modern test methods such as fuzz testing (or fuzzing) can cover more scenario boundaries using data considered to be otherwise invalid from network protocols, application programming

interface calls, files, etc.. These invalid data better ensure that a proper set of vulnerability analyses is performed to prevent exploits.

Further, we are interested in leveraging AI and machine learning techniques combined with these modern methods such as fuzzing, to more completely perform system tests and vulnerability analyses.

5G Core Security Research

Andrew Karam
(315) 330-2639
Andrew.Karam@us.af.mil

Very often most cyber-attacks exploit vulnerabilities and misconfigured system settings. The AFRL Laboratory for Telecommunications Research (LTR) is interested in researching and developing methodologies for identifying vulnerabilities in software implementations of 4G/5G global telecommunications specifications. Our goal is to protect core telecom network elements from cyber intrusions. LTR conducts in-depth security assessment across all core network layers and the interaction with the radio access network so that designers can build in resiliency. We seek to identify software security issues that adversaries use to penetrate network defenses. LTR maintains a commercial implementation of 4G/5G network to equip the cyber research professional with the tools necessary to develop and validate novel methodologies for the protection of modern mobile telecommunications networks.

Audio & Acoustic Processing

Darren Haddad
(315) 330-2906
Darren.Haddad@us.af.mil

The acoustic processing work is involved in all aspects of researching and developing state of the art (SOA) acoustical analysis and processing capabilities, to address the needs and requirements that are unique to the DoD counter UAS program. This research area allows us to tackle topics, such as detecting, tracking, beamforming and classifying specific acoustical signatures in dynamic environments via array processing (using both stationary and mobile arrays). The group is focused on developing technology from a basic research level and advancing it to be implemented in the field. Other significant thrusts in noise estimation and noise mitigation (both spectral and spatial), acoustical identification are necessary components of the acoustical program. SOA techniques such as I-vectors, deep neural networks, bottleneck features, and extreme learning are used to pursue solutions for real-time and offline problems

Communications Processing Techniques

Doug Smith
(315) 330-3474
Douglas.Smith.44@us.af.mil

We are focusing our research on exploring new and novel techniques to process existing and future wireless communications. We are developing advanced technologies to intercept, collect, locate and process communication signals in all parts of the spectrum. Our technical challenges include: interference

cancellation in dense co-channel environments, multi-user detection (MUD) algorithms, hardware architecture and software methodologies, techniques to geo-locate and track emitters and methodologies to improve the efficiency of signal processing software. Research into developing unique and advanced methods to process communication signals in a high density, rapidly changing environment is of great importance. The research is expected to be a combination of analytical and experimental analyses. Experimental aspects will be performed via simulations using an appropriate signal processing software tool, such as MATLAB.

Assurance in Mixed-Trust Cyber Environments

Paul Ratazzi
(315) 330-3766
Edward.Ratazzi@us.af.mil

Operations in and through cyberspace typically depend on many diverse components and systems that have a wide range of individual trust and assurance pedigrees. While some components and infrastructures are designed, built, owned and operated by trusted entities, others are leased, purchased off-the-shelf, outsourced, etc., and thus cannot be fully trusted. However, this heterogeneous collection of mixed-trust components and infrastructures must be composed in such a way as to provide measurable and dependable security guarantees for the information and missions that depend on them.

This research topic invites innovative research leading to the ability to conduct assured operations in and through cyberspace composed of many diverse components with varying degrees of trust. Topics of interest include, but are not limited to:

- Novel identity and access control primitives, models, and mechanisms.
- Secure protocol development and protocol analysis.
- Research addressing unique concerns of cyber-physical and wireless systems.
- Security architectures, mechanisms, and protocols applicable to private, proprietary, and Internet networks.
- Embedded system security, including secure microkernel (e.g., seL4) research and applications.
- Zero-trust computing paradigms and applications.
- Legacy and commercial system security enhancements that respect key constraints of the same, including cost and an inability to modify.
- Secure use of commercial cloud infrastructure in ways that leverage their inherent resilience and availability without vendor lock-in.
- Novel measurement algorithms and techniques that allow rapid and accurate assessment of operational security.
- Obfuscation, camouflage, and moving target defenses at all layers of networking and computer architecture.
- Attack- and degradation-recovery techniques that rapidly localize, isolate and repair vulnerabilities in hardware and software to ensure continuity of operations.
- Design of trustable systems composed of both trusted and untrusted hardware and software.
- Non-traditional approaches to maintaining the advantage in cyberspace, such as deception, confusion, dissuasion, and deterrence.

Assurance and Resilience through Zero-Trust Security

Soamar Homsi
(917) 870 - 0232
Soamar.Homsi@us.af.mil

Zero-trust cybersecurity is a security model that requires rigorous verification for any user or device requesting access to computing or network resources. In the context of cloud security, zero-trust means that no one is Zero-trust cybersecurity is a security model that requires rigorous verification for any user or device requesting access to computing or network resources. In the context of cloud security, zero-trust means that no one is trusted by default from inside or outside the commercial and public cloud systems, including the Cloud Service Provider (CSP). This security model incorporates several expensive approaches and complex technologies that rely on public-key machinery, zero-knowledge-proof, etc., making designing efficient and scalable solutions based on zero-trust challenging and almost infeasible in practice.

This research topic seeks novel approaches to: 1) enabling warfighters to efficiently and securely outsource private data and computation with mission assurance and verifiable correctness of results to untrusted commercial clouds without relying on a Trusted Third Party (TTP); 2) improving the resilience and robustness of the Air Force's mission-critical applications by effectively distributing them across multiple heterogeneous CSPs to prevent a single point of failure, avoid technology/vendor lock-ins, and to enhance availability and survivability; 3) optimize the trade-off between strict zero-trust security and rigid performance requirements for time-sensitive mission applications. Research topics of interest include, but are not limited to:

- Decentralized identity and access control mechanisms and protocols, including those that support anonymity.
- Novel application of existing cryptographic primitives and protocols to zero-trust computing paradigms.
- Design cross-cloud, CSP-independent, privacy-aware protocols and frameworks that operate in the presence of emerging zero-trust security mechanisms, enable secure and transparent migration of application and data across heterogenous CSPs, and facilitate multi-objective optimization in the security-mission trade space.
- End-to-end data protection, concurrency, and consistency for multi-user multi-cloud environments.
- Access patterns and volume leakage prevention for oblivious data stores under malicious security.
- Verification and authentication schemes for query evaluation over outsourced encrypted and unencrypted data.

The development of new cryptographic primitives or protocols are not of interest under this topic.

Discovery and Retrieval of Publicly Available Internet Information (PAI)

Soamar Homsi
(917) 870 - 0232
Soamar.Homsi@us.af.mil

The Air Force Research Laboratory / Information Directorate seeks novel methodologies to conduct comprehensive and secure searches across the vast amounts of Publicly Available Information (PAI) on the Internet. PAI is multilingual in nature and takes the form of continuously emerging new data types, such as

online publications, news, blogs, social media, ChatGPT, etc. The goal is to develop novel technologies that can enable analysts to perform secure, efficient and scalable retrieval of PAI while protecting their identity and/or intent and to prevent websites owners and operators from tracking collected data or linking online activities back to the users or their agency. Research topics of interest, include but not limited to:

- Confidential and scalable PAI gathering technologies without having to rely on a trusted third party, modify public data at its source, or collaborate with PAI website operators.
- Management attribution and web browsing anonymization approaches.
- Computational Private information Retrieval (PIR), information-theoretic private information retrieval, and differentially-private information retrieval protocols.

Assurance in Containerized Environments

Nathan Daughety
(740) 350-6567
nathan.daughety@us.af.mil

Containers are portable, but restricted, computing environments packaged with the bare requirements necessary for an application to run. Containers provide efficiency, speed, resilience, and management for the projects they support and have facilitated the characterization of DevSecOps as a force enabler. Containers and container orchestration technology are becoming more popular due to the performance benefits, portability, and the ability to leverage them in many different environments/architectures. However, security remains the barrier to widespread adoption in operational environments. The container threat model is headlined with the lack of high assurance and weak security isolation properties. As cloud and microservice architecture expansion continues, the assurance of container security has become a requirement.

This research topic invites innovative research providing high assurance computing capability in a variety of container architectures. Research areas of interest include, but are not limited to:

- Novel high assurance architectural designs
- Secure container technology for deployment in legacy technology stacks and/or commercially owned/operated cloud infrastructures
- Non-traditional and/or novel trustworthy virtualization methods lending to high assurance security with high performance benefits
- Secure deployment techniques to support DevSecOps
- Design of cloud-ready, container interfacing enclave solutions for data protection
- Novel data and tenant separation primitives, models, and mechanisms
- Methods for verifying data storage sanitization
- Approaches for remote attestation to assure that a container is running in an authorized environment
- Approaches to zero-trust in containerized environments
- Novel accreditation algorithms and techniques to provide rapid and accurate assessment of container images

Data Driven Approaches to Multimodal Sensor Data Information Extraction and Fusion for Collaborative Autonomy Designs in Detection, Estimation, and Characterization

Paul Schrader
(315) 330-2464
paul.schrader.1@us.af.mil

Modern, contested Air Force mission spaces are varied and complex involving many sensing modalities. Mission success within these spaces is equally critical to the engaged Warfighter, and, Command, Control, Communications, Computer, Cyber, and Intelligence (C5I) systems, which both leverage actionable information from these heterogeneous sensing landscapes. Interfering sources, low probability of intercept signals, and dynamic scenes all collude to deceive the Air Force's ability to derive accurate, relevant situational awareness in a timely fashion. Furthermore, legacy sensing systems which typically provide stove-piped human interpretable intelligence with potentially missing information are likely be more valuable and less vulnerable if aggregated with other sensing data upwardly located in their processing pipelines (i.e., upstream data fusion). Our overall research goal is to leverage all available signals, data from sensed environments, and domains leveraging collaborative/distributed systems for generating a cohesive situational awareness of a complete strategic/tactical space. The fundamental research objectives under this topic, within the context of emerging collaborative autonomy, includes areas such as multi-modal target association/fusion, multi-sensor/modal detection, tracking, characterization, multi-sensor selection, and parameter optimization for improved sensor fusion performance, interpretability, explainability, and optimization/orchestration tasking. We are interested in innovative discovery and designs within these areas that may come from a variety of novel discrete and stochastic methodologies (e.g., topological data analysis, artificial intelligence/machine learning, the interfacing of these approaches and other mathematical representations, Bayesian and information theory, etc.). These advancements, considered within the context of optimizing computational complexity and managing constrained communication/bandwidth, ideally must balance intelligent computational nodes and centralized/distributed processing to obtain desired deployment/transitional thresholds.

FutureG and AI/ML Technologies for Processing, Exploitation and Dissemination

Jonathan Ashdown
(315) 571-5339
Jonathan.Ashdown@us.af.mil

FutureG and AI/ML technologies are indispensable for military advancement, providing not only secure and instantaneous access but also optimizing data processing, exploitation and dissemination (PED) capabilities. With the ability to deliver higher data rates and lower latency while enhancing security measures, FutureG technologies coupled with AI/ML have the potential to unlock a myriad of capabilities related to several areas including:

- Big Data and Analytics within Open Radio Access Networks (ORAN)
- Signal detection, classification and geolocation
- Advanced security waveforms
- Artificial Intelligence and Machine Learning in 5G/FutureG Network Analysis
- Secure Low Probability of Intercept (LPI), Low Probability of Detect (LPD) and Anti-Jam Waveforms

- Physical Layer Security utilizing Massive MIMO and millimeter-wave (mmWave) Technologies
- Integrated Sensing, Communications and Cybersecurity
- Agile spectrum sensing and dynamic spectrum utilization
- Internet of Things (IoT) Networks and Aerial IOT Networks
- Unmanned Aerial Systems (UAS) Swarms and Coalitions and Counter-UAS Swarms and Coalitions

Advancing the state-of-the-art in any or all of these areas has the potential to propel military capabilities to new heights, ensuring agility, efficiency, and resilience in an evolving security landscape.

LLM-based Agents for the Cyber and Information Domain

Daniel Park
315.330.2602
daniel.park.18@us.af.mil

Automation is a key component, if not necessary, for bolstering our ability to understand the cyber domain and defend our networks. Researchers have attempted to apply multiple AI/ML techniques as solutions to critical cybersecurity problems, e.g., object detection for malware detection and reinforcement learning for vulnerability discovery. Similarly, researchers have demonstrated the ability of Large Language Models to be applied across multiple problems if harnessed and prompted correctly. A critical aspect of this prompting is to 1) provide augmenting context or knowledge or 2) develop a persona around a task or context. For example, one may prompt a model to respond as a developer while augmenting it with a separate database containing useful API's.

In this topic, we are interested in innovative approaches to using LLM-based agent to automate and assist in tasks throughout the cyber and information domains. Topics of interest include, but are not limited to:

- Novel applications of LLM-based agents for synchronous and asynchronous tasks
- Management of multi-agent systems
- Persona development and management
- Parametric and non-parametric memory mechanisms for personas, e.g., fine-tuning or RAG.

Development of intrusion-detection and endpoint detection and response systems are not of interest under this topic.

Assets Mapping for Mission Relevant Terrain in Cyber

Jonathan Amezcua, Makenzie Cosgrove
(315) 330 2404
{jonathan.amezcua_aguiluz, **gage.cosgrove}@us.af.mil**

The multitude of physical cyber assets possessed by the Air Force are connected to a large computer network, but this network's mathematical structure is not well-understood. For a given mission task, specific assets will be involved in execution of the task, but it is not known *a priori* which assets will be involved. Likewise, given an asset, it is not known which mission tasks will recruit this asset. Our overall research goal is to use AI/ML techniques to determine a mapping of the mission tasks to the relevant terrain

in cyber, most importantly, without having to store a blueprint of the entire network. The fundamental research objectives under this topic includes areas such as topological data analysis, which has been used to perform a similar structure analysis of human brains in applied neuroscience; data mining, which can be used to obtain information about the cyber terrain and the physical assets underlying it; and machine learning, which can be used to process the data obtained in order to form predictive models that can make decisions about how assets are used in mission-relevant tasks. We are interested in forming an initial dataset that we can use to train the AI/ML models.

This research topic invites innovative research on feature extraction and pattern recognition techniques/approaches including, but not limited to:

- Topological Data Analysis approaches.
- Novel Data Mining Techniques.
- ML-based Feature extraction methods.
- Innovative methods for Pattern Recognition.
- Graph Neural Networks
- Generative Topographic Mapping.
- Novel Supervised/Unsupervised learning approaches.

Graph Network for Recommendation System in Dynamic Resources

Laurent Njilla
(315) 330-4939
Laurent.Njilla@us.af.mil

Air Force warfighters require cross-domain tools to engage in the multidimensional contested domain, spanning kinetic, cyber, physical network and other capabilities. To succeed against peer adversaries, warfighters must be equipped with real-time, rapid threat response methods requiring robust, dynamic, and proactive guardrails for model trust to enable assured operations. This requires capability to dynamically discover information assets from different subnets and utilize them to disseminate information across globally distributed federations of users spread across platforms.

By integrating a new research and development paradigm in support of dynamic mobile networking we look to achieve the capability to change topologies based on mission priorities and other known constraints. This results in a dynamically reconfigurable network where nodes are connected based on resources recommended by the graph network though anticipation of interactions between node resources and/or components.

This research topic invites innovative research leading to the ability to conduct assured operations in cyberspace composed of heterogeneous components with varying degrees of trust.

Areas to consider under this research topic include but are not limited to:

- Developing a theoretical foundation for modelling graph network on dynamic data-driven IoT systems and a practical Automated Components Dataflow Modelling Framework (ACDMF).

- Practical machine learning models for graph network recommendation based on resource anticipation/prediction driven by the ACDMF data sets.

Information Assurance and Trust for Cyber Defense

Laurent Njilla
(315) 330-4939
Laurent.Njilla@us.af.mil

The Air Force's mission in cyberspace involves the ability to provide information to warfighters anywhere, anytime, and for any mission. This far-reaching endeavor will necessarily span multiple networks and computing domains not exclusive to military. Cyberspace remains beneficial and a technological advantage when vulnerabilities are under control. Cyber defense is concerned with the protection and preservation of critical information infrastructures available in cyberspace and has implications in air and space.

This research topic seeks innovative approaches to 1) protect our own resources through information assurance; 2) enable our systems to automatically interface with multi-domain systems through information sharing, while possessing the ability to operate correctly in unanticipated states and environments; 3) provide the means to circumvent attacks by learning new configurations and understanding vulnerabilities before exploitation.

Fundamental research areas of interest within this topic include:

- Design of trusted systems composed of both trusted and untrusted hardware and software components with reconfigurability on-the-fly.
- Mathematical concepts and distinctive mechanisms that enable systems to formal verification.
- Information flow theory and collaborative design describing interactions of systems of systems that lead to better consideration and interactions of their emergent behaviors and ease proactive resource sharing.
- Study and application of emerging security technologies, such as blockchain technology and formal methods.

Development of new cryptographic methods are not of interest under this topic.

Topological Data Analysis for Cyber Assurance

MaKenzie Cosgrove
(315) 330-2822
gage.cosgrove@us.af.mil

Topological Data Analysis (TDA) gives us rigorous theory and implementations for understanding the structure of collected heterogeneous data by the measuring, tracking, and algebraically encoding its topological characteristics and persistent features through compressed representations of high fidelity. However, existing TDA tools may not be sufficient for robust data driven analyses that fully supports the evolving mission success and decision speed of the USAF/USSF Warfighter in (hyper) contested environments containing various concentrations of physical (e.g., multimodal sensor data information) and human (e.g., multimedia sources) based data inundated with attenuation/adversarial deception. Furthermore, much of the data collected in cyberspace has complex topologies that are not suited for many of the existing TDA methods. One approach in this case is to embed the data into a graph and use TDA techniques on the graph structure. While this is useful, it is not clear from the existing body of research that this captures all the essential features of the data for the purposes of inference and decision-making. Within the emerging field of topological deep learning (TDL) Hajij et al. developed combinatorial complexes leveraging higher-dimensional features and n-ary (i.e., binary, trinary, …, n-ary) non-Euclidean relation analysis of graph-embedded data. This project aims to develop implementations and test beds for using

these complexes to perform deep learning tasks within AFRL mission spaces of data assurance and information exploitation. Concurrently, we aim to develop TDL and other modern TDA methodology inspired novel approaches (e.g., multi-parameter persistent homology) for performing topologically informed autonomy on non-metrizable

Intelligence Systems (AFRL/RIE)

Processing Publicly Available Information (PAI)

Aleksey Panasyuk
(315) 330-3976
Aleksey.Panasyuk@us.af.mil

Publicly Available Information (PAI) includes a multitude of digital unclassified sources such as news media, social media, blogs, traffic, weather, scholarly articles, the dark web, and others. Being able to extract relevant supplementary information on demand could be a valuable addition to conventional military intelligence.

It would be of interest to: (1) categorize trustworthy PAI sources, (2) pull in textual information in English (generate English translation over major foreign languages), and (3) setup a library of natural language processing (NLP) tools which will summarize entities, topics, and sentiments over English texts. Examples of trustworthy PAI sources include highly credible users that belong to major and local news, emergency responders, government, university, etc. Topics of interest relate to business and economics, conflicts, cybersecurity, infrastructure, disasters and weather, etc. Important to have capabilities to resolve location even in the absence of geotags. Finally need to have confidence metrics for all capabilities developed. The researcher may chose, based on their expertise, to work on a subset of the outlined tasks.

Short-Arc Initial Orbit Determination for Low Earth Orbit Targets

Andrew Dianetti
(315) 330-2695
Andrew.Dianetti.1@us.af.mil

When new objects are discovered or lost objects rediscovered in Low Earth Orbit (LEO), very short arcs are obtained due to limited pass durations and geometrical constraints. This results in a wide range of feasible orbit solutions that may well-approximate the measurements. Addition of a second tracklet obtained a short time later – about a quarter of the orbit period or more – leads to substantially improved orbit estimates. However, the orbit estimates obtained from performing traditional Initial Orbit Determination (IOD) methods on these tracklets are often insufficient to reacquire the object from a different sensor a short time later, resulting in an inability to gain custody of the object. Existing research in this area has applied admissible regions and multi-hypothesis tracking to constrain the solutions and evaluate candidate orbits. These methods have been primarily applied to Medium Earth Orbit and Geostationary Orbit and have aimed to decrease the total uncertainty in the orbit states. The objective of this topic is to research and develop methods to minimize propagated measurement uncertainty for LEO objects at future times, as opposed to minimizing the orbit state uncertainty over the observed tracklet. This will improve the ability to reacquire the object over the course of the following orbit or orbits to form another tracklet, which will result in substantially better orbit solutions. Sensor tasking approaches which maximize the likelihood of re-acquisition are also of interest.

Feature-Based Prediction of Threats

Carolyn Sheaff
(315) 330-7147
Carolyn.Sheaff@us.af.mil

Methods have been developed to detect anomalous behaviors of adversaries as represented within sensor data, but autonomous predictions of actual threats to US assets require further investigation and development. The proposed research will investigate foundational mathematical representations and develop the algorithms that can predict the type of threat a red (adversary) asset poses to a blue (friendly) asset. The inputs to the system may be assumed to include: 1) an indication/warning mechanism that indicates the existence of anomalous behavior, and 2) a classification of the type of red/blue asset. Approaches to consider include, but are not limited to, predictions based on offensive/defensive guidance templates and techniques associated with machine learning, game theoretic approaches, etc.. The proposed approach should be applicable to a variety of threat scenarios.

The example that follows illustrates an application to U.S. satellite protection. The offensive template determines the type of threat. Mechanisms such as templates are used to predict whether or not this asset is a threat by comparing configuration changes with known threatening scenarios through probabilistic analyses, such as Bayesian inferences or game theoretic analyses. Robustness tests may be employed as well. (For example, a threat can be simulated that is not specific to one template.) Once the threat is determined, the classification algorithm provides notification of the type of asset. The classification approach is employed to (for example) determine whether the asset is intact or a fragment, its control states, the type of control state, and whether it is a rocket body, payload, or debris. (An example of an offensive assessment is a mass-inertia configuration change in an active red asset that is specific for robotic arm-type movements.) In the above example, a question to be answered is: can a combination of the templates handle this case? The defensive portion must also provide recommended countermeasures, i.e. as in the case of a blue satellite, thruster burns to move away from possible threats. Although our specific application interests for this research topic are represented by the above example, many application areas are likely to benefit from this research, including cyber defense, counter Unattended Aerial Systems (UASs), etc.

Computational Trust in Cross Domain Information Sharing

Colin Morrisseau
(315) 330-4256
Colin.Morrisseau@us.af.mil

In order to transfer information between disjointed networks, various domains, or disseminate to coalition partners, Cross Domain Solutions (CDS) exist to examine and filter information that ensures only appropriate data is released or transferred. Due to the ever-increasing amount of data needing to be transferred and newer, more complex data format or protocols created by different applications, the current CDSs are not keeping up with the current cross domain transfer demands. As a result, critical information is not being delivered to the decision makers in a timely manner, or sometimes, even at all. In order to meet today's cross domain transfer needs, CDSs are looking to employ newly emerging technologies to better understand the information that they use to process and adapt to large workloads. These emerging technologies include, but are not limited to, machine learning based content analysis, information sharing across mobile and Internet of Things (IoT) based devices, cloud based cross domain filtering systems, passing information across nonhierarchical classifications and processing of complex data such as voice and video. While adding these new technologies enhance CDSs' capabilities, they also add a substantial

complexity and vulnerabilities to the systems. Some common attacks may come from a less critical network trying to gain critical network access, or malware on the critical side trying to send data to the less critical side. Research should investigate and examine methods to efficiently secure emerging technologies beneficial to CDSs. Researchers will collaborate heavily with the AFRL's cross domain research group for better understanding of cross domain systems as they apply their specific areas of emerging technology expertise to these problems. The expected outcome may include a design and/or a proof-of-concept prototype to incorporate emerging technologies into CDSs. It may also include vulnerability analysis and risk mitigation for those emerging technologies operated in a critical environment.

Data Fusion and Processing using Machine Learning

Erika Ardiles-Cruz
(315) 330-2348
Erika.Ardiles-Cruz@us.af.mil

Due to the volume, variety, complexity, and decision timelines associated with real-time data collection from air- and space-based platforms, it is not viable for human operators to monitor, comprehend and act. The aim of this research thrust is to investigate topological data analysis, artificial intelligence, and machine learning approaches to system analysis, anomaly and threat detection, graph/data representation and nodal analysis. These techniques can be applied to quantify threats, attacks, nodal analysis and graph cuts, patterns of life, landscape changes over time, critical infrastructure anomalies and (rare) events leading to cascading effects pertaining to large-scale cyber-physical systems. Machine learning approaches could speed these processes but require massively curated datasets for training and parameter tuning, must be robust to a variety of adversarial attacks, and be re-trained during execution time. This topic will explore approaches that include: data sensing, collection, fusion, and augmentation at the edge; processing and exploitation of multimodal data using machine learning and topological data analysis approaches; development of explainable AI models and incorporation of human interaction; including feedback loops to improve parameter tuning and real-time training; and identification and quantification of physical and digital attacks to AI/ML lifecycles; to include real-time identification of when a deployed model may be used out of context or beyond its training data. Special consideration will be given to proposals that include innovative approaches for in low-SWaP (Space Weight and Power) constrains.

Autonomous Model Building for Conceptual Spaces

Jeremy Chapman
(315) 330-2017
jeremy.chapman.6@us.af.mil

Conceptual Spaces are a new form of cognitive model that seeks to represent how the human mind represents concepts. Conceptual Spaces allow for a geometrical representation of concepts allowing for a model to be built linking inputs and outputs. They are advantageous to other machine learning algorithms in the fact that they do not hold the common frame problem (i.e. they are not a "black box") and the

underlying model is capable of being manipulated to fix underlying issues. Originally Conceptual Spaces were developed as a physiological model with little to no underlying mathematical framework. Later mathematical model were developed to represent Conceptual Spaces. However, current techniques for building the models involve intensive human interaction which can be tedious and are subject to human biases. The research goal is to implement machine learning and/or other autonomous approaches for the development of autonomous model building and implementation of Conceptual Spaces.

Identification of Data Extracted from Altered Locations (IDEAL)

Michael Manno
(315) 330-7517
Michael.Manno@us.af.mil

The primary objective of this effort is to extract information from documents in real time, without the need to install additional software packages, utilize specialized development, or train agents to each source, even if the location of that data changes.

Seeking data from multiple documents is a manual, time consuming, undocumented process, which needs to be repeated every time an update, or change, to that data is requested. Automating this process is a challenge because the documents routinely change. Sometimes, the mere act of refreshing a web page changes the document as the ads cycle. Such changes are damaging to most of today's web scraping techniques. The lack of data, or inaccurate data, from failed updates during the extraction process also creates many problems when attempting to update the data, as unexpected results are returned. Extracting data from documents, typically requires training or expert analysis for each source before the data can be used. This means that documents must first be identified before a script or agent can be written to extract data from it by a developer. A user cannot discover a document, and immediately begin extracting data from it. This diverts time away from an analyst, as the analyst begins spending more time managing data, opposed to performing the intended analysis. Services that provide access to data such as RSS feeds, Web Services, and APIs, are useful, but are not necessarily what is needed by the requestor. For example, the Top Story from a news publisher may be available as an RSS feed, whereas the birth rate of the country may not be.

This assignment will focus heavily on enhancing the web browser extension prototype. The extension will be used for routine extraction of data elements from open source web pages/documents, and be developed for the Firefox web browser. In addition to Web Browser extension development, this assignment will include adding additional functionality such as visualization enhancements, search and transposition, crawl, and a process for identifying similar data. Consideration will also include expanding to additional web browsers such as Internet Explorer.

Classification of users in chat using Keystroke Dynamics

Michael Manno
(315) 330-7517
Michael.Manno@us.af.mil

Traditional username and password techniques, or Common Access Card, (CAC) login, does not continually monitor usage behavior over time. Keystroke Dynamics is a technique used to measure timing information for keys pressed/depressed on a computer keyboard and identifying unique signatures for the way an individual types. The current practice of Keystroke Dynamics, also known as Keystroke Biometrics,

is understanding this rhythm, to distinguish between users for authentication – even after a successful login. Current enrollment techniques require users to establish a consistent baseline and is traditionally accomplished by typing common words multiple times.

While effective, this process is sometimes rejected by users who do not see the value in an extensive enrollment process by typing large volumes of data. The challenge is determining the balance between effective enrollment, and user satisfaction. This effort will identify the most important features that will be used to allow for accurate classification of users from keystroke data. Specifically, classifying commonly typed digraphs to verify the claimed identity of the user, by developing binary classifiers trained with Machine Learning (ML) algorithms, to identify the most efficient signatures generated from frequent keystroke patterns. The goal is to create a trusted chat exchange between users for secure communications beyond traditional encryption and authentication techniques.

Elegant Failure for Machine Learning Models

Walter Bennette
(315) 330-4957
Walter.Bennette.1@us.af.mil

The need for increased levels of autonomy has significantly risen within the Air Force. Thus, machine learning tools that enable intelligent systems have become essential. However, analysts and operators are often reluctant to adopt these tools due to a lack of understanding – treating machine learning as a black box that introduces significant mission risk. Although one may hope that improving machine learning performance would address this issue, there is in fact a trade-off: increased effectiveness often comes at the cost of increased complexity. Increased complexity then leads to a lack of transparency in understanding machine learning methods. In particular, it becomes unclear when such methods will succeed or fail, and why they will fail. This limits the adoption of intelligent systems.

This topic focuses on building trust in machine learning models by designing models that fail elegantly. Of particular interest are model calibration techniques for object detection and classification, novelty detection, open-set recognition, and post-hoc filters to identify instances prone to causing model failure. Other topics related to this area will also be considered.

Recommendations Under Dynamic Incomplete and Noisy Data

Chris Banas
315-330-2202
Christopher.banas.1@us.af.mil

The DoD conducts Intelligence Surveillance and Reconnaissance (ISR) by focusing on optimal sensor placement for coverage. During the execution of the ISR plan, the DoD utilizes an ad-hoc manual process to prioritize and track existing and emergent objects-of-interest. Automating the ranking of these objects-of-interest is a critical component of operating within these near-peer contested environments. In contested environments, we expect to encounter enemy countermeasures such as jamming, spoofing, etc. that reduce the quality of the data needed for ranking. In other words, the central challenge of this effort is ranking objects-of-interest given the uncertainty and accuracy of the data.

AFRL seeks novel research into recommender-based approaches that can utilize noisy and incomplete data to rank a set of trackable objects-of-interest. Experimental datasets can comprise some mix of semi-realistic

or synthetic data representing both multi-int sensor information, as well as other higher level data sources for context. This topic is interested in exploring hybrid approaches that can represent conflicting data points. Given the model must represent these conflicting data points, non-linear approaches are desired. These approaches may include but are not limited to preference learning, active learning, and adaptive neural networks.

Recommendations with Human-on-the-Loop Interaction

Chris Banas
315-330-2202
Christopher.banas.1@us.af.mil

AFRL is focused on autonomous systems, as it pushes AI capabilities to the edge, to combat near-peer competitors. Increased emphasis on autonomy requires effective human-machine interaction to guarantee human judgment in decisions. This interaction should allow for a supervised autonomous mode i.e. 'Human on the Loop (HOTL). As stated, by General Terrence J. O'Shaughnessy, USAF (ret.), 'machine- enabled insights … can identify anomalous events, anticipate what will happen next, and generate options with associated repercussions and risks [https://warontherocks.com/2022/06/whats-wrong-with-wanting-a-human-in-the-loop/].

AFRL seeks novel research into various aspects of human-on-the-loop interactions including: representing context in encoding spaces, context aware recommendation methodologies, sorting and ranking methods for multi-criteria decision analysis, active learning to reinforce context within recommendations, and large language models for recommendations. Experimental datasets ideally include partially observable contextual information and can comprise a mix of semi-realistic or synthetic data. Additionally, contextual data can be represented as low-level attributes, as well as other higher-level information.

Adaptable Methods for Applying and Understanding Artificial Intelligence and Machine Learning

Maria Cornacchia
315-330-2296
maria.cornacchia@us.af.mil

Artificial intelligence and machine learning applications have exploded over the last decade. However, under some scenarios there has been slower adoption of such approaches.

While there are several potential reasons for slow adoption of AI/ML, one reason is that there must be trust and a responsible use of such approaches. This research topic is therefore interested in methods for instilling trust in AI/ML, either through better performance metrics or human understandable presentations of an AI/ML algorithms decision. This includes methods that explain the numerical impacts of training examples on the models being learned or novel methods that conceptually describe what an algorithm is learning. As part of understanding, this topic is also interested in new approaches that artificially alter or create data.

Additionally, a single model trained on specific data might not always allow for direct application to another use case. This research topic is therefore also interested in methods for applying models in unique scenarios, including at the edge. This might require advancements in the application of transfer-learning approaches or scenarios where it is necessary to fuse or correlate the output of multiple AI/ML models and/or algorithms. Hence, this research topic is interested in novel methods for fusing and building ensembles of

pre-trained models that are task agnostic and can more easily mimic the agility that humans possess in the learning process.

Being able to explain the impact of specific examples on the learning process, adapting a model to be deployed at the edge, and building novel algorithms and architectures will support the realization of more adaptable learning methods.

Data Driven Model Discovery for Dynamical Systems

Peter Rocci
(315) 330-4654
Peter.Rocci@us.af.mil

The discovery and extraction of dynamical systems models from data is fundamental to all science and engineering disciplines, and the recent explosion in both quantity and quality of available data demands new mathematical methods. While standard statistical and machine leaning approaches are capable of addressing static model discovery, they do not capture interdependent dynamic interactions which evolve over time or the underlying principles which govern the evolution. The goal of this effort is to research methods to discover complex time evolving systems from data. Key aspects include discovering the governing systems of equations underlying a dynamical system from large data sets and discovering dynamic causal relationships within data. In addition to model discovery, the need to understand relevant model dimensionality and dimension reduction methods are crucial. Approaches of interest include but are not limited to: model discovery based on Taken's theorem, learning library approaches, multiresolution dynamic mode decomposition, and Koopman manifold reductions

Predictive Knowledge Graphs for Situational Awareness

Claire Thorp
(315) 330-2620
claire.thorp@us.af.mil

Knowledge Graphs capture information about entities and the relationships between those entities, represented as nodes and edges within a graph. Entities can be comprised of objects, events, situations, or concepts. Knowledge Graphs are typically constructed from various data sources with diverse types of data, creating a shared schema and context for formerly disparate pieces of data. As such, Knowledge Graphs provide a rich source of information, enabling capabilities like question and answering systems, information retrieval, and intelligent reasoning. Areas of specific interest for this topic include (but are not limited to): identification of information gaps (i.e. spatial, temporal, reasonability) in a KG, prediction of additional information to augment a KG, recommending visualization techniques (i.e. timeline, heatmap) based on KG content, and neural KG search techniques. This research should be in support of more efficient situational awareness, pattern of life analysis, threat detection, and targeting operations. Proposers are strongly encouraged to contact the topic POC to discuss possible proposals.

Exploring Relationships Among Ethical Decision Making, Computer Science, and Autonomous Systems

Tim Kroecker
(315) 330-4125
Timothy.Kroecker@us.af.mil

The increased reliance on human-computer interactions, coupled with dynamic environments where outcomes and choice are ambiguous, creates opportunities for ethical decision making situations with serious consequences where errors could cost loss of life. We are developing approaches that make autonomous system decisions more apparent to its users, and capabilities for a system to tailor the amount of automation based on the situation and input from the decision maker. This allows for dynamically adjustable human/machine teaming addressing C2 challenges of Autonomous Systems, Manned/Unmanned Teaming, and Human Machine Interface and Trust. The work focuses on developing a system for modeling and supporting human decision making during critical situations, providing a mechanism for narrowing choice options for ethical decisions faced by military personnel in combat/non-combative environments.

We propose developing software (an "ethical advisor") to identify and provide interventions in situations where ethical dilemmas arise and quick, reliable decision making is efficacious. Our unique approach combines behavioral data and model simulation in the development of an interactive model of decision making that emphasizes the human element of the decision process. In the long term, understanding the fundamental aspects of human ethical decision making will provide key insights in designing fully autonomous computational systems with decision processes that consider ethics. As autonomous systems emerge and military applications are identified, we will work to provide verifiable assurance that our autonomous systems are making decisions that reflect USAF moral and ethical values. The first step towards realizing this vision is focusing on human decision processes and clarifying those values in a quantifiable model. The team has developed an ethical framework and preliminary model of ethical decision making that will be more fully developed with the Air Force Academy (AFA) and Air University (AU). In Year 1, we will articulate the individual psychological characteristic and situational factors impacting ethical dilemmas and develop realistic ethical dilemmas and situations. These scenarios will use computational agents employing AI and military personnel, requiring ethical decisions to be made by personnel in combat and non-combative environments. In year 2, we will develop the Ethical Advisor prototype, test the individual psychological characteristics and situational factors, refine the scenarios, and establish and implement collaborations across different commands/services. In year 3, we will test and integrate the model and Ethical Advisor into a mission system, and conduct joint war game testing.

We are seeking individuals from a variety of educational disciplines (Psychology, Philosophy, Computer Science) with experience in data gathering and summarization techniques, programming, and testing. The gathered data would be used for developing algorithms and programming to begin enabling software to mimic human decision making in complex ethics-laden situations.

Dataset Quality Metric for Object Detection Tasks

Jing Lin
(315) 709-4552
Jing.lin@us.af.mil

Despite the growing trend to dedicate money and resources to produce synthetic data via simulated environments, it remains undetermined if training algorithms on simulated data is an operational advantage to the Air Force. This research topic will develop a dataset quality metric such that a high-scoring dataset correlates to a high likelihood of obtaining a high-performing object detection

model trained on it. This topic is particularly interested in exploring and evaluating the quality of simulated data, the effect of photorealism on model performance, the diversity, coverage, and representativeness of the dataset needed to improve model reliability and resiliency, the transfer learning algorithms on simulated data, algorithms for determining the ideal composition of simulated and real-world data for a user case, and algorithms for guiding edge case development for improving model robustness.

Other topics related to data quality metrics will also be considered.

Feature Extractor for Overhead Images

Jing Lin
(315) 709-4552
Jing.lin@us.af.mil

ResNet, VGG, Inception, and AlexNet are some of the popular models that researchers used as image feature extractors. However, these models are usually pre-trained on ImageNet, which is not in an overhead perspective. Some researchers have fine-tuned these models on overhead imagery [1, 2]. Nevertheless, the attributes such as:

- Scale, rotation, and viewpoint invariance
- Spatial invariance
- Scene/background/context information understanding
- Adaptability and transferability
- Computation resource efficiency

need to be thoroughly studied and further improved. This research topic focuses on developing a state-of-the-art feature extractor for overhead images with these attributes. Some research areas of interest include but are not limited to unsupervised and self-supervised representation learning, such as contrastive learning models, mask image modeling, deep clustering, CLIP model, manifold learning techniques, and zero-shot learners.

[1] Artashes Arutiunian, Dev Vidhani, Goutham Venkatesh, Mayank Bhaskar, Rito-brata Ghosh, and Sujit Pal. 2021. Fine tuning CLIP with Remote Sensing (Satellite) images and captions. **https://huggingface.co/blog/fine-tune-clip-rsicd**

[2] Muhtar, Dilxat, et al. 2023. CMID: A Unified Self-Supervised Learning Framework for Remote Sensing Image Understanding. IEEE Transactions on Geoscience and Remote Sensing.

Information Institute®
26 Electronic Pkwy
Rome, NY 13441
P# 315-330 3251

Approved for Public Release; Distribution Unlimited: Case No. : AFRL-2023-3802,
Dated 4 Aug 2023