Information Institute®

Visiting Faculty Research Program

Summer Faculty Fellowship Program

Research Fellowship Program

2024 Research Topics

Version 1.0

Visiting Faculty Research Program
Summer Faculty Fellowship Program
Research Fellowship Program

2024 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**

Mathematical Theory for Advances in Machine Learning and Pattern Recognition

Ashley Prater-Bennette
(315) 330-2804
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 extraction of intelligence from large amounts of 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 pattern recognition with a special emphasis techniques that admit sparse, low-rank, overcomplete, or hierarchical methods on multimodal data. Research may be performed in, but not limited to: sparse PCA, generalized Fourier series, low-rank approximation, tensor decompositions, and compressed sensing. 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.

Optimal Routing for Dynamic Demand in Networks with Limited Capacity

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

Hierarchical network structures are known to facilitate efficient transport of materiel under constrained flow capacities. If the demand remains consistent over time, tree-like structures are optimal, however, under dynamic resource gathering and demands the emergence of loops are likely to play a crucial role in enabling flexible adaptation to changing signals. We seek to explore mathematical frameworks for studying the efficient flow of materiel over networks through the development of routing protocols and network optimization strategies. Given an existing graph, we seek to study optimization problems that involve the delivery of resources initially located on one set of nodes to demand signals at another set. These basic network flow optimization problems have applications in logistics and the wider command and control structure, where the flow can range from materiel to influence and information.

Feature Synchronization of High Dimensional Information States

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

Synchronization has been studied extensively in the context of coupled oscillatory systems, e.g. linearly coupled Lorenz attractors, but many more general AF relevant applications of synchronization can involve slower dynamics on high dimensional information states. In such cases, including distributed sensor networks and/or databases used for online Machine Learning applications, it is likely more important to maintain synchrony of large-scale features of the information states rather than requiring fully synchronized copies. Using coarse-grained quantities, e.g. informativeness or cluster coherence, we seek to identify the minimal amount of information passing between networked nodes (relying on concepts like symbolic dynamics and transfer entropy) that can maintain synchrony of such features within a given tolerance over time. An interesting application that might be useful in bridging the two paradigms is the maintenance of a genetically viable population of endangered species living in separated fractured habitats. The genetic basis for this application allows for direct comparison with the symbolic dynamics approaches of oscillatory dynamics, while enabling a transition to a slow changing, but truly high dimensional state space, where distribution of SNPs might provide a good target for synchronization.

James Lu
(315) 330-3906
James.Lu@us.af.mil

Our team is seeking advanced Machine Learning (ML) applications to improve the geospatial intelligence (GEOINT) processing. Enhancements in capabilities, such as effectively identifying objects of interest on overhead/satellite imageries and discovering patterns of human behaviors/events though analyzing geological information system (GIS) data, are critical for improving efficiency and decision-making.

Following are the identified topics of interest as being potential high-risk, high-reward research areas.

1) **Novel Methods for Applying Computer Vision to GEOINT:** A key facet of computer vision is object detection - finding objects and their specific location or boundaries within an image. By applying object detection to overhead/satellite imageries can be rapidly and automatically analyzed for infrastructure mapping, anomaly detection, and feature extraction. Advances in detecting difficult to identify objects are of particular interest. In addition, insight into the meaning of GIS observations could be greatly enhanced by incorporating ML models of the environment and common-sense knowledge. Novel approaches to fusing computer vision with semantic models are needed.

   Examples of this topic includes, but not limited to: object detection comprised primarily of linear shapes and computer vision with semantic reasoning for GIS observations.

2) **Techniques for Reasoning across Multiple Data Domains:** Explosive growth in geospatial, temporal, and social media data paired with the development of new ML and visualization technologies have provided an opportunity to fuse disparate data sources into an unparalleled situational awareness platform. Social media outlets increasingly include geolocated evidence in connection with individual activity and correspondence. Innovative techniques for reasoning across social networks within the context of GIS will allow us to model and predict human behaviors/events within complex geographic landscapes.

Example of this topic includes, but not limited to: automation of socio-temporal-geo correlation to drive predictive modeling.

3) **Advances in Synthetic Data Generation:** While there is an abundance of available GIS data, fully aligned and annotated ground truth data for training and testing is difficult to acquire. Methods for rapidly generating realistic geospatial landscapes with known features (infrastructure, anomalies, etc.) and automatically translating such landscapes into realistic satellite collection simulations is needed.

Example of this topic includes, but not limited to: automated generation of aligned data sets across multiple phenomenologies (electrooptical, synthetic aperture RADAR, etc.).

Multi-Domain Mission Assurance

Jason Bryant
(315) 330-7670
Jason.Bryant.8@us.af.mil

In an effort to support the Air Force's mission to develop Adaptive Domain Control for increasingly integrated Mission Systems, we are interested in furthering the identification of problems, and development of solutions, in increasing Full-Spectrum Mission Assurance capabilities across joint air, space, and cyberspace operations. Modern multi-domain mission planning and execution integrates tightly with cyber and information infrastructure. To effectively direct and optimize complex operations, mission participants need timely and reliable decision support and an understanding of mission impacts that are represented and justified according to their own domain and mission context. We are interested in understanding, planning, and developing solutions for Mission Assurance that supports operations requiring Mission Context across multiple domains, and spans both Enterprise and constrained environments (processing, data, and bandwidth). The following topic areas are of interest as we seek to provide solutions that are domain adaptive, mission adaptive, and provide rich, critical situational awareness provisioning to Mission Commanders, Operators, and technologies that support autonomous Mission Assurance.

- Summary, Representation, and Translation of Multi-Domain Metrics of Mission Health - Expansive Mission Assurance requires adequate mechanisms to describe, characterize, and meaningfully translate mission success criteria, mission prioritization, information requirements, and operational dependencies from one domain to another in order to react to events, deliver them appropriately to mission participants, and thereby increase the agility, responsiveness, and resiliency of ongoing missions.
- Multi-Domain Command and Control information Optimization - Currently, information can be disseminated and retrieved by mission participants through various means. Increasingly, mission participants will face choices of what, how, and where information will reach them or be pushed back to the Enterprise. Deciding between C2 alternatives in critical situations requires increased autonomy, deconfliction, qualitative C2 mission requirements, and policy differentials. We are seeking representations, services, configuration management, and policy approaches towards solving multi-domain multi-C2 operations.
- Complex Event Processing for Multi-Domain Missions - The ability to better support future missions will require increased responsiveness to cyber, information, and multi-domain mission dynamics. We are seeking mission assurance solutions that process information event logs, kinetic operation event data, and cyber situational awareness in order to take data-driven approaches to

validating threats across the full-spectrum of mission awareness, and justify decisions for posturing, resource and information management, and operational adjustments for mission assurance.

- Machine Learning for Mission Support - Decreasing the cost and time resource burdens for mission supporting technologies is critical to supporting transitioning to relevant domains and decreasing solution rigidity. To do this requires advanced approaches to zero shot learning in attempts to understand mission processes, algorithms to align active missions with disparate archival and streaming information resources, analysis of Mission SA to determine cross-domain applicability, and autonomous recognition of mission essential functions and mission relevant events. Additionally, ontologies and semantic algorithms that can provide mission context, critical mission analytics relationships, mission assurance provenance and response justifications, as well as mission authority de-confliction for intra-mission processes and role-based operational decisions, are topics that would support advanced capabilities for advanced mission monitoring, awareness, and assurance decisions.

Jeffrey Hudack
(315) 330-4741
Jeffrey.Hudack@us.af.mil

The deployment of many airborne wireless sensors is being made easier due to technological advances in networking, smaller flight systems, and miniaturization of electromechanical systems. Mobile wireless sensors can be utilized to provide remote, persistent surveillance coverage over regions of interest, where the quality is measures as the sum of coverage and resolution of surveillance that the network can provide. The purpose of this research is provide efficient allocation of mobile wireless sensors across a region to maintain continuous coverage under constraints of flight speed and platform endurance. We seek methods for the structuring constraint optimization problems to develop insightful solutions that will maximize persistent coverage and provide analytical bounds on performance for a variety of platform configurations.

Multi-Resolution Modeling and Planning

Jeffrey Hudack
(315) 330-4877
Jeffrey.Hudack@us.af.mil

Modeling and simulation is a powerful tool, but must be calibrated to a level of detail appropriate for the current planning objective. Tools that provide high fidelity modeling (flight surfaces, waypoint pathing, etc..) are appropriate for tactical scenarios, but at the strategic level representing every platform and resource at high fidelity is often too complex to be useful. Conversely, lower fidelity simulation can provide strategic assessment, but lacks the specific space and timing detail to be used for issuing orders to elements. We seek to develop and demonstrate methods for multi-resolution modeling and planning, bridging the gap between multiple levels of representation that can support abstraction and specialization as we move between the different fidelities of action. Areas of interest include Automated Planning, Modeling and Simulation, Discrete Optimization and Machine Learning.

Automated Planning Decision Support with Uncertainty

Jeffrey Hudack
(315) 330-4877
Jeffrey.Hudack@us.af.mil

Automated planning generates valid action sequences for problems with clearly defined goals, resources, constraints and dependencies. For military applications, any proposed plan must be human understandable and communicated clearly to command staff to motivate action. Leveraging these techniques to support human decision-making will likely require methods for human planners to explore, customize and compare plan options in the context of the problem being solved. There are additional challenges with planning for real-world problems that include interpreting and solving large-scale problems and uncertainty about the state of the environment. We seek to develop and demonstrate methods for automated planning to guide and evolve with human decision-making processes in complex problem spaces. Areas of interest include Automated Planning, Data Mining, Discrete Optimization, and Robust Optimization.

Jessica Dorismond
(315) 339-2168
Jessica.Dorismond@us.af.mil

A key concern for the Air Force and Joint Force is the ability to leverage multi-domain (MD) operations. There is a fundamental lack of understanding about how to measure, analyze, and quantify the imposition of MD actions to maximize operational effects. In this research, we seek to examine decision processes, given some mathematical representation, in which we impose prescribed courses of action. The purpose is to understand the influencing of behaviors, reshaping of expected traversals, and maximizing of desired outcomes. Our goal is to investigate novel approaches and explore various modes of analysis that aid in the development of a scheme for classifying the sets of actions into varying levels or notions of complexity. Some areas of interest include stochastic optimization, game theory, complexity theory, graph theory, and complex adaptive systems.

Measuring Decision Complexity for Military Scenarios

Jessica Dorismond
(315) 339-2168
Jessica.Dorismond@us.af.mil

The goal of this research is to develop metrics that quantify the complexity of an adversary decision-making process, as well as measure complexity imposed on an adversary by United States Air Force (USAF) actions. The goal is to define potential complexity metrics to assess the state of an adversary decision system before and after an attack, model the impacts of complexity imposition on an adversary's decision system to develop analytical assessments strategies, and to compare the relative efficiency of different military actions. The analysis will provide as a means for assessing and quantifying the value of different military actions against an adversary. The end goal is to provide new insights into using complexity as a measure of how effective a military action will be in a military conflict. Some areas of interest include operations research, stochastic optimization, game theory, complexity theory, graph theory, and complex adaptive systems.Persistent Sensor Coverage for Swarms of UAVs

Jessica Dorismond
(315) 330-2168
Jessica.Dorismond@us.af.mil

Data-Efficient Machine Learning

Lee Seversky
(315) 330-2846
Lee.Seversky@us.af.mil

Many recent efforts in machine learning have focused on learning from massive amounts of data resulting in large advancements in machine learning capabilities and applications. However, many domains lack access to the large, high-quality, supervised data that is required and therefore are unable to fully take advantage of these data-intense learning techniques. This necessitates new data-efficient learning techniques that can learn in complex domains without the need for large quantities of supervised data. This topic focuses on the investigation and development of data-efficient machine learning methods that are able to leverage knowledge from external/existing data sources, exploit the structure of unsupervised data, and combine the tasks of efficiently obtaining labels and training a supervised model. Areas of interest include, but are not limited to: Active learning, Semi-supervised leaning, Learning from "weak" labels/supervision, One/Zero-shot learning, Transfer learning/domain adaptation, Generative (Adversarial) Models, as well as methods that exploit structural or domain knowledge.

Furthermore, while fundamental machine learning work is of interest, so are principled data-efficient applications in, but not limited to: Computer vision (image/video categorization, object detection, visual question answering, etc.), Social and computational networks and time-series analysis, and Recommender systems.

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.

Mission Driven Enterprise to Tactical Information Sharing

Matthew Paulini
(315) 330-3330
Matthew.Paulini.1@us.af.mil

Forward deployed sensors, communication, and processing resources increase footprint, segregate data, decrease agility, slow the speed of command, and hamper synchronized operations. Required is the capability to dynamically discover information assets and utilize them to disseminate information across globally distributed federations of consumers spread across both forward-deployed tactical data links and backbone enterprise networks. The challenges of securely discovering, connecting to, and coordinating interactions between federation members and transient information assets resident on intermittent, low

bandwidth networks need to be addressed. Mission prioritized information sharing over large-scale, distributed, heterogeneous networks for shared situational awareness is non-trivial. The problem space requires investigation, potential solutions and technologies need to be identified, and technical approaches need to be articulated which will lead to capabilities that enable forward deployed personnel to reach back to enterprise information assets, and allow rear deployed operators the reciprocal opportunity to reach forward to tactical assets that can address their information needs.

- Anticipating versus Reacting - Conditions in real-world environments are dynamic - threats emerge and may be neutralized, opportunities appear without warning, etc. - and robust autonomous agents must be able to act appropriately despite these changing conditions. To this end, we are interested in identifying events which signal that a change must be made in one agent's behavior by mining past data from a variety of sources, such as its own history, messages from other autonomous agents, or other environmental sensors. This capability would allow agents to learn to anticipate and plan for scenario altering events rather than reacting to them after they have already occurred.

Blockchain-based Information Dissemination Across Network Domains

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

While crypto currency research has been around for decades, Bitcoin has gained a significant adaptation in recent years. Besides being an electronic payment mechanism, Bitcoin's underlying building blocks known as Blockchain, has profound implications for many other computer security problems beyond cryptocurrencies such as a Domain Name System, Public Key Infrastructure, filestorage and secure document time stamping. The purpose of this topic is to investigate Blockchain technologies, and develop decentralized highly efficient information dissemination methods and techniques for sharing and archiving information across network domains via untrusted/insecure networks (internet) and devices.

Areas of consideration include but are not limited to: security design and analysis of the state of the art open source Blockchain implementations (e.g., IOTA), developing the theoretical foundation of Blockchain-based techniques for different application domains, block editing, and smart contracts in such application domains.

Secure Function Evaluation for Time-Critical Applications:

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

Secure Function Evaluation (SFE) enables two participants (sender and receiver) to securely compute a function/exchange data without disclosing their respective data. Garbed Circuit (GC) has been proposed to address this problem. State-of-the-art solutions for implementing GC employ Oblivious Transfer (OT) algorithms and/or Predicate Based Encryption (PBE) based on Learning With Errors (LWE) algorithms. The performance of these solutions are not practical for time-critical applications. Existing GC-based SFE protocols have not been explored for applications with multiple participants in controlled/managed settings (i.e., event-based systems/publish and subscribe) where the circuit construction can be simplified with a limited set of gates (e.g., AND, OR, and/or NAND) while excluding the inherent complexity for the arithmetic operations (Addition and Multiplications). Areas of consideration under this research topic

include developing and implementing time-constraint cryptographic protocols using universal GC for a given applications type with relaxed constraints.

Automated Threat Modeling and Attack Prediction for Cloud Computing Systems and Software

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

Traditional threat modeling schemes for a given software is typically developed from the software architecture diagrams and the subsystems (network topology) which is very effective when the applications are within the organizational boundaries. However, cloud-native software applications evolve over time by following the Continuos Integration and Continuous Development, referred to CI/CD, best practices to support the ever changing demand of the businesses with the help of the dynamicity of the underlying cloud infrastructure deployment service models (Iaas, Paas, SaaS, FaaS, VMs, Containers). Thus, the prescribed CI/CD architecture does not reflect the descriptive architecture of the software (i.e., initial Docker image) and all its interacting subsystems (Services, Docker swarms, etc.), thereby, ineffective for exiting thread modeling and attack prediction techniques.

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

1) Developing a sound theoretical foundation for modelling threats on dynamic cloud computing systems and a practical Automated Threat Modelling Framework (ATMF).
2) Practical machine learning models for attack prediction driven by the ATMF data sets.

Decentralized Secure Information Dissemination Middleware

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

The current Information Management (IM) systems design practices are based on a centralized middleware services that mediate information exchanges between data producers and consumers. Typically, the IM services are protected with a perimeter/defense-in-depth security approach with specialized hardware in a private network assuming both the nodes deployed on the services and users are trustworthy. However, this is proven to be ineffective to address future secure information dissemination challenges in highly contested environments. One promising approach of a growing significance in recent years is Decentralized Application design practices, referred to as DApps, with Zero-Trust (ZT) security model. ZT is an evolving set of cybersecurity paradigms that shifts from the centralized application security schemes to securing users, assets, and resources in segregated and decentralized fashion. Topics of interest include but are not limited to:

- Decentralized middleware application design and implementation methodologies.
- Zero-Trust security model for time-sensitive information producer and consumer interaction.
- Smart-contract based security policy enforcement model.
- Decentralized data oracle framework linking external data to the smart contracts.
- Decentralized secure file storage and query repository model that can utilize public hyper ledgers.

Ralph Kohler
(315) 330-2016
Ralph.Kohler@us.af.mil

This in-house research effort focuses on working on the Android Tactical Assault Kit (ATAK), which is an extensible, network-centric Moving Map display with an open Application Programming Interface (API) for Android devices developed by Air Force Research Laboratory (AFRL). ATAK provides a mobile application environment where warfighters can seamlessly exchange relevant Command and Control (C2), Intelligence Surveillance and Reconnaissance (ISR), and Situational Awareness (SA) information for domestic and international operations. This capability is key to the Department of Defense's (DoDs) goal of digitizing the Air Force for MDC2 efforts because it serves as the backbone for connecting numerous platforms, people, and information sources.

Efficient Transfer Learning in Reinforcement Learning (RL) Domains

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

Reinforcement learning (RL) model has achieved impressive feats in simulation (e.g., low-fidelity physics-based simulator) but has been a challenge when transferring into high-fidelity physics-based simulator/real world scenarios. To train an RL based model, it needs enough samples to produce impressive results. Therefore, it poses two challenges when transferring into high-fidelity physics-based simulator/real world scenarios: a) generating samples every time to run on an RL based model are computationally expensive and can cause policies (i.e., maps perceived states to actions to be taken in those states) to fail at testing b) it does not make sense to train policies separately to accommodate all the environments that an agent may see in high-fidelity physics-based simulator/real world. As a result, under this topic, we seek novel projects to understand the following issues:

1) Novel algorithm to perform transfer learning efficiently from low-fidelity to high-fidelity physics-based simulator or the real world
2) Novel experimental design for an effective transfer learning by measuring jumpstart, asymptotic performance, total reward, transfer ratio and time to threshold.
3) How to fuse uncertainty-aware neural network models with sampling-based uncertainty propagation in a systematic way
4) How to effectively perform transfer learning between a low fidelity to high fidelity physics-based simulator with minimally similar observational spaces and dynamic transitions

Explainable Reinforcement Learning (XRL)

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

The demand for explainable Reinforcement Learning (RL) has been increased due to its ability to become a powerful and ubiquitous tool to solve complex problems. However, RL exhibits one of the problematic characteristics: an execution-transparency trade off. For instance, the more complicated the inner workings of a model, the less clear it is how the predictions/decisions are made. Since the RL model learns autonomously, the importance of the underlying reason of each decision becomes imperative for gaining trust between an agent and a user, which is based on the success or failure of the model. The problem with current XRL is that most of the methods do not design an inherently simple RL model, instead, they imitate

and simplify a complex model, which is cumbersome. Furthermore, XRL methods often ignore the human aspect of the field such as behavioral and cognitive science or philosophy by not taking them into account in XRL. Therefore, we seek novel projects to understand the following issues:

1) Provide experimental design to explain end goals by developing world models, counterfactuals (what-if) to build trust between an agent and a user, and adversarial explanations to provide validity of the surroundings.

2) Develop a novel algorithm to be able to accurately provide why each decision/prediction is made by the model.

Computing & Communications (AFRL/RIT)

Optimization for Data Analysis

Donald Telesca
(315) 330-3606
Donald.Telesca@us.af.mil

In aerospace systems, there is a growing gap between the amount of data generated and the amount of data that can be stored, communicated, and processed. Moreover, this gap keeps widening. One promising approach to solving this problem is to utilize optimization to reliably extract patterns for large scale data. This topic addresses the theory and application of optimization for pattern analysis. This includes the development of:

- An optimization-based theoretical framework for pattern analysis. Some promising directions are based in part on the study of multilevel and nonconvex optimization.
- Paradigms based on the idea that accuracy can be enhanced for many important problems (including important nonconvex problems) by utilizing their common geometric structures, while exploiting approximation theory to yield speed improvements.
- Optimization applications to permit novel computational paradigms, such as computation of numerical rank, which is critically important for machine learning and signal processing.

Dynamic Resource Allocation in Airborne Networks

Elizabeth 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

Erin Tripp
(315) 330-2483
Erin.Tripp.4@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.

Wireless 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. Many of these techniques are known however there is little commercial demand for products that are difficult and time consuming to reprogram no matter how much security they provided. As a result 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

Kathy-Anne Soderberg
(315) 330-3687
Kathy-Anne.Soderberg@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

Kathy-Anne Soderberg
(315) 330-3687
Kathy-Anne.Soderberg@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.

Quantum Information Processing

Michael Fanto
(315) 330-4682
Michael.Fanto@us.af.mil

The topic of Quantum Information Processing and quantum photonic enabling components covers computational methods, entanglement characterization, methods for large scale entanglement generation, and device architectures. It has been well established that a computer based on quantum interference could offer significant increases in processing efficiency and speed over classical versions, and specific algorithms have been developed to demonstrate this in tasks of high potential interest such as data base searches, pattern recognition, and unconstrained optimization.

The experimental progress is rapidly catching up to the theoretical research as these small-scale devices, which are demonstrating quantum processes, continue to grow in their number of available qubits. The focus of this research is the generation, manipulation, and characterization of entangled photon states for quantum information processing, quantum networking, entanglement distribution, and heterogeneous qubit integration. The research focuses strongly on integrated photonics and expertise in this area is beneficial.

Theoretical advances will also be pursued with existing and custom quantum simulation software to model computational speedup, error correction, de-coherence effects, and modeling physical devices to fabricate. Algorithm investigation will focus on hybrid approaches which simplify the physical realization constraints and specifically address tasks of potential military interest.

Airborne Networking and Communications Links

Michael Medley
(315) 330-4830
Michael.Medley@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 Computing Theory and Simulation

Paul Alsing
(315) 330-4960
Paul.Alsing@us.af.mil

Quantum computing (QC) research involves interdisciplinary theoretical and experimental work from diverse fields such as physics, electrical engineering, computer science, and engineering and from pure and applied mathematics. Objectives of AFRL's Quantum Information Science (QIS) Branch include the development of quantum algorithms with an emphasis on large scale scientific computing and search/decision applications/optimization on QC hardware, the simulation of quantum gates/circuits/processing, and quantum entanglement schemes with an emphasis on modeling experiments. Topics of special interest include the cluster state quantum computing paradigm, quantum simulated annealing, NISQ-based quantum algorithms, the behavior of quantum information and entanglement under arbitrary motion of qubits, measures of generation and detection of quantum entanglement, and the distinction between quantum and classical information and its subsequent exploitation.

Ryan Luley
(315) 330-3848
Ryan.Luley@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.

Many-Node Computing for Cognitive Operations

Thomas Renz
(315) 330-3423
Thomas.Renz@us.af.mil

The sea of change in computing hardware architectures, away from faster cycle rates and towards processor parallelism, has expanded opportunities for development of large scale physical architectures that are optimized for specific operations. Porting of current cognitive computing paradigms onto systems composed of parallel mainstream processors will continue in the commercial world. What higher cognitive functionality could we achieve if we take better advantage of physical capabilities enabled by new multi-processor geometries?

Perception, object recognition and assignment to semantic categories are examples of lower level cognitive functions. Assignment of valence, creation of goals and planning are mid level functions. Self awareness and reflection are higher level processes that are so far beyond current cognitive systems that relatively little has been done to model the processes. Often, models assume higher cognitive processes will emerge, once the computing system reaches some level of speed/complexity. The problem is that the computational power required exceeded the reachable limit of single processor architectures and probably exceeds the limits of conventional parallel architectures. This topic seeks to enable mid and higher level cognitive function by creation of new physical architectures that address the computation demand in novel ways.

We are interested in developing models for the computational scale of the mid and higher functions and processor / memory node architectures that facilitate cognitive operations by configuring the physical architecture to closely resemble the functional cognitive architecture, e.g., where each node in a network represents and functions as a processor for a single semantic primitive. What new hierarchical architectures could we design for million node systems, where the individual nodes may be small ASPs, with very fast communication between nodes? A project of interest would combine both sides, new algorithms for higher level cognitive functions and new architectures to enable the computation in a realistic time frame. AFRL/RIT has projects on line to enable million node systems.

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.

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.

Next Generation Wireless Networking: 5G Mesh Networking

Amjad Soomro
(315) 330-4694
Amjad.Soomro@us.af.mil

5G networks have introduced innovative concepts such as Non-Terrestrial Networks (NTN) , Integrated Access and Backhaul (IAB), virtual Radio Access Networks (vRAN) and Network Slicing (NS). These concepts make it possible, in unified communication infrastructure, to provide multiple customized networks over terrestrial and aerial domains.

The topic seeks highly motivated research on how 5G and its enabling technologies – virtual Radio Access Networks (vRAN), Integrated Access and Backhaul (IAB), Software Defined Networking (SDN), Network Function Virtualization (NFV), cloud infrastructure along with network management and orchestration – can support dynamic, resilient local and global communications. For example, high level network control makes it possible for network designers to specify more complex tasks that involve integrating many disjoint network functions (e.g., security, resource management, and prioritization, etc.) into a single control framework, which enables: (1) robust and agile network reconfiguration and recovery; (2) flexible network management and planning; and, in turn, (3) improvements in network efficiency and controllability.

Emerging 5G Technologies for Military Applications

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

5G- to-Next-G (5G-XG communications and network technologies can be leveraged to enhance military communication capabilities. In particular, 5G- XG -enabling technologies are envisioned to provide higher data rates, lower latency, lower power consumption, security enhancements and ubiquitous access including non-terrestrial links. The three major use case domains of 5G-XG —enhanced mobile broadband (eMBB), ultra-reliable low latency communication (URLLC) and massive machine type communications (mMTC)—provide the opportunity to harness commercial technology for future AF use cases such as smart bases, self-driving vehicles, augmented and virtual reality technologies for training, dynamic spectrum management and sharing technologies to facilitate coexistence of commercial and military spectrum dependent systems (SDSs). The 5G-XG research areas of interests for this topic include but not limited to:

- Dynamic spectrum management and sharing with unlicensed and shared bands
- Aerial Internet of Things (IoT)
- Waveform design for enhanced security and high mobility
- Small cell mission scenarios
- AI and ML enhanced/incorporated spectrum management, dynamic sensing and sharing
- Smart base/smart port use cases with small cell, V2X, low power and localization technologies
- Advanced physical layer techniques such as carrier aggregation, full-duplex and massive MIMO
- Beamforming and adaptive nulling for interference tolerance and spectrum sharing/co-existence
- Millimeter-wave and terahertz band communications
- Spectrum-sharing-by-Design for the Internet of Things
- Shapeshifting Neural Networks for Effective, Efficient and Secure Hardware-based Inference
- Edge-Assisted Task Offloading Through Real-Time Deep Reinforcement Learning
- Quality of Service (QoS) enhancement via Non-terrestrial Networking (NTN)

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).

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.

Information Exploitation & Operations (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.

Machine Learning Applications for Geospatial Intelligence Processing

Bernard Clarke
(315) 330-2106
Bernard.Clarke@us.af.mil

Audio & Acoustic Processing

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

AFRL/RIGC is involved in all aspects of researching and developing state of the art audio and acoustical analysis and processing capabilities, to address needs and requirements that are unique to the DoD and intelligence communities. The group is a unique combination of linguists, mathematicians, DSP engineers, software engineers, and analysts. This combination of individuals allows us to tackle a wide spectrum of topics from basic research such as channel estimation, robust word recognition, language and dialect identification, and confidence measures to the challenging transitional aspects of real-time implementation for speech; as well as detecting, tracking, beamforming and classifying specific acoustical signatures in dynamic environments via array processing. AFRL/RIGC also has significant thrusts in noise estimation and removal (both spectral and spatial), speaker identification including open-set identification, acoustical identification, keyword spotting, robust feature extraction, language translation, analysis of stressed speech, coding algorithms along with the consequences of the compressions schemes, watermarking, co-channel mitigation, and recognition of background events in audio recordings. 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 such as SID, LID, GID, etc.

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.

Application of Game Theory and Mechanism Design to Cyber Security

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

Cyber attacks pose a significant danger to our economic prosperity and national security whereas cyber security seeks to solidify a scientific basis. Cyber security is a challenging problem because of the interconnection of heterogeneous systems and the scale and complexity of cyberspace. This research opportunity is interested in theoretical models that can broaden the scientific foundations of cyber security and develop automated algorithms for making optimum decisions relevant to cyber security. Current approaches to cyber security that overly rely on heuristics have been demonstrated to have only limited success. Theoretical constructs or mathematical abstractions provide a rigorous scientific basis for cyber security because they allow for reasoning quantitatively about cyber attacks.

Cyber security can mathematically be modeled as a conflict between two types of agents: the attackers and the defenders. An attacker attempts to breach the system's security while the defenders protect the system. In this strategic interaction, each agent's action affects the goals and behaviors of others. Game theory provides a rich mathematical tool to analyze conflict in strategic interaction and thereby gain a deep understanding of cyber security issues. The Nash equilibrium analysis of the security games allows the defender to allocate cyber security resources, understand how to prioritize cyber defense activities, evaluate the potential security risks, and reliably predict the attacker's behavior.

Securing cyberspace needs innovative game theoretic models that consider practical scenarios such as: incomplete information, imperfect information, repeated interaction and imperfect monitoring. Moreover, additional challenges such as node mobility, situation awareness, and computational complexity are critical to the success of wireless network security. Furthermore, for making decisions on security investments,

special attention should be given to the accurate value-added quantification of network security. New computing paradigms, such as cloud computing, should also be investigated for security investments.

We also explore novel security protocols that are developed using a mechanism design principle. Mechanism design can be applied to cyber security by designing strategy-proof security protocols or developing systems that are resilient to cyber attacks. A network defender can use mechanism design to implement security policies or rules that channel the attackers toward behaviors that are defensible (*i.e.*, the desired equilibrium for the defender).

Cyber Security Research and Applications for Cyber Defense

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

The Air Force's mission to fly and fight in Air, Space, and Cyberspace involve the technologies 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.

Economics, a study of resource allocation problems, has always been a factor in engineering, and promises to address many issues surrounding the management and operation of large-scale information systems. The introduction of mobile agents, autonomy, computational economy, pricing mechanisms, and game theory mechanisms in a virtual domain such as cyberspace may unveil the same set of phenomena as seen in real domains. Studying these from an economics perspective may provide insights related to cyberspace's arbitrary scale, heterogeneity of resources, decentralized operation, and tolerance in presence of vulnerability.

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, and 4) reconstitute systems, data, and information from different domains rapidly to avoid disruptions.

Fundamental research areas of interest within this topic include:

- Design of systems composed of both trusted and untrusted hardware and software; study of virtualization of hardware components and platforms with configurability on-the-fly.
- Mathematical concepts and distinctive mechanisms that enable systems to automatically continue correct operation in the presence of unanticipated input or an undetected bug or vulnerability.
- Examination of assumptions, mechanisms, and implementations of security modules with capability to rewrite itself without human interactions in the presence of unwanted/unanticipated configurations.
- Information theory and category theory describing interactions of systems of systems that lead to better consideration of their emergent behaviors during attack and reconstitution; models used to predict system responses to malwares and coordinated attacks as well as analyses of self-healing systems.

- Study and application of emerging security technologies, such as blockchain.

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

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
(315) 330-2561
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 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.

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

SIKE for Post-Quantum Cryptography

Todd Cushman
(315) 533-2265
Todd.cushman@us.af.mil

The study of post-quantum cryptography (PQC) has developed mightily over the past decade, with the National Institute of Standards and Technology (NIST) even holding a contest to standardize a set of PQC algorithms for various cryptographic tasks. While this contest is still ongoing, several promising candidates have been excluded for reasons other than theoretical security. In particular, the Supersingular Isogeny Key Encapsulation (SIKE) has been implemented at the highest level of security while offering quantum computers no advantage over classical computers. Moreover, SIKE is compatible with several other elliptic curve algorithms, hence, is a promising candidate for a hybrid scheme. The advantage of combining PQC and classical cryptography is that it requires less overhaul than replacing classical techniques, while still improving security and eliminating the threat of quantum computers. To date, however, no satisfactory

hybrid schemes exist. The fundamental areas of research related to this project, therefore, can be described in the following steps:

1. Determine parameter sets that allow for seamless interaction between SIKE and other elliptic curve cryptography;
2. Determine how to combine SIKE and classical elliptic curve cryptography to maintain efficiency and security;
3. Discover efficient algorithms to generate instances of SIKE;
4. Determine parameter sets that allow for adaptations of SIKE to lightweight devices;
5. Study the practical implementations of SIKE and their resilience against side-channel attacks. Development of new cryptographic methods are not of interest under this topic.

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.

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

Neuromorphic Computing

Clare Thiem
(315) 330-4893
Clare.Thiem@us.af.mil

Qing Wu
(315) 330-3129
Qing.Wu.2@us.af.mil

The high-profile applications of machine learning (ML)/AI, while impressive, are a) not suitable for Size, Weight, and Power (SWaP) limited systems and b) not operable without access to "the cloud." Neuromorphic computing is one of the most promising approaches for low-power, non-cloud-tethered ML, potentially operable down at the sensor level, also called "edge computing," \ because it implements aspects of biological brains, e.g., trainable networks of neurons and synapses, in non-traditional, highly parallelizable, reconfigurable hardware. As opposed to typical ML approaches today, our research aims for "the physics of the device" to perform the computations and for the reconfigurable hardware itself to be the ML algorithm. This research effort encompasses mathematical models, hardware characterization, hardware emulation, hybrid 46 VLSI CMOS architecture designs, and algorithm development for neuromorphic computing processors. We are particularly interested in approaches that exploit the characteristic behavior of the physical hardware itself to perform computation, e.g., optics, memristors/ReRAM, metamaterials, nanowires. 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.

Multi-sensor and Multi-modal Detection, Estimation and Characterization

Schrader, P.
(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, and Intelligence (C4I) personnel/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 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 and data from the sensed environments and domains ultimately generating a cohesive situational awareness of the complete mission space. The fundamental research objectives under this topic 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, and explainability. We are interested in advancements 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 smart computational nodes and centralized/distributed processing to obtain desired deployment/transitional thresholds.

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.

Robust Adversarial Resilience

Benjamin Ritz
(315) 330-4173
Benjamin.Ritz@us.af.mil

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.

Analyzing Collateral Damage in Power Grids

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

Reliability assessment in distribution of power grids has played an important role in systems operation, planning, and design. The increased integration of information technology, operational technology, and renewable energy resources in power grids have led to the need of identifying critical nodes whose compromise would induce cascading failures impacting resilience and safety. Several approaches have been proposed to characterize the problem of identifying and isolating the critical nodes whose compromise can impede the ability of the power grid to operate. The goal of this research is to develop a computational model for the analysis of collateral damage induced by the disruption of critical nodes in a power grid. The proposed model must provide strategic response decision capability for optimal mitigation actions and policies that balance the trade-off between operational resilience and strategic risk. Special consideration will be given to proposals that include and are not limited to data-driven implementation, fault graph-based model, cascading failure model, among others.

Modeling Battle Damage Assessment

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

Combat Assessment is the determination of the overall effectiveness of force employment during military operations. Combat Assessment provides key decision makers the results of engaging a target and consists of four separate assessments: Battle Damage Assessment (BDA), Collateral Damage Assessment, Munitions Effectiveness Assessment, and Re-attack Recommendations. BDA is the core of combat assessment and is a necessary capability to dynamically orchestrate multi-domain operations and impose

complexity on the adversary. The goal of this effort is to research methods to model complex and evolving systems from incomplete, sparse data to support BDA uses cases. Emphasis will be given to models which accurately reflect the underlying physics and other domain specific constraints of systems. Of additional interest is the development of domain-aware graph analysis techniques for assessing resiliency of adversary systems, multi-INT data fusion to address gaps in data, and analytic process automation.

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

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.

Adaptable Methods for Applying and Understanding Artificial Intelligence and Machine Learning

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

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

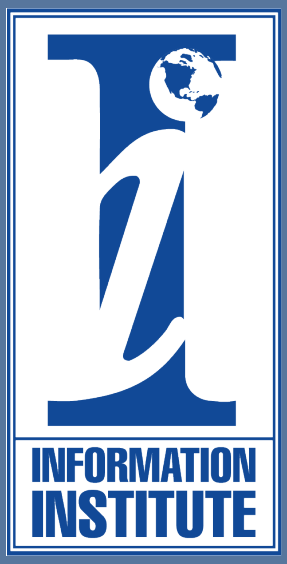
Tim Kroecker
(315) 330-4125
Timothy.Kroecker@us.af.mil

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.



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