SPAWAR
Systems Center
PACIFIC

TECHNICAL DOCUMENT 3386
October 2018

Report on the Second Annual Workshop on Naval Applications of Machine Learning

Katie Rainey
Josh Harguess

SSC Pacific
San Diego, CA 92152-5001

SSC Pacific
San Diego, California 92152-5001

M. K. Yokoyama, CAPT, USN
Commanding Officer

W. R. Bonwit
Executive Director

ADMINISTRATIVE INFORMATION

The work described in this report was performed by the Advanced Analysis Systems Branch (Code 56220) of the Advanced Intelligence, Surveillance and Reconnaissance Division (Code 56200), Space and Naval Warfare Systems Center Pacific (SSC Pacific), San Diego, CA. Funding for this Technology Transition project was provided by the Naval Innovative Science and Engineering (NISE) Program at SSC Pacific.

Released by
Matthew C Bowes, Head
Advanced Analysis Systems Branch

Under authority of
Bryan W. Tollefson, Head
ISR Division

EXECUTIVE SUMMARY

The second annual workshop on Naval Applications of Machine Learning (NAML) was held February 13–15, 2018, at the Space and Naval Warfare (SPAWAR) Systems Center Pacific (SSC Pacific), a U.S. Navy research laboratory in San Diego, California, USA. The workshop events included invited speakers, demonstrations, discussion sessions, and oral and poster presentations. The workshop co-chairs were Josh Harguess and Katie Rainey, both from SSC Pacific. The poster presentations were coordinated by Chris Ward also from SSC Pacific. This report discusses the motivation, goals, and impact of the workshop and highlights some of the topics covered. It also includes photographs taken at the workshop, the full agenda, and abstracts describing many of the oral and poster presentations.

This page is intentionally blank.

ACRONYMS

3D	Three Dimensional
AI	Artificial Intelligence
AMRDEC	Aviation and Missile Research, Development, and Engineering Center (Army lab based in Huntsville, AL)
APL-UW	University of Washington Applied Physics Laboratory (University affiliated research center based in Settle, WA)
ArcGIS	Geographic Information System
ARL	Army Research Laboratory (Army lab based in Adelphi, MD)
ATE	Automatic Test Equipment
ATML	Automatic Test Markup Language
BCI	Brain Computer Interfaces
CID	Combat Identification
C-ISR	Counter-Intelligence Surveillance and Reconnaissance
CL	Causal Learning
CNN	Convolutional Neural Network
COCO	Common Objects in Context
COTS	Commercial off the Shelf
CTAP	Common Tactical Air Pictures
DAG	Directed Acyclic Graphs
DCL	Detection, Classification, and Localization
DCNN	Deputy Chief of Naval Personnel
DIUx	Defense Innovation Unit Experimental
DNN	Deep Neural Network
DoD	Department of Defense
DoN	Department of the Navy
EEG	Electroencephalography
EMG	Electromyography
EMR	Electronic Medical Record
EO	Electro-Optic
EW	Electronic Warfare
FCN	Fully Convolutional
FEC	Forward Error Correction
GA	Genetic Algorithm
GPS	Global Positioning System
GPU	Gas Particulate Unit
GSD	Ground Sample Distance
GUI	Graphical User Interface
HDCA	Hierarchical Discriminant Component Analysis
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
IQR	Interactive Query Refinement
ISM	Integrated Sustainment Maintenance
ISR	Intelligence, Surveillance, and Reconnaissance

JAIC	Joint Artificial Intelligence Center
LLA	Lexical Link Analysis
LoD	Linked Object Data
LOS	Line of Sight
LOTIS	Library of Typical Infrasonic Signals
LSTM	Long Short-term Memory
mAP	mean Average Precision
MDP	Markov Decision Process
ML	Machine Learning
MLA	Machine Learning Algorithms
MLO	Mine Like Objects
NAML	Naval Applications of Machine Learning
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Engineering Education Consortium
NAWCAD	Naval Air Warfare Center Aircraft Division (Navy labs based in Patuxent River, MD)
NGA	National Geospatial-Intelligence Agency
NHRC	Naval Health Research Center (Navy lab based in San Diego, CA)
NIDS	Network Intrusion Detection System
NMT	Neural machine translation
NN	Neural Network
NR&DE	Naval Research and Development Establishment (Consortium of US Navy Laboratories)
NREIP	Naval Research Enterprise Internship Program
NRL	Naval Research Laboratory (Navy lab based in Washington, DC)
NSWC	Naval Surface Warfare Center (Navy labs based in Crane, IN; Dahlgren, VA Port Hueneme, CA, and elsewhere)
NUWC	Naval Undersea Warfare Center (Navy labs based in Keyport, WA and Newport, RI)
OODA	Observe-Orient-Decide-Act
ORCA	Cyber Analytics
OUSD(I)	Office of the Undersecretary of Defense for Intelligence
PCA	Principal Component Analysis
PEO IWS	Program Executive Office, Integrated Warfare Systems (Navy program office based in Washington DC)
PSO	Particle Swarm Optimization
RC	Reserve Component
ReLU	Rectified Linear Units
RF	Radio Frequency
RGB	Red Green Blue
RNN	Recurrent Neural Network
SC	Supercomputing
SDG	Sustainable Development Goal
SEI	Carnegie Mellon Software Engineering Institute (Federally funded research and development center based in Pittsburgh, PA)
SISO	Single

SMART	Science, Mathematics And Research for Transformation (DoD scholarship program)
SMEs	Subject Matter Experts
SMQTK	Social Media Query Toolkit
SMU	Southern Methodist University
SNN	Self-Normalizing
SOC	Security Operations Center
SRDR	Software Resources Data Report
SSC	Space and Naval Warfare (SPAWAR) Systems Center (Navy labs based in San Diego, CA — (Pacific) and Charleston, SC (Atlantic))
SSL	Secure Sockets Layer
SVM	Support Vector Machine
TPSs	Test Program Sets
UAS	Unmanned Aircraft System
UBF	Unified Behavioral Framework
UCLA	University of California, Los Angeles
UCSD	University of California, San Diego
USMC	United States Marine Corps
UxVs	Unmanned Vehicles

This page is intentionally blank.

CONTENTS

EXECUTIVE SUMMARY ..... **iii**
ACRONYMS ..... **v**
1. INTRODUCTION **1**
1.1 OVERVIEW 1
1.2 HISTORICAL FRAMEWORK 1
2. BACKGROUND AND MOTIVATION **3**
3. WORKSHOP OVERVIEW **5**
3.1 AGENDA HIGHLIGHTS 5
3.2 RESEARCH HIGHLIGHTS 5
4. CONCLUSION **9**
4.1 IMPACTS OF NAML 9
4.2 SUMMARY 9
4.3 FUTURE PLANS 9
REFERENCES **11**

APPENDICES

A: NAML PHOTOGRAPHS **A-1**
B: NAML 2018 AGENDAS **B-1**
C: PRESENTATION ABSTRACTS **C-1**

Figures

A-1. Lee Zimmerman, Technical Director, SSC Pacific. A-1
A-2. Lee Zimmerman welcomes attendees to NAML 2018. ..... A-1
A-3. Selected images from the NAML 2018 poster session. A-2
A-4. Ben Migliori presents his work on bio-inspired ML to NAML 2018. ..... A-2
A-5. Justin Mauger leads a tutorial on topological data analysis. A-3
A-6. Tom Schlosser and Joe Drobick lead a demonstration on Navy collaboration tools. 3
B-1. NAML 2018 Agenda. 1
B-2. NAML 2018 Agenda, Roundtable Discussions. 2
B-3. NAML 2018 Agenda, Poster Session 1. 3
B-4. NAML 2018 Agenda, Poster Session 2. 4

This page is intentionally blank.

1. INTRODUCTION

1.1 OVERVIEW

This report is a recounting of the 2018 Naval Applications of Machine Learning (NAML) workshop and its' impacts. The report is organized as follows. After providing an overview of the NAML workshops conducted, Section 2 gives a brief background and the motivation behind NAML. Section 3 gives an overview topics presented at the NAML workshop and a discussion a few selected presentations from the workshop in further detail. In Section 4 we conclude the report by discussing the impact of NAML and future plans for the event. The appendices contain photographs from the workshop (Appendix A), the workshop agenda (Appendix B), and full abstracts from the talks and posters (Appendix C).

1.2 HISTORICAL FRAMEWORK

Machine Learning (ML) and artificial intelligence (AI) are rapidly accelerating fields, with estimated investments into AI startups alone of more than $6 billion over the last three years [1]. The importance of ML and AI with respect to national security has recently been underscored by the creation of the Joint AI Center (JAIC) [2], whose goal is to have oversight over almost all service and defense agency AI efforts and to establish common "standards, tools, shared data, reusable technology, processes, and expertise" for the Department of Defense (DoD). The annual workshop on NAML has been organized and held at Space and Naval Warfare Systems Center (SSC) Pacific twice in the past two years with similar goals to the JAIC and has been seen as a great success in at least starting the conversation in each of the stated goals of the JAIC. This article discusses the motivation, goals, and impact of NAML and highlights some of the topics covered.

SSC Pacific conducts research and development in support of Integrated Command, Control, Communications, Intelligence, Surveillance And Reconnaissance (ISR), cyber, and space systems across all warfighting domains. These mission areas contain a multitude of applications for machine learning, and SSC Pacific's community of machine learning researchers has been actively growing for the past several years.

SSC Pacific hosted first NAML workshop in January, 2017, with the intention of showcasing the work of the machine learning community to a mostly internal audience. As interest grew, participation expanded to other Department of Defense-affiliated laboratories, academia, and industry. The workshop chairs were surprised and encouraged by the large variety of people supporting the Navy in solving problems in these areas. The request for participation for the 2018 workshop was sent to a broad audience. Through improved publicity and more advanced planning (in addition to the explosion of interest in machine learning), attendance increased two-fold over the 2017 workshop, to nearly 400 people, see Appendix A.

This page is intentionally blank.

2. BACKGROUND AND MOTIVATION

As previously mentioned, interest in ML and AI is accelerating and the establishment of the JAIC is the DoD's first step in officially recognizing the importance of this area and their commitment to building and maintaining the ML and AI communities within the DoD. The NAML workshop was one of the first events to provide visibility into ML and AI projects within the Navy and DoD, and no other venue has had such a large and varied audience in attendance. Most projects in ML and AI within the DoD are very small, with common budgets from $100,000 to $500,000 per year and teams of only one to four people. Collaboration opportunities can help researchers on small projects maintain awareness of other related efforts to avoid duplicating efforts and to accelerate their progress. NAML provides a venue for sharing research ideas and results in ML and AI to the broader Navy and DoD communities to provide support to researchers who most likely work on smaller projects with little-to-no DoD-wide visibility.

DoD research efforts are often shared at outside venues such as industry and academic conferences. But there are many unique requirements when applying machine learning to Navy and DoD needs. Data availability and operating conditions, for example, may be significantly different than in industrial applications. The NAML workshop provides a forum at which to discuss approaches to some of these challenges with an audience closely connected to the Warfighter. The goals of NAML are to spread awareness of current machine learning research relevant to Navy applications, to connect machine learning researchers with experts in Navy needs and requirements, and to build and strengthen collaborations within the DoD research community.

Most of the work presented was at the unclassified, publicly releasable level; however, NAML also provides a unique venue for attendees to discuss their work at higher classification levels, which is very uncommon at other venues.

This page left blank intentionally.

3. WORKSHOP OVERVIEW

The NAML workshop welcomed participants from dozens of organizations within the DoD, including many of the laboratories in the Naval Research and Development Establishment (NR&DE), as well as laboratories and commands under the Army, Air Force, Marine Corps, and Intelligence Community. There were also attendees from industry, including traditional defense contractors and other companies, from universities and university-affiliated research centers, and from federally funded research and development centers.

The workshop general chairs were Josh Harguess and Katie Rainey. The poster session was chaired and coordinated by Chris Ward. The session chairs were Jamie Lukos, Mike Walton, John Reeder, Ben Migliori, and Kimberly Ferguson-Walter (National Security Agency). The roundtable discussions and tutorials were led by Justin Mauger , Ben Migliori, Chris Ward, John Reeder, Kristin Lauter (Microsoft Research), Tom Schlosser, Joe Drobick, Mark Iversen, Johnny Phan, Richard Phipps, LCDR Niels Olson (Naval Medical Center San Diego), Luke Overbey (SSC Atlantic), Doug Lange, Keith Anthony (NASIC), Erin Daly, and Mark Owen. All workshop chairs and facilitators were from SSC Pacific, except where noted.

3.1 AGENDA HIGHLIGHTS

The workshop also featured three invited speakers. David Aha from the Naval Research Laboratory (NRL) gave a talk titled "Machine Learning in the Context of Goal Reasoning and Explainable AI." Guna Seetharaman, also from NRL, gave a talk titled Computing Architectures: Post Moore's Law and AI/ML/DL Era. Travis Axtell from the Office of the Undersecretary of Defense for Intelligence gave a talk titled AI Ignition, in which he discussed Project Maven, an effort which is providing computer vision algorithms for object detection, classification, and alerts in video and still imagery.

The main program consisted of short technical talks and poster presentations on wide variety of topics related to machine learning. Most of the presenters shared current research efforts in support of Navy or DoD programs, while some discussed strategic considerations of the Navy with respect to machine learning or related issues. The oral presentations were organized into sessions on the topics of computer vision, autonomy, cognitive electronic warfare, algorithms and theory, and cybersecurity. In Figure 2 on page 6, Ben Migliori gives his presentation on "Bio-inspired Algebraic Topology for Machine Learning." Two additional sessions showcased work by NR&DE researchers on an assortment of topics. Thirty-five short talks were given, and over 50 posters presented, all selected from 110 abstract submissions. See Appendix B for the workshop agenda, and Appendix C for abstracts of the presentations. There are 78 abstracts provided in Appendix B.

3.2 RESEARCH HIGHLIGHTS

The Navy acquires data from a wide variety of sensors, presenting many opportunities for exploitation with machine learning. Several researchers presented their work investigating ways to analyze maintenance data to detect faults or to predict part life cycles. Conventional machine learning methods are used on radar signals to identify behavior changes or to classify emitters. Scheduling algorithms are applied to ship data from Navy ranges and to active sonar arrays. Several other presenters also discussed their work with yet other distinctive data types of interest to the Navy, including infrasonic waves, marine geologic data, atmosphere aerosol data, and side-scan sonar.

Other presentations were about work with data types which are common in work outside of the DoD, but with Navy-specific targets or goals. Some examples include detecting or tracking unmanned aerial vehicles in video, autonomous swarm tactics, sentiment analysis in social media data, classification of cognitive-motor interaction tasks in muscle and brain activity data, and network traffic classification.

Several presenters discussed military-relevant datasets, including a computer vision dataset collected in operational environments, and a set of 3-dimensional point clouds from Navy ships. There was also a presentation on the Defense Innovation Unit Experimental (DIUx) xView 2018 Detection Challenge [3], including a publicly available satellite imagery dataset released by the DIUx and the National Geospatial-Intelligence Agency (NGA).

The Navy is interested in fundamental questions about the capabilities and limitations of machine learning. Several presentations discussed basic and applied research efforts and the ways in which that research advances Navy goals. Some of the work presented was performed by students supporting the Naval Research Enterprise Internship Program (NREIP) and the Science, Mathematics and Research for Transformation (SMART) Scholarship for Service Program. There were also presentations from some of the Navy's academic and industrial partners.

On the final afternoon of the workshop, several tutorials, demonstrations, and discussion sessions were held in two concurrent tracks. Justin Mauger and Benjamin Migliori of SSC Pacific gave a tutorial on topological data analysis and spiking neural nets (see Figure 3 and Figure 4 in Appendix A). Kristin Lauter of Microsoft Research gave a tutorial on homomorphic encryption. Tom Schlosser and Joe Drobick of SSC Pacific gave a demonstration of a suite of Navy collaboration tools (see Figures 3 and 4 in Appendix A). Chris Ward of SSC Pacific demonstrated recent work on microelectronics characterization and analysis. Informal discussion sessions, intended to enable attendees to meet one another and establish collaborations, were held on the topics of autonomy, biologically-inspired machine learning, computer vision, cognitive electronic warfare, cybersecurity, and predictive analytics. While several discussion sessions this afternoon were open only to restricted audiences, the rest of the workshop was held at the unclassified level and was open to all attendees.

The following are some selected presentations from the workshop.

Dean Lee of SSC Pacific presented "Applications of Machine Learning with V-22 Operational Data."

In his work he applies machine learning and data mining to predictive maintenance for the V-22 program [4].

Jennifer Williams of Naval Undersea Warfare Center (NUWC) Keyport Division and Emily Nystrom of SPAWAR Systems Center Atlantic presented their work on obsolescence management in two talks titled "Applying Machine Learning and Data Mining to Obsolescence Management" and "Applications of Random Forests for Modeling Obsolescence", respectively.

Andrew Christianson of Naval Surface Warfare Center (NSWC) Crane Division presented a talk titled "Classification of Radar Signals" [5], while Diego Marez of SSC Pacific presented his recent work on "Electronic Warfare Activity Recognition".

Work by Sandy Kelly of NUWC Keyport Division and Thomas Powers of the University of Washington looked at optimization and scheduling for Navy missions in two presentations titled "Support Vessel Scheduling for Pacific Northwest Test Ranges" and "Avoiding Catastrophes: Worst-Case Optimization with Applications to Multistatic Active Sonar Arrays."

Finally, two presenters focused on underwater applications of machine learning. First, Warren Wood of NRL, Stennis Space Center, MS, presented his work on “Machine Learning Prediction of Seafloor Properties [6].” Second, Daniel Gebhardt of SSC Pacific presented recent work on “Hunting for Naval Mines with Deep Neural Networks” [7].

This page left blank intentionally.

4. CONCLUSION

4.1 IMPACTS OF NAML

Impacts of NAML are several-fold. First, new collaborations between Navy and DoD researchers were formed. These include a data collection for a "military relevant" small robotic platform dataset in real-world degraded environments between SSC Pacific, NRL, and Army Research Laboratory (ARL). This collaboration will directly support a research effort at SSC Pacific to better understand the effects of real-world data on motion estimation from imagery [8, 9]. Another new collaboration was a research proposal on topological data analysis between mathematicians at SSC Pacific and NRL. Additionally, to meet the demands of data-starved machine learning algorithms and the lack of relevant annotated data, a collaboration between NR&DE laboratories was formed to build and maintain a data repository for storing and sharing large datasets between the NR&DE and the larger Navy and DoD communities. Second, the meeting satisfied its main motivation, which was to provide an avenue for Navy and DoD researchers to present and participate in discussions on the applications of machine learning to relevant problems and datasets. While there are other venues to present this type of work, NAML's audience is very unique due to the large attendance by Navy and DoD researchers vice other venues with mostly academic or industry attendees. The third and possibly most important impact of NAML is the establishment of a grassroots-driven Community of Interest (CoI) around the topics of machine learning, computer vision, and artificial intelligence.

It is our intention to continue holding the NAML workshop annually at SSC Pacific, although with a few potential changes and additions. First, due to the popularity and limited space for the event, we will steer the workshop towards specific technology and problem areas for the Navy and accept abstracts in those areas instead of opening the workshop to any application of machine learning. For instance, there was a lot of interest in the use of machine learning on cyber problems, so we will plan to hold a session focused on that area. Second, we plan to hold smaller, more focused workshops whose goal is to tackle, or at least make progress, on a specific problem within the Navy. We hope to have researchers from other Navy labs and organizations lead these workshops and report back their findings to the larger NAML audience each year. At this point, we are planning to run and hold the third annual NAML workshop again at SSC Pacific in February, 2019. For more information or to add your name to our mailing list to be notified about upcoming events, please visit our website[1].

4.2 SUMMARY

SSC Pacific organized and ran the second annual workshop on Naval Applications of Machine Learning (NAML) on February 13–15, 2018. The event was well-attended and was largely considered a great success. This paper is an attempt to summarize the event, impact, and future plans. Many new collaborations were spurred from the event as well as fostering of continuing collaborations.

4.3 FUTURE PLANS

We plan to continue organizing the workshop annually and holding it at SSC Pacific every winter, with the addition of specialized and more focused workshops to be held between the annual events. Events such as this are crucial to the communication of ideas, problems, and solutions between researchers in labs around the Navy and DoD and other organizations.

---

[1] https://sites.google.com/go.spawar.navy.mil/naml2018/ .

This page is intentionally blank.

REFERENCES

1 Agarwal D., J. Bersin, G. Lahiri, J. Schwartz, E. Volini, J. Schwartz, and E. Volini. 2018 “AI, robotics, and automation: Put humans in the loop”. Available online at https://www2 . deloitte.com/insights/us/en/focus/human-capital-trends/2018/ai- robotics-intelligent-machines.html.

2 Sydney J. Freedberg Jr. 2018. “Joint Artificial Intelligence Center Created Under DoD CIO”. Available online at https://breakingdefense.com/2018/06/joint- artificial-intelligence-center-created-under-dod-cio/

3 Darius L., R. Kuzma, K. McGee, S. Dooley, M. Laielli, M. Klaric, Y. Bulatov, and B. McCord. 2018. “xView: Objects in context in overhead imagery”. In: CoRR abs/1802.07856 . arXiv: 1802.07856. URL: http://arxiv.org/abs/1802.07856.

4 D. Lee, V. Siu, R. Cruz, and C. Yetman. 2016.“Convolutional neural net and bearing fault analysis.” In: Proceedings of the International Conference on Data Mining (DMIN). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). July 25–28, Las Vegas, NV, USA, p. 194.

5 Sean A Kaiser, Andrew J Christianson, and Ram M Narayanan. 2016. “Multistatic radar exploitation of for- ward scattering nulls.” In: Radar Conference (RadarConf). IEEE. May 2–6, Philadelphia, PA, USA, pp. 1–6.

6 Kylara M Martin, Warren T Wood, and Joseph J Becker. 2015. “A global prediction of seafloor sediment porosity using machine learning.” In: Geophysical Research Letters 42.24 .

7 D. Gebhardt, K. Parikh, I. Dzieciuch, M. Walton, N. Anh, and V. Hoang. 2017.“Hunting for naval mines with deep neural networks.” In: OCEANS. IEEE. September 18–21, Anchorage, AL, USA, pp. 1–5.

8 J. Harguess, C. Barngrover, and A. Rahimi. 2017. “An analysis of optical flow on real and simulated data with degradations.” In: Geospatial Informatics, Fusion, and Motion Video Analytics VII. Vol. 10199. Proc. SPIE. May 1, Anaheim, CA, USA.

9 J. Harguess, D. Marez, and N. Ronquillo. 2018. “An investigation into strategies to improve optical flow on degraded data.” In: Geospatial Informatics, Motion Imagery, and Network Analytics VIII. Vol. 10645. Proc. SPIE. May 8, Anaheim, CA, USA.

This page left blank intentionally.

APPENDIX A
NAML PHOTOGRAPHS

A.1 OVERVIEW

Appendix A contains six figures that feature attendees at NAML 2018.

A.2. VARIOUS PHOTOS TAKEN

A.2.1 ATTENDEES WELCOME

Figure A-1. Lee Zimmerman, Technical Director, SSC Pacific.

Figure A-2. Lee Zimmerman welcomes attendees to NAML 2018.

Figure A-3. Selected images from the NAML 2018 poster session.

A.2.2 NAML 2018 TUTORIALS AND DEMONSTRATIONS

Figure A-4. Ben Migliori presents his work on bio-inspired ML to NAML 2018.

Figure A-5. Justin Mauger leads a tutorial on topological data analysis.

Figure A-6. Tom Schlosser and Joe Drobick lead a demonstration on Navy collaboration tools.

This page intentionally left blank.

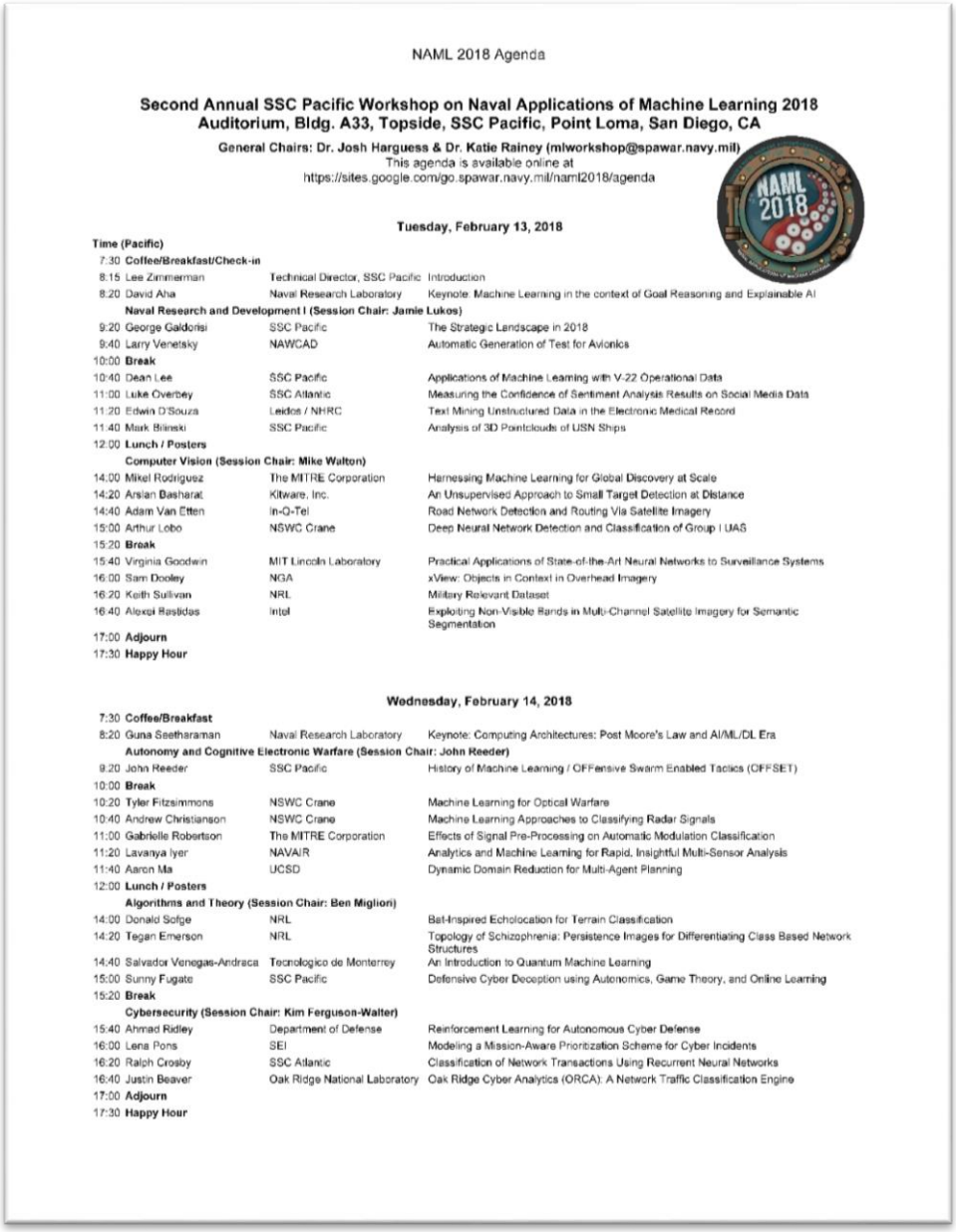
APPENDIX B
NAML 2018 AGENDAS

B.1 WORKSHOP AGENDA

This section contains NAML workshop agendas distributed to attendees.

B.2 AGENDA DETAIL

The agenda for Tuesday, February 13, 2018 and Wednesday, February 14, 2018 is detailed in Figure B-1:



NAML 2018 Agenda

Second Annual SSC Pacific Workshop on Naval Applications of Machine Learning 2018
Auditorium, Bldg. A33, Topside, SSC Pacific, Point Loma, San Diego, CA

General Chairs: Dr. Josh Harguess & Dr. Katie Rainey (mlworkshop@spawar.navy.mil)
This agenda is available online at
https://sites.google.com/go.spawar.navy.mil/naml2018/agenda

Tuesday, February 13, 2018

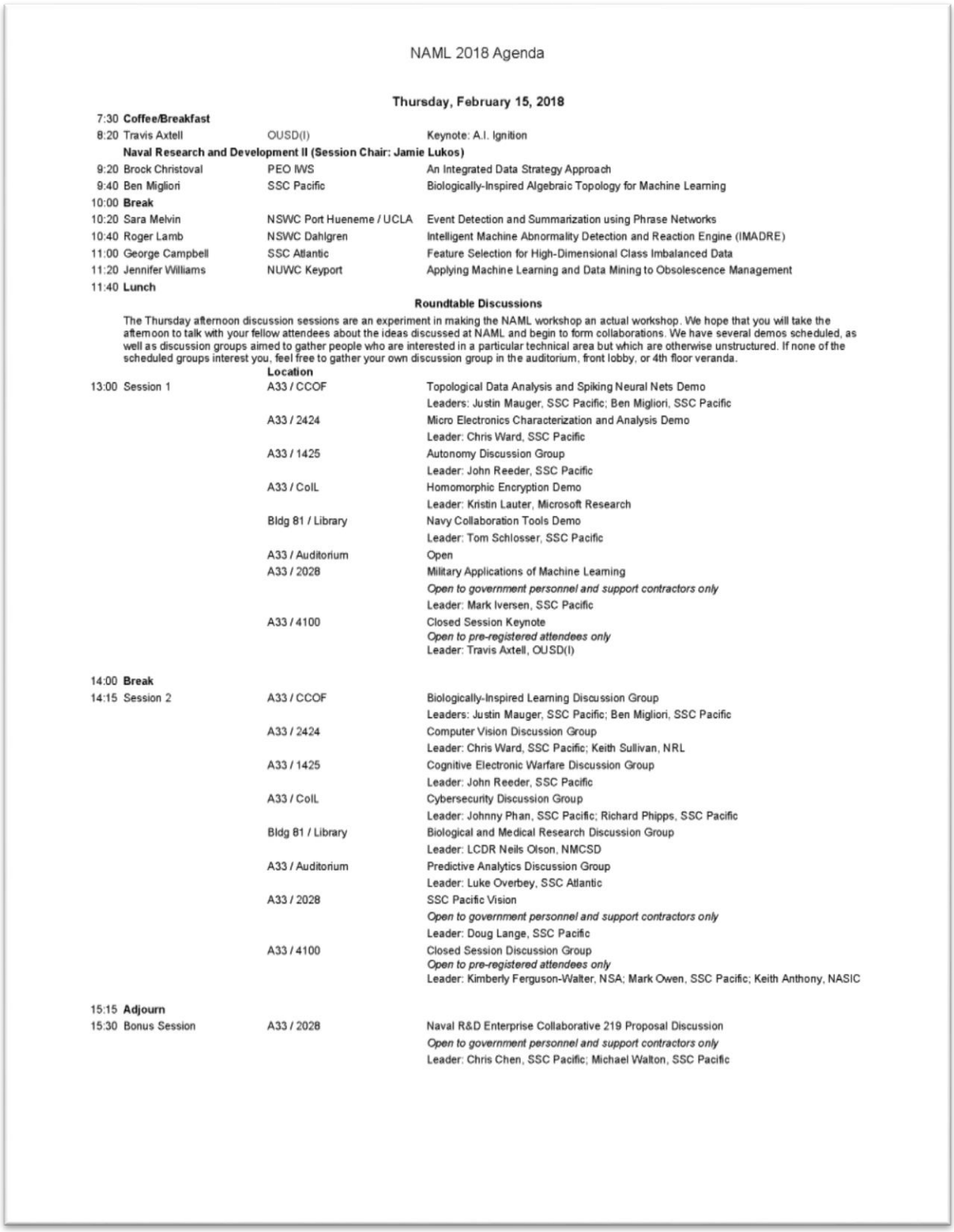
Time (Pacific)			
7:30	**Coffee/Breakfast/Check-in**		
8:15	Lee Zimmerman	Technical Director, SSC Pacific	Introduction
8:20	David Aha	Naval Research Laboratory	Keynote: Machine Learning in the context of Goal Reasoning and Explainable AI
	Naval Research and Development I (Session Chair: Jamie Lukos)		
9:20	George Galdorisi	SSC Pacific	The Strategic Landscape in 2018
9:40	Larry Venetsky	NAWCAD	Automatic Generation of Test for Avionics
10:00	**Break**		
10:40	Dean Lee	SSC Pacific	Applications of Machine Learning with V-22 Operational Data
11:00	Luke Overbey	SSC Atlantic	Measuring the Confidence of Sentiment Analysis Results on Social Media Data
11:20	Edwin D'Souza	Leidos / NHRC	Text Mining Unstructured Data in the Electronic Medical Record
11:40	Mark Bilinski	SSC Pacific	Analysis of 3D Pointclouds of USN Ships
12:00	**Lunch / Posters**		
	Computer Vision (Session Chair: Mike Walton)		
14:00	Mikel Rodriguez	The MITRE Corporation	Harnessing Machine Learning for Global Discovery at Scale
14:20	Arslan Basharat	Kitware, Inc.	An Unsupervised Approach to Small Target Detection at Distance
14:40	Adam Van Etten	In-Q-Tel	Road Network Detection and Routing Via Satellite Imagery
15:00	Arthur Lobo	NSWC Crane	Deep Neural Network Detection and Classification of Group I UAS
15:20	**Break**		
15:40	Virginia Goodwin	MIT Lincoln Laboratory	Practical Applications of State-of-the-Art Neural Networks to Surveillance Systems
16:00	Sam Dooley	NGA	xView: Objects in Context in Overhead Imagery
16:20	Keith Sullivan	NRL	Military Relevant Dataset
16:40	Alexei Bastidas	Intel	Exploiting Non-Visible Bands in Multi-Channel Satellite Imagery for Semantic Segmentation
17:00	**Adjourn**		
17:30	**Happy Hour**		

Wednesday, February 14, 2018

7:30	**Coffee/Breakfast**		
8:20	Guna Seetharaman	Naval Research Laboratory	Keynote: Computing Architectures: Post Moore's Law and AI/ML/DL Era
	Autonomy and Cognitive Electronic Warfare (Session Chair: John Reeder)		
9:20	John Reeder	SSC Pacific	History of Machine Learning / OFFensive Swarm Enabled Tactics (OFFSET)
10:00	**Break**		
10:20	Tyler Fitzsimmons	NSWC Crane	Machine Learning for Optical Warfare
10:40	Andrew Christianson	NSWC Crane	Machine Learning Approaches to Classifying Radar Signals
11:00	Gabrielle Robertson	The MITRE Corporation	Effects of Signal Pre-Processing on Automatic Modulation Classification
11:20	Lavanya Iyer	NAVAIR	Analytics and Machine Learning for Rapid, Insightful Multi-Sensor Analysis
11:40	Aaron Ma	UCSD	Dynamic Domain Reduction for Multi-Agent Planning
12:00	**Lunch / Posters**		
	Algorithms and Theory (Session Chair: Ben Migliori)		
14:00	Donald Sofge	NRL	Bat-Inspired Echolocation for Terrain Classification
14:20	Tegan Emerson	NRL	Topology of Schizophrenia: Persistence Images for Differentiating Class Based Network Structures
14:40	Salvador Venegas-Andraca	Tecnologico de Monterrey	An Introduction to Quantum Machine Learning
15:00	Sunny Fugate	SSC Pacific	Defensive Cyber Deception using Autonomics, Game Theory, and Online Learning
15:20	**Break**		
	Cybersecurity (Session Chair: Kim Ferguson-Walter)		
15:40	Ahmad Ridley	Department of Defense	Reinforcement Learning for Autonomous Cyber Defense
16:00	Lena Pons	SEI	Modeling a Mission-Aware Prioritization Scheme for Cyber Incidents
16:20	Ralph Crosby	SSC Atlantic	Classification of Network Transactions Using Recurrent Neural Networks
16:40	Justin Beaver	Oak Ridge National Laboratory	Oak Ridge Cyber Analytics (ORCA): A Network Traffic Classification Engine
17:00	**Adjourn**		
17:30	**Happy Hour**		

Figure B-1. NAML 2018 Agenda.

The agenda for Thursday, February 15, 2018 is detailed in Figure B-2:



NAML 2018 Agenda

Thursday, February 15, 2018

7:30	**Coffee/Breakfast**		
8:20	Travis Axtell	OUSD(I)	Keynote: A.I. Ignition
	Naval Research and Development II (Session Chair: Jamie Lukos)		
9:20	Brock Christoval	PEO IWS	An Integrated Data Strategy Approach
9:40	Ben Migliori	SSC Pacific	Biologically-Inspired Algebraic Topology for Machine Learning
10:00	**Break**		
10:20	Sara Melvin	NSWC Port Hueneme / UCLA	Event Detection and Summarization using Phrase Networks
10:40	Roger Lamb	NSWC Dahlgren	Intelligent Machine Abnormality Detection and Reaction Engine (IMADRE)
11:00	George Campbell	SSC Atlantic	Feature Selection for High-Dimensional Class Imbalanced Data
11:20	Jennifer Williams	NUWC Keyport	Applying Machine Learning and Data Mining to Obsolescence Management
11:40	**Lunch**		

Roundtable Discussions

The Thursday afternoon discussion sessions are an experiment in making the NAML workshop an actual workshop. We hope that you will take the afternoon to talk with your fellow attendees about the ideas discussed at NAML and begin to form collaborations. We have several demos scheduled, as well as discussion groups aimed to gather people who are interested in a particular technical area but which are otherwise unstructured. If none of the scheduled groups interest you, feel free to gather your own discussion group in the auditorium, front lobby, or 4th floor veranda.

		Location	
13:00	Session 1	A33 / CCOF	Topological Data Analysis and Spiking Neural Nets Demo
			Leaders: Justin Mauger, SSC Pacific; Ben Migliori, SSC Pacific
		A33 / 2424	Micro Electronics Characterization and Analysis Demo
			Leader: Chris Ward, SSC Pacific
		A33 / 1425	Autonomy Discussion Group
			Leader: John Reeder, SSC Pacific
		A33 / CoIL	Homomorphic Encryption Demo
			Leader: Kristin Lauter, Microsoft Research
		Bldg 81 / Library	Navy Collaboration Tools Demo
			Leader: Tom Schlosser, SSC Pacific
		A33 / Auditorium	Open
		A33 / 2028	Military Applications of Machine Learning
			Open to government personnel and support contractors only
			Leader: Mark Iversen, SSC Pacific
		A33 / 4100	Closed Session Keynote
			Open to pre-registered attendees only
			Leader: Travis Axtell, OUSD(I)
14:00	**Break**		
14:15	Session 2	A33 / CCOF	Biologically-Inspired Learning Discussion Group
			Leaders: Justin Mauger, SSC Pacific; Ben Migliori, SSC Pacific
		A33 / 2424	Computer Vision Discussion Group
			Leader: Chris Ward, SSC Pacific; Keith Sullivan, NRL
		A33 / 1425	Cognitive Electronic Warfare Discussion Group
			Leader: John Reeder, SSC Pacific
		A33 / CoIL	Cybersecurity Discussion Group
			Leader: Johnny Phan, SSC Pacific; Richard Phipps, SSC Pacific
		Bldg 81 / Library	Biological and Medical Research Discussion Group
			Leader: LCDR Neils Olson, NMCSD
		A33 / Auditorium	Predictive Analytics Discussion Group
			Leader: Luke Overbey, SSC Atlantic
		A33 / 2028	SSC Pacific Vision
			Open to government personnel and support contractors only
			Leader: Doug Lange, SSC Pacific
		A33 / 4100	Closed Session Discussion Group
			Open to pre-registered attendees only
			Leader: Kimberly Ferguson-Walter, NSA; Mark Owen, SSC Pacific; Keith Anthony, NASIC
15:15	**Adjourn**		
15:30	Bonus Session	A33 / 2028	Naval R&D Enterprise Collaborative 219 Proposal Discussion
			Open to government personnel and support contractors only
			Leader: Chris Chen, SSC Pacific; Michael Walton, SSC Pacific

Figure B-2. NAML 2018 Agenda, Roundtable Discussions.

The agenda for Tuesday, February 13, 2018 Poster Sessions is detailed in Figure B-3 and Figure B-4: Figure 4 shows the acronym list provided to the NAML attendees.

NAML 2018 Agenda

Poster Session I (Session Chair: Chris Ward)
Tuesday, February 13, 2018
12:00-14:00

Jason Kha	SSC Pacific	Structured Objects to Optimize Machine Learning with Large Datasets
Kaylen J. Bryan	Florida Institute of Technology	Deep Wavelet Scattering Features for Infrasonic Threat Identification
Mark Jenne	NSWC Crane	Machine Risk Assessment
Mitchell Solomon	Florida Institute of Technology	Infrasound Threat Classification: A Statistical Comparison of Deep Learning Architectures
Oliver Hui	SSC Pacific	Human Presence Detector
Peter Ateshian	Naval Postgraduate School	Low $WaP Trained Neural Net for NLoS applications
Phi "Vu" Tran	Booz Allen Hamilton	Relational Learning in Graphs with Deep Autoencoders
Jamie Lukos	SSC Pacific	Classification of Cortical Responses to Visual Targets During a Physical-Cognitive Interaction Task
Roger Hallman	SSC Pacific	An Approach to Botnet Malware Detection Using Nonparametric Bayesian Methods
Eriko Nurvitadhi	Intel Corporation	In-Package Domain-Specific ASICs for Intel® Stratix® 10 FPGAs: A Case Study of Accelerating Deep Learning Using TensorTile ASIC
Kristin Lauter	Microsoft Research	Training Logistic Regression Over Encrypted Data
Joshua Rudiger	SSC Pacific	A Machine Learning Approach for Predicting Atmospheric Aerosol Size Distributions
Brian Ruther	IBM	IBM Data Science Experience
David Crandall	Indiana Unversity	Addressing Supply Chain Risks of Microelectronic Devices Through Computer Vision
David Zubrow	SEI	Causal Learning: Analysis for Action
Emily Nystrom	SSC Atlantic	Applications of Random Forests for Modeling Obsolescence
Samuel Dooley	NGA	Overhead Detection: Beyond 8-bits and RGB
Katie Rainey	SSC Pacific	Explaining Classifiers Via Information Tracking
Sheila Bent	Laboratory for Analytic Sciences	Laboratory for Analytic Sciences' OpenKE Methodology to Manage the Big 'D'
James Ezick	Reservoir Labs	ENSIGN: Unsupervised Multidimensional Pattern Discovery Scaled to HPC
Neal Anderson	Northrop Grumman	GLOBALEYES
Ramesh Bharadwaj	NRL	Object Tracking in Contested Environments Using Deep Learning
Stuart Rubin	SSC Pacific	Transformational Learning
Thomas Powers	University of Washington	Avoiding Catastrophes: Worst-Case Optimization with Applications to Multistatic Active Sonar Arrays
Tiffany Helling	Henry M. Jackson Foundation	Information Table for Henry M. Jackson Foundation
Sandy Kelly	NUWC Keyport	Support Vessel Scheduling for Pacific Northwest Test Ranges
Warren Wood	NRL Stennis	Machine Learning Prediction of Sea Floor Properties (Environmental Inputs to Models)

Figure B-3. NAML 2018 Agenda, Poster Session 1.

NAML 2018 Agenda

Poster Session 2 (Session Chair: Chris Ward)
Wednesday, February 14, 2018
12:00-14:00

Ari Goodman	NAWCAD Lakehurst	Applying Autonomy on the Carrier Flight Deck
2d Lt Taylor Bodin	Air Force Institute of Technology	A Task Flexible UAS Development Platform
David W. Krout	APL-UW	Acoustic Model Emulation using a Neural Network
Hope Allen	Northrop Grumman	Advanced Automation to Cognitive Autonomy
Daniel Donavanik	ARL	Automatic Calibration of Multi-Sensor State Estimation for Autonomous Systems
Daniel Donavanik	ARL	Relevance and Redundancy as Selection Techniques For Human Machine Sensor Fusion
Ying Zhao	Naval Postgraduate School	Big Data, ML and AI for Combat ID and Combat Systems – Design, Demonstrate and Proof of Concept: Discover Virtual Airways and Patterns Using Automatic Dependent Surveillance – Broadcast (ADS-B) Data
Donovan Lo	Booz Allen Hamilton	Bounding Box Prediction in Video Object Tracking with Reinforcement Learning Techniques
Kim Laine	Microsoft Research	CryptoNets: Evaluating Deep Neural Networks on Encrypted Data
Jim Pietrocini	Sentek Global	Danger, Danger, Ensign Will Robinson! How Artificial Intelligence will play a role in the Navy's focus on Cybersecurity
Chris Ward	SSC Pacific	Deep Learning for Integrated Circuit Segmentation
Diego Marez	SSC Pacific	Electronic Warfare Activity Recognition (EWAR)
Mark Mote	MIT Lincoln Laboratory	Formal Verification of Image Classifier Neural Networks
Michael Ouimet	SSC Pacific	Hierarchical planning for Human-Autonomy Teaming
Daniel Gebhardt	SSC Pacific	Hunting for Naval Mines with Deep Neural Networks
Nancy Ronquillo	UCSD	Informativeness of Degraded Data in Training a Classification System
Rafael Dinner	Areté Associates	Multi-Spectral Image Recognition for Coastal Reconnaissance
David Emerson	NSWC Crane	Neural Network Hyper-Parameter Optimization using Particle Swarm Optimization (PSO)
Lauren Christopher	Indiana University – Purdue University at Indianapolis	Particle Swarm Optimization (PSO) for Asset Allocation in a Dynamic Electronic Spectrum
Philip Colangelo	Intel	Reduced Numeric Precision Neural Networks on Intel FPGAs
Michael Hazoglou	UCSD	Saccadic Predictive Vision Model
Matt Zaber	SSC Atlantic / SMU AT&T Virtualization Research Center	Secure Analytics on Public Clouds with SGX
Michael Walton	SSC Pacific	Measuring Strategic Coordination in Multi-Agent Autonomous Systems
Kurt Rohloff	New Jersey Institute of Technology	SUSTAIN: Semi-Autonomous Distributed SCADA Reconfiguration System
Mohammad Alam	SSC Pacific	Using Gait Information to Classify Cognitive-Motor Interaction Tasks
Benjamin Michlin	SSC Pacific	High Performance Computing at SPAWAR Systems Center Pacific
Robert Lim	UCSD	Exploring Hyper-parameter Optimization for Neural Machine Translation

Figure B-4. NAML 2018 Agenda, Poster Session 2.

APPENDIX C
PRESENTATION ABSTRACTS

Section C contains 78 presented abstracts. The Sections are organized by topics presented, and then presenter and supporting group. Following that is a brief overview of the sub-supporting topics that were covered.

C.1 PRESENTED ABSTRACTS

Some of the Abstracts shown here contain References specific to the shown Abstract only, and do not apply to the other References or the main body of the report.

The Strategic Landscape in 2018

George Galdorisi[1] and Rachel Volner[1]

[1]SPAWAR Systems Center Pacific

THE STRATEGIC LANDSCAPE IN 2018

Our briefing will provide a summary of the strategic landscape facing SSC Pacific, our government, academic and industry partners, as well as the DoN and the DoD in 2018. The purpose of this briefing will be to provide a stage-setter and strategic and operational "grounding" for the discussions throughout the 2018 Workshop on Naval Applications of Machine Learning

In support of SSC Pacific's mission to deliver C4ISR, cyber, and space capabilities to the warfighter, it is important to understand the current — and future — strategic environment our warfighters will face. The reasons this look-ahead is important include:

- We support today's Navy (the Navy Sailing) by installing and maintaining our C4ISR systems.
- We support tomorrow's Navy (the Navy in Construction) by designing new C4ISR systems.
- We hire professionals with specific skill sets to support the Navy of today and tomorrow, as well as the Navy in Planning.
- We invest internal S&T funding on projects for the Navy of today and tomorrow as well as the Navy in Planning.

Our briefing will address the strategic landscape for the Navy Sailing and the Navy in Construction, looking out roughly five years across the Future Years Defense Plan (FYDP). This briefing will also look beyond the FYDP, and will address the strategic landscape the Navy in Planning will likely face.

One way of breaking down our analysis of the strategic landscape is to use the familiar Rudyard Kipling verse from The Elephant's Child:

> I keep six honest serving-men
> (They taught me all I knew);
> Their names are What and Why and When
> And How and Where and Who.

Thus, if we know who our warfighters will likely have to take on, and where they will fight them, and we have a sense of when and why this fight might begin, and understand how our warfighters will work to defeat an enemy, then we will know what C4ISR, cyber, and space platforms, systems, sensors and weapons SSC Pacific needs to deliver to our warfighters today and tomorrow.

THE STRATEGIC ENVIRONMENT

In examining the strategic landscape facing our warfighters today and tomorrow, as well as in a more distant future, we have mined documents from a wide array of sources. Collectively, these sources help us understand who our warfighters will likely have to take on, and where they will fight them. Further, they help us gain a sense of when and why this fight might begin.

The current DoD thinking is that the United States faces, and will continue to face, four contingencies and one condition — frequently referred to as the "4+1 construct." The contingencies include: China, Russia, North Korea and Iran. The condition involves a long-term fight against global terrorism.

Automatic Generation of Test for Avionics

Larry Venetsky[1], Russell Shannon[1], Daniel Collins[1], George Lehaf[1], and Ross Boczar[1]

[1]Naval Air Warfare Center Aircraft Division

This research offers a biologically inspired approach for creating the test program sets (TPSs) that are used by automatic test equipment (ATE) to test electronic circuits and devices. We present an architecture consisting of a genetic algorithm (GA) test proposer and a pattern classifier test evaluator. This architecture has been shown to produce optimized test sequences without human intervention. In contrast to the above, the current method of developing TPSs and test sequences is an analytical process involving the building of fault trees using circuit diagrams of the unit under test and industrial-strength circuit simulation models. Since TPS software currently is coded manually, it can cost millions of dollars and take 12 months to 18 months of lead time to produce. In the prototype system, both the GA and the test evaluator are used to optimize input stimuli, significantly reducing the labor hours of a human TPS developer. The outputs of the process are a stimulus signals specification and a diagnostics reasoning system that could be deployed to ATE. The system has been demonstrated on a small scale using a band-pass filter circuit with twenty components, and in simulation on circuits with up to three hundred components. Success was shown by automatically generating a TPS that provided full fault detection and full fault isolation of the band-pass filter circuit. The next steps in the development process include demonstrating the technology on Fleet asset circuit cards, improving the scalability using high-performance computing assets, and implementing external interfaces using Automatic Test Markup Language (ATML).

Measuring the Confidence of Sentiment Analysis Results on Social Media Data

Lucas A. Overbey[1], Robert Regal[1], Jamie Lyle[1], and George Campbell[1]

[1]SPAWAR Systems Center Atlantic

Sentiment analysis in social media is commonly practiced in commercial marketing and customer relations applications. Unlike many machine learning-based classification problems, the 'ground truth' of this application can be quite subjective. The certainty of manually labeled ground truth is inexplicit because of this subjectivity and lack of inter-reviewer agreement. Therefore, with a sentiment analysis task, it is important to also consider whether a given message is too ambiguous to classify at all. In this work, we develop approaches to measuring confidence and "classifiability." We compare a combination of methods, including a parametric approach, an ensemble of supervised machine learning models, and a separate random-forest classifier. We utilize the output of a sentiment classifier as part of the feature set for the confidence model. Results are evaluated on geopolitical messages collected from Twitter.

Text Mining Unstructured Data in the Electronic Medical Record

Edwin D'Souza[1,2], James Zouris[2], and Vern Wing[1]

[1]*Leidos*
[2]*Naval Health Research Center*

The electronic medical record (EMR) in combat medical data repositories can contain a vast amount of unstructured free text that record the history, diagnoses, and treatments of patients suffering injuries and illnesses on the battlefield. These unstructured data are typically recorded by clinicians at medical treatment facilities, or by experienced medical coders, summarizing patient diagnosis and treatment. Examples of unstructured data are the Subjective, Objective, Assessment, and Plan of Care fields that can contain up to 4,000 bytes of data in each EMR in the Theater Medical Data Store repository. To date, little or no analysis has been done on the unstructured data in the combat EMR. This presentation demonstrates the application of current, state-of-the-art text mining methods to extract useful information from free text data within the EMR.

Analysis of 3D Pointclouds of USN Ships

Mark Bilinski[1]

[1]*SPAWAR Systems Center Pacific*

SPAWAR is creating 3D pointclouds of US Navy (USN) ships using LiDAR and other sensors. We have established a pipeline for data collection and will be regularly collecting and updating data, which incidentally is incredibly large – on the order of 100 GBs–1 TB per hull. We are interested in a host of machine learning problems related to processing this type of data and are seeking ideas and collaborators.

The purpose of this talk is to familiarize the audience with exactly the type of data we are collecting and to discuss some directions for machine learning we anticipate pursuing. Detecting and recognizing the many objects on a ship is of primary concern; the list of possible objects is known and in some cases CAD models of those objects exist. Localization within a ship is a particular challenge as even a human can easily get disoriented. Constructing higher order 3D objects such as textured meshes or CAD models from the scan data is needed for more immersive augmented and virtual reality experiences. Classification and segmentation of pointclouds can help in subdividing our analysis.

An Unsupervised Approach to Small Target Detection at Distance

Arslan Basharat[1]**, Z. Harry Sun**[1]**, and Anthony Hoogs**[1]

[1]*Kitware Inc.*

Detecting small targets, such as boats or vessels, from distance on open water is an important yet challenging technical task. In this paper, we propose an unsupervised approach to learn the visual states of open waters, at different wave and weather conditions, date and time, and viewing angles, build a normalcy model for the observed videos, and call out the abnormal outliers as target candidates. Although it is hard, if not impossible, to locate and annotate all rare events of small targets on various backgrounds for supervised learning, it is relatively easy to find hours and hours of videos of open water, which can be used for unsupervised training. We build a deep convolutional neural network with layers of convolutional layers, rectified linear units (ReLU), and pooling layers. It captures the normal states of the open water, and can be trained from a large number of visual sampled from videos without the small targets. During testing, a large reconstruction error within a region is an indication of abnormal spatial and motion pattern, which can lead to small target detection.

Furthermore, target detection in videos with long duration needs to automatically identify frames with open sea that may or may not contain vessels, distinguishing those from frames with clouds, parts of the plane, sky, littoral zone, etc. We have developed a light-weight, pre-processing stage to classify the relevant scene content. This model is generated through deep learning descriptors and Interactive Query Refinement (IQR) instead of a conventional training process of labelling hundreds of frames. We have developed this capability based on our open source Social Media Query Toolkit (SMQTK)[1] for image matching and retrieval, and have shown compelling results for scene classification and vessel matching at short distances.

[1] `https://github.com/Kitware/SMQTK`

Road Network Detection and Routing Via Satellite Imagery

Adam Van Etten[1]

[1]*In-Q-Tel*

Determining optimal routing paths in near real-time is at the heart of many humanitarian, civil, military, and commercial challenges. In areas of low population density or undergoing rapid change (e.g., natural disasters), commercial or open source mapping products are often inadequate. The rapid revisit rates of satellite imaging constellations have the potential to alleviate this capability gap, if road networks can be inferred directly from imagery. We demonstrate techniques for extracting the physical and logical topology of road networks from satellite imagery via computer vision and graph theory techniques; the road network graph structure inferred from our algorithms can be used directly for routing. We also develop a new metric based upon shortest path algorithms for measuring network similarity, and show how road network inference performance varies between differing scenes and environments.

Deep Neural Network Detection and Classification of Group I UAS

Arthur Lobo[1]

[1]*Naval Surface Warfare Center, Crane*

The proliferation of Group I UAS and their use by non-state actors for delivering explosive payloads and ISR has resulted in an urgent need for their detection and classification as part of the complete kill chain which includes direction finding, neutralization and forensics. We will present results of our work in RF and Electro-Optic (EO) detection and classification of Group I UAS using Deep Convolutional Neural Networks (DCNN). We have trained DCNNs for classifying RF spectrograms of UAS uplinks and downlinks in four ISM bands which are computed after RF sampling by a software defined radio. Our results show high accuracy detection and classification of single transmitter RF spectrograms for the RF classifier and UAS/aircraft types and tracking from video for the EO classifier. Significantly we show detection and classification of multiple simultaneous RC transmitter/UAS with an RF Object Detection DCNN. Trained models have been exported to a NVIDIA Jetson TX2 embedded GPU platform for field testing. Initial results on Specific Emitter Identification will be presented.

Practical Applications of State-of-the-Art Neural Networks to Surveillance Systems

Virginia Goodwin[1], Peter Morales[1]

[1]*MIT Lincoln Laboratory*

Traditional air surveillance systems rely on sparse target density; they are detection systems, and classification is assumed based on the targets location and dynamics. However, modern air surveillance problems are much more challenging, including dense, complex clutter such as urban environments and small, highly maneuverable targets such as commercial unmanned aerial systems (UAS). Performance of current surveillance systems are degraded in this environment, resulting in either unacceptably high leakage or false alarms. The Department of Homeland Security, Science & Technology Directorate (DHS S&T) is investigating solutions to the urban, counter-UAS problem for point and area-defense.

Current deep learning algorithms have the potential to offer a solution to the urban, counter-UAS surveillance problem. Such algorithms can mitigate the high false alarm problem by enabling a camera to interrogate targets and reject false alarms without involving an operator. A camera network can mitigate the leakage problem by covering all the sight angles, allowing for surveillance where long-range sensors would be impaired.

We present two algorithms that enable deep learning to be leveraged for surveillance: a region proposal network (RPN) based on modifications to current state-of-the-art deep learning algorithms that improves detection of small targets, and a novel sensor fusion network that addresses the unique challenges presented by the urban counter-UAS surveillance problem.

The RPN addresses the problem of robustly detecting small image cross-section targets. We present results on the Common Objects in COntext (COCO) database, which defines a small object as having a pixel area less than 32×32 pixels. Current state-of-the-art networks show a decrease in mean Average Precision (mAP) of approximately a factor of two between large objects and small objects. Our modified RPN achieves best-in-class performance on the small object subset of the COCO data, from 24.3 to 35.2 mAP, while only reducing the overall mAP from 48.1 to 47.4. We will also present results collected on our own testbed — flying small, quadcopter UAVs, recording with a commercial surveillance camera, and processing the video in real time on a single NVIDIA Pascal GPU — that demonstrate robust detection results down to 12×8 pixels on target.

A second challenge specific to surveillance systems is the ability to fuse different sensor modalities to create a robust common operating picture, and achieve high-precision target localization. We propose a novel sensor fusion network that can fuse any spatially coherent sensors, including radar, acoustic, and imagery, to generate a target localization solution that is more robust than each sensor could achieve independently, while maintaining real-time processing speed. The results collected from our testbed show an increase in localization precision.

xView: Objects in Context in Overhead Imagery

Samuel Dooley[1], Darius Lam[1], Richard Kuzman[1], Kevin McGee[1], Matt Klaric[1], Mike Laielli[1], and Brendan McCord[1]

[1]*National Geospatial-Intelligence Agency*

We present a new large-scale dataset with the goal of advancing the state of the art in object detection in overhead imagery. Applications in the developing world include disaster response and public safety, Sustainable Development Goal (SDG) indicators, human mobility and mapping, and novel use cases.

This is achieved by gathering overhead images at 0.3 m ground sample distance (GSD) of complex scenes across the world. On release, xView will be the largest and most diverse public dataset for object detection in overhead imagery. With a total of 60 object classes and 1 million labeled instances spanning over 1400 km^2, building xView required a novel process for geospatial category detection, bounding box annotation, and hierarchical class labeling. We present a statistical analysis of the dataset in comparison to existing overhead imagery datasets as well as baseline performance analysis for object detection using Single Shot MultiBox Detector.

Military Relevant Dataset

Keith Sullivan[1], Chris Barngrover[2], Josh Harguess[2], Allison Mathis[3], Daniel Donavanik[3], and William Nothwang[3]

[1]*Naval Research Laboratory*
[2]*SPAWAR Systems Center Pacific*
[3]*Army Research Laboratory*

Autonomous robot research is critically dependent on vast quantities of real-world data to train robust machine learning solutions to various robotics problems. Current datasets are either heavily focused on city streets, or consist of clean images (uniform lighting, advantageous perspectives, no occlusions). While these datasets work well for civilian applications, the military does not operate in clean, structured environments, and the lack of a militarily relevant dataset limits the applicability of autonomous systems in the military domain. This work presents a new military relevant dataset collected at the Laboratory for Autonomous Systems Research at the Naval Research Laboratory. The publicly available dataset contains over 110,000 RGB and depth images along with time coordinated laser pointclouds, GPS, and IMU data. When possible, the robot ground truth position was collected via motion capture. Data was collected in three environments: desert, open highbay, and rainforest. Each run through each environment changed lighting conditions and visible objects. In the highbay, we include standing water, while in the rainforest, we also introduced wind and rain. We feel this dataset will enable research across a broad range of topics of military interest, including optical flow, vehicle state estimation, visual navigation, and anomaly detection.

Exploiting Non-Visible Bands in Multi-Channel Satellite Imagery for Semantic Segmentation

Alexei Bastidas[1], **Hanlin Tang**[1]

[1]*Intel Corporation's Artificial Intelligence Lab*

State of the art deep learning approaches for semantic segmentation were developed for natural scenes with three-band (RGB) images. These models rely on networks pre-trained on common RGB-based datasets such as ImageNet, PASCAL VOC 2012 or MS-COCO 2014. On the other hand, existing approaches to semantic segmentation of satellite imagery rely on graph-based algorithms, such as Conditional Random Fields or Hidden Markov Models.

Applying these deep neural network models to satellite imagery present several challenges. Many remote sensing datasets contain multiple spectral channels of information, and have different underlying properties compared to common computer vision datasets. With this research, we propose a novel convolutional neural network architecture to exploit these additional spectral bands. This model consumes visible and near-infrared bands in separate input streams and utilizes an attention mechanism to softly weight the multi-band features at each pixel location. We jointly train the model and attention mechanism on the 8-band SpaceNet dataset. The model offers multiple advantages over the naive single-stream approach: (1) the RGB stream can be pre-trained on common datasets, (2) the separate streams prevent early mixing of the band information, and (3) the attention masks offer interpretable visualizations of important features at different spectral wavelengths.

We establish baselines using the naive single-stream approach and measure performance on the SpaceNet dataset, which includes imagery of four cities (Khartoum, Paris, Vegas, and Shanghai) taken at 30 cm spatial resolution with 8 spectral bands. Each image includes building segmentation labels. We measure baseline performance with the F1 score using the single-stream SegNet model. We note that the single-stream SegNet model trained only on infra-red bands outperformed the same model trained on RGB bands by 3%, a non-trivial amount that demonstrates the importance and value of the material and reflectance information encoded in the additional bands. However, when we train a SegNet model with all 8 available bands, we find that the performance is on par with the model trained exclusively on infrared.

To test the hypothesis that our proposed attention-based architecture can exploit these additional bands better than the naive band-stacking approach, we intend to compare performance of this novel architecture against both the single-stream SegNet baseline, the single stream variant of our own architecture, and the latest winners of the SpaceNet challenge.

We hope that by leveraging the deep learning based methods with satellite data, we can create solutions that assist in building and object detection, automated mapping efforts, humanitarian relief efforts, establishing pattern of life, battle damage assessments, and more.

Machine Learning for Optical Warfare

Tyler Fitzsimmons[1], Lauren Christopher[2], and Christopher Summitt[1]

[1]*Naval Surface Warfare Center Crane Division*
[2]*Indiana University — Purdue University Indianapolis*

The U.S. Navy has witnessed a proliferation in Intelligence Surveillance and Reconnaissance (ISR) activity from adversaries in the form of ISR aircraft and unmanned aerial vehicles (UAV). One response to ISR activity is the use of lasers to actively engage adversaries in a non-lethal manner. Naval Surface Warfare Center (NSWC) Crane has established standards and methods for quantitatively determining the effects of laser interaction on optical payloads for Counter-Intelligence Surveillance and Reconnaissance (C-ISR) purposes. NSWC Crane has aggregated data from thousands of low power laser tests with multiple lasers in multiple environments utilizing specific optical assets to better understand C-ISR scenarios. Crane has tested multiple machine learning algorithms (MLA) to classify the success of the C-ISR into three levels. By using machine learning, our dataset of thousands of experimental test events can be systematically ranked by a MLA. Once fully trained, a weeks' worth of testing can be reduced from 1-2 weeks required for human scoring to a matter of minutes for a MLA to score. To date, we have tested artificial neural networks, support vector machines, autoencoder networks, and convolutional neural networks. By comparing four different algorithms with two different representations of the same dataset, we are able to gain insight into the better performing algorithms for our needs, while also playing to the strengths of the different MLAs. Our research is ongoing, but to-date has achieved a classification accuracy of 99.7% using an artificial neural network with human-engineered feature extraction (best performing MLA thus far). Our end goal is to have a thorough understanding of the cause and effect on an optical payload during a laser engagement in the field. Using our system, the U.S. Navy has experimental data to use in real-world engagements when encountering adversarial assets and the research provides information to choose the proper laser response needed to counter the adversary's ISR capabilities in a non-lethal but effective manner.

Machine Learning Approaches to Classifying Radar Signals

Andrew Christianson[1], Anthony Tai[1]

[1]*NSWC Crane Division*

Three experiments investigating approaches to radar waveform classification are performed. In particular, the ability of various approaches to classify a burst of RF data as having a constant frequency or a linear frequency modulation is investigated. The first experiment compared the use of raw data to expert derived features as inputs to both neural networks and support vector machines. The second experiment investigated the introduction of sparsity into the neural network classifier and demonstrated that the common driver was the sparsity of the first layer of the neural network with later layers being less important. Finally, the importance of noise in training data was investigated showing the support vector machines improved when training data included less noise. The neural network on the other hand did not have a linear relationship between training noise level and error performance. These three experiments offer a first effort in the application of modern machine learning to radar waveform characterization and begin to answer some important questions that arise in this field.

Effects of Signal Pre-Processing on Automatic Modulation Classification

Gabrielle Robertson[1], Kevin Burke[1]

[1]*The MITRE Corporation*

As an emerging field, Radio Frequency Machine Learning has yet to characterize the effects of different processing steps on model performance. We present a potential system for discovering signals present in a wide band, processing them for machine learning classification, and performing the classification. In this context, we anticipate that the signal pre-processing step of converting passband signals to baseband will affect the machine learning classifier. We present experiments on a Convolutional Neural Network (CNN) applied to automatic modulation classification, showing the change in performance when the input data includes baseband conversion. We anticipate that a CNN model trained on signals synthesized at baseband will less accurately classify signals synthesized at passband and converted to baseband. We study the effects of signal to noise ratio on this accuracy disparity. Additionally, we anticipate that a CNN model trained and tested on signals synthesized at passband and converted to baseband will be able to classify less accurately than a CNN model trained and tested on signals synthesized at baseband.

Analytics/Machine Learning for Rapid Insightful Multi-Sensor Analysis

Lavanya B. Iyer[1], Daniel K. Omoto[1]

[1]*Naval Air Systems Command*

With the increasing complexity of threats across our peer and near-peer adversaries, the value of tactical data collected across all our sensors aboard aircrafts increases in orders of magnitude with the ability to extract information in regards to the behavior of these systems. The insights gained from such analyses could be applied not just to better comprehend trends in red systems but could also aid in understanding the performance of our blue sensors against these hostile environments. Our recent efforts have started in the field of post mission analysis to capture patterns, trends and outliers from tactical data recordings, one of the purposes being to perform multi-sensor analytics using machine learning techniques. This increases confidence on the known intelligence and helps analyze data with regards to the unknowns and unknown probabilities. The faster these analytics can be performed, the quicker will be the feedback for consequent missions increasing chances of mission success, safety and effectiveness. There are myriad future possibilities to include rapid integration into data reprogramming efforts, real-time on-board data analytics, real time decision aids based on extending the a priori learning using live sensor data feeds. Much as these techniques might be limited compared to a more elaborate post-mission analysis approach, it helps provide real-time decision support critical to the warfighter of today. The viability and reliability of these various approaches that are in their infancy is to be determined, but have promise. They might have a long maturation process, which can be expedited through collaborative capability advancement across DoD organizations and national partners.

Dynamic Domain Reduction for Multi-Agent Planning

Aaron Ma[1], Mike Ouimet[2], and Jorge Cortes[1]

[1]*University of California, San Diego*
[2]*SPAWAR Systems Center Pacific*

We consider a scenario where a swarm of arbitrary unmanned vehicles (UxVs) are used to spatially satisfy a multitude of diverse objectives. The UxVs strive to determine an efficient schedule of tasks to service the objectives while operating as a swarm. We focus on developing autonomous high-level planning, where low-level controls are leveraged from previous work in distributed motion, target tracking, localization, and communication algorithms. We take a Markov decision processes (MDP) approach to develop a multi-agent framework that can extend to multi-objective optimization and human-interaction for swarm robotics. Utilizing state and action abstractions, we introduce a hierarchical algorithm, dynamic domain reduction for multi-agent planning, to enable multi-agent planning for large multi-objective environments. Simulated results show significant improvement over using a standard Monte Carlo tree search in an environment with massive state and action spaces. This research is a joint collaboration between the University of California, San Diego (UCSD) and SPAWAR Systems Center Pacific, funded through the Office of Naval Research (ONR), with Dr. Jorge Cortes, Dr. Michael Ouimet, and Aaron Ma.

Bat-Inspired Echolocation for Terrain Classification

Donald Sofge[1], Nathon Riopelle[1], and Philip Caspers[1]

[1]*Naval Research Laboratory*

Many types of bats use echolocation to sense their environment. Despite often have little or no visual acuity, they are able to acquire very detailed views of their surroundings through emission, receipt, and analysis of acoustic pulses. This allows them to locate and track prey, but also to identify landmarks and other environmental features useful in navigation. An autonomous vehicle with limited sensing capabilities could use an echolocation-like system for navigation as an alternative to traditional sensors. A single sensor package that gives a vehicle the ability to both gauge its distance from objects and determine their characteristics would be an invaluable tool in any autonomous system. In this study, autonomous navigation was examined with respect to classification of nearby terrain. The ability to discriminate and distinguish between the different features of the topographical surroundings of an autonomous vehicle is a key component in determining its overall mobility and survivability. A vehicle must know how to respond when it approaches terrain significantly different from that it is traveling on, otherwise it runs the risk of becoming incapacitated, as occurred with the Mars rover Spirit when it became permanently stuck in soft soil in 2010. The goal of this effort was to demonstrate that a bat-inspired acoustic sensor could be built, and when trained using advanced signal filtering and machine learning techniques, could be used to accurately classify terrain types for a small mobile robot. A dual channel in-air sonar was constructed using two common piezoelectric transmitter elements with 25 kHz and 40 kHz nominal center frequencies, and echo data was collected from grass, concrete, sand, and gravel terrain substrates. The process was broken down again into the following steps: modification of the raw echo data, feature extraction from the modified signal, and classification

of the signals using a machine learning algorithm. For the modification of the raw data we used a bandpass filter centered on the target frequency of the transmitted signal. Principal component analysis (PCA) was used to reduce the dimensionality of their spectrogram features before sending the reduced vector to a support vector machine (SVM). Classifier feature representations were compared using sample statistics derived from time, frequency, and time-frequency domains. Higher dimension time, frequency, and time-frequency PCA scores were used to discriminate between terrain substrates. These features were used to train a support vector machine (SVM) to classify the terrain types. The SVM-based classifier was able to classify terrain types at a greater than 95% success rate using the constructed bat-inspired echolocation sensor.

An Introduction to Quantum Machine Learning

Salvador E. Venegas-Andraca[1], William Cruz-Santos[2], and Marco Lanzagorta[3]

[1] *Tecnológico de Monterrey, Mexico*
[2] *Universidad Autonóma del Estado de México, Chalco*
[3] *Naval Research Laboratory*

Quantum computation can be defined as the interdisciplinary scientific field devoted to build quantum computers and quantum information processing systems, i.e. computers and information processing systems that use the quantum mechanical properties of Nature. Research on quantum computation heavily focuses on building and running algorithms which exploit the physical properties of quantum computers.

The existence of quantum technology for developing quantum algorithms to solve combinatorial optimization problems [1] has boosted the interest of the scientific and engineering communities to think of novel applications of quantum algorithms in fields like Machine Learning.

Quantum Machine Learning is an emerging paradigm in quantum computation that has attracted considerable attention over the last few years. In this talk, we shall introduce the main ideas, proposals and results of quantum machine learning, preceded by a concise introduction to the foundational concepts of quantum computing needed to understand the structure of quantum machine learning algorithms.

References

1 *D-Wave Systems*. https://www.dwavesys.com/.

2 Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, Seth Lloyd. 2017. "Quantum machine learning." In: *Nature* 549.7671, pp. 195–202.

Defensive Cyber Deception using Autonomics, Game Theory, and Online Learning

Sunny Fugate[1], Kimberly Ferguson-Walter[2], and Jason Landsborough[1]

[1]*SPAWAR Systems Center Pacific*
[2]*National Security Agency*

Cyber attackers currently enjoy a significant asymmetric advantage. Network reconnaissance and maneuver are essentially uncontested and current defenses easily circumvented. We do not think this is an inevitable consequence or flaw of information systems and networks in general, but is due to fundamental weaknesses in how strategies for network and computer defense are employed. Our computing systems tend to be naive to attacker manipulation, dumbly trusting relations and data provenance based simply on convention and proximity. Our network defenses also tend to embody the posture and tactics of victims, taking passive approaches to defense as simply a task of detection with meager allowances for responses, actions, or countermeasures.

To address these issues, our research team has been exploring the theory and practical application of network-based deception. Specifically, we have put into practice a combination of modern game theory, novel cyber-deception techniques, and online learning. Our cyber deception games focus on interfering with attacker reconnaissance and maneuver with the hopes of learning attacker preferences and dissuading attackers due to significantly increased attack difficulty and the potential for discovery. We are currently exploring techniques to harness artificial intelligence techniques to enable our cyber deception to evolve over time, changing as attacks change, thus maintaining an enhanced defensive posture.

In this talk we will discuss the novel nature and structure of asymmetric cyber deception games, explore the use of online learning to optimize deception strategies against dynamic attackers, and propose a series of research topics which have promise to revolutionize the way we defend computer systems from criminal misuse.

Reinforcement Learning for Autonomous Cyber Defense

Ahmad Ridley[1]

[1]*Department of Defense*

Our research goal is to build an autonomous cyber defense system that will make an enterprise network, and its associated missions/services, more resilient to cyber-attack. Such a cyber-defense system should make decisions and implement appropriate responses to anticipate, withstand, recover from and/or evolve in the presence of cyber-attacks. Since attack methods are constantly evolving, this defense system must be adaptive, and also operate in real-time and at network scale. Therefore, in our research, we apply reinforcement learning to train the system to perform sequential decision making under uncertainty to defend the network.

Modeling a Mission-Aware Prioritization Scheme for Cyber Incidents

Lena Pons[1], LT Peyton Price[2]

[1]Software Engineering Institute Carnegie Mellon University
[2]CNSP Force C4I

Network situational awareness in a military operational context can be thought of as the cyber common operational picture. Previous work has been done to characterize critical assets that describe cyber key terrain in a mission context for use in network situational awareness. Capturing the complexities of network topology and cyber critical asset determination is a challenging problem. Prior research has used a variety of business process and risk analysis frameworks to address parts of the problem. In an operational context, operators have varying expertise. Defining risk characteristics helps to abstract information such that it can be quickly and unambiguously digested by operators without requiring a depth of domain knowledge. One example of how abstraction could improve situational awareness is developing a cybersecurity incident alert prioritization scheme that can account for mission and context-specific criticality of affected systems.

Tools to provide information about network conditions are not currently well-tuned to provide alerts that are prioritized with mission awareness. As a result, analysts may spend time triaging issues and making judgments that are not reflective of the mission context. With a model that provides mapping of critical assets to missions, we can contemplate ways of producing an adaptive triage system for cybersecurity events.

We are investigating use of decision tree modeling to incorporate mission criticality of the affected assets or systems in prioritizing alerts and assigning their severity. Incorporating this mission awareness would allow such a prioritization system to give the analyst an additional layer of information over the Cyber Incident Severity Schema. This would significantly improve the process as this Schema is optimized for coordination of event severity, not for the local context of a ship on a mission under specific conditions.

We are building on a simplified network topology that comprises a minimal set of systems to describe a representative US Navy ship-board industrial control system, and three missions for which we have previously collected data about the mission-specific asset criticality. For the purposes of this modeling, we are demonstrating whether we can incorporate a measure of mission-specific asset criticality into prioritizing a cyber-alert. Success will be evaluated based on whether the decision tree model assigns alerts to an escalated alert category consistent with the relative mission-specific criticality of an affected system.

Classification of Network Transactions Using Recurrent Neural Networks

Ralph Crosby[1], Sarah Darley[1]

[1]*SPAWAR Systems Center Atlantic*

The classification of streaming network data is important for applications ranging from intrusion detection to dynamic routing. While most network activity classification has been focused at the packet level, these methods, by nature disregard the higher level, user, aspect of network interactions. In this presentation, we present a novel technique for classification at the user or conversation level (e.g. HTTP, SSL). We pre-process network data by accumulating the packets into logical, user layer, transactions. These transactions are then presented to a recurrent neural network composed of layers of long short-term memory and rectified linear units for classification. This technique is shown to correctly classify up to 97% of network activity into two categories as would be the case in an intrusion detection application. This method retains the service level (HTTP, SSL) structure of the transactions and classifies transactions using a recurrent neural network composed of multiple layers of long short-term memory cells.

Oak Ridge Cyber Analytics (ORCA): A Network Traffic Classification Engine

Justin M. Beaver[1], Brian C. Jewell[1], Chelsey D. Stahl[1], Christopher T. Symons[1], and Robert E. Gillen[1]

[1]*Oak Ridge National Laboratory*

The Oak Ridge Cyber Analytics (ORCA) network intrusion detection system (NIDS) is a passive network sensor that uses supervised machine learning to analyze behaviors in channels of communication between individual computers. With examples of malicious and benign network traffic in the target environment, ORCA trains a classifier to recognize and discriminate between these traffic types, and generates alerts when it discovers traffic consistent with malicious traffic. Sensing via classification allows for detecting network behaviors similar to known intrusion tactics, yet not necessarily an exact pattern match, thereby broadening the detection aperture. The keys to ORCA's classification capability are a set of carefully selected learning algorithms, and a new method for simulating in-situ training data that makes the acquisition of labeled data more automated, practical, and cost-effective. The classifiers provide strong generalization performance, and provide an insight that would be difficult for a human to explicitly code as a set of rules because they evaluate dozens of interdependent metrics simultaneously. ORCA has been experimentally verified and is currently in the process of being operationally piloted on Department of Defense (DOD) networks. An overview of the ORCA technology will be provided, and also a description of the challenges and operational concepts for fielding a network traffic classification system.

Biologically-Inspired Algebraic Topology for Machine Learning

Ben Migliori[1,2], Justin Mauger[1], Daniel Gebhardt[1], and Brad Theilman[3]

[1]SPAWAR Systems Center Pacific [3]University of California, San Diego
[2]Los Alamos National Laboratory

The majority of neural encoding research uses expert-designed statistical or spectral features to convert neural signals to meaningful information. This empirical technique generalizes poorly between sensory domains, and is time-intensive to implement. Machine learning techniques may be used to similar effect, but they are not inherently suited to sparse sequences of events such as action potentials recorded by multi-electrode arrays. As array channel counts increase towards the millions, the high dimensionality and volume of data will make scaling either of these methods difficult.

The research presented here applies algebraic topology, in a biologically-inspired way, to the complex temporal interactions found in populations of spiking neurons (both simulated and measured). The use of algebraic topology (a field concerned with the geometry of high-dimensional data) exposes meaningful interactions not detected by traditional statistical analysis or other machine learning techniques. These interactions, captured by topological features or invariants, may then be used for discrimination tasks in both artificial and natural spiking neural networks. The presented results describe the use of such invariants to classify signals in artificial spiking neural networks.

As the fundamental principles by which living systems encode sensory stimuli are not yet analytically described, this research utilizes an animal model for architectural inspiration. Prior research has shown that topological invariants measured in starling auditory cortex have high discriminative power for song related tasks.

Using multi-electrode array recordings obtained in behaving starlings, algebraic topology can be employed to create simplicial complexes from n-wise temporal correlations of neuronal activity. The simplicial complexes capture ensemble spiking behaviors and the temporal dynamics of complex neural groups. Features such as persistent homology act as discriminators for neural activity caused by heterogeneous inputs. Topological features identified in biological recordings can be used to train artificial spiking neural networks, which are then tested against fully artificial inputs from non-sensory sources (specifically, digitally modulated radio-frequency transmissions). The performance of these algorithms are then compared and contrasted with standard artificial networks and with songbird behavior on related discrimination tasks. These results characterize the importance of topological invariants in spike timing dynamics to both natural and artificial sensory perception.

This research will establish a fundamental method for the unsupervised selection of features directly from spike encodings, and will have broad implications in both machine learning and computational neuroscience.

Event Detection and Summarization Using Phrase Networks

Sara Melvin[1,2], Wenchao Yu[2], Peng Ju[2], Sean Young[2], and Wei Wang[2]

[1]*Naval Surface Warfare Center Port Hueneme Division*
[2]*University of California, Los Angeles*

Identifying events in real-time data streams such as Twitter is crucial for many occupations to make timely, actionable decisions. It is, however extremely challenging to identify events because of the subtle difference between events and trending topics, the definitive rarity of these events, and the complexity of modern Internet's text data. Existing approaches often utilize topic modeling technique and keywords frequency to detect events on Twitter, which have three main limitations: 1) supervised and semi-supervised methods run the risk of missing important, breaking news events; 2) existing topic/event detection models are based on words, while the correlations among phrases are ignored; 3) many previous methods identify trending topics as events. To address these limitations, we propose the model, PhraseNet, an algorithm to detect and summarize events from tweets. To begin, all topics are defined as a clustering of high-frequency phrases extracted from text. All trending topics are then identified based on temporal spikes of the phrase cluster frequencies. PhraseNet thus filters out high-confidence events from other trending topics using number of peaks and variance of peak intensity. We evaluate PhraseNet on a three-month duration of Twitter data and show the both the efficiency and the effectiveness of our approach.

Intelligent Machine Abnormality Detection and Reaction Engine (IMADRE)

Roger Lamb[1], Dave Marchette[1], Matt Hackman[1], and David Johannsen[1]

[1]*NSWC Dahlgren Division*

IMADRE is a machine learning-based malware detection program intended to complement a signature based detection system. This type of detection is useful in environments where signature-based methods cannot be updated in a reasonable amount of time and to fill the gap of detecting zero-day malware. The focus of Phase I development was building models based off of n-grams of the executable file using implementations that are similar to language processing. Various methods of feature selection techniques were used including maximal differential and information gain in order to feed into a random forest-based model. Observing just n-grams (mainly uni-grams and bi-grams where a word is a byte), we maintained a success rate between 80% to 99% depending on which feature selection and model parameters were used. Overall, we found that n-gram analysis has impressive performance in identifying malicious files. Phase II of the project is an attempt to validate the findings of Phase I. The first (and narrowest) aspect of validation consisted of having an independent group use the same data as that used in Phase I to train random forest and k-nearest neighbor classifiers and verify the performance (classification error rates) reported. The second (and more important and more difficult) aspect of validation is to attempt to determine whether the classifier is actually classifying the byte-count signature of benign vs. malicious executables or whether it is some other aspect of the data that is being classified. This second aspect, though harder to answer, is more important because it determines whether the classifier will generalize (i.e., perform reasonably when presented with data that differs from that with which it was trained). Phase II is still ongoing at this time, however the validation

test runs performed so far have led to the formulation of a few hypotheses which we are currently exploring through additional test cases in an attempt to understand the model and determine whether it is operating as intended. Additionally, in the future, we intend to explore other features besides n-grams and examine data in motion for more dynamic malware detection.

Feature Selection for High-Dimensional Class Imbalanced Data

George Campbell[1]

[1]*SPAWAR Systems Center Atlantic*

High-dimensional data are common occurrences that can hinder the performance of classifiers. Their performance is further reduced when classes are imbalanced. Feature selection methods can be utilized to reduce the number of variables in a model and address the issues associated with high-dimensionality. Despite advantages of such methods, feature selection can increase the bias seen toward the majority class.

Various methods that have been developed and utilized for feature selection, such as information gain, correlation coefficient scores, and embedded algorithms, will be further analyzed to examine their performance on high-dimensional class imbalanced data. Results from simulations will illustrate the effects of feature selection and discuss difficulties commonly faced when classifying data including the following: sample size, imbalance ratios, dimension, and variance. Naval application areas discussed will include classifying natural language text data and detecting anomalous behavior in network traffic.

Applying Machine Learning and Data Mining to Obsolescence Management

Jennifer Williams[1], **Dennis Summers**[1], **Jordan Love**[1], **Connor Bradley**[1], **and Dallas Rosson**[1]

[1]*Naval Undersea Warfare Center Keyport*

Obsolescence management is a vital process when considering product implementation and design. It is particularly important when using Commercial off the Shelf (COTS) parts. The goal of obsolescence management is not only to determine when a part will become obsolete, but also to have a plan in place to account for future obsolescence issues. Having a tool that can provide a reliable early prediction of a parts date of obsolescence would be invaluable, especially in the early phases of acquisition. With this in mind, we explored machine learning and data mining approaches to determine whether machine learning is a feasible tool for obsolescence management.

There are several areas within machine learning methods that could be useful when managing the problem of obsolescence. Our research explored both supervised and unsupervised learning. While the main goal of this research was to predict the obsolescence date, there are several areas that need to be addressed before those predictions can take place. One area is identifying the part type. With part type information available, we can create a single model or individual models for each part type when predicting the obsolescence date. Differentiating between the part types could be addressed with a clustering approach (unsupervised learning) or a classification approach (supervised learning). While both were explored, we found that the classification approach performed the best, achieving 98% accuracy when classifying 34 part types.

Another area explored is handling missing data. Applying machine learning algorithms allow us to handle the missing values that are invariably present within any dataset. In this research, one of the missing features we focused on was the introduction date. To do this, we utilized regression algorithms (supervised learning) to predict the introduction date and fill-in the missing values. On average the prediction had between a 0.5 and 1.5 years error from the actual date.

With limited common data available for any part (i.e., data that can be collected from multiple sources), we explored data mining techniques to gather as much information from the data as possible. For instance, we could utilize extracted information about the relationship between part number and manufacturer to determine the numbering policy. This could help improve the prediction for the introduction date.

While these examples are not the only areas that have been addressed, they illustrate the various aspects within obsolescence management where machine learning can be utilized. As the main goal of this research was to predict obsolescence date, we focused on areas that would enhance the obsolescence prediction. Again, we utilized regression algorithms to predict the obsolescence date; on average the prediction had between 0.16 and 1.52 years error from the actual date. By applying machine learning algorithms to this problem set, we have been able to predict the part obsolescence date early enough to account for any issues that might arise.

Deep Wavelet Scattering Features for Infrasonic Threat Identification

Kaylen J. Bryan[1], Kaleb E. Smith[1], Mitchell Solomon[1], Dean A. Clauter[1], Anthony O. Smith[1], and Adrian M. Peter[1]

[1]*Florida Institute of Technology*

Infrasonic waves continue to be a staple of threat identification due to their presence in a variety of natural and man-made events, along with their low-frequency characteristics supporting detection over great distances. Considering the large set of phenomena that produce infrasound, it is critical to develop methodologies that exploit the unique signatures generated by such events to aid in threat identification. In this work, we propose a new infrasonic time-series classification technique based on the recently introduced Wavelet Scattering Transform (WST). Leveraging concepts from wavelet theory and signal processing, the WST induces a deep feature mapping on time series that is locally time invariant and stable to time-warping deformations through cascades of signal filtering and modulus operators. We demonstrate that the WST features can be utilized with a variety of classification methods to gain better discrimination. Experimental validation on the Library of Typical Infrasonic Signals (LOTIS) — containing infrasound events from mountain associated waves, microbaroms, internal atmospheric gravity waves and volcanic eruptions—illustrates the effectiveness of our approach and demonstrate it to be competitive with other state-of-the-art classification techniques.

Machine Risk Assessment

Mark Jenne[1], Ben Conley[1], and Mehmet Dalkilic[1]

[1]Naval Surface Warfare Center Crane Division

While the mission of the warfighter has remained unchanged since mankind began engaging in war, the contemporary warfighter has been continually augmented with technologies to improve effectiveness. Decisions are supplemented by sensor fusion: increasingly diverse, broader, and faster sensor data. These new modalities promise improved decision making that translates into markedly better mission success. The difficulty for the warfighter is that the original and simple problem of survival remains the same: the need to easily and extemporaneously assess risk — threat assessment — is paramount. Our work focuses on providing simple, real-time threat assessment to the warfighters so that they have the opportunity to take advantage of data fusion. The threat assessment provides varying levels of intrusiveness — visual cues that indicate both threat and (currently) non-lethal behaviors to decrease threat. An AI agent continually checks the warfighters actions to learn his preferences too — so that these personal behaviors become available in the future. Threat assessment is shared among warfighters and assets too. The area of decision theory, the study of normative rational choice, provided a starting point for our system, but the area remains relatively unchanged from its inception 50 years ago. Risk historically has been defined as uncertainty associated with some outcome based on an action. The outcomes are uniquely benign — loss of money, missed opportunity to purchase something more cheaply, or where to likely strike oil, and so forth. Our initial task was to characterize risk as it is faced by the warfighter: harm and exposure. Harm is the degree of lethality, as a function of time and space, that an object of interest poses to the warfighter: object detection. The exposure characterizes likelihood and frequency garnered from in the field data. Secondly, an AI threat agent must continually update and improve the system adding new experiences to the library of existing ones. More difficult is the black swan predictive system that works to signal possible novel risks that have not yet been encountered. The mission objective — initially very crude, provides required context to alternative paths given the exposure. A threat assessment system should eventually incorporate other modalities as the warfighter becomes accustomed to the unit — the motivation is that the warfighter must adopt the data organically. Aggregating warfighters and assets together provides a systemic threat assessment that allows for active sharing of data, risk, and solutions.

Infrasound Threat Classification: A Statistical Comparison of Deep Learning Architectures

Mitchell Solomon[1], Kaleb E. Smith[1], Kaylen J. Bryan[1], Anthony O. Smith[1], Dean A. Clauter[1], and Adrian M. Peter[1]

[1]*Florida Institute of Technology*

Infrasound propagation through various atmospheric conditions and interaction with environmental factors induce highly non-linear and non-stationary effects that make it difficult to extract reliable attributes for classification. We present featureless classification results on the Library of Typical Infrasonic Signals (LOTIS) using several deep learning techniques, including Long Short-Term Memory (LSTM), Self-Normalizing (SNN), and Fully Convolutional (FCN) networks with statistical analysis to establish significantly superior models. In general, the deep classifiers achieve near-perfect classification accuracies on the four classes of infrasonic events including mountain associated waves, microbaroms, internal atmospheric gravity waves and volcanic eruptions. Our results provide evidence that deep neural network architectures be considered the leading candidate for classifying infrasound waveforms which can directly benefit applications that seek to identify infrasonic events such as severe weather forecasting, military threat detection, natural disaster early warning systems, and nuclear weapons monitoring.

Human Presence Detector

Oliver Hui[1], Daniel Gebhardt[1], and Jason Landsborough[1]

[1]*SPAWAR Systems Center Pacific*

Cybercrime detection will be dependent on machine learning techniques, rather than signature-based detection methods, due to the increasing sophistication of attacks and growing amount of data. A component of such detection is user-based activity analysis or answering the question, "what general type of operation is the user performing on the computer?" We perform user activity classification utilizing long short-term memory neural networks to observe the series of system calls (or other low-level machine data sources). For this initial work, we classify the state as "user physically using system" or "not using system", which may provide a useful feature to a higher-level intrusion or insider threat detection system.

Low $WaP Trained Neural Net for NLoS applications

Peter Ateshian[1], CAPT A.W. Felder[2], Gurminder Singh[1], and David Wayne[3]

[1]*Naval Postgraduate School*
[2]*United States Marine Corps*
[3]*SPAWAR Systems Center Pacific*

Optical communications from simple hybrid RF/FSO Morse code as a SISO system and a MIMO laser diode QR code pattern transmissions can be implemented with simple low cost quad ARM Cortex A53 64bit (aka Rpi3) IoT devices. We are investigating RNN/CNN machine learning to compensate for the laser beam divergence or Raleigh smearing effects at reflected surfaces for nLoS and LoS applications at the receiver. Python QR, PyCrypto (for SHA3, RSA, Elliptic Curve Crypto) provide protected communications capabilities and 7-30% Forward Error Correction(FEC). We are investigating a minimum 21 × 21 QR array with 441 parallel channels (MIMO) and a single (SISO) Morse and quad Morse code (MIMO) systems. RNN/CNN on a Neural Compute Stick (fathom from Movidius) is the low $WaP device for 1.5 Watts for portable or Drone applications. These FSO systems are being designed for Undersea, Terrestrial, Marine, Airborne and Space application use cases by wavelength selection.

Relational Learning in Graphs with Deep Autoencoders

Phi "Vu" Tran[1]

[1]*Booz Allen Hamilton*

In this talk, we examine the task of learning to make predictions in graphs. A graph can be a partially observed set of nodes and edges, and the learning task is to predict the labels for nodes and edges. In realworld applications, the input graph is a network where nodes represent unique entities and edges (or links) represent relationships between entities. Moreover, the labels of nodes and edges are often correlated, exhibiting complex relational structure that breaks the assumption of independent and identical distribution. We propose a supervised model based on deep autoencoder that is trained end-to-end for collective link prediction and entity classification on a wide range of relational graphs. Our model extracts latent link patterns from globally sparse graph topology and combines latent features with optional explicit features to improve prediction. Numerical experiments illustrate significant improvement in accuracy over previously published research across multiple real-world graph datasets. Finally, we conclude the talk with remarks on the operational utility of this work to defense intelligence mission contexts.

Classification of Cortical Responses to Visual Targets During a Physical-Cognitive Interaction Task

Jamie Lukos[1], Michael Nonte[2], and Cortney Bradford[2]

[1]SPAWAR Systems Center Pacific
[2]Army Research Laboratory

In recent years, machine learning techniques such as hierarchical discriminant component analysis (HDCA) have been successfully applied to electroencephalography (EEG) data to classify neural responses associated with visual target detection [1, 2]. Although significant progress has been made to improve these algorithms for use on noisy data by enhancing the signal-to-noise ratio with novel transforms [3] and accounting for temporal variability through sliding windows [4], the application of these algorithms to data obtained during more complex, military-relevant scenarios remains unclear. Here, we apply this machine learning technique to EEG data collected while subjects were exposed to a physical-cognitive dual task.

Specifically, subjects walked on a treadmill for an hour carrying 40% of their body weight while performing a visual oddball task. Although we have previously shown differences in cognitive neural activity associated with variations in physical demands at the electrode level [5] and using cortical source localization techniques [6], here our goal is to determine if HDCA can successfully be used to classify single-trial neural responses. This work is an important step towards fielding brain-computer interface (BCI) technologies in real world environments.

References

1 Lucas C. Parra, Christoforos Christoforou, Adam Gerson, Adam Gerson, and Mads Dyrholm. 2007. "Spatio-temporal linear decoding of brain state: Application to performance augmentation in high-throughput tasks," In: *Signal Processing Magazine, Special Issue on Brain Computer Interfaces.*

2 David C. Jangraw, Jun Wang, Brent J. Lance, Shih-Fu Chang, and Paul Sajda. 2014. "Neurally and ocularly informed graph-based models for searching 3D environments," In: *Journal of neural engineering* 11.4.

3 Amar R. Marathe, Anthony J. Ries, and Kaleb McDowell. 2014. "Sliding HDCA: single-trial EEG classification to overcome and quantify temporal variability." In: *IEEE Transactions on Neural Systems and Rehabilitation Engineering* 22.2, pp. 201–211.

4 Amar R. Marathe, Anthony J. Ries, and Kaleb McDowell. 2013. "A novel method for single-trial classification in the face of temporal variability." In: *International Conference on Augmented Cognition.* Springer. July 21–26, Las Vegas, NV, USA, , pp. 345–352.

5 J. Cortney Bradford et al. 2016. "Effect of locomotor demands on cognitive processing." In: *38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC).* IEEE. August 16–20, Lake Buena Vista, FL, USA,

6 Jamie R. Lukos, J. Cortney Bradford, and Daniel P. Ferris. 2016. "Compensatory neural responses during a physical-cognitive dual task." In: *Society for Neuroscience Conference*. Soc Neuroscience. November 12–16, San Diego, CA, USA,

An Approach to Botnet Malware Detection Using Nonparametric Bayesian Methods

Roger Hallman[1], Joseph Divita[1], and Robert Morris[1]

[1]SPAWAR Systems Center Pacific

Botnet malware, which infects Internet-connected devices and seizes control for a remote botmaster, is a long-standing threat to Internet-connected users and systems. Botnets are used to conduct DDoS attacks, distributed computing (e.g., mining bitcoins), spread electronic spam and malware, conduct cyberwarfare, conduct click-fraud scams, and steal personal user information. Current approaches to the detection and classifcation of botnet malware include syntactic, or signature-based, and semantic, or context-based, detection techniques. Both methods have shortcomings and botnets remain a persistent threat. In this paper, we propose a method of botnet detection using Nonparametric Bayesian Methods.

In-Package Domain-Specific ASICs for Intel® Stratix® 10 FPGAs: A Case Study of Accelerating Deep Learning Using TensorTile ASIC

Eriko Nurvitadhi[1], Jeff Cook[1], Asit Mishra[1], Debbie Marr[1], Kevin Nealis[1], Philip Colangelo[1], Andrew Ling[1], Davor Capalija[1], Utku Aydonat[1], Sergey Shumarayev[1], and Aravind Dasu[1]

[1]Intel Corporation

Machine learning (ML) enables new capabilities/applications, including those of strategic importance to Navy. ML algorithms, such as deep neural networks (DNNs), demand high performance and efficient platforms to accommodate their tremendous compute requirements, as well as flexibility to accommodate myriad algorithm variants. Such high compute requirements drove the market towards accelerator solutions, such as FPGAs and ASICs. For example, Microsoft used FPGAs in Azure configurable cloud, while Google used TPU ASICs. FPGAs are extremely flexible (fine-grained, spatially programmable), while ASICs is efficient but inflexible.

We believe that FPGAs and ASICs are better together, to offer both flexibility and efficiency. We propose heterogeneous multi-chip integration of FPGAs and domain-specific ASICs in a single package, using Intels Embedded Multi-Die Interconnect Bridge (EMIB). Since the ASICs are separate chips from the FPGA, this approach (1) does not require FPGA fabric change, allowing re-use of existing ecosystems (FPGA chips, packaging, boards, tools, software, etc.), and (2) provides freedom in the ASIC design (area/freq/process/etc unconstrained by the FPGA). This approach is much cost-effective with faster time to-solution than developing traditional stand-alone ASICs. Intel® Stratix® 10 FPGAs are already built with EMIB extensibility, allowing single-package integration with other chips, or tiles, in an extremely versatile manner (can mix-and-match any Stratix 10 FPGAs with desired tile(s)). We propose leveraging such feature to integrate any domain-specific ASIC accelerator extensions for FPGAs.

In this work, we present a case study for the deep learning (DL) domain, which demands highly efficient tensor operations (i.e., matrix/vector multiply/accumulate). We propose TensorTiles, a family of ASICs to complement Stratix 10 FPGAs to execute DL tensor operations with ASIC efficiency, while

utilizing FPGAs flexibility to implement application/use-case specific portions (e.g., Winograd) of the target DL workloads. First, we explore the design space across various tensor precisions. On average, a small TensorTile (10s of mm^2, 14 nm process) can offer ~4x of peak tensor throughput of a large (2.7M LEs) Stratix 10 2800 FPGA, i.e., 30 FP16 TOPs in <15W. We show extremely scalable solutions. A large Stratix 10 2800 FPGA with 6 small tiles offers ~194 peak FP16 TOPs, which is higher than the through-put of the latest high-end Volta GPU. On the other hand, a small Stratix 10 400 (378K LEs) with one tile offers ~69 INT8 TOPs. Second, we evaluate known DNNs and show that EMIB serves as an efficient FPGA/ASIC link, enabling high utilization of TensorTiles. Finally, we present a case study in accelerating Intel OpenCL Deep Learning FPGA solution with 2x tiles, and shows 4x and 3.3x improvements in performance and performance/watt on AlexNet over FPGA-only solution. Overall, this approach is an effective, versatile, and scalable solution.

Training Logistic Regression Over Encrypted Data

Hao Chen[1], Kyoohyung Han[1], Zhicong Huang[1], Amir Jalali[1], Kim Laine[1], Ran Gilad-Bachrach[1], and Kristin Lauter[1]

[1]Microsoft Research

Machine learning over encrypted data has important applications for cloud security and privacy. It allows sensitive data such as genomic data to be stored in the cloud in encrypted form without losing the utility of the data.

For the third task of the iDASH 2017 Secure Genome Analysis Competition, participants are challenged to train a machine learning (ML) model on encrypted genomic data, in order to predict disease based on patients' genomes. Training ML models on encrypted data had up until now only been done for very simple ML algorithms such as Linear Means and Fisher's Linear Discriminant algorithms. The 2017 iDASH competition task is to train a logistic regression model, and although in theory it can be done using Fully Homomorphic Encryption (FHE), until now the feasibility and efficiency of this approach had not been studied.

In this work, we show that training a logistic regression model over binary data is possible using FHE. In particular, we use gradient descent and stochastic gradient descent algorithms, and we demonstrate that it takes several minutes to one hour to run each gradient descent step. This is possible using bootstrapping, which we have implemented for the first time for the SEAL library. SEAL is a publicly released Homomorphic Encryption library developed by Microsoft Research. It uses the FV encryption scheme and parameters can be set to achieve various desired security levels, such as 80-bit, 128-bit, or 256-bit security.

A Machine Learning Approach for Predicting Atmospheric Aerosol Size Distributions

Joshua Rudiger[1], Kevin Book[1]

[1]SPAWAR Systems Center Pacific

An accurate model and parameterization of aerosol concentration is needed to predict the performance of electro-optical imaging systems. Current models have been shown to vary widely in their ability to accurately predict aerosol size distributions and subsequent scattering properties of the atmosphere. One of the more prevalent methods for modeling particle size spectra consists of fitting a modified gamma function to measurement data, however this limits the distribution to a single mode. Machine learning models have been shown to predict complex multimodal aerosol particle size spectra. Here we establish an empirical model for predicting aerosol size spectra using machine learning techniques. This is accomplished through measurements of aerosols size distributions over the course of eight months. The machine learning models are shown to extend the functionality of Advanced Navy Aerosol Model (ANAM), developed to model the size distribution of aerosols in the maritime environment.

IBM Data Science Experience

Brian Ruther[1]

[1]IBM

Data scientists are tasked with turning raw data into meaningful insight using state of the art analytics. Doing so requires the best tooling, including open source innovation, coupled with social features for sharing and collaborating. IBM Data Science Experience provides a one-stop-shop for data scientists to learn about new tools and trends, create value using the best of open source and IBM, and collaborate on projects with their teams and the broader data science community.

Addressing Supply Chain Risks of Microelectronic Devices Through Computer Vision

David Crandall[1], Zhenhua Chen[1], and Robert Templeman[2]

[1]Indiana University
[2]Naval Surface Warfare Center Crane Division

Microelectronics now control nearly all devices, ranging from small embedded integrated circuits inside household products to complex microprocessors that power critical infrastructure systems. Devices often consist of numerous ICs from a variety of different manufacturers and procured through different vendors, all of whom may be trusted to varying degrees. Ensuring the quality, safety, and security of these components is a critical challenge. One possible solution to combat counterfeit or malicious components from entering devices in high-volume manufacturing contexts is to use automated imaging

techniques to ensure that their physical appearance is consistent with known reference models. This analysis can be performed at both a macro level (i.e. ensuring that the packaging of the IC appears legitimate and undamaged) and the micro level (i.e. comparing microscopic, transistor-level imagery of the circuit itself to detect suspicious deviations from a reference model). This latter problem in particular is very challenging, considering that modern devices an contain billions of transistors. We discuss our recent work on the application of computer vision and machine learning to microelectronic inspection, presenting initial results and recommending directions for future work.

Causal Learning: Analysis for Action

David Zubrow[1], Mike Konrad[1], and Bob Stoddard[1]

[1]*Software Engineering Institute Carnegie Mellon University*

Many machine learning and statistical algorithms utilize various measures of correlation or bivariate association for classifying and making predictions. Many years of advances have allowed algorithms based on these measures to perform amazingly well. However, this capability is not sufficient for guiding action. Rather, causal knowledge must be at the foundation for understanding where to intervene to improve a situation or to remedy a root cause. Traditionally, controlled experimentation has been the gold standard and remains so today. Unfortunately, in many circumstances controlled experimentation is either too expensive or unethical to perform. Over the past 30 years, a form of machine learning called Causal Learning (CL) has become increasingly practical to perform. CL makes use of observational data and seeks to discover and estimate candidate causal models from data.

Key to CL is the ability to make a causal inference in a bivariate relationship. Simply stated, if x causes y then when x changes ys value (or the probability of a particular value for y) should change. However, the converse should not be true. If y is directly changed it should have no effect on x. In a multivariate situation, this idea is extended based on techniques for testing conditional independence. By testing for conditional independence, the algorithms build directed acyclic graphs (DAG). Here is a brief description of how such a DAG is constructed. Imagine a complete graph G that includes variables X and Y. If there exists any subset S (including the empty set) of the remaining variables in G such that in the original dataset X and Y are conditionally independent given S, then the edge between X and Y is removed. This test is iterated in a selective and time efficient manner across the graph. The orientations of edges (whether X directly influences Y; conversely; bi-directionally, which indicates presence of a confounder; or indeterminate) are typically determined in a later phase of the algorithm.

We are applying CL to identify drivers of software effort and cost. Cost models contain a wide array of parameters which are used to predict software effort and cost. Such knowledge is inadequate, however, as a guide for how to intervene or take corrective action during a program. Until recently, there was no way to efficiently separate the causal influences from non-causal statistical correlations and, therefore, to make reliably actionable inferences from the models. In this presentation, we will present and discuss our results of applying causal learning to Software Resources Data Report (SRDR) data from 134 DOD software projects where we had initial estimates and final actual software measures. The results of this early analysis show some expected and some surprising results. We will also present a brief introduction to CL as well as lessons learned regarding its use.

Applications of Random Forests for Modeling Obsolescence

Emily Nystrom[1], Anthony Leclerc[1]

[1]SPAWAR Systems Center Atlantic

We are interested in predicting the obsolescence date, the time at which a component will be discontinued by the original manufacturer. The inconvenience of system disruption (e.g., due to component non-availability) motivates the development of analytical tools that are able to support proactive strategies for anticipating future obsolescence. Building on the application-methods pairing highlighted in [1], we consider using random forests to predict obsolescence for Navy systems. Our research extends the literature by also considering random survival forests, which can account for censoring encountered in obsolescence data.

References

1 Connor Jennings, Dazhong Wu, and Janis Terpenny. 2016. "Forecasting obsolescence risk and product life cycle with machine learning." In: *IEEE Transactions on Components, Packaging and Manufacturing Technology* 6.9, pp. 1428–1439.

Overhead Detection: Beyond 8-bits and RGB

Samuel Dooley[1], Eliza Mace[1], Monica BarbuMcGinnis[1], Matt Klaric[1], and Mike Laielli[1]

[1]National Geospatial-Intelligence Agency

This study uses the challenging and publicly available SpaceNet dataset to establish a performance baseline for a state-of-the-art object detector in satellite imagery. Specifically, we examine how various features of the data affect building detection accuracy with respect to the IoU metric. We demonstrate that the performance of the R-FCN detection algorithm on imagery with a 1.5-meter ground sample distance and 3 spectral bands increases by over 32% by using 13-bit data, as opposed to 8-bit data at the same spatial and spectral resolution. We also establish accuracy trends with respect to the parameters building size and building density. Interestingly, our results are fairly robust to the choice of spectral bands and do not improve by using more than three. Finally, we propose and evaluate multiple methods for integrating additional spectral information into off-the-shelf deep learning architectures.

Explaining Classifiers Via Information Tracking

Katie Rainey[1], Marissa Dotter[1], and Donald Waagen[1]

[1]SPAWAR Systems Center Pacific
[3]Air Force Research Laboratory
[2]Point Loma Nazarene University

To fully understand deep learning, we must understand both the algorithms and the data. Very often the generalizability of an algorithm — its ability to apply what it has learned in the training phase to previously unseen data — is overlooked in favor of impressive accuracy results. This white paper outlines several approaches for understanding how deep learning algorithms represent the data that they are applied to, and how to best design a network based on the complexity of the data at hand. The proposed work will investigate ways to characterize the performance of an algorithm with respect to a dataset. It will trace data distributions through various pieces of deep learning architectures, and develop methods to design appropriate architectures for tactical applications. This work is an important step towards understanding the generalizability of deep learning algorithms, and therefore explaining their performance as part of more complex systems.

Laboratory for Analytic Sciences' OpenKE Methodology to Manage the Big 'D'

Sheila Bent[1], Robert Beck[1]

[1]Laboratory for Analytic Sciences

The Laboratory for Analytic Sciences blends art, science and technology to design Open Source (OS) Tradecraft and advance analytic workflow by developing and automating techniques, capabilities, and processes to leverage publicly available information (PAI). According to Executive Order 12333, "1.1 (e)

Special emphasis shall be given to the production of timely, accurate, and insightful reports, responsive to decision-makers in the executive branch, that draw on all appropriate sources of information, including OS information, meet rigorous analytic standards, consider diverse analytic viewpoints, and accurately represent appropriate alternative views."

Growing worldwide Internet access, the rise of social media, advances in technology, and the general proliferation of PAI provide compelling reasons to employ OS to defend and protect the nation. Open Source is immeasurable as it can support indications and warning, tip and cue other intelligence disciplines, validate context for classified information, compensate for reductions in other intelligence capabilities, ensure better global coverage and a more holistic view of an event, fill gaps or eliminate erroneous subjects, assess population sentiment, discern trends and patterns, track scientific and technological developments, aid in researching and understanding crises, disease outbreaks, economic instability and many other anomalies.

LAS has developed a platform called OpenKE. OpenKE is an Open Source Knowledge Enrichment database to manage the complexities of capturing, formatting, manipulating and making sense of Big Data. The platform hosts techniques and analytics designed to be semi-automated and allow for configuration to scan a wide range of structured and unstructured data sources. OpenKE will help capture the 'right' information from the right (reliable) sources and feed selective relevant information into the classified environment; thus, delivering the capability to holistically analyze Big Data within the unclassified environment and integrating data of value into the mission environment.

OpenKEs initial use case employed PAI to research emerging technologies, specifically hobby drones.

The emergence of hobby drones, now used as weapons by terrorists organizations, presented numerous challenges in the IC. One challenge analysts encountered was the lack of capabilities to quickly scan large data sets, in near real-time, from PAI sources. Additionally, analysts lack scientific methods to efficiently and effectively make sense of PAI to assess the value and reliability of that information.

The OpenKE prototype will provide a mechanism to retrieve, structure, organize, assess, and filter OSI Investigate, test, and evaluate new technologies, scientific methods, processes and analytics in an unclassified setting. Create a collaborative, scalable, and agile environment for general research and discovery.

ENSIGN: Unsupervised Multidimensional Pattern Discovery Scaled to HPC

James Ezick[1], Muthu Baskaran[1], Thomas Henretty[1], M. Harper Langston[1], Aditya Gudibanda[1], Pierre-David Letourneau[1], and Richard Lethin[1]

[1]Reservoir Labs

ENSIGN is a high-performance tensor decomposition suite that enables the unsupervised discovery of deep patterns in structured, multidimensional datasets. Tensor decompositions represent a new paradigm in big data analytics — one where pattern discovery is the starting point rather than the end goal of the analysis. Tensor methods extract discrete, coherent patterns of activity captured as weighted components. These methods go far beyond other unsupervised methods, such as clustering or PCA, in that they can discover recurrent patterns spanning multiple dimensions of data simultaneously. Tensor methods have shown promise in application to large-scale problems in cybersecurity and geospatial intelligence analysis.

In this presentation, we provide an overview of the ENSIGN technology, its applications, and a survey of current research and engineering directions. ENSIGN is being developed to bring the power of tensor methods to data scientists operating in modern, interactive environments backed up by HPC resources. The core of ENSIGN is a suite of decomposition routines built on specialized data structures that are optimized for large shared-memory, distributed memory (cluster), and cloud architectures. Using these modern high performance computing resources, ENSIGN has succeeded in factoring thousands of components from datasets containing billions of entries. On top of these methods, ENSIGN provides support for modern Python-based workflows and integrates with existing popular machine learning packages such as those included in Anaconda.

Operating the past three years in the Security Operations Center (SOC) at SCinet — the large-scale research network stood up each year in support of Supercomputing (SC) — ENSIGN has analyzed

metadata collected for more than one-billion network flows. From that data, ENSIGN has separated normal and off-normal patterns leading to the discovery of anomalous and alarming behavior, including distributed scans evolving to machine takeover, data exfiltration through abuse of control and backchannel message streams, and exploitation of application-specific port vulnerabilities. Applied to open geospatial data sources published by state and municipal governments, ENSIGN has extracted recognizable patterns of human behavior. A demonstration of this capability applied to Yellow Cab Taxi data from NYC shows how it identified popular nightlife destinations and residential districts associated with interest in the arts.

Frontiers in ENSIGN include further optimization of incremental decomposition update methods useful for streaming data sources, support for automating classification of tensor components, and development of unique visualization and integrated data-exploration tools specialized to tensor methods. The overarching goal of ENSIGN is to provide the foundation for building automated workflows that can deliver to analysts' decisive insight from large-volume data sources in a timely and trustworthy manner.

GLOBALEYES

Neal Anderson[1]

[1] *Northrop Grumman*

Big Data research focuses on identifying disruptive technologies and developing prototypes that will capitalize on their unified capabilities. Combining todays open-source tools into an integrated extensible platform with pluggable analytics architecture; extensible distributed system and analytic metrics and monitoring with visualization tools; a highly optimized data ingest, storage, and age-off architecture enables a big data platform for streaming and forensic data analysis.

Our approach moves sense making analytics forward in the processing stream to support better insights for cyber missions and large distributed cloud analytic environments. Focus areas include exploring large-scale streaming updatable graphs for new mission analytics, object based tracking, Linked Object Data (LoD), and distributed Internet of Things (IoT) analytic architecture challenges. Research from this investment enables several cost effective and mission oriented benefits for better analytic insights and quicker intelligence for "Cyber-time" results as demonstrated on the Globaleyes and Maritime prototype concepts.

Globaleyes combines streaming data analytic harness with a graph database platform for next generation linked objects. It demonstrates a generalized open source based graph based data analytic prototype concept aimed at scalable analysis of very large graph data structures represented by the Linked Open Data (LoD) community. Open source and synthetic data sets are combined for complexity and performance at extreme data rates to evaluate ingest rates, size, bandwidth limitations and visualization capabilities.

Maritime prototype explores high volume real-time object based tracking with open source geographic mapping. It demonstrates ability to provide flexible, scalable, real-time cloud analytics with streaming data, real-time alerts, bare metal cloud and virtualization. The interoperable framework bridges streaming data and big data analytic cloud with virtualized workflow at scale.

Adversarial Learning for Deep Neural Networks (ALaDNN)

Ramesh Bharadwaj[1]

[1]*Naval Research Laboratory*

TECHNICAL OBJECTIVE

Deep learning has received wide press in the recent past. Although requiring massive computational power to train, these algorithms show great promise by being able to recognize objects with human level precision and translating human speech in real-time. The stunning performance of deep learning compared to extant methods, including pattern matching, statistical, and legacy machine learning algorithms, has taken the world by storm. This naturally leads the DoD and the expeditionary cyber community to ask the question: "How do we harness this technology being unleashed upon the world?"

To answer this question, we not only have to come to grips with — fast paced — recent advances in deep learning, but also understand its limitations. For instance, data sparsity and data poisoning attacks may lead to classification and training errors, producing incorrect results which can be both embarrassing and damaging. Two recent examples are Google's image classifier mis-identifying humans as gorillas and Microsoft's chatbot Tay learning to spew racist and misogynistic hate speech minutes after being turned on. More disturbingly, the invention of generative adversarial networks (GAN) shows that deep learning algorithms can be deliberately tricked by adversarial examples. A trained neural network can be tricked into grossly misclassifying objects with extremely high confidence, by mere manipulation of their images not discernable to the human eye or even by images that look like noise to the human viewer. The dangers of adversarial attacks can have a profound impact on society — self-driving vehicles can be hijacked or mis-directed with seemingly innocuous signage, and system security can be compromised with tampered data.

TECHNICAL APPROACH

This project will explore strategies to harness deep learning algorithms, including convolutional and recurrent neural networks (CNN and RNN), and reinforcement learning (RL), for the design and development of machine learning tools that provide robust, secure, timely, and dependable command, control, communications, computers, and intelligence (C4I) at the tactical edge. Systems developed with our carefully crafted set of tools would be deployable on expeditionary platforms that are limited by size, weight, and power (SWaP) constraints. Additionally, they will achieve real-time performance for anomaly detection and mitigation of threats to blue force platforms and assets, in an anti-access area denial (A2AD) environment, while denying the adversary use of limited resources such as the electromagnetic spectrum.

The toolset we propose to build will center around data that can be modeled by two-dimensional tensors (2-D tensors), which includes images and handwriting commonly handled by commercial tools. Datasets within the DoD, however, include numerous other categories that may also be modeled as 2-D tensors. These includes spectrograms — visual representations of the spectrum of frequencies of electromagnetic waves, sound, or other signals as they vary with time, and pulse-Doppler videograms of received radar returns. In the cyber domain, as well as in statistics, econometrics, epidemiology, genetics, and related disciplines, causal graphs — also known as path diagrams or causal Bayesian networks — encode assumptions about the data generation process, which can also be modeled as 2-D tensors. They are widely used for communication, to provide a formal and perspicuous representation of the assumptions and flows, and inference, enabling derivation of testable implications of the encoded

assumptions. One of the major challenges of making deep learning widely accessible to the military is hyperparameter tuning. In machine learning, parameters are variables that are tuned by the learning algorithms. Hyperparameters govern the effectiveness of the training process and serve as configuration variables. We will explore automated approaches to hyperparameter selection and tuning, on the lines of technology being developed by Google known as CloudML. In collaboration with Prof. Xue Lin and her approach of Alternating Direction Method of Multipliers (ADMM), we propose to harness unified methods for the generation of adversarial examples with high success rates. Network traffic, for instance, can be characterized as normal and abnormal, on which a neural network can be trained to provide alerts (with associated confidence levels). Further, these alerts can help trigger mitigating actions such as disabling network devices or powering down sensitive equipment. ADMMs will provide the tools necessary to determine whether or not these defensive measures are effective. Among approaches for attack mitigation, we propose to explore regularization and adversarial training methods documented in the literature. More promising approaches include adaptive regularization, which encourages robustness against all attacks, and semidefinite relaxation methods, which provide certificates guaranteeing that for a given network and test inputs no attack can force the classification error to exceed a given value.

Transformational Learning

Stuart Rubin[1]

[1]*SPAWAR Systems Center Pacific*

One of the major unsolved problems involving machine learning pertains to the effective transference of knowledge. Humans learn by analogy with past experiences. For example, identical twins — each new to the game of chess, but one of whom knows checkers will learn chess at different rates because some, but not all of the checkers knowledge, maps onto the game of chess. The parts that so map are said to be symmetric; whereas, the remaining parts are said to be random. Almost all real-world knowledge falls into a mixture of the two categorizations. The task, addressed in this talk, pertains to how to effectively perform the symmetric mapping for more or less arbitrary domains, what it means to be random or thus symmetric, and the type of problems amenable to symmetric solutions. It is now a known fact that neural networks (e.g., deep learning) do not learn by symmetric mapping; although, akin to other AI technologies, they can be trained to effect it [1, 2]. It follows that the function of the brain is not isomorphic with the function of hidden-layer neural networks. The theory of randomization will be introduced and holds that knowledge can be compressed to unbounded density. This means that the virtual knowledge space is $\gg$ the actual knowledge space. We will discuss the role of transformation in creating a virtual knowledge space. Moreover, such transformations cannot be effectively hill-climbed — implying the need for realization on massively parallel architectures (MPP). The brain is representative of such a massively parallel architecture and provides the biological inspiration for the approach. Moreover, hidden-layer neural networks are inherently intractable to train [3] — unlike transformative approaches. Furthermore, transformative approaches allow for symbolism and explanations — ameliorating two deficiencies in all neural networks. As a result, it should be possible for transformative learning to enable higher memory densities, commonsense, deduction, induction, and fuzzy logic within the context of massively parallel search. In conclusion, the theory of randomization predicts non-computable behaviors concomitant with a scale permitting self reference. It is the non-computable elements that cannot be effectively learned and serve to differentiate the brain from the computer. Could it be any other way?

References

1 Hossein Hosseini and Radha Poovendran. 2017. "Deep neural networks do not recognize negative images." In: *arXiv preprint*.

2 Hossein Hosseini, Sreeram Kannan, Sreeram Kannan, Baosen Zhang, and Radha Poovendran. 2017. "Deceiving Google's perspective API built for detecting toxic comments." In: *arXiv preprint arXiv:1702.08138*.

3 Jyh-Han Lin and Jeffrey Scott Vitter. 1991. "Complexity results on learning by neural nets." In: *Machine Learning* 6.3, pp. 211–230.

Avoiding Catastrophes: Worst-Case Optimization with Applications to Multistatic Active Sonar Arrays

Thomas Powers[1], David W. Krout[2], Jeff Bilmes[1], and Les Atlas[1]

[1]*University of Washington*
[2]*University of Washington Applied Physics Laboratory*

A central consideration in multi-objective optimization problems is how to balance the objectives. For some such problems, simply averaging the objectives is sufficient, but often success is measured by the objective on which the estimated solution performs worst, as is the case in applications like multi-target tracking and outbreak detection.

We address scheduling for deep water active sonar arrays, in which the goal is to transmit a signal and generate reflections off of a detectable target. In our framework, each buoy has a co-located transmitter and receiver that operates monostatically. However, we propose an algorithm that allows for multiple buoys to be selected, and so the array functions multistatically in that multiple receivers are operating simultaneously and at potentially overlapping coverage regions. In any depth of water, the sound from a buoy at the surface will propagate along the surface for a few kilometers until it attenuates significantly, and will propagate much further downward due to temperature and pressure gradients. Then the sound arcs back up to the surface and back down, forming concentric rings around the transmitter called convergence zones.

In the first convergence zone, there is enough sound energy that a reflection off of a target is potentially detectable. In the second convergence zone, there is still significant signal energy, just not enough to reflect all the way back. However, if there is a second buoy in this region, the signal energy will only serve to interfere with the second buoy as it listens for reflections from its own ping. The result is a combinatorial constraint on the non-interfering subsets of buoys, which can be optimized over directly. We can select buoys based on target state that significantly improve the probability of detecting targets over a standard approach and achieve equivalent performance to an optimal exhaustive search approach. Moreover, our approach allows for simultaneous search and track objectives within the system.

This problem is an instance of a more general problem: constrained maximization of the minimum of a set of submodular functions. Unfortunately, this problem is both non-submodular and inapproximable, meaning no meaningful lower bound can be computed. However, by relaxing the problem, an approximate solution can be found. We propose the algorithm Generalized Saturate (GenSat) that

exploits the submodular structure of the problem. As a result, GenSat returns a solution with a constant-factor approximation guarantee on the relaxed problem. GenSat and can also handle any submodular constraint, e.g. matroids, cover, and knapsack, that is compatible with an appropriate submodular maximization algorithm. In doing so, we unlock a new and useful class of discrete optimization problems and demonstrate the utility of GenSat on sensor selection and facility location applications.

Support Vessel Scheduling for Pacific Northwest Test Ranges

Sandy Kelly[1], Nicholas Rau[1]

[1]*Naval Undersea Warfare Center, Keyport Division*

Naval test ranges in the Pacific Northwest are used heavily for a variety of test and special in-water events. In order to support customer needs, range assets, such as support vessels, must be available to support the testing on range. Two main vessels are regularly used in range testing events. As the vessels age, resolving operational and maintenance schedules become increasingly complicated. Range scheduling is traditionally done manually by subject matter experts (SMEs). This project was started to reduce the time spent generating these schedules and to better understand the maintenance impact. To do this, multiple range scheduling approaches were investigated. The goal of the effort was to predict which activities the vessels will perform per month for future years, as well as the impact to range testing that may need to be mitigated.

Queueing theory and predictive modeling through machine learning techniques were pursued with promising results. Existing data sets were used to build 30+ models and assess their performance. Additional work is being conducted to expand this work from two vessels to overall range operation. This additional effort expands the results of the range scheduling work by creating more comprehensive data sets and by analyzing and predicting more than range schedules. This presentation will discuss the methods and techniques used to rapidly produce predictive schedules for future year activities of two key range vessels, software used, data that was important to use and maintain, as well as follow on work.

Machine Learning Prediction of Seafloor Properties

Warren Wood[1]

[1]*Naval Research Laboratory, Stennis Space Center, MS*

OBJECTIVE

Use a machine to find multidimensional correlations between geologic parameters from the global store of marine geologic data, and use those correlations to predict seafloor parameters in places they were not directly measured.

INEXPERIENCE — WHERE GEOGRAPHICALLY, WOULD MORE SAMPLES HELP MOST?

Inexperience is a measure of how well the predictor space is sampled by the observations. The map below indicates at each geospatial point, the relative distance (in parameter space) to the nearest neighbors. Geographic locations where we have data show up as low inexperience. Geographic locations that are geologically dissimilar to any observed point manifest as more distant in predictor space, and therefore higher inexperience.

UNCERTAINTY IN PREDICTION

We use the standard deviation of the k values of the nearest neighbors as an estimate of the prediction error (uncertainty). If the observed values of the k nearest neighbors in predictor space are all very similar, the standard deviation (error, uncertainty) will be low. A well sampled parameter space will ensure the smallest spread of values for any given set of predictors.

Applying Autonomy on the Carrier Flight Deck

Ari Goodman[1], **James Hing**[1], **and Kyle Hart**[1]

[1]*Naval Air Warfare Center Aircraft Division*

Automation is a key technology for optimizing workload, improving safety, and increasing the efficiency of our Sailors onboard aircraft carriers in the Navy. A potential application of autonomy is the Strike Up Process aboard aircraft carriers which involves the movement of ordnance from the magazine to the flight deck using weapon skids. A number of challenges need to be addressed to achieve autonomous weapons movement through the use of robotic mechanized weapon skids. This paper culminates the work from several projects, each of which addresses unique challenges associated with developing the autonomous capabilities of robotic mechanized weapon skids. We address GPS denied, external infrastructure free, autonomous local and global planning for simulated carrier environments through an arc routing algorithm and Reciprocal Velocity Obstacles, and test our algorithms in simulation in a physics simulator and in the real world using multiple Robotnik Summit XLs. The challenge of formation distribution and control, which is necessary for the efficient parking of multiple weapon skids within staging areas, is addressed through convex optimization and Hungarian Optimization algorithms. A sensor suite and set of algorithms were explored to allow for non-reference based anomaly detection and robust localization in degraded visibility environments expected on a carrier deck, specifically fog. Multiple user interfaces were developed in an attempt to optimize the

information presented to the user to allow for easy operation and quick error awareness. The capability to verify and validate the robots performance is being developed through the applications of Monte Carlo simulations and formal methods. The culmination of the solutions to the aforementioned challenges moves toward the capability of using autonomous mechanized weapon skids to move ordnance onboard an aircraft carrier.

A Task Flexible UAS Development Platform

2d Lt Taylor Bodin[1], Maj. Jason Bindewald[1], and Gilbert Peterson[1]

[1]*Air Force Institute of Technology*

Fully autonomous sea, land, and air vehicles represent one of the most disruptive innovations in modern warfare. As such, it is of the utmost strategic importance that the U.S. and its allies lead in the areas of autonomy research and adoption of capable autonomous systems. This imperative is made difficult by the fact that such systems are incredibly complex, time consuming to design, and highlyunpredictable without extensive testing in the field. Furthermore, it is often difficult to extend a system's functionality to cover additional use-cases or reuse components. To enable rapid development and extensibility, the DoD requires a modular platform for the development and modification of vehicle-borne agents.

The Unified Behavioral Framework (UBF) [1] aids in producing modular robotic agents that are both responsive and robust in dynamic, unpredictable environments. The UBF improves upon traditional behavior based approaches by abstracting behavior logic from the underlying robotic controllers. This allows new behaviors to easily be incorporated and existing behaviors to be modified, extended, and reused. Although past implementations of the UBF have produced capable agents [2, 3, 4, 5], overall task flexibility was limited by their ground-based platforms. In contrast, Unmanned Aerial Systems (UAS) offer great task flexibility to robotic agents due to their high mobility. Additionally, open-source development platforms, such as the Robot Operating System (ROS) and the PX4 autopilot, offer rich APIs capable of integrating the UBF with other components. This research presents, as a work-in-progress, the design and test of platform for the development of task-flexible autonomous agents by integrating the UBF with ROS on a UAS.

To assess the task flexibility of the platform, a multirotor UAS agent executed a series of dynamic navigation tasks. Simulated flights in Gazebo, a high-fidelity robotic simulator, established baseline agent performance according to a objective metric. Flight tests using a X8 multirotor later validated these results. Demonstrated performance shows the platform to be an effective means to rapidly develop and tune behavior-based agents for a variety of tasks. This platform allows users to focus on research interests as opposed to implementation details tangential to their work. For example, a COTS UAS could easily be integrated with additional sensors and actuators using ROS and then utilize a library of trusted behaviors from the UBF to perform a novel function. Permissive licensing of opensource components allow the DoD to close the architecture if elevated classification is necessary. Finally, the UBF ROS integration lays the ground work for future work on the platform offering fully autonomous agents which are cognitively flexible through the addition of a deliberative components and peer flexible through the addition of social components.

References

1 Brian G Woolley and Gilbert L Peterson. 2009 "Unified behavior framework for reactive robot control." In: *Journal of Intelligent and Robotic Systems* 55.2-3, pp. 155–176.

2 Brian G Woolley. 2007. "*Unified behavior framework for reactive robot control in real-time systems*." Technical Representative, Air Force Institute of Technology Wright-Patterson Air Force Base, OHIO School Of Engineering and Management.

3 Daylond J Hooper. 2007. "*A Hybrid Multi-Robot Control Architecture*." Technical Representative, Air Force Institute of Technology Wright-Patterson Air Force Base, OHIO School Of Engineering.

4 Jeffrey P Duffy. 2008. "*Dynamic Behavior Sequencing in a Hybrid Robot Architecture*." Technical Representative, Air Force Institute of Technology Wright-Patterson Air Force Base, OHIO School of Engineering and Management.

5 Stephen S Lin. 2009. "*Unified Behavior Framework in an Embedded Robot Controller*." Technical Representative, Air Force Institute of Technology Wright-Patterson Air Force Base, OHIO School of Engineering and Management.

6 Taylor B Bodin. 2018. "*Behavior Flexibility for Autonomous Unmanned Aerial Systems*." Technical Representative, Air Force Institute of Technology Wright-Patterson Air Force Base, United States.

Acoustic Model Emulation Using a Neural Network

David W. Krout[1]

[1]*University of Washington Applied Physics Laboratory*

A common issue in solving any optimization problem that involves underwater acoustics, is the computational cost of the acoustic model. In order to minimize the computational cost of the acoustic model, an artificial Neural Network (NN) was trained to emulate acoustic model input/output relationships. This was originally motivated by the difficult task sonar operators face during operations. Operators adjust sonar settings for optimal performance as tactical goals change and as the underwater acoustic environment changes in space and time. Effective sonar control requires accurate prediction of how the sonar will perform in a given configuration and in a given environment. This presentation will outline a methodology for training NNs in order to provide the necessary performance predictions for an automated sonar controller. The initial research and development for these NNs was in the mid 2000s, and later they were used in other optimization algorithms to solve sensor management problems such as ping sequencing and sensor placement. A few of the ONR D&I funded projects most directly associated with this work are summarized below and will be discussed in the presentation:

ENVIRONMENTALLY ADAPTIVE SONAR CONTROL

This project explored a method of statistically characterizing a given operations area, generating a large ensemble of acoustic model runs, and training specialized artificial neural networks to emulate acoustic model input/output relationships for sonar controller environment optimization.

DISTRIBUTED ENVIRONMENTALLY-ADAPTIVE DETECTION, CLASSIFICATION, AND LOCALIZATION USING A COOPERATIVE SENSOR NETWORK

This project developed algorithms for environmentally adaptive sonar signal processing using a distributed network of active acoustic sensors. In particular, we developed distributed detection, classification, and localization (DCL) algorithms incorporating environmental inversion. This effort addressed some of the unanswered scientific issues at the heart of the deployment and operation of a distributed sensor network.

MULTI OBJECTIVE SENSOR MANAGEMENT

This work investigated the multiobjective nature of the sensor management problem, specifically ping optimization, without sacrificing accuracy and objectives (Coverage, Track Hold, Field Longevity, etc.).

From Advanced Automation to Cognitive Autonomy

Hope Allen[1]

[1] *Northrop Grumman*

Fundamental to advancing our autonomous capabilities is the ability to rapidly integrate and effectively manage a variety of on-board sensors and actuators required for accomplishing mission objectives in ever-changing environments. The autonomous system needs to understand commanders intent and collaborate with other warfighters and systems in achieving mission goals. Rapid advances in low-SWAP high-performance computation are enabling the practical deployment of Artificial Intelligence techniques, including machine learning, knowledge representation, and decision-making. Advanced autonomous systems must support a seamless transition path from readily deployable advanced automation solutions to future cognitive decision aiding and cognitive autonomy solutions. The underlying autonomy system architecture must be open, reusable, and extensible while remaining secure and reliable.

To this end, Northrop Grumman has designed and implemented a reusable software framework that automates the time-honored Observe-Orient-Decide-Act (OODA) Loop. The Autonomy Engine software kernel manages the flow and processing of data across the components described below. Northrop Grumman has demonstrated the applicability of this approach through a prototype of a UUV mine detection mission.

Sense (Observe): Receive and process data from attached sensors. Sensor drivers in the system apply data analytics to raw data from sensors to extract relevant knowledge, such as event patterns and anomalies.

Model (Orient): Create and maintain a *World Model* based upon knowledge received from the Sense component via the sensors.

The World Model uses the OWL semantic web standard to represent not only the environment in which the agent operates, but also knowledge about the agent itself, external agents/humans, and the mission(s). Knowledge is of past, current, and future world states.

Deep learning (on either simulations or real world experience) is used to automatically generate and enhance the ontology, minimizing the brittleness that is often associated with manually generated ontologies.

Machine learning and data analytics techniques such as information fusion, event correlation, anomaly detection, threat classification, and predictive analysis are applied to the world model to derive further information required for automated decision making that, in turn, is also asserted into the world model.

Decide: The World Model provides the situational context enabling computational decision making.

Reactive behavior is enabled by automatically selecting mission plans as triggered by changes in the World Model based upon pre-defined or learned rules.

Deliberative behavior is enabled by using automated planning and scheduling techniques to generate mission plans and allocate resources based on pre-conditions and expected effects of actions as represented in the world model.

Act: The Act component is responsible for executing the actions and tasks as defined by the selected mission plan in the Decide component. All pre-conditions are verified prior to executing actions and the world model is updated with expected effects of the actions.

Collaborate: Collaboration with human and autonomous teammates is performed according to the OODA loop framework.

The IEEE FIPA standards for agent communication and collaboration present a formal framework for multi-agent collaboration based on how humans communicate.

FIPA interaction protocols support collaborative processes such as tasking, resource allocation, and negotiation.

Automatic Calibration of Multi-Sensor State Estimation for Autonomous Systems

Stephan Weiss[1], Alexander Hardt-Stremayr[1], Eren Allak[1], and Daniel Donavanik[2]

[1]Alpen-Adria University, Austria
[2]Army Research Laboratory

Recently, great advances were made in autonomous navigation of aerial vehicles. In particular visual inertial based and multi-sensor navigation frameworks allow a fairly reliable localization and control even in challenging environments. However, such frameworks usually are designed for a specific sensor suite on a specific platform, often require offline/manual calibration procedures, and are not robust against sudden loss and in-flight (re-)additions of sensor modalities.

We present an approach that analyzes the observability of a specific set of states in the system to generate motion such that these states converge best. This observability aware motion allows for automatic calibration of state estimators on multi-sensor systems. The approach effectively eliminates manual calibration procedures, handles self-healing and re-calibration aspects on sensor-signal loss/addition and is vehicle agnostic as it directly acts on the non-linear, time-continuous system defined by the available sensor modalities. In practical examples on real systems, we show the benefit of the observability aware motion to quickly converge calibration states upon mission start for subsequent higher navigation precision and to eliminate tedious calibration procedures by experts. As an addition, the observability aware motion can also be performed during a mission to re-calibrate the system. The trajectories optimized for state convergence can be bound into user defined volumes such that the vehicle continues on the main mission path while superposing motion for best re-calibration.

In collaboration with ARL we show next steps in this direction for modular multi-sensor fusion systems where sensor modalities can arbitrarily be eliminated or made available.

Relevance and Redundancy as Selection Techniques For Human Machine Sensor Fusion

Daniel Donavanik[1], Justin Brody[1], Anna Dixon[1], Ryan Robinson[1], and William Nothwang[1]

[1]Army Research Laboratory

Human-autonomy teaming using physiological sensors poses a novel sensor fusion problem due to the dynamic nature of the sensor models and the difficulty of modeling their temporal and inter-subject variability. Developing analytical models therefore requires defining objective criteria for selection and weighting of sensors under an appropriate fusion paradigm. We investigate a selection methodology grounded in two intuitions: 1) that maximizing the relevance between sensors and target classes will enhance overall performance within a given fusion scheme; and 2) that minimizing redundancy amongst the selected sensors will not harm fusion performance and may improve precision and recall. We apply these intuitions to a human-autonomy image classification task. Preliminary results indicate strong support for the relevance hypothesis and weaker effects for the redundancy hypothesis. This relationship and its application to human-autonomy sensor fusion are explored within a framework employing three common fusion methodologies: Naive Bayes fusion, Dempster-Shafer theory, and Dynamic Belief Fusion.

Big Data, ML and AI for Combat ID and Combat Systems — Design, Demonstrate and Proof of Concept: Discover Virtual Airways and Patterns Using Automatic Dependent Surveillance — Broadcast (ADS-B) Data

Ying Zhao[1], Anthony Kendall[1]

[1]Naval Postgraduate School

There have been significant advances recently in commercial applications using Big Data, Deep Analytics including machine learning (ML) and artificial intelligence (AI) methods. These methods must address the unique challenges in applications supporting the Common Tactical Air Pictures (CTAP) and Combat Identification (CID) and therefore imperative to test and adapt commercially available Big Data, ML/AI methods tools to meet these ongoing needs and requirements. Specifically, we will show the feasibility of using Big Data, ML/AI methods to Automatic Dependent Surveillance — Broadcast (ADS-B) Data and how to apply these methods such as Lexical Link Analysis (LLA) and visualizing with Google Earth and Maps to 1) identify and filter out neutral airborne objects with a higher fidelity and reduced latency than the traditional methods such as the CEC composite ID methods; 2) to build virtual airways using ADS-B or Mode-S data. We will show how to detect commercial flight baselines, anomalies and patterns using the Big ADS-B Data to analyze aircraft tracks over a period time.

This research could potentially improve situational awareness for Naval air warfare decision makers. LLA is a form of text mining showing relationships and associations with the given data. Because there is a large amount of daily ADS-B data, a Hadoop cluster is utilized for parallel processing and then LLA

provides data visualizations, patterns and associations for profiling the aircraft based on the kinematic and other characteristics. Based on the correlation to the speed and altitude of aircraft and its country of origin, our results did identify unusual behavior for some aircraft. When the kinematic and behavior patterns are discovered from historical ADS-B data, the resulted models can also be used to identify flying patterns and anomalies that can increase CTAP and the prediction accuracies of CID.

CryptoNets: Evaluating Deep Neural Networks on Encrypted Data

Kim Laine[1], Hao Chen[1], Ran Gilad-Bachrach[1], and Kristin Lauter[1]

[1]*Microsoft Research*

Machine learning over encrypted data has important applications for cloud security and privacy. It allows sensitive data such as genomic data to be stored in the cloud in encrypted form without losing the utility of the data. For the third task of the iDASH 2017 Secure Genome Analysis Competition, participants are challenged to train a machine learning (ML) model on encrypted genomic data, in order to predict disease based on patients' genomes. Training ML models on encrypted data had up until now only been done for very simple ML algorithms such as Linear Means and Fisher's Linear Discriminant algorithms. The 2017 iDASH competition task is to train a logistic regression model, and although in theory it can be done using Fully Homomorphic Encryption (FHE), until now the feasibility and efficiency of this approach had not been studied.

In this work, we show that training a logistic regression model over binary data is possible using FHE. In particular, we use gradient descent and stochastic gradient descent algorithms, and we demonstrate that it takes several minutes to one hour to run each gradient descent step. This is possible using bootstrapping, which we have implemented for the first time for the SEAL library. SEAL is a publicly released Homomorphic Encryption library developed by Microsoft Research. It uses the FV encryption scheme and parameters can be set to achieve various desired security levels, such as 80-bit, 128-bit, or 256-bit security.

Danger, Danger, Ensign Will Robinson! How Artificial Intelligence Will Play a Role in the Navy's Focus on Cybersecurity.

Jim Pietrocini[1]

[1]*Sentek Global*

The reality is that artificial intelligence cannot wholly replace people, especially in areas that are innovation driven such as the ones you would find within the Navy C4I community. If there is an increasing demand for creativity within this environment, a human will be the best suited to fill the position.

However, what Artificial Intelligence can do is enhance skill-related labor and quicken the process of manually processing tasks critical to the management and day to day operations of the C4ISR community.

A MARRIAGE BETWEEN AUTOMATION AND COMMUNITY

Automation is beneficial in reducing the number of tasks associated with workspace management, event management, certain parts of the Research and Development process (i.e., searching for information). What else Artificial Intelligence does is provide avenues for team collaboration and bringing people together.

Now, C4ISR related software is in high demand for the way in which it brings people together and on the same operational picture with performing critical tasks and the future of the battlespace.

COMPARE TO CORRELATION DEVELOPMENT IN THE LATE 80'S FOR NAVY C4I

I was involved in early days of Navy C4I and remember very detailed mathematical centric discussions around the OTHDCT correlator. Today's Navy must have the same rigor focus on AI and Machine Learning. It will quickly become a key component of our C4ISR systems.

Related to the trust side of the equation, Cybercriminals invent new attack vectors and fraud techniques every day. Like any other technology, machine learning is not something you can install once and forget. We need to assure continuous training with new datasets, quite frequently under the careful supervision of expensive human experts. Make sure that the human costs required to keep a critical C4ISR program's technology up to date align with the benefits that it can deliver.

A machine learning algorithm builds a model that represents the behavior of a real-time C4ISR system from data that represents samples of its action. Testing and Training can be supervised — with prelabeled example data — or unsupervised. Either way, the data needs to be a representative of the real world. Without representative data, no algorithm can offer useful and generalizable insights.

The challenge in cybersecurity is that the initial phases of an attack, such as malware or spear-phishing emails, vary every time the attack is launched, making it impossible to detect and classify with confidence. History has shown it impossible for a computer program to determine whether another program supports a positive outcome or is just wrong.)

To summarize, Machine Learning is inhibiting when there is the massive variation in the data that makes training useless. For example, in anti-virus, polymorphism makes every attack using the same underlying malware look different. AI can help provide variance and over time produce some relevant outcomes.

Deep Learning for Integrated Circuit Segmentation

Chris Ward[1], Brendan Crabb[1]

[1]*SPAWAR Systems Center Pacific*

Physical inspection and analysis of Printed Circuit Boards (PCBs) is a tedious task that we seek to automate. We apply traditional image processing techniques, Convolutional Neural Networks, Conditional Random Fields, and Recurrent Neural Networks to perform semantic segmentation of complex circuit boards. We generate a pixel-wise segmentation mask that is used to enumerate instances of Integrated Circuits on a PCB and generate a Bill-of-Materials with minimal operator input.

Electronic Warfare Activity Recognition (EWAR)

Diego Marez[1], John Reeder[1], Samuel Borden[1], and Gregori Clarke[1]

[1]*SPAWAR Systems Center Pacific*

Current challenges in Electronic Warfare (EW) involve the lack of mechanisms to assess the realtime effectiveness EW. In order to address this issue, we are seeking to develop a machine learning system that can recognize changes in radar activity in order to determine state of EW engagement. With recent improvements in deep neural network (DNN) models for structured data such as time series or images in particular recurrent neural network (RNN) models and convolutional neural network (CNN) models, we are seeking to use RNN and CNN models for our approach. Currently, the problem is being casted as a clustering problem, and the current approach centers around using an underlying deep model to learn a low dimensional feature representation in the service of a clustering tasks.

Hierarchical Planning for Human-Autonomy Teaming

Michael Ouimet[1], Leah Kelley[1], Bryan Croft[1], Luis Martinez[1], and Eric Gustafson[1]

[1]*SPAWAR Systems Center Pacific*

This poster describes the work of the NISE-funded Human-Autonomy Teaming project at SSC Pacific. We aim to apply artificial intelligence planning algorithms to Navy-relevant scenarios, feeding in high-level human insight and intelligence, where appropriate, to improve the runtime and performance of the algorithms. The domain presented is cooperative multi-robot mapping of an unknown environment to search for either dynamic or static objects of interest, subject to limited battery life. Overall, the planning takes place over two levels. At the (higher) centralized level, an optimization algorithm fuses all robots data and periodically retasks all agents to different tasks/portions of the environment/go recharge battery. At the (lower) agent level, each uses a Markov Decision Process (MDP) to quickly navigate through the environment safely without striking obstacles. A human operator influences the high-level optimization algorithm by providing preferences and interpreting data not digestible by the planning algorithms, to improve the overall performance. Current work this FY is on

extending the scenario to allow the optimization algorithm to plan sequences of tasks over longer horizons as well as to planning for scenarios where agents periodically go in and out of communication with the network.

Hunting for Naval Mines with Deep Neural Networks

Daniel Gebhardt[1], Keyur Parikh[1], Iryna Dzieciuch[1], Michael Walton[1], and Nhut Anh Vo Hoang[1]

[1]SPAWAR Systems Center Pacific

Explosive naval mines pose a threat to ocean and sea faring vessels, both military and civilian. This work applies deep neural network (DNN) methods to the problem of detecting minelike objects (MLO) on the seafloor in side-scan sonar imagery. We explored how the DNN depth, memory requirements, calculation requirements, and training data distribution affect detection efficacy. A visualization technique (class activation map) was incorporated that aids a user in interpreting the models behavior. We found that modest DNN model sizes yielded better accuracy (98%) than very simple DNN models (93%) and a support vector machine (78%). The largest DNN models achieved <1% efficacy increase at a cost of a 17x increase of trainable parameter count and computation requirements. In contrast to DNNs popularized for many-class image recognition tasks, the models for this task require far fewer computational resources (0.3% of parameters), and are suitable for embedded use within an autonomous unmanned underwater vehicle.

Informativeness of Degraded Data in Training a Classification System

Nancy Ronquillo[1], Josh Harguess[2]

[1]University of California, San Diego
[2]SPAWAR Systems Center Pacific

Consider the task of developing a vision classification system via supervised learning. Huge success has been achieved by the computer vision community in automatic classification tasks, especially concerning image and video data, by implementing state of the art machine learning models. Techniques based on deep neural networks, for example, achieve impressive performance by using datasets with millions of high quality training images. Even so, some of these methods have been shown to be vulnerable in the presence of adversarial examples, or when training with limited data causing classification inaccuracies. Although, many recent solutions have been proposed to mitigate the vulnerability of machine learning models when they are subject to limited or degraded data, the effects and potential benefits of using de-graded data for purposes of training or testing a classification system are not fundamentally studied. In this work, we propose a methodology for studying the effects of degradations (due to additive noise, compression artifacts, and blur) that is based on the active learning framework for studying the informativeness of data samples.

By carefully selecting data instances which have the potential to be the most informative to a classification model, active learning frameworks help to mitigate the annotation costs and manage the resources needed to extract an accurate predictive model from a set of unlabeled training data. As a first

step toward characterizing informativeness in terms of video degradations in this work, we take advantage of the active learning framework using uncertainty sampling for measuring informativeness to study the effects of using degraded data for training and testing a classifier. In particular, we aim to characterize the informativeness of video data samples in terms of their video quality, which we define based on degradations due to additive Gaussian Noise, Compression artifacts, and blurring effects. We apply this methodology to the action recognition dataset UCF101, to validate its utility. By studying the effects of degradations on samples using active learning, our work sheds light on the impact of quality of data on training a classifier, and quantitatively describes to what extent the use of degraded samples, versus the use of high quality samples, in training a classifier may be more desirable. In doing so, we hope this work will motivate a further study on the unknown benefits of working with degraded data in a classification system.

Multispectral minefield recognition via deep learning

Rafael Dinner[1]

[1]*Areté Associates*

Via the US Navy's Coastal Battlefield Reconnaissance and Analysis (COBRA) program, Areté Associates has fielded a multispectral imager for detection of minefields and obstacles. To improve false alarm discrimination, we created a custom deep neural network (DNN) classifier based on the ResNet architecture. It operates on the multispectral chips and scalar features produced by our image processing algorithm. We trained and tested on real imagery, and were able to significantly improve the object-level ROC curve as compared to the baseline discrimination algorithm. Further evaluation for robustness, as well as real-time implementation, will be necessary before this promising algorithm is incorporated into the fielded system.

Neural Network Hyper-Parameter Optimization Using Particle Swarm Optimization (PSO)

David Emerson[1]

[1]*Naval Surface Warfare Center, Crane Division*

One of the biggest challenges of developing successful Neural Network and Machine Learning (ML) frameworks is the determination of the optimal hyper-parameters that are used to configure the network prior to training. Unfortunately, there is no one size fits all recipe for determining these parameters. These parameters can be integer or string based (number of neurons, number of hidden layers, activation functions, etc.) and real number based (learning rate, data ratios, etc.) making this optimization problem a mixed-integer programming problem. This research will investigate the use of Particle Swarm Optimization (PSO) to solve the problem of selecting the optimal hyper-parameters. PSO is an optimization technique that does not require the use of derivatives to determine the optimal solution, but uses an iterative stochastic approach to obtain an optimal solution. This optimization technique is well suited to the hyper parameter optimization problem since the governing equation is not known and there might not even be a single equation that governs the behavior of the neural network with respect to the

hyper-parameters. In the testing that was conducted eight hyper-parameters were selected for optimization. These parameters were, 1) the number of neurons, 2) the hidden layer activation function, 3) the output layer activation function, 4) the performance/loss metric function, 5) the learning rate, 6) The training data ratio, 7) the validation data ratio, and 8) the test data ratio. This research also investigated the use of the DoDs High Performance Computing Modernization Program (HPCMP) computing resources as a target to deploy the PSO algorithm. The original data set used in this work is not releasable, however the MNIST digit recognition data set will be used as a surrogate data set. This research will compare the results of traditionally hand designed neural networks and the PSO algorithm designed neural networks to determine which produces the better results.

Particle Swarm Optimization (PSO) for Asset Allocation in a Dynamic Electronic Spectrum

Lauren Christopher[1], William Boler[1], Md Saiful Islam[1], and Paul Witcher[1]

[1]*Indiana University Purdue University at Indianapolis*

Electronic Warfare (EW) assets that communicate or jam battlefield radios need optimal placement in 3 Dimensional (3D) space and in frequency. The optimization problem must be solved in near real time, with constantly updating complex naval battlefield conditions. This research uses a Machine Learning (ML) bio-inspired technique for the solution to the non-Polynomial (NP) problem of asset allocation: Particle Swarm Optimization (PSO). This research is a continuation of prior work in which frequency assignments and multi-dimensional asset placement was performed. Further work has been completed integrating 3D elevation data from a Geographic Information System (ArcGIS) database, implementing a propagation model of transmitters and receivers with respect to line of sight (LOS) constraints, adding pheromones as a continuation to the human-in-the-swarm constraints, and simulating the entire PSO environment using 3D data visualization. The ArcGIS elevation data are taken from real geographic locations, and this terrain constraint is used in the PSO. Human interaction is accomplished with the concept of pheromones which act as attracting or repelling components in the 3D optimization. The 3D visualization gives the user an understanding of asset placement in 3D space and displays real-time updates of asset locations over time. Statistics are collected and solutions are evaluated based on repeatability, accuracy, and runtime. The improvements and Graphical User Interface (GUI) enhancements in this research provides a more realistic EW battlefield constraints on the PSO while maintaining a below 1 second runtime benchmark. This research is sponsored by the Naval Engineering Education Consortium (NAVSEA) contract N00174-16-C-0024, with support of NSWC Crane Division in Crane, Indiana.

Reduced Numeric Precision Neural Networks on Intel FPGAs

Philip Colangelo[1], Kevin Nealis[1], Eriko Nurvitadhi[1], and Asit Mishra[1]

[1]Intel Corporation

Deep Neural Networks (DNNs) that rely on dense floating-point matrix multiplications are typically deployed on GPUs today because of their many highly data parallel compute cores capable of producing the highest peak TFLOP/sec when compared to other competing hardware architectures. Current FPGAs offer superior energy efficiency (Ops/Watt), but they do not offer the performance of todays GPUs on this type of DNN. The question becomes, do FPGAs have a place in future DNN deployment? The upcoming 14-nm Intel®Stratix® 10 FPGAs have thousands of hard floating-point units (DSPs) and on-chip RAMs (M20K). They will also have high bandwidth memories and improved frequency (HyperFlex™ core architecture). This combination of features brings FPGA raw floating-point performance within striking distance of GPUs. Further, DNNs have been shown to maintain reasonable classification accuracy when quantized to lower precisions, however sub 8-bit activations and weights can result in classification accuracy falling below an acceptable threshold. Techniques exist for closing the accuracy gap of limited numeric precision networks typically by means of increasing computation resulting in a trade-off between throughput and accuracy. Customizable hardware architectures like FPGAs provide opportunity for data width specific computation through unique logic configurations leading to highly optimized processing. Specifically, ternary and binary weighted networks offer an efficient method of inference for 2-bit and 1-bit data respectively. Most hardware architectures can take advantage of the memory storage and bandwidth savings that come along with smaller datapaths, but very few architectures can take full advantage of limited numeric precision at the computation level. We present a hardware design for FPGAs that takes advantage of the bandwidth, memory, and computation savings of limited numerical precision data. We provide insights into the trade-offs between throughput and accuracy for various networks and how they map to our framework. Further, we show how limited numeric precision computation can be efficiently mapped onto FPGAs for both ternary and binary cases. Starting with Intel® Arria® 10 FPGA, we show a 2-bit activation and ternary weighted AlexNet running in hardware that achieves 3,500 images per second on the ImageNet dataset with a top-1 accuracy of 0.49, only .07 away from full precision. Using a hardware modeler designed for our low numeric precision framework, we project performance most notably for an effective 67 TOP/sec Intel® Stratix® 10 FPGA device running a modified ResNet-34 with only 3.7% accuracy degradation compared with single precision. Further, our results show that Intel® Stratix® 10 FPGA is 10%, 50%, and 5.4x better in performance (TOP/sec) than Titan X Pascal GPU on GEMM operations for pruned, Int6, and binarized DNNs, respectively. Our results indicate that FPGAs may become the platform of choice for accelerating next-generation DNNs.

Saccadic Predictive Vision Model

Michael Hazoglou[1], Todd Hylton[1]

[1]*University of California, San Diego*

The Predictive Vision Model (PVM) developed in [1] is a biologically inspired model which combines elements of recursive neural networks and several short cuts for predictive modelling, allowing for both supervised and unsupervised training for the task of object tracking. I will present a modified form of the PVM that takes inspiration from the saccadic eye movement observed in humans. This has the advantage of decreasing the number of PVM units used, decreasing the number of model parameters and reducing the resources need for calculations.

References

1 Filip Piekniewski, Patryk Laurent, Csaba Petre, Micah Richert, Dimitry Fisher, and Todd Hylton. 2016. "Unsupervised learning from continuous video in a scalable predictive recurrent network." In: *arXiv preprint arXiv:1607.06854*.

2 Michael Hazoglou and Todd Hylton. 2018. "Saccadic predictive vision model with a fovea." In: *Proceedings of the International Conference on Neuromorphic Systems*. ACM. July 23–26, Knoxville, TN, USA, p. 2.

Secure Analytics on Public Clouds with SGX

Matt Zaber[1,2]

[1]*SPAWAR Systems Center Atlantic*
[2]*SMU AT&T Virtualization Research Center*

Our research focuses on using Intel SGX trusted enclaves to support private distributed analytics on a public cloud.

Commercial cloud providers offer scalable, cost efficient infrastructure and software services for many machine learning tasks. However, deployment requires trusting the CSP with low level access to the application data and code.

Recently, some CSPs have made available trusted execution enclaves to guarantee the integrity and confidentiality of a running application. SGX enforces hardware level access protection to data and code in execution, effectively preventing actors at the hypervisor or operating system level from reading or modifying the application.

To run distributed analytics platforms like Apache Hadoop and Storm inside a trusted enclave, the sensitive components must be identified and added to the trusted computing base. Identifying these sensitive sections of code requires understanding the threat models of both SGX and the analytics platform. For example, side channel attacks against SGX exist in practice. Likewise, distributed software platforms are susceptible to access pattern analysis.

The specific goals of our research are: (1) partition Apache Storm to run in an enclave, (2) enumerate the attack surface of SGX and Storm, (3) measure the performance impact of running distributed jobs in an enclave, (4) identify security metrics and evaluate the value added and ROI for using enclaves.

Measuring Strategic Coordination in Multi-Agent Autonomous Systems

Michael Walton[1], **Benjamin Migliori**[1], **and John Reeder**[1]

[1]*SPAWAR Systems Center Pacific*

Cooperative Multi-agent Reinforcement Learning (coop-MARL) defines a class of control problems in which a team of decentralized autonomous agents must learn to jointly maximize a shared global reward signal. Models in this paradigm describe a variety of DoD and industry application domains including self-driving cars, multi UxV systems, game AI and many more. As the variety and complexity of multi-agent systems increases, learning to cooperate towards a common goal becomes essential. However, many of the RL algorithms that enjoy desirable theoretical properties and work well in practice in the single agent case do not readily generalize to accommodate multiple agents. In this work, we empirically study the dynamics and failure cases of Q-learning (a popular single-agent, model-free RL algorithm) to a coop-MARL task and propose new extensions to the algorithm for encouraging multi-agent coordination using preference learning and imitation learning methods.

SUSTAIN: Semi-Autonomous Distributed SCADA Reconfiguration System

Kurt Rohloff[1], Senjuti Basu Roy[1]

[1]*New Jersey Institute of Technology*

The goal of SUSTAIN is to provide autonomous reconfiguration capabilities for Industrial Control Systems (ICS) that allow for run-time adaptation to cybersecurity threats. We consider the automation and runtime reconfiguration of Operational Parameters, Networking Parameters and Control Logic such as the redeployment of functional control application components — shift to healthy PLCs, diversion of system data flows and restoration of compromised functionality with remaining assets. Traditional approaches cybersecurity for ICS assume prior knowledge of (fixed) system architecture, topology and assets (field and/or IoT devices). However, ICS are becoming increasingly dynamic, configuration and runtime ICS systems are separate and security deployed only before or during commissioning — no real-time adaptation to, recovery from security threats. We focus on the needs of a Naval surface ship use case and address the above challenges with semi-autonomous distributed anomaly detection and analytics, architecture redesign and dynamic state estimation and resource allocation. The goals of this approach are semiautonomous reconfiguration for distributed SCADA systems to reduces human involvement without compromising reliability and reconfigure adaptively in real time. Innovation comes from optimization techniques generalizable to many applications with distributed and adaptive (efficient solution to handle large scale and adapts with the dynamicity of the platform.)

Using Gait Information to Classify Cognitive-Motor Interaction Tasks

Mohammad Alam[1], Jamie Lukos[1]

[1]*SPAWAR Systems Center Pacific*

When locomotor and cognitive tasks are combined, cognitive-motor interference (CMI) occurs where participants adopt altered strategies for performing the dual tasks [1] that can result in suboptimal task performance [2, 3]. Despite these known behavioral changes, the ability to detect these changes in realtime settings at a neurophysiological level remains limited. Our objective is to investigate various machine learning approaches to discriminate biosignals during walking with and without cognitive load. To test this, we used data from a study where subjects walked on a treadmill for an hour carrying 40% of their body weight while performing a visual oddball task. Although we have previously shown differences in cognitive neural activity associated with variations in physical demands at the electrode level [4] and using cortical source localization techniques [5], here our goal is to determine if machine learning techniques could be used to classify neurophysiological responses from gait information. Electroencephalography (EEG), electromyography (EMG), and force plates in the treadmill were used to calculate gait information for classification. If successful, this approach can aid feed-forward brain computer interfaces (BCI) to help isolate periods when the BCI should function while the user is walking.

References

1 Galit Yogev-Seligmann, Jeffrey M Hausdorff, and Nir Giladi. 2008. "The role of executive function and attention in gait." In: *Movement Disorders: Official Journal of the Movement Disorder Society* 23.3, pp. 329–342.

2 Emad Al-Yahya, Helen Dawes,Lesley Smith, Andrea Dennis, Ken Howells, and Janet Cockburn. 2011. "Cognitive motor interference while walking: a systematic review and meta-analysis." In: *Neuroscience & Biobehavioral Reviews* 35.3, pp. 715–728.

3 Marjorie Woollacott and Anne Shumway-Cook. 2002. "Attention and the control of posture and gait: A review of an emerging area of research." In: *Gait & Posture* 16.1, pp. 1–14.

4 J Cortney Bradford, Keith W. Whitaker, Kaleb McDowell, Kaleb McDowell, Ross Arena, Jamie Lukos, Jamie Lukos, Peter E Pidcoe, and Peter E. Pidcoe. 2016. "Effect of locomotor demands on cognitive processing." In: *38th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*. IEEE. August 16–20, Lake Buena Vista, FL, USA.

5 Jamie R Lukos, J Cortney Bradford, and Daniel P Ferris. 2016. "Compensatory neural responses during a physical-cognitive dual task." In: *Society for Neuroscience Conference*. Soc Neuroscience. November 12–16, San Diego, CA, USA.

Effects of Signal Pre-Processing on Automatic Modulation Classification

Gabrielle Robertson[1], Kevin Burke[1]

[1]*The MITRE Corporation*

As an emerging field, Radio Frequency Machine Learning has yet to characterize the effects of different processing steps on model performance. We present a potential system for discovering signals present in a wide band, processing them for machine learning classification, and performing the classification. In this context, we anticipate that the signal pre-processing step of converting passband signals to baseband will affect the machine learning classifier. We present experiments on a Convolutional Neural Network (CNN) applied to automatic modulation classification, showing the change in performance when the input data includes baseband conversion. We anticipate that a CNN model trained on signals synthesized at baseband will less accurately classify signals synthesized at passband and converted to baseband. We study the effects of signal to noise ratio on this accuracy disparity. Additionally, we anticipate that a CNN model trained and tested on signals synthesized at passband and converted to baseband will be able to classify less accurately than a CNN model trained and tested on signals synthesized at baseband.

Exploring Hyper-parameter Optimization for Neural Machine Translation

Robert Lim[1], Kenneth Heafield[2,3], Hieu Hoang[3], Mark Briers[3], and Allen Malony[1]

[1]*University of Oregon*
[2]*University of Edinburgh*
[3]*The Alan Turing Institute*

Neural machine translation (NMT) has been accelerated by deep learning neural networks over statistical based approaches, due to the plethora and programmability of commodity heterogeneous computing architectures such as FPGAs and GPUs and the massive amount of training corpuses generated from news outlets, government agencies and social media. Training a learning classifier for neural networks entails tuning hyper-parameters that would yield the best performance. Unfortunately, the number of parameters for machine translation include discrete categories as well as continuous options, which makes for a combinatorial explosive problem. This research explores optimizing hyper-parameters when training deep learning neural networks for machine translation. Specifically, our work investigates training a language model with Marian NMT. Results compare NMT under various hyper-parameter settings across a variety of modern GPU architecture generations in single node and multi-node settings, revealing insights on which hyperparameters matter most in terms of performance, such as words processed per second, convergence rates, and translation accuracy, and provides insights on how to best achieve high-performing NMT systems.

This page is intentionally blank.

INITIAL DISTRIBUTION

84300	Library	(1)
85300	Archive/Stock	(1)
56220	K. Rainey	(1)
56220	J. Harguess	(1)

Defense Technical Information Center
Fort Belvoir, VA 22060–6218 (1)

This page intentionally left blank.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-01-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
October 2018	Final	

4. TITLE AND SUBTITLE

Report on the Second Annual Workshop on Naval Applications of Machine Learning

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHORS

Katie Rainey
Josh Harguess

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

SSC Pacific
53560 Hull Street
San Diego, CA 92152–5001

8. PERFORMING ORGANIZATION REPORT NUMBER

TD-3386

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

SSC Pacific
Naval Innovative Science and Engineering (NISE) Program
53560 Hull Street
San Diego, CA 92152–5001

10. SPONSOR/MONITOR'S ACRONYM(S)

NISE

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This technical document contains an overview of the second annual workshop on Naval Applications of Machine Learning (NAML) that was held February 13-15, 2018, at the Space and Naval Warfare (SPAWAR) Systems Center Pacific (SSC Pacific), a U.S. Navy research laboratory in San Diego, California, USA. NAML workshop events included invited speakers, demonstrations, discussion sessions, and oral and poster presentations. The workshop co-chairs were Josh Harguess and Katie Rainey, both from SSC Pacific. The poster presentations were coordinated by Chris Ward also from SSC Pacific. This report discusses the motivation, goals, and impact of the workshop and highlights some of the topics covered. It also includes photographs taken at the workshop, the full agenda, and abstracts describing many of the oral and poster presentations.

15. SUBJECT TERMS

NAML 2018; machine learning;

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Katie Rainey
U	U	U	U	90	19B. TELEPHONE NUMBER *(Include area code)* (619) 553-3472

This page is intentionally blank.

This page is intentionally blank.

Approved for public release.

SSC Pacific
San Diego, CA 92152-5001