

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
Accelerated Learning and Engineering Research Training (ALERT) Program
In Cyber and Electronic Warfare
Final Report

Date of Report: April 16, 2024

Project Title: Accelerated Learning and Engineering Research Training (ALERT) Program in
Cyber and Electronic Warfare for Undergraduate Midshipmen and Cadets
Award Number: N-00014-21-1-2217

Submitted by:

Natasha A. Mamaril, PhD
1304 W Springfield Ave, 3278 Digital Computer Lab, Urbana, IL 61801

Telephone: 217-244-9995
Email: nmamaril@illinois.edu

Security Classification – Unclassified

Table of Contents

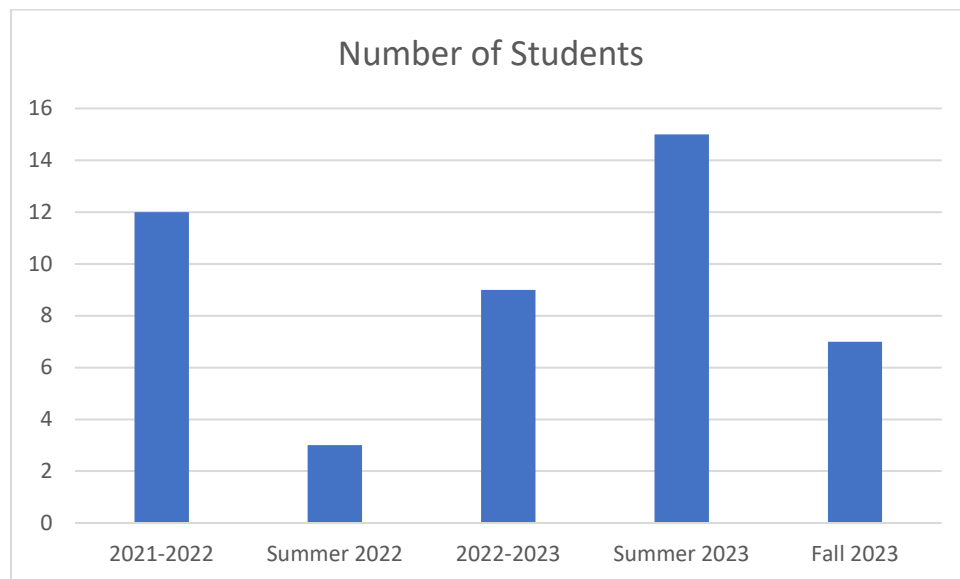
Major Goals of the ALERT Program.....	1
Undergraduate Student Accomplishments	2
Graduate Student Mentor Accomplishments	3
Project Teams.....	4
Partner Organizations.....	6
Other Collaborators.....	6
Program Evaluation/Assessment in Relation to Project Goals	7
Impact of Program Participation	7
Program Assessment	7
Student Learning Outcomes (SLO).....	8
Assessment Methods	8
Changes and Problems.....	21
Individual Project Reports	22
Fall 2021 – Spring 2023	22
Project 1 and 2: Reconfigurable Antenna System to Detect and Mitigate GPS Spoofing/Jamming; Small Phase Array Behavior on Portable/Mobile Platforms	22
Project 3: Advanced Photon Sources for Secure Quantum Communications	24
Project 4: Next Generation Power Electronics.....	28
Project 5: Trustworthy Machine Learning	31
Project 6: Detecting Anomalous Behaviors for Assured Command and Control.....	32
Project 7: Machine-Learning Based Anomaly Detection and Resiliency for Autonomous UUV Swarms	33
Summer - Fall 2023	34
Project 1: Development of Wearable Graphene Array Sensors	34
Project 2: Characterization of Strain Distribution in 2D Materials to Engineer Electrical Properties.....	35
Project 3: Development of Autonomous Drone to Navigate Obstacles Using Depth Camera Technology.....	38
Project 4: Utilization of Audio and Sensing Data for Multi-Factor Authentication and Location-Based Proofs	39
Project 5: Study of Robustness of Machine Learning Models to Semantic Perturbations	40
Project 6: Improving Trustworthiness of Machine Learning Compilers	42
Project 7: Cloud Infrastructure for IoT Security	42

Project 8: Security of Network Functions	43
Activities to Guarantee Long-term Sustainability of the Project.....	44
Future Plans Post-Award	44
Products Resulting from the Award - Undergraduate Student Posters.....	45

Major Goals of the ALERT Program

The University of Illinois at Urbana-Champaign (U of I) originally proposed **to train 10 to 14 undergraduate students, specifically ROTC midshipmen and cadets, in the areas of cyber and electronic warfare research** through the **ALERT (*Accelerated Learning and Engineering Research Training*) Program** in Cyber and Electronic Security. The program entailed two-phases. In the first phase, students developed their background knowledge and trained to use equipment/software and perform laboratory techniques. In the second phase, students applied what they have learned in the first phase and conducted research.

We also planned to offer **multidisciplinary/interdisciplinary research experiences** to the students. In collaboration with our faculty members and graduate students, we were able to offer **15 multidisciplinary/interdisciplinary research projects and trained a total of 37 (unique) undergraduate students**. Figure 1 shows the number of students for each academic year and summer term. Seven research projects were offered from fall 2021 to spring 2023. Our first cohort of undergraduate students (n=12) in fall 2021 to spring 2022 were all ROTC midshipmen and cadets. Our second cohort of undergraduate students (n=9) included ROTC students and students from underrepresented groups in STEM. These students participated in the program from fall 2022 to spring 2023. We also supported undergraduate students in summer 2022 (n=3) and summer 2023 (n=15). In fall 2023, we had seven (7) students continue working on their research projects that they started in summer 2023.



Our undergraduate students in the program attended the required undergraduate research seminar course that **developed their technical communication skills (written and verbal) and presentation skills**. Class assignments included reading scientific papers, writing technical summaries, evaluating, and citing scholarly work, literature reviews, ethical and responsible conduct of research, and creating research presentations. They attended monthly research seminars and professional development workshops. Alex Withers, Assistant Director of Cybersecurity at the National Center for Supercomputing Applications (NCSA) talked about

Shared Intelligence Platform for Protecting our National Cyberinfrastructure. We also invited guest speakers from the Navy who talked about their work and shared their career experiences with our program participants. In particular, Commander Branden K. Woods, Commanding Officer for Patrol Squadron NINE (VP-9), spoke to the students about his career path and his experience navigating different roles (see photo below).



Through learning-by-apprenticeship, ALERT Program participants learned about basic and applied research and the research process in general. Graduate students provided guidance, supervision, and instruction to the undergraduate researchers on their respective projects. They were responsible for training the undergraduate students on tasks needed to complete the project. Graduate student mentors also attended mentoring and professional development workshops. The undergraduate researchers also submitted abstracts and presented their research posters at the Illinois Scholars Undergraduate Research (ISUR) Program Research Expo in April or the Engineering Research Fair (see section on Products Resulting from Award section for research posters presented).

Undergraduate Student Accomplishments

1. Adam Spitzner received the Armed Forces Communications and Electronics Association (AFCEA) Award. He is currently in the US Marine Corps in Quantico Base, Virginia.
2. Samuel Weiss received The Association of Old Crows (AOC) awards 2023 STEM Student of the Year, an award given to students studying engineering or engineering technology and interested in working in the aerospace and defense industry. His research into diamond-based semiconductors led him to perform work at Argonne National Lab's Center for Nanoscale Materials (ANL CNM) to fabricate and test various crystalline chips. The research program was funded through the Office of Naval Research (ONR) and has applications to many high power/efficiency systems such as satellites and power

plants. Samuel received a full ride to a Navy graduate program in Israel in government diplomacy and conflict studies.

3. Recipients of the Windy City AOC Scholarship Award Program. Awards were established in the names of chapter individuals who made major contributions in technology.
 - a. 2023: Max Damewood and Samuel Weiss
 - b. 2022: Jisu Kim, Neel Khattri, Mary Pelzer, and Samuel Weiss
4. Josh Carpenter is a student naval aviator in the US Navy, stationed at Corpus Christi Texas studying military aviation systems and procedures.
5. Christelle Seri is a GDP Engineer at the Electric Reliability Council (ERCOT) in Texas.
6. Henry Feldhaus is a Platoon Leader in the 3rd Infantry Division in Fort Stewart, Georgia.
7. Teague Mitchell is a PhD student in Electrical and Computer Engineering at UIUC.
8. Thinh Nguyen is a navigation systems engineer at Northrop Grumman. He is also pursuing a master's degree in aerospace engineering at UIUC.
9. Victoria Garcia is a program manager at Phigenics, an independent company focused on developing and implementing comprehensive water management programs.
10. Jessica Rangel-Galera is a process engineer at Procter & Gamble.
11. Jisu Kim is currently a nuclear surface warfare officer in the U.S. Navy.
12. Ben Candee is a U.S. Naval Officer in-training.
13. Luke Lalumandier received his MS in aerospace, aeronautical and astronautical engineering from Naval Postgraduate School and is currently a U.S. Naval Officer.
14. Neel Khattri received a Boren Scholarship to spend a semester studying Russian at the Anglo-American University in Prague, Czech Republic.
15. Emily Grob is pursuing a Master of Science degree in electrical engineering at George Washington University.

Graduate Student Mentor Accomplishments

1. Yeageun Lee was awarded first prize for Functional Materials Division (FMD) Graduate Technical Division Student Poster Contest in the TMS 2022 conference.

Project Teams

Table 1. Project leads, graduate students, and undergraduate researchers who participated during fall 2021 to spring 2023*

	Project	Faculty Lead	Graduate Student Mentor(s)	Undergraduate Student(s)
1	Reconfigurable Antenna System to Detect and Mitigate GPS Spoofing/Jamming	Prof. Jennifer Bernhard (Department of Electrical and Computer Engineering)	Kara Mauer Guilherme Jurgensen	Adam Spitzner Josh Carpenter Natasha Sherlock Max Damewood
2	Small Phase Array Behavior on Portable/Mobile Platforms	Prof. Jennifer Bernhard (Department of Electrical and Computer Engineering)	Kara Mauer Guilherme Jurgensen	Patrick Yim Christelle Seri
3	Advanced Photon Sources for secure Quantum Communications	Prof. SungWoo Nam (Department of Mechanical Science and Engineering)	Yeageun Lee Jim Myung Kim	Henry Feldhaus Mary Pelzer Teague Mithcell Thinh Nguyen
4	Next Generation Power Electronics	Prof. Can Bayram (Department of Electrical and Computer Engineering)	Yu-Chieh Chu Zhuoran Han	Samuel Weiss Victoria Garcia Jessica Rangel-Galera Aleksai Herrera
5	Trustworthy Machine Learning	Prof. Bo Li (Department of Computer Science)	Huichen Li	Krishna Vasudev Jisu Kim
6	Detecting Anomalous Behaviors for Assured Command and Control	Prof. Huy Tran (Department of Aerospace Engineering)	Jacob Heglund	Ben Candee Luke Lalumandier Peter Baffoe Vivek Thatte
7	Machine-Learning Based Anomaly Detection and Resiliency for Autonomous UUV Swarms	Prof. Sabin Mohan (Department of Computer Science)	Kyo-Hyun Kim	Neel Khattri Riley Hudson Emily Grob Nandika Vuyyuri

*Undergraduate students participated in the program at different time points during this period.

Table 2. Project leads, graduate students, and undergraduate researchers who participated in summer and fall 2023**

	Project	Faculty Lead	Graduate Student Mentor(s)	Undergraduate Student(s)
1	Development of Wearable Graphene Array Sensors	Profs. SungWoo Nam and Elizabeth Hsiao-Wecksler (Department of Mechanical Science and Engineering)	Ezekiel Hsieh	Grace Zhen Ashley Saju Justin Macatangay
2	Characterization of Strain Distribution in 2D Materials to Engineer Electrical Properties	Profs. SungWoo Nam and Arend van der Zande (Department of Mechanical Science and Engineering)	Shahriar Nahid	Ezra Chiou Kareef Haque
3	Development of Autonomous Drone to Navigate Obstacles Using Depth Camera Technology	Prof. Naira Hovakimyan (Department of Mechanical Science and Engineering)	Chuyuan Tao	JiWoo Lee Hyrum Dickinson
4	Utilization of Audio and Sensing Data for Multi-Factor Authentication and Location-Based Proofs	Prof. Yih-Chun Hu (Department of Electrical and Computer Engineering)	Bo-Rong Chen	Zachary Mattingly
5	Study of Robustness of Machine Learning Models to Semantic Perturbations	Prof. Sasa Misailovic (Department of Computer Science)	Jacob Laurel	Jonah Black
6	Improving Trustworthiness of Machine Learning Compilers	Prof. Sasa Misailovic (Department of Computer Science)	Yifan Zhao	Jason Zalewski
7	Cloud Infrastructure for IoT Security	Prof. Matthew Caesar (Department of Computer Science)	Gabriella Xue	Tomas Sagartz Daniel Yu
8	Security of Network Functions	Prof. Matthew Caesar (Department of Computer Science)	Kuan-Yen Chou	Diego Del Carpio

** Undergraduate students participated in the program in summer 2023 and some continued in fall 2023.

Partner Organizations

- A. Engineering Undergraduate Research (EUR), The Grainger College of Engineering
Lead Unit
1304 W Springfield Ave, 3278 Digital Computer Lab, Urbana, IL 61801
Specific Contribution
EUR led by PI Dr. Mamaril organized and managed all program activities from identifying faculty collaborators, partnering with the ROTC units on campus, and leading recruitment efforts. Dr. Mamaril is responsible for the oversight of the ALERT Program including the appointments of undergraduate researchers, management and disbursement of funds, planning and execution of events, and consolidation and submission of reports (RPPR and final report).
- B. Office of Research, The Grainger College of Engineering. Co-PI Dr. Takehara, Director for Research, participated in discussions about administrative decisions and facilitated workshops about leadership and mentoring with program participants.
- C. ROTC Unit Heads and Staff, University of Illinois at Urbana-Champaign. The ROTC leads helped recruit participants and confirm the eligibility of ROTC students ensuring they are in good standing. ROTC staff served as guest speakers in seminars on relevant topics such as communications/electronic warfare experience.

Other Collaborators

- A. Morrill Engineering Program (MEP), The Grainger College of Engineering – helped advertise the research opportunity to students from underrepresented groups in STEM (i.e., Black/African Americans, Hispanic/Latine). They encouraged their students to apply to the ALERT Program.
- B. Engineering Human Resources, The Grainger College of Engineering - processed the undergraduate hourly appointments and onboarded participants regarding timesheet completion and submission
- C. Sponsored Programs Administration (SPA) and Engineering Grants and Contracts – provided guidance and services to ensure proper submission and execution of grant including financial expenditures and confirmations. They also facilitated requests for no-cost extension and inquiries with their ONR counterparts.

Program Evaluation/Assessment in Relation to Project Goals

Impact of Program Participation

Inputs	Outputs		Outcomes – Impact		
	Activities	Participation	Short-Term	Medium-Term	Long-Term
Undergraduate Students (ROTC midshipmen/cadets)	Build knowledge base - Undergraduate research course in fall - Courses relevant to research area - Monthly research seminars Train students in research and develop technical skills (incl. verbal and written communication) - Learn to use research equipment/facilities - Work on research projects - Present research in symposium/conferences Provide professional development workshops - Talk About Graduate School - Talk About Naval programs and Careers	Students/Faculty/ISUR	Students develop technical and science communications skills	Students apply their communication skills verbally and in written form as they write scholarly papers and technical reports	Students increase their research activities in areas related to cyber and electronic warfare
Graduate Student Mentors			Students increase knowledge about topics related to cyber and electronic warfare	Students expand their technical skills	Students are equipped with skills to defend against emergent cyber and electronic warfare threats as they join the STEM workforce
Faculty Members who collaborate			Students learn about science and engineering research	Students learn to collaborate with mentor/research team on conference papers and journal articles for publication	
Research Projects		Faculty/Graduate Student Mentors/ROTC leadership/ISUR	Students gain an understanding of the research process, principles, and methodologies	Students develop their capacity for more research in cyber and electronic warfare	Students pursue graduate degrees and/or naval STEM careers in cyber security and electronic warfare
Funding			Students learn to work effectively in teams	Students are socialized into their disciplinary culture	
Equipment/Facilities		Students/Graduate Mentors/ISUR	Students gain confidence in presenting their research	Students apply to graduate programs and/or internships in Naval laboratories	
ROTC leadership	Complete Progress/Final Reports to ONR	Students/ROTC leadership	Students gain knowledge of careers in academia and in the Navy		
ISUR Program Staff		Faculty/ROTC leadership/ISUR			

Figure 2. Logic Model Showing the Relationship Between Resources, Activities, and Outcomes

As seen in the logic model, we expect short-, medium, and long-term outcomes. We conducted direct and indirect assessments to examine the impact of program participation.

Program Assessment

1. Train 10 – 14 undergraduate students, especially ROTC midshipmen and cadets, in areas of cyber and electronic warfare research

Metrics

- Total Number of ROTC students in the program: 22
 - 2021-2022: 12 ROTC midshipmen and cadets
 - 2022-2023: 2 ROTC midshipmen and cadets
 - Summer – Fall 2023: 8 ROTC midshipmen and cadets
- Total Number of students from underrepresented groups in STEM (added objective later to broaden participation): 15 (unique)
 - 2022-2023: 10 students from underrepresented groups in STEM
 - Summer – Fall 2023: 7 students from underrepresented groups in STEM

2. Offer multidisciplinary/interdisciplinary research experiences to undergraduate students

Metrics

- Number of research projects
 - 2021-2023: 7
 - Summer 2023: 10

- Fall 2023: 5
- Nature of research projects (See individual project reports for descriptions)
- Disciplines of researchers involved in the research projects (See Tables 1 and 2)
- 3. Encourage students to pursue advance degrees to further STEM education
 - Metrics
 - Percentage of students who pursued/are pursuing graduate degrees after graduation
 - Of the 1st cohort of 12 ROTC students, 11 have graduated and 1 is graduating this spring 2024. Two students have pursued graduate degrees.
 - Of the non-ROTC students who have graduated, 1 is pursuing a PhD in electrical and computer engineering, whereas 2 are pursuing master's degrees (i.e., aerospace engineering, electrical engineering).
 - Majority of program participants are still pursuing their bachelor's degree in a STEM discipline.
- 4. Develop research and technical communication skills necessary to the naval workforce
 - Metrics
 - Students' performance in research projects
 - Results of the mentor evaluations are presented in Table X
 - Students' performance in required undergraduate research seminar course
 - See Student Learning Outcomes and the Assessment Methods below.

Student Learning Outcomes (SLO)

At the end of the school year, the program participant will be able to:

1. Describe the basic elements of research including the logical framework of research
2. Identify articles relevant to the chosen research topic
3. Evaluate information of a research study published in a scholarly journal
4. Communicate effectively about research work in oral and written form
5. Demonstrate a scholarly approach to engineering problems
6. Demonstrate appropriate levels of independent thought
7. Work effectively in teams (i.e., with faculty sponsors/graduate mentors, other research lab members) on a research project (e.g., completion of assigned tasks, integrate individual contributions into a final deliverable)
8. Reflect on one's progress as an undergraduate researcher

Assessment Methods

Direct Methods	SLO
In-class group work: Students present and discuss the basic elements of research and the importance of each	1
Assignment: Students read and summarize a technical paper/published article	2 & 3
Assignment: Students pick a research topic and summarize at least 3 relevant articles	2 & 3
Assignment: Students draft a research abstract	4
Assignment: Peer-review of class work	7
Posters: Students prepare and present posters about their research	4 & 5

Indirect Methods	SLO
Undergraduate Student End of Semester Surveys	4, 5, 6, 7, 8
Graduate Mentor End of Semester Surveys (includes evaluation of mentees research skills)	4, 5, 6, 7

The following tables show the descriptive statistics and correlations of the variables considered in evaluating student learning and research performance. In Table 2, we see the participants in the 1st cohort (ROTC students, fall 2021) reported less hours working on their research compared to the 2nd cohort (fall 2022) and 3rd cohort (summer 2023) of students.

Table 2. Number of Hours Spent Working on Research

Number of Hours	Fall 21	Spring 22	Fall 22	Spring 23	Summer 23
Less than 5 hours	38%	62%		50%	28%
5 to less than 10 hours	50%		66%	33%	14%
Approximately 10 hours			17%		29%
More than 10 hours	12%		17%	17%	29%
Did not answer		38%			

Since most of the participants may not have prior research experience, we expected them to meet with their mentors at least 1 – 2 hours per week. As seen in Table 3, all the participants met this expectation with a few students meeting more than 2 hours per week with their respective mentors.

Table 3. Number of Hours Spent Meeting with Mentor

	Fall 21	Spring 22	Fall 22	Spring 23	Summer 23
1 to 2 hours*	100%	62%	67%	60%	57%
2 to 4 hours			33%		29%
More than 4 hours					14%
Did not answer		38%		40%	

*Students are expected to meet at least 1-2 hours a week with their mentor.

We also asked the undergraduate students to rate the value of their research experience. Based on the means, Table 4 shows that the 1st cohort of students rated the experience “somewhat valuable,” whereas the 2nd and 3rd cohort of students rated their experience as “valuable.”

Table 4. Mean Student Rating of the Value of the Research Experience

Term	μ	SD
Fall 21	2.88	1.64
Spring 22	3.20	1.30
Fall 22	4.50	.55
Spring 23	4.33	.82
Summer 23	4.86	.38

Scale: 1 = Not at all valuable to 5 = Very valuable

The program is a structured mentored research experience with the graduate student serving as the primary supervisor. Students in all cohorts were relatively satisfied with the support they received from their mentors. We noted that satisfaction ratings were higher in the fall semesters, and this result indicates that mentors were more supportive in the beginning since they onboard the students and give close attention to students as they train and guide them. The 3rd cohort of students reported the highest mean ratings (M=4.43, SD=.79); This rating suggests that graduate student mentors may have given time and effort to their students in the summer and worked closely with them.

Table 5. Mean Student Rating of Satisfaction with Support Received from Mentor

Term	μ	SD
Fall 21	4.13	.99
Spring 22	3.40	1.82
Fall 22	4.17	1.17
Spring 23	3.67	1.03
Summer 23	4.43	.79

Scale: 1 = Very dissatisfied to 5 = Very satisfied

To ensure that students receive appropriate support from the program administrators, we asked them how satisfied they were with the administration. The first cohort of students reported lower ratings compared to the 2nd and 3rd cohort (see Table 6). We noted that the 1st cohort were students that returned to university after the COVID 19 pandemic. Some activities (e.g., scheduling training, ordering materials) were behind schedule and were beyond the control of administration. Administrators were adapting to unfamiliar situations and expecting more time commitment from the participants. Based on the feedback from the students, program administrators implemented changes to better support future cohorts, especially with setting clear expectations on the work hours and quality of work and providing feedback to the mentors.

Table 6. Mean Student Rating of Satisfaction with Support Received from Program Administration

Term	μ	SD
Fall 21	3.88	.64
Spring 22	3.40	1.52
Fall 22	4.17	.75
Spring 23	4.17	.41
Summer 23	4.71	.49

Scale: 1 = Very dissatisfied to 5 = Very satisfied

One of the goals of the ALERT Program is to train students in research. Table 7 shows students' self-reported gains resulting from participating in the research training program. The 1st cohort (fall 2021) reported highest means in understanding the research process (M=3.88, SD=1.25), followed by readiness for more research (M=3.63, SD=1.30), and learning to work independently (M=3.57, SD=1.40). The lowest gains were reported for learning laboratory skills and skill in scientific writing. The 2nd cohort (fall 2022) had the highest gains in learning to work independently (M=4.5, SD=.84) and learning laboratory skills (M=4.5, SD=.55), and the lowest

gains in skills in scientific writing ($M=3.33$, $SD=1.21$). The 3rd cohort (summer 2023) reported highest gains in understanding the research process ($M=4.43$, $SD=.54$) and readiness for more research ($M=4.43$, $SD=.79$), followed by ability to read and understand scientific literature ($M=4.14$, $SD=.69$). Through learning by apprenticeship, students developed research and technical skills. The skills they learn vary depending on the nature of their projects. Some students did not require learning laboratory skills as they had computational projects. Overall, the data suggests that the three major gains for the program participants are: learning to work independently, understanding the research process, and readiness to do more research.

Table 7. Students' Self-Reported Gains in Skills as a Result of Program Participation

	Fall 21		Spring 22		Fall 22		Spring 23		Summer 23	
	μ	SD	μ	SD	μ	SD	μ	SD	μ	SD
Ability to read and understand scientific literature	3.00	1.07	3.20	1.30	4.00	1.26	4.17	1.17	4.14	.69
Learning to work independently	3.57	1.40	3.20	1.48	4.50	.84	4.00	1.55	4.00	.58
Learning laboratory skills	2.86	1.57	3.00	2.00	4.50	.55	3.83	1.60	3.71	1.38
Skill in scientific writing	2.86	1.46	2.60	1.52	3.33	1.21	3.50	1.64	2.29	.95
Ability to analyze data	3.00	1.41	2.25	.96	3.50	1.64	4.17	.98	3.57	.98
Skill in interpreting results	2.88	1.64	2.00	1.41	3.80	1.10	4.17	.98	3.57	.98
Understanding the research process	3.88	1.25	3.60	1.14	4.33	1.21	4.17	1.17	4.43	.54
Readiness for more research	3.63	1.30	3.00	1.41	4.33	.52	3.33	1.21	4.43	.79

Scale: 1 = Gained nothing to 5 = Gained a great deal

Our mentors also provided feedback on their students' research performance. Mentor satisfaction regarding students' progress was typically higher during the fall term than the spring term (see Table 8). In spring, senior students focused on fulfilling requirements for graduation. This situation seemed to be the case for program participants given that several of program participants were graduating seniors, ROTC and non-ROTC students alike. Mentors also noted that students put in more time in the beginning as they build their background knowledge and undergo training (e.g., software, laboratory techniques). The main concern of mentors with ROTC students primarily was time commitment. Progress would be slow for students who did not put in the time and effort to do the research. ROTC students had a full schedule of training and other activities such that their work hours ranged from "less than 5 hours" to "5 to less than 10 hours" as reported in Table 2. Feedback from students suggests that some mentors expected more time than they could do. Some students put in more than 10 hours a week for a whole semester to learn technical skills in the first semester.

Table 8. Mean Mentor Ratings of Satisfaction with Students' Progress

Term	M	SD
Fall 21	4.08	.79
Spring 22	3.87	1.19
Fall 22	4.38	.52
Spring 23	3.67	.58
Summer 23	3.92	.95
Fall 23	4.20	.84

Scale: 1 = Very dissatisfied to 5 = Very satisfied

Mentors also reported that students improved in their ability to conduct research primarily in understanding content (see Table 9). Program participants were doing multidisciplinary research. To conduct research, they had to learn new skills and understand new concepts and principles which entailed training and reading scholarly articles. Most of the participants had no prior research experience (novice level) and needed guidance and instruction as reflected in the mentors' mean rating for independence, research design, and intellectual curiosity in Table 9. With the participants reporting readiness for more research, they eventually will be at the advanced level given more research/technical opportunities.

Table 9. Mean Mentor Ratings on Students' Abilities to Conduct Research

	Fall 21		Spring 22		Fall 22		Spring 23		Summer 23		Fall 2023	
	M	SD	μ	SD	μ	SD	μ	SD	μ	SD	μ	SD
Independence	2.13	1.13	2.63	1.12	2.38	1.06	1.67	1.15	2.00	.82	2.40	1.34
Research Design	2.40	.55	2.95	1.08	2.50	1.07	2.00	.00	2.67	1.15	2.60	.89
Intellectual Curiosity	2.88	.83	2.74	.99	3.13	1.13	1.67	1.15	2.38	.96	2.80	.84
Understanding Content	3.13	.83	3.37	.68	3.38	1.06	3.00	.00	3.15	.90	3.20	.84

Scale: 1 = Novice Level to 4 = Advance Level

Throughout the academic year, participants' research performance was evaluated. In Table 10, mentors' mean ratings show that participants in the 1st cohort had good performance of lab techniques (when applicable) by end of the fall term (M=4.17, SD=.41) and end of spring term (M=4.59, SD=.62), good quality of work (M=4.44, SD=.70) and good initiative (M=4.35, SD=1.06) by end of spring. For the 2nd cohort, the highest ratings were for initiative (M=4.38, SD=1.06) and performance of lab techniques (M=4.29, SD=1.11). For the 3rd cohort, participants were rated with good initiative for summer (M=4.23, SD=1.30) and fall (M=4.40, SD=.89). Students in 3rd cohort who continued their research in fall 2023 have highest ratings for performance of lab techniques (M=4.60, SD=.55) and ability to carry out research (M=4.20, SD=1.30). Across the three cohorts, mentor ratings were lowest for knowledge of subject matter in the first term of participation (i.e., fall 2021, fall 2022, summer 2023). These ratings are expected considering that students are learning about their research projects and building their knowledge and skills in the beginning.

Table 10. Mean Mentor Ratings on Students' Research Skills

	Fall 21		Spring 22		Fall 22		Spring 23		Summer 23		Fall 2023	
	μ	SD	μ	SD	μ	SD	μ	SD	μ	SD	μ	SD
Initiative	3.75	1.28	4.35	1.06	4.38	1.06	3.67	1.15	4.23	1.30	4.40	.89
Reliability	4.00	1.31	4.06	1.00	4.00	1.20	3.67	1.15	3.92	1.12	4.00	1.22
Quality of Work	4.14	.38	4.44	.70	4.25	1.39	4.00	1.00	4.08	1.12	4.00	.71
Time Commitment	3.88	1.25	3.53	1.26	4.13	1.46	3.67	.58	3.69	1.25	3.80	1.10
Knowledge of Subject Matter	3.38	.92	3.95	.78	3.50	1.31	3.33	.58	3.38	1.19	3.80	.84
Performance of Lab Techniques	4.17	.41	4.59	.62	4.29	1.11	3.67	.58	4.09	1.30	4.60	.55
Understanding of the Research Process	3.86	.69	3.94	.94	4.13	1.36	3.67	.58	3.83	1.34	4.00	1.22
Ability to Carry Out Research	3.83	.41	3.89	1.18	3.75	1.39	3.67	.58	3.67	1.30	4.20	1.30

Scale: 1 = Poor to 5 = Excellent

Table 11 shows the correlations among the different variables of interest in student learning and research performance. For the fall term of the 1st cohort, the number of work hours per week was strongly correlated with ability to read and understand scientific literature and skill in scientific writing. The value of research experience was significantly related to readiness for more research. The ability to understand literature was strongly correlated with skill in scientific writing. Learning to work independently was strongly correlated with ability to analyze data whereas the latter was strongly positively correlated with skill in interpreting results. Understanding the research process was also significantly related to readiness for more research.

Table 11. Correlations among Variable – Fall 2021

	1	2	3	4	5	6	7	8	9
1. Work hours									
2. Value of Research Experience	0.252								
3. Ability to Read and Understand Scientific Literature	.809*	0.407							
4. Learning to Work Independently	0.398	-0.043	0.516						
5. Learning Laboratory Skills	0.085	0.683	0.113	-0.315					
6. Skill in Scientific Writing	.797*	0.569	.867*	0.171	0.525				
7. Ability to Analyze Data	0.408	0.492	0.661	.850*	-0.062	0.447			
8. Skill in Interpreting Results	0.340	0.682	0.570	0.620	0.010	0.376	.923**		
9. Understanding the Research Process	0.679	0.480	0.643	0.014	0.574	0.706	0.162	0.270	
10. Readiness for More Research	0.623	.776*	0.616	0.012	0.592	0.736	0.310	0.443	.759*

*Correlation is significant at the 0.05 level (2-tailed).

**Correlation is significant at the 0.01 level (2-tailed).

In Table 12, ability to read scientific literature was found to be strongly correlated with skill in scientific writing and understanding the research process for the spring semester of the 1st cohort. Understanding the research process was found to be significantly related to skill in scientific writing and readiness for more research.

Table 12. Correlations among Variable – Spring 2022

	1	2	3	4	5	6	7	8
1. Value of Research Experience								
2. Ability to Read and Understand Scientific Literature	0.559							
3. Learning to Work Independently	-0.026	0.233						
4. Learning Laboratory Skills	0.767	0.767	-0.169					
5. Skill in Scientific Writing	0.556	.936*	0.044	0.659				
6. Ability to Analyze Data	0.000	-0.636	0.899	-0.636	-0.522			
7. Skill in Interpreting Results	0.500	-0.492	0.375	0.000	-0.471	0.739		
8. Understanding the Research Process	0.740	.908*	0.355	0.658	.896*	-0.091	0.000	
9. Readiness for More Research	0.813	0.813	0.477	0.707	0.699	0.174	0.471	.930*

*Correlation is significant at the 0.05 level (2-tailed).

**Correlation is significant at the 0.01 level (2-tailed).

Table 13 shows the correlations for the 2nd cohort of participants in fall 2022. Strong positive correlations were found for 1) value of the research experience and the helpfulness of the seminars, 2) ability to read and understand scientific literature and learning to work independently, 3) ability to read and understand scientific literature and understanding the research process, 3) learning to work independently and understanding the research process, 4) skill in scientific writing and ability to analyze data, 5) skill in scientific writing and skill in interpreting results, 6) ability to analyze data and skill in interpreting results, 7) ability to analyze data and helpfulness of seminars, and 8) skill in interpreting results and understanding the research process.

Table 13. Correlations among Variable – Fall 2022

	1	2	3	4	5	6	7	8	9	10
1. Work hours										
2. Value of Research Experience	0.655									
3. Ability to Read and Understand Scientific Literature	0.378	0.577								
4. Learning to Work Independently	0.429	0.655	.945**							
5. Learning Laboratory Skills	0.655	0.333	0.577	0.655						
6. Skill in Scientific Writing	0.790	0.603	0.261	0.395	0.302					
7. Ability to Analyze Data	0.509	0.556	0.096	0.218	-0.111	.905*				
8. Skill in Interpreting Results	0.663	0.667	0.840	0.868	0.583	.921*	.932*			
9. Understanding the Research Process	0.395	0.603	.914*	.987**	0.603	0.455	0.302	.910*		
10. Readiness for More Research	0.463	0.707	0.612	0.463	0.000	0.426	0.471	0.583	0.426	
11. Helpfulness of Seminar	0.612	1.000**	0.490	0.612	0.167	0.840	.944*	0.927	0.612	0.667

*Correlation is significant at the 0.05 level (2-tailed).

**Correlation is significant at the 0.01 level (2-tailed).

In Table 14, several variables were found to be strongly positively correlated with each other. For the 2nd semester of the 2nd cohort, understanding the research process was significantly related to ability to read and understand literature, value of the research experience, and the helpfulness of the seminars. Learning to work independently was significantly related to learning laboratory skills, skill in scientific writing, ability to analyze data, skill in interpreting results, readiness for more research, and satisfaction with mentor support. These results indicate that gains in students' research skills contribute to their ability to work independently. Moreover, mentor support is essential in developing these research skills. Students who are satisfied with the support they received from their mentors are more likely to develop their research skills.

Table 14. Correlations among Variable – Spring 2023

	1	2	3	4	5	6	7	8	9	10	11
1. Work hours											
2. Value of Research Experience	0.070										
3. Ability to Read and Understand Scientific Literature	0.610	0.768									
4. Learning to Work Independently	0.552	0.791	0.773								
5. Learning Laboratory Skills	0.303	0.663	0.445	.886*							
6. Skill in Scientific Writing	0.364	0.745	0.573	.943**	.950**						
7. Ability to Analyze Data	0.551	0.664	0.667	.919**	0.783	.928**					
8. Skill in Interpreting Results	0.551	0.664	0.667	.919**	0.783	.928**	1.000**				
9. Understanding the Research Process	0.171	.978**	.854*	0.773	0.552	0.677	0.667	0.667			
10. Readiness for More Research	0.612	0.674	0.800	.853*	0.756	0.804	0.784	0.784	0.659		
11. Helpfulness of Seminar	0.156	.894*	0.781	0.707	0.456	0.667	0.743	0.743	.937**	0.603	
12. Satisfaction with Support from Mentor	0.442	0.632	0.552	.875*	.927**	.825*	0.657	0.657	0.552	0.746	0.354

*Correlation is significant at the 0.05 level (2-tailed).

**Correlation is significant at the 0.01 level (2-tailed).

Table 15 shows the correlations for the 3rd cohort of participants. Students' value of the research experience was significantly related to readiness for more research. Echoing the finding from the 2nd cohort, satisfaction with mentor support was found to be strongly correlated with research skill development especially in their ability to read and understand scientific literature, ability to analyze data, and understanding the research process.

Table 15. Correlations among Variable – Summer 2023

	1	2	3	4	5	6	7	8	9	10
1. Work Hours										
2. Ability to Read and Understand Scientific Literature	-0.488									
3. Learning to Work Independently	0.227	0.418								
4. Learning Laboratory Skills	0.298	0.400	0.000							
5. Skill in Scientific Writing	0.118	0.689	0.607	0.707						
6. Ability to Analyze Data	-0.173	0.601	0.296	0.389	0.693					
7. Skill in Interpreting Results	-0.173	0.601	0.296	0.389	0.693	1.000**				
8. Understanding the Research Process	0.070	0.258	0.540	0.194	0.702	0.730	0.730			
9. Readiness for More Research	0.547	-0.439	0.367	-0.022	0.255	0.062	0.062	0.679		
10. Value of Research Experience	0.545	-0.548	0.000	0.228	0.132	-0.194	-0.194	0.354	.801*	
11. Satisfaction with Support from Mentor	-0.452	.789*	0.367	0.285	0.700	.930**	.930**	0.679	-0.077	-0.320

*Correlation is significant at the 0.05 level (2-tailed).

**Correlation is significant at the 0.01 level (2-tailed).

We also asked students the following questions, 1) what does joining the program mean to you? and 2) what did you like best about the program? Students' responses to the first question ranged from having the opportunity to do research and building/expanding their knowledge to clarifying their interest in research and pursuing graduate degrees. Students shared that what they liked best about the program was the skills they gained while conducting research, learning something new (e.g., interdisciplinary approach), and meeting other researchers and knowing more about their research.

VERBATIM RESPONSES TO OPEN-ENDED QUESTIONS

1. What does joining the program mean to you?

A. 2021 – 2022 Cohort

- I joined ALERT for a good research experience, and that's what I've gotten. I'm learning a lot at a far deeper level than any content in my classes.
- Being a part of the ALERT program means being part of a group of motivated and intellectual individuals who are excited to learn about emerging technologies that pertain to the future of our nation's military.
- It gives me some exposure to some cool research topics that I wouldn't see otherwise.
- Being a better researcher!
- An opportunity to study a niche field and expand my engineering knowledge in a more focused environment.
- Conducting research for the ALERT program has been very special to me as I am directly researching topics that I may encounter in my career in the Navy. I hope to improve upon the existing technologies the military uses such that it can better conduct its mission.
- New opportunities!!
- It means gaining some more experience in a very unique job field.
- It's a chance to practice the kind of work I want to do in the future.

B. Summer 2023 Cohort

- I believe being in the ALERT program allows you experience what research is like. It also allows you to learn a specific area and see if its something you want to go deeper into in the future.
- Being in the Summer ALERT Program means that people think my research is a valuable contribution to society and worth funding. It gives me confidence that my work is meaningful and that I can make a real positive difference through it.
- It helped me learn about research methods and gave me great insight into 2D Material
- This program meant gaining hands on experience with engineering research as well as an idea for how much I'd enjoy graduate school. I was also able to learn more concretely some topics related to my major.
- Being in the ALERT program was important to me because it was a way to gain some valuable research experience and get a feel for what research is like after learning all about it in GFX.
- Being in the ALERT program was a great opportunity for me to learn what being in a real research environment is like. My goal is to do research some day after I graduate, and the ALERT program has made me even more interested in pursuing undergraduate research opportunities. I will learn from my successes and mistakes in the program and apply them to my future work.
- Summer ALERT Program was my first exposure to research; I have decided to do a Master's degree as I have had a great first impression of research experience.

2. What did you like best about the program?

A. 2021 – 2022 Cohort

- Developing my lab skills, particularly on specialized machines
- I like how it forces you to work independently and try to learn things on your own first.
- The fact that I can bring some experiences from ROTC to help my graduate student better develop his experiments.
- Learning of the cool projects.
- The opportunity to learn something new in a more personal, one on one way. More than some of my classes, I feel that I have learned a great deal in this group: I previously had a negative perception of electrical engineering, but that has since changed.
- My favorite part about conducting research is the ability to create change and develop innovations for the military.
- Opportunity to try new things
- Very unique fields of research
- It's a good look into how research functions. I haven't been able to join the research group meetings, so I don't know what the graduate perspective is like, but from a "technician" perspective it's been a good way to understand choosing a research question, working towards that goal, and interacting with multiple people working on interrelated tasks.

B. 2022 – 2023 Cohort

- The diversity and ability to come together to share our learnings.
- I got to learn how research works, got to work with peers with the same interest.
- I specifically like the design of the program where I initially learn basics of research and implement
- The best part is learning about something interdisciplinary from my own subject I study academically (Physics). Sure it is frustrating at times, working on machine learning techniques have taught me several things on data analysis that are applicable to lab work within Physics.
- I like that it provided me with experience such as AFM and SEM that undergraduates would have not normally been able to use.
- Learning to work as part of a research group
- My program was geared toward learning
- The supporting activities and workshops
- I liked how I could take my project where I wanted to.
- I liked the monthly seminars as well as being able to hear about other people's projects through the class
- I got to meet other undergraduate researchers.
- I love the multidisciplinary aspect of the program. Interacting with and learning from other undergraduates from different academic disciplines was inspiring and interesting.

C. Summer 2023 Cohort

- I enjoyed learning about my research topic and running experiments to compare the results for different pruning methods.
- I enjoyed the DCL meeting where my mentor was blindfolded, and I got to help direct him to find and use a pool noodle. That was a fun experience that helped us grow closer.
- Learning to use all the equipment for collecting data.
- I liked that I worked whenever I wanted and that it was very self-paced.
- I liked the flexibility that the program offered. There were days when I had to be in the lab creating samples and running tests, but on the days that I didn't have to come in, I was reading research papers and creating experiments, which helped create variation throughout the week.
- I liked being exposed to a very interesting area of research that I had no previous knowledge of. My graduate student mentor was very good at explaining the technical details of the project that I was unfamiliar with. I also like that I was able to experiment with a set of interesting software tools that I had never used before.
- Being on campus during the summer when labs are less crowded, and I could go in whenever I want because there are no classes.

Changes and Problems

The ALERT Program officially started in August 2021. Recruitment of participants for the fall 2021 cohort began in spring 2021. **A major change from the plan was the program's end date.** In May 2022, we requested a 12-month no-cost extension (NCE) to complete original project objectives and phase out projects that will no longer receive continued support. A late start to the project due to circumstances beyond the control of the principal investigators necessitated the extended due date. The project expiration date was then changed to 7/31/2023.

One key learning from our 1st cohort of 12 participants, who were all ROTC students, was that the demands of their **ROTC workload posed a challenge to do research for at least 10 hours a week.** Most of the ROTC students were unable to do research in the summer due to boot camps and summer internships with their military units. Consequently, we **sought approval to include non-ROTC students in the program. We also shifted our efforts to recruiting students from underrepresented groups in STEM and successfully recruited more women, 1st generation students, African American, and Hispanic/Latino students.**

With the addition of new participants come training expenses and support for their graduate student mentors. We asked for **budget reallocations** of a portion of participant support cost to cover expenses related to research lab training of the new undergraduate researchers.

In February 2023, we encountered changes to participant numbers due to various personal reasons shared by our undergraduate students. A decrease in participants resulted to unspent funds. We then reported that we expected to carryover funds to summer 2023 and **proposed a**

summer research program to utilize the remaining funds. The summer research program was open to both ROTC students and students from underrepresented groups in STEM. Our proposed adaptations caused by unexpected events were approved and carried out.

From our update meeting in July 2023, students informed us of some challenges hindering progress to their projects. Primarily, there were **unforeseen delays in the delivery of materials and equipment for some of the summer projects.** In particular, the delivery date of an essential component of the project was pushed back to September. Unexpected supply chain problems delayed the progress and completion of the project. Due to circumstances beyond the control of the principal investigator, an extended due date was necessary. Given this information, we requested an exceptional no-cost extension on July 18, 2023. The approved exceptional NCE changed the project expiration date to 12/31/2023.

Throughout the period of performance, we faced several challenges that led to changes in program end dates and budget utilization. For every challenge, **we were able to pivot, and propose plans of action that were successfully executed from recruitment to budget reallocations.** We were proactive in communicating potential changes to our Sponsored Programs Administration and the Naval STEM Grants Program Officer to ensure successful accomplishment of project plans. The entire budget was spent judiciously to meet our program goals.

With the NCEs, **we were able to broaden participation in STEM,** specifically in undergraduate research through the ALERT program. We **expanded the research opportunities to people of diverse racial/ethnic, and socioeconomic backgrounds and to women who continue to be underrepresented in engineering fields.** 25 new undergraduate student participants joined the ALERT program by summer 2023. A total of 37 undergraduate students participated in interdisciplinary research projects.

Individual Project Reports

Fall 2021 – Spring 2023

Project 1 and 2: Reconfigurable Antenna System to Detect and Mitigate GPS Spoofing/Jamming; Small Phase Array Behavior on Portable/Mobile Platforms

A. Goals and Accomplishments

The primary goal of this project was to work towards **designing a reconfigurable antenna array.** The students were to gain experience with a commercial simulator, fabrication tools, and top of the line equipment to investigate the behavior of antennas and arrays, as well as their construction. Students also investigated the behavior of reconfigurable antennas and their benefits, culminating in a combination reconfigurable antenna array. This could also involve further investigation into the platforms these arrays will be implemented on, including unmanned ariel vehicles (UAVs)

To accomplish the primary goal, a three-step approach was taken.

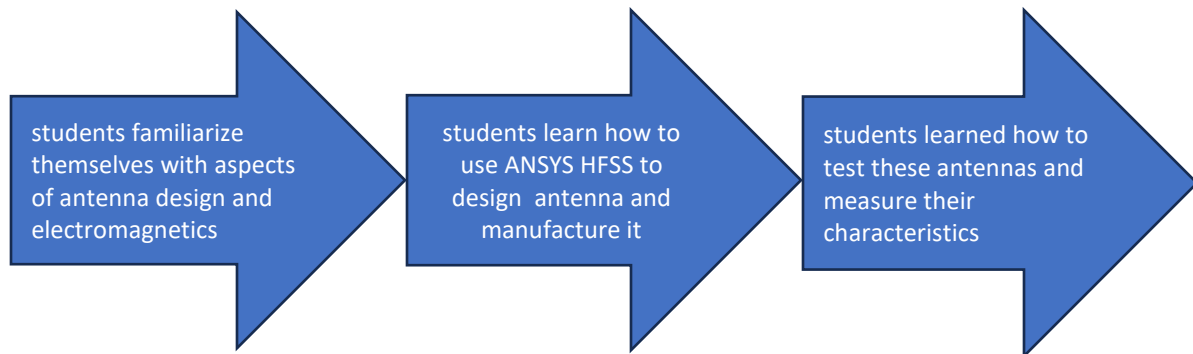


Figure 3. Three-step process to designing a reconfigurable antenna

As seen in Figure 3, the first step was to have students familiarize themselves with aspects of antenna design and electromagnetics, reading papers and learning antenna language so that they can both study and communicate their findings with the scientific world. The second step entailed having students learn how to use ANSYS HFSS, one of the primary antenna design simulators and the main tool in our lab so that they can design their own microstrip patch antennas. Then, they should take their designs from HFSS to the milling machine and manufacture their designed antennas on the substrate they have chosen. In the third step, the students learned how to test these antennas and measure their characteristics to see how simulation translates to design and the differences in substrates regarding results. All these objectives were accomplished and each of the three students designed, manufactured, and tested microstrip patch antennas that function at 3 GHz, a common radar frequency.

Each of the three students used different substrates to see the differences made in just the material used for them to select one they would eventually build their array on, looking at how closely each matched their design goals. They found that the thicker substrates required smaller patches and had less manufacturing errors that interfered with their design objective.

The students also began to design and simulate a reconfigurable loop, that, given more time, they would also build and test the same way they did the microstrip patch antennas, and after this finally pick their substrate and construct a four by one antenna array to test as well. This should be done in future work.

A. Opportunities for Training and Professional Development

The main opportunity with this project is learning ANSYS HFSS, as this is an extremely useful and widely used tool in industry and provides valuable skills to the students. The students also attended a virtual conference in January to have exposure to the conference environment and observe examples on how to present their work effectively. The students also spent many hours in a research lab testing their work and processing the data from their experiments, yet another valuable skill that is not just specific to antenna design.

B. Dissemination of Results

ROTC students presented at the ISUR Research Expo on April 12, 2022. A poster was presented highlighting the work done, and the manufactured antennas were put on display as well. Max Damewood presented their project at the poster session of the ISUR Research Expo in April 2023.

Project 3: Advanced Photon Sources for Secure Quantum Communications

A. Goals and Accomplishments

This project aimed to advance our knowledge and capability in secure communication and digital transactions relevant to electronic warfare. More specifically, we aim to develop a photon source that can emit one photon at a time (i.e., single photon emitter, SPE), critical to quantum communications and information processing. Our approach will be to use next generation, atomically-thin transition metal dichalcogenides (TMDs) and apply localized strain. Although TMDs are promising for their high light extraction efficiency, it has been challenging to modulate the emission sites and emission energy of TMD based SPEs. Strain engineering allows precise control of band structure and photon energy of TMDs. In particular, mechanical instability driven wrinkles on stretchable substrates are an excellent platform for tuning TMDs' electronic structures via local strain manipulation. Spatially localized straining will allow realization of deterministic SPE arrays, crucial for next generation quantum cryptography.

We applied biaxial strains on plasma-treated polydimethylsiloxane (PDMS) substrates. Depending on the prestrain and release method, various types of wrinkle structures were created on the skin layer of the PDMS substrates. Figure 1 shows the images of different samples obtained by 3D laser scanning confocal microscope. For the 'sequentially' released samples, x-directional prestrain was released prior to the y-directional prestrain. For the 'simultaneously' released samples, both x- and y-directional prestrains were released together. There was a clear difference in topography between sequentially and simultaneously released samples. Non-uniform wrinkle structures were observed from the sequentially released substrates, whereas simultaneously released substrates showed uniformly distributed wrinkle structures. Due to the non-uniformity, the sequentially released samples had locally densified wrinkle areas where the y-directional strain was concentrated (horizontal lines of x15%, y5% sample and herringbone structured areas of x15%, y10% and x,y15% samples).

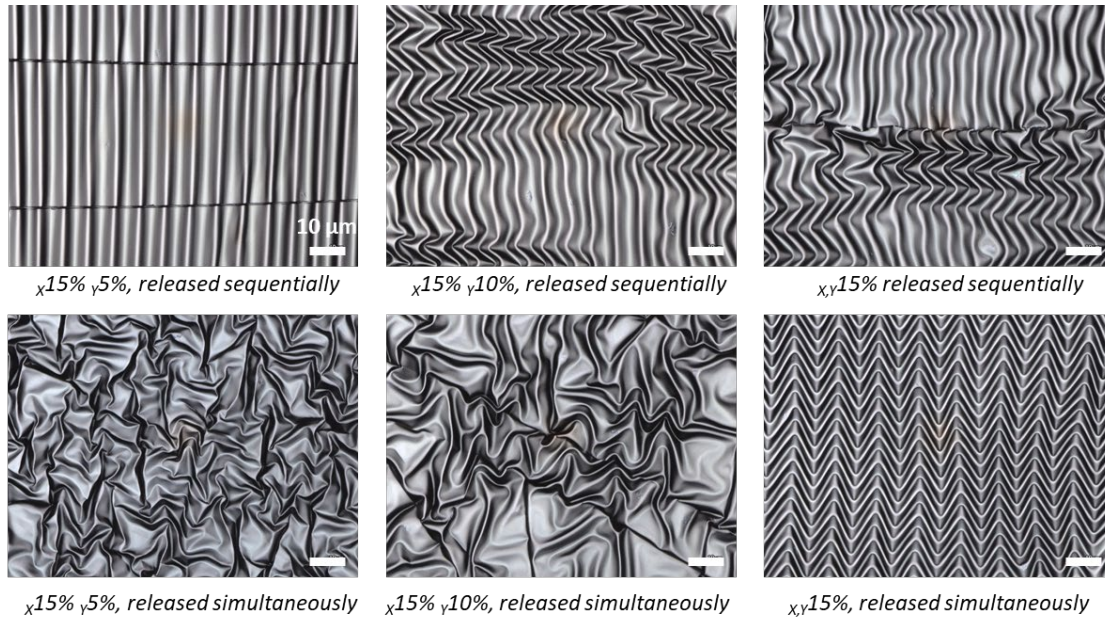
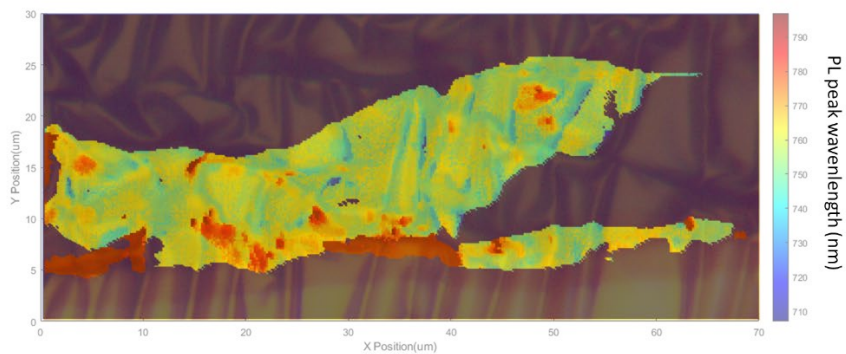
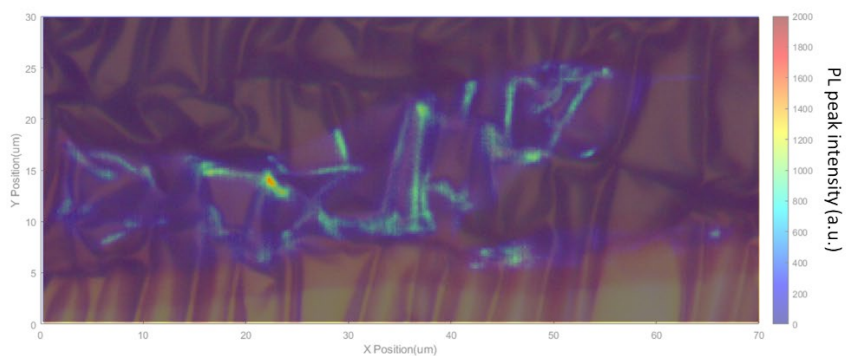


Figure 4. 3D laser scanning confocal microscope images of various types of wrinkle structures created by different pre-strain and release method. Scale bar is 10 μm .

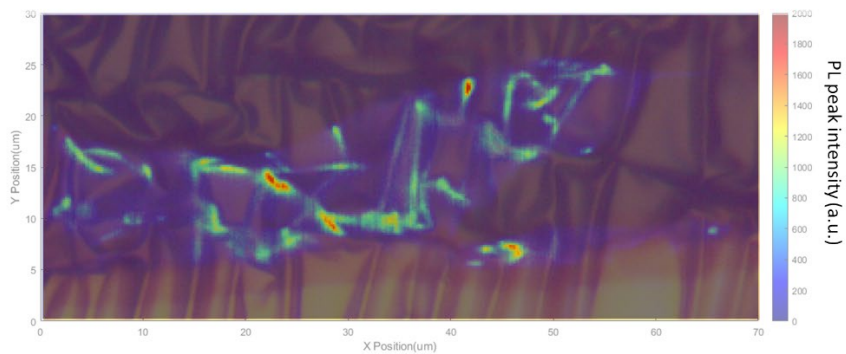
To investigate local straining of monolayer WSe_2 using the wrinkled substrate, we placed monolayer WSe_2 on a x25 %, y25 % pre-stretched PDMS and released the prestrains sequentially. Then, we measured photoluminescence (PL) of the monolayer WSe_2 on the locally densified wrinkle area. Without any strain, the PL emission peak of monolayer WSe_2 is about 750 nm. However, as shown in Figure 2, WSe_2 on valleys of the wrinkle structure showed blueshifted PL emission peak down to 730 nm, whereas WSe_2 on apexes of the wrinkle structure showed a redshifted PL emission peak up to 790 nm. The PL intensity mapping at 780 nm shows that the most redshifted PL emission peak was observed at the cross-shaped wrinkle locations, where the tensile stress was applied on both x- and y-directions. These results show that the PL emission peak of the monolayer WSe_2 can be significantly modulated by applying different degrees of prestrain. In addition, it is able to obtain highly localized areas with shifted PL emission peak which is a possible candidate for SPE applications.



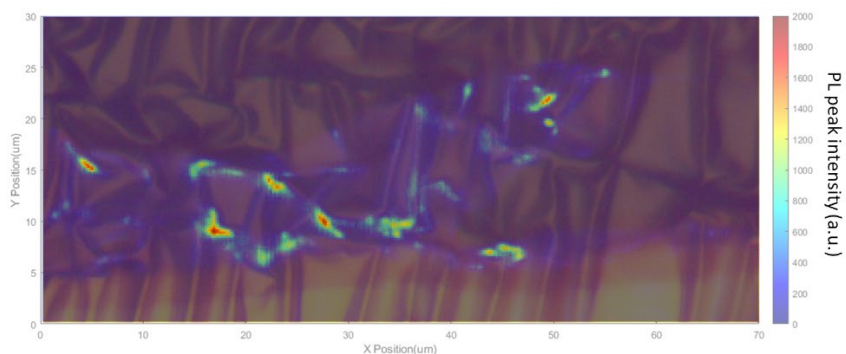
PL peak wavelength mapping of WSe₂ on x,y25% PDMS, released sequentially.



PL intensity mapping at 740 nm.



PL intensity mapping at 760 nm.



PL intensity mapping at 780 nm.

Figure 5. PL mapping images of monolayer WSe₂ on a x,y25% pre-stretched PDMS, released sequentially.

B. Opportunities for Training and Professional Development

The participants of the project have experienced cleanroom facilities and been trained to handle various instruments related to microfabrication, such as spin-coater and oxygen plasma descum system. The participants have also developed professional skills on exfoliation of 2D materials, dry transfer of 2D materials, and wet transfer process. Moreover, the participants learned how to utilize characterization tools such as optical microscope, atomic force microscope, laser scanning confocal microscope, and Raman/PL spectroscopy. Each participant has contributed to all research steps from fabrication to analysis and presented the results in TMS* 2022 and MRS** 2022 conference.

*The Minerals, Metals & Materials Society

** Materials Research society

C. Dissemination of Results

1. Jin Myung Kim gave an oral presentation in TMS 2022 conference: “Exciton Transport in Strained Two-dimensional Semiconductors”
2. Yeageun Lee gave a poster presentation in TMS 2022 conference: “Crumpled MoS₂ Flexoelectric Energy Harvester”
3. Jin Myung Kim gave an oral presentation in MRS 2022 conference: “Tailoring Exciton Transport in Strained Two-Dimensional Tungsten Diselenide Toward Straintronics”
4. Yeageun Lee gave an oral presentation in MRS 2022 conference: “Converse Flexoelectric Two-Dimensional MoS₂ Actuator”
5. Yeageun Lee was awarded first prize for FMD Graduate Technical Division Student Poster Contest in TMS 2022 conference.
6. Henry Feldhaus and Mary G. Pelzer gave a poster presentation in MRS 2022 conference: “Stretchable Wrinkled WSe₂ for Tunable Single Photon Emitters”
7. Mary Pelzer and Henry Feldhaus presented their research in the poster session of the ISUR Research Expo in April 2022.
8. Publication(s)

Zhang, Z., Lee, Y., Haque, M. F., Leem, J., Hsieh, E. Y., & Nam, S. (2022). Plasmonic sensors based on graphene and graphene hybrid materials. *Nano convergence*, 9(1), 28. <https://doi.org/10.1186/s40580-022-00319-5>

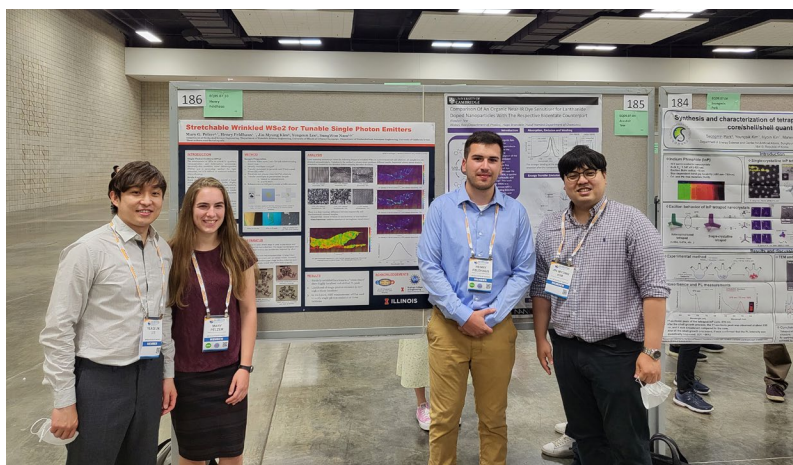


Figure 6. Photo from MRS 2022 Conference Poster Session. From left to right: Yeageun Lee (mentor), Mary G. Pelzer (ROTC Army undergraduate researcher), Henry Feldhaus (ROTC Army undergraduate researcher), Jim Myung Kim (mentor)

Project 4: Next Generation Power Electronics

A. Goals and Accomplishments

By 2030, 80% of all electric power will flow through Power Electronics at some point between generation and distribution (currently 30%). The research objective was to explore the next generation diamond-based power electronics. Diamond makes it possible to reduce energy losses, weight, volume, and life-cycle costs in a wide range of power applications. Harnessing these capabilities can fulfill advanced DoD needs in mobilization, secure grids, and reliable communication, lead to dramatic energy savings in industrial processing and consumer appliances, accelerate widespread use of electric vehicles and fuel cells, and help integrate renewable energy onto the electric grid. For instance, diamond materials have the potential to reduce transformer size by a factor of ten or more and cut transmission losses by 75%. The project goal is to research the disruptive diamond electronics technology which could significantly improve energy efficiency and rapidly transform the existing DOD capabilities in vital electronics domain.

Property		Si	4H-SiC	GaN	Ga ₂ O ₃	AlN	Diamond
Bandgap(eV)		1.1	3.3	3.4	4.9	6.1	5.5
Breakdown field (MV/cm)		0.3	2.8	3.5	8	10	7.7-20
RT mobility (cm ² /V-s)	electron	1500	1000	>1000 (bulk)	300	300	1060
	hole	480	120	<200 (bulk)	-	14	2100 (bulk)
Thermal conductivity (W/cm-K)		1.5	3.7	1 (on Si) 165 (on sapphire) 253 (on GaN)	0.11-0.27	2.53-3.19	22
Saturation velocity (x10 ⁷ cm/s)	electron	1	1.9	2.5	2	1.4	2.5
	hole	0.8	1.2	-	-	-	1.4
Baliga's figure of merit (Si = 1)		1	165	635	1231	7905	23017

Table 1. Comparison of Semiconductor Properties for Use in Power Electronic Devices

To accomplish the research objective, two major tasks were completed: 1) Multiphysics modeling and structure device design, and 2) Material characterization.

The first task involved simulation of diamond-based power devices through industrial TCAD Sentaurus software. Theory and simulations are vital to interpretation of measurement data and, in tandem, guidance of the experimental efforts. We created a multi-physics computational framework that is unique to diamond by integrating materials synthesis, characterization, and device-specific phenomena (i.e., high field, high temperature, defect transients). Computational studies provided insight into the impact of materials on transport characteristics of devices and are necessary to identify heterostructures with superior power-handling capabilities.

The team worked on the design, simulation, and process flow (based on available cleanroom infrastructure) of the project objective: Diamond Power Schottky Diodes with up-to-3kV target breakdown voltage. The schematic, fabrication process flow, and Synopsys Sentaurus TCAD simulation of the diamond power Schottky diode are shown in Figure 6. Boron-doped p-type diamond layers are currently being grown via chemical vapor deposition on a high pressure/high temperature (HPHT) diamond substrate by the PI-vetted commercial vendor. The HPHT diamond is highly insulating thus minimizes substrate leakages and hence prevents premature breakdown.

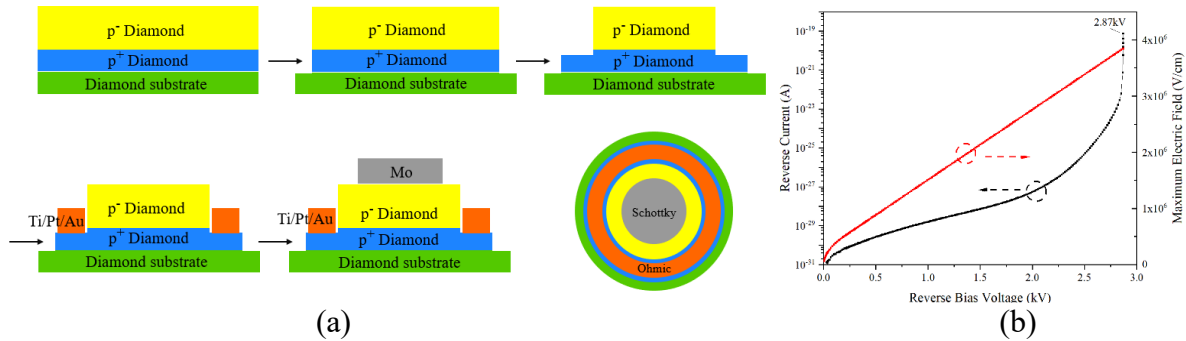


Figure 6. (a) Fabrication process flow and top view schematic of the designed diamond power Schottky diode. (b) TCAD Simulation shows the device being rated for up to 2.87 kV operation. (b).

In addition, they designed the schematic, fabrication process flow, and Synopsys Sentaurus TCAD simulation of the diamond power RB-MESFETs are shown in Figure 7. Compared to the standard MESFET structure, in an RB-MESFET the drain contact is Schottky instead of ohmic. The RB-MESFETs can be used for bi-directional switches which are critical for applications such as power conversion and charging. The device will allow current to flow from source to drain only when $V_{GS} < V_{TH}$ and $V_{DS} < 0$. Here V_{TH} is the threshold gate bias voltage, and V_{DS} is the drain-to-source bias.

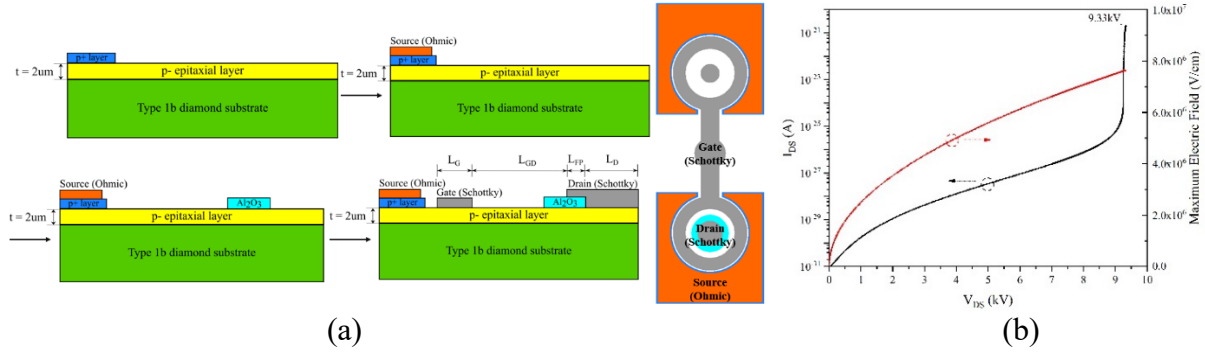


Figure 7. (a) Fabrication process flow and top view schematic of the diamond power reverse-blocking metal semiconductor transistor (RB-MESFET). t is the thickness of the p- diamond layer; L_{FP} is the length of the field plate oxide (i.e., Al_2O_3); L_D is the radius of the drain contact; L_G is the length of the gate contact; L_{GD} is the separation between the gate and drain. (b) TCAD Simulation shows the device being rated for up to 9.33 kV operation. ($V_{GS} = 0V$)

The second task involved structural (e.g., optical microscopy, atomic force microscopy, scanning electron microscopy, X-ray diffraction), optical (e.g., temperature dependent photo- and cathodoluminescence), and electrical (e.g., Hall-effect) measurements. The team focused on studying methodologies for synthesizing low-defect-density ($< 10^8 \text{ cm}^{-2}$), low-background-impurity ($< 10^{14} \text{ cm}^{-3}$) single crystal diamond, based on microwave plasma CVD. A primary objective is to study defect creation, propagation, and electrical behavior. Extensive structural, optical, electrical, and thermal properties of lab-grown diamond are to be reported, with a focus on exploring how semiconducting diamond properties vary with growth conditions and growth techniques, and what properties electronic-grade diamond has.

B. Opportunities for Training and Professional Development

This research will enable safe and detailed measurements of such power devices. The students are identifying the failure mechanisms in diamond-centric power devices; demonstrating how to mitigate them through material innovation. This research is creating immense knowledge for the student in power semiconductors. Overall, the students gain significant experience on the materials design, growth, fabrication, and measurement better understanding of how to conduct scientific experiments in power semiconductors area.

C. Dissemination of Results

Research was presented in the poster session at the 2022 Compound Semiconductor Conference in Ann Arbor, Michigan.

- Zhuoran Han, Samuel Weiss, Victoria Garcia, Can Bayram, *Diamond for Advanced Power Electronics*, Compound Semiconductor Week, Ann Arbor, MI, June 1- 3 (2022).
- Z. Han and C. Bayram, "Diamond p-Type Lateral Schottky Barrier Diodes with High Breakdown Voltage (4612 V at 0.01 mA/Mm)," in *IEEE Electron Device Letters*, vol. 44, no. 10, pp. 1692-1695, Oct. 2023, doi: 10.1109/LED.2023.3310910.

Sam Weiss presented his poster at the ISUR Research Expo in April 2022, whereas Victoria Garcia and Aleksai Herrera presented their respective posters at the ISUR Research Expo in April 2023.

Project 5: Trustworthy Machine Learning

A. Goals and Accomplishments

One goal was for the student to conduct a literature survey on the topics related to the robustness of image classification methods. The student was encouraged to learn basic machine learning background knowledge and to read papers.

The overall technical goal was to train the student to use machine learning techniques to analyze network traffic data and detect anomalies for security considerations. The student learned about basic machine learning techniques and became familiar with how to apply those techniques to real-world situations.

1. The student finished a complete series of online courses on machine learning and read several papers.
2. A malicious network traffic data packet with specific features that set itself apart from normal packets was provided. We used Intrusion Detection Systems (IDS) to detect such data packets. It is essential to detect such attacks because they can cost entities millions in lost revenue, research, or progress. There are three kinds of IDS:
 - a) Signature Based: Utilizes a feature of traffic to predict a class. Hard to generalize to unknown/novel attack classes
 - b) Anomalous Based: Detects deviations from normal learned behaviors. Unable to compensate for changes in everyday operations.
 - c) Hybrid: Combination of the above two approaches
3. The student utilized a Feed-forward Neural Network (NN) to build an effective hybrid IDS. The NN has two parts: Part 1: Autoencoder to reduce the dimension of the data packet to something more manageable; Part 2: Cross-entropy loss NN to categorize the truncated data packets.
4. The student tested multiple learn rates to determine the peak accuracy of my model. Additionally, specific kinds of errors over others were prioritized. It was assumed that predicting malicious traffic as the normal class carries the most harmful implications. A confusion matrix was used to conclude that the IDS is vulnerable to “back” attacks because the model classifies around $\frac{1}{2}$ of those attacks as normal traffic.

B. Opportunities for Training and Professional Development

The student learned machine learning techniques through taking an online course and reading and discussing scholarly articles. The student also conducted a literature survey and learned how to analyze and compare papers, which helped build the student’s background knowledge. He also

gained hands-on experience with the application of machine learning techniques to real-world scenarios.

C. Dissemination of Results

Krishna Vasudev presented his research project at the poster session in the ISUR Research Expo in April 2022 and 2023.

Project 6: Detecting Anomalous Behaviors for Assured Command and Control

A. Goals and Accomplishments

The overall objective of this project is to develop methods for the unsupervised and weakly-supervised detection of anomalies in networked systems. More specifically, we aim to achieve the following objectives:

(1) develop an appropriate dataset and processing pipeline for anomaly detection in a networked system; (2) develop a machine learning approach for unsupervised and weakly-supervised anomaly detection which incorporates inductive biases relevant for network-structured data; (3) compare our approach to existing methodologies and benchmarks.

Our major activities over the past two semesters focused on the following specific objectives:

(1) perform literature review of unsupervised and weakly-supervised anomaly detection methods for networked data; (2) develop a dataset using the Madrid traffic network to serve as a proxy for cyber networks (due to security and data scarcity issues); (3) perform literature review of accident detection algorithms in traffic networks.

Regarding objective (1), we guided the students in performing a literature review of anomaly detection methods to develop their understanding of different possible approaches. During this time, students also developed simple anomaly detection models using pre-existing datasets so they could become familiar with the process of implementing and validating these methods.

Regarding objective (2), we performed a brief literature review of traffic network data and found existing options to be insufficient for our purposes. In particular, many existing datasets only consider either urban or highway traffic settings, and therefore do not include more complex network dependencies expected to be present in cyber systems. We found the open-source data provided by the city of Madrid to be more complex and therefore more appropriate to serve as a proxy for cyber networks. The students developed a preprocessing pipeline for these datasets to be used for unsupervised and weakly-supervised anomaly detection methods.

Regarding objective (3), we guided the students in performing a literature review of traffic incident detection methods. This review was used to identify specific methods which we plan to use as baselines for our approach. In particular, we identified several promising approaches which utilize a supervised learning approach, and several which utilize unsupervised or weakly-supervised approaches.

B. Opportunities for Training and Professional Development

The students met with a graduate mentor for at least one hour per week to meet and discuss materials related to the project. These meetings were an opportunity for the students to learn skills such as the basics of machine learning and data processing, literature review techniques, problem formulation skills, and research project planning.

C. Dissemination of Results

Vivek Thatte presented his research project at the poster session in the ISUR Research Expo in April 2023.

Project 7: Machine-Learning Based Anomaly Detection and Resiliency for Autonomous UUV Swarms

A. Goals and Accomplishments

The usage of unmanned vehicles, for military and civilian purposes, is gaining traction. Although current usage of unmanned vehicles (both aerial and ground) requires human operators, there is active research into autonomous control for such vehicles. With increased deployment, we also see an increase in attacks that target such systems. Successful attacks can have serious effects on the safety and security of the system as well as the human operators; it could also jeopardize the missions at hand. Hence, there is a strong need to mitigate the effect of an adversary's potential compromise of such systems. In this work we focused on the security of unmanned aerial vehicles (UAVs), but the concepts are generalizable to other autonomous systems such as ground and underwater vehicles.

One of the methods that an adversary can compromise a UAV is via sensor spoofing, say by man-in-the-middle attacks between the sensor hardware and the flight controller. Figure 8 shows an example of the effect of the attack where the UAV starts deviating from the mission specifications (i.e., its original flight path). Therefore, our goal was to build an anomaly detector (AD) to detect such attacks. In our preliminary work on ADs [1], it came to our attention that finding an effective method to evaluate an AD is non-trivial. Therefore, we must establish the metric on the effectiveness of our method:

- a) Measure the limits of the adversary's ability to thwart a mission
- b) Measure the sensitivity of the anomaly detector

To measure the limits of an adversary's abilities, we first developed a "worst-case scenario" attack for the UAVs. Such classes of attacks are stealthy where the adversary itself tries to evade detection while manipulating the UAVs. Our current objective was to develop such attacks and demonstrate their practicality by deployment on a real UAV. To achieve the objective, first we established a testbed where we can run experiments. The focus of the students in the ALERT program was to develop and validate software and hardware testbeds for UAVs and then demonstrate the attacks on them.

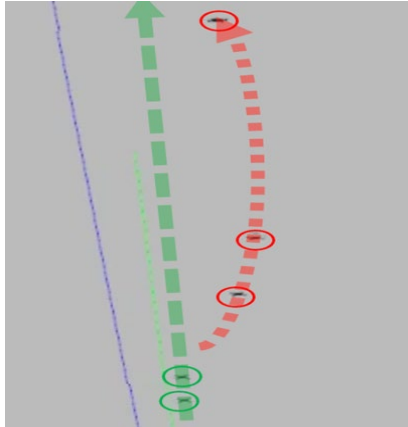


Figure 8. Overlay of the simulation images across different time of the mission captured from simulation. The green arrow represents the path specified by the mission and the red arrow shows the deviated path resulting from the attack. Position of the UAV is highlighted in circle. Green circles represent positions when UAV is in mission specification. Red circles represent positions when UAV is out of the mission specification.

We have developed a software-in-the-loop (SITL) simulation platform to validate our experiments. We also successfully developed a hardware drone platform. In both cases, we can customize and deploy different flight controllers. While testing the hardware deployments, we realized that the inertial sensors were noisy. The ALERT students designed a CAD model to dampen the noise -- primarily by readjusting how the sensor board is being mounted to the frame of the drone.

B. Opportunities for Training and Professional Development

The students were trained to develop the hardware drone platform, deploy, and use the SITL simulation engines and conduct physical drone experiments. They also received lab training and drone flight training. In addition, they were given training on various aspects of research such as literature survey, design of experiments, data collection and analysis, research presentations and writing.

C. Dissemination of Results

Posters were submitted for presentation in the ISUR Research Expo in April 2023 and the Fall Engineering Research Fair in September 2023.

Summer - Fall 2023

Project 1: Development of Wearable Graphene Array Sensors

A. Goals and Accomplishments

This project primarily focused on developing pectin/graphene composite iontronic sensors for infrared sensing and detection of human body temperature objects in complex environments. Students will develop electronic hardware to interface with the iontronic sensors and log and process the data. They were trained in materials characterization and cleanroom fabrication techniques to assist in the fabrication and testing of the iontronic sensors.

B. Opportunities for Training and Professional Development

Participants were all trained in pectin film synthesis procedures including basic fume hood wet chemistry, mold manufacturing, film gelation and dehydration, and sensor testing. The participants additionally developed electrical and mechanical hardware to support the evaluation of pectin film sensors under varying environmental conditions.

C. Dissemination of Results

1. Ezekiel Hsieh gave an oral presentation at MRS 2023 conference: “Flexible and Biocompatible Pectin-Graphene Thin Film Sensor Arrays for Ultra-High Sensitivity Temperature Sensing”.
2. Ashley Saju, Grace Zhen, and Justin Macatangay gave a poster presentation at the UIUC 7th Fall Engineering Research Fair: “Pectin-based Temperature Sensors”

Project 2: Characterization of Strain Distribution in 2D Materials to Engineer Electrical Properties

A. Goals and Accomplishments

The major goal of the project is to probe the flexoelectric effect on ferroelectric materials and to realize flexoelectricity as a universal mechanism of actuation. The specific objectives are as follows:

1. Measuring the flexoelectric coefficient of a two-dimensional ferroelectric α -In₂Se₃.
2. Measuring the strain gradient induced polarization in α -In₂Se₃ at different strain gradients.
3. Comparing the effective flexoelectricity induced polarization with typical piezoelectric materials to realize its potential as actuators.

We have established the technique to transfer α -In₂Se₃ on elastomer substrate and induce strain gradient by elastic-modulus mismatch driven wrinkle formation. We studied the conditions to control the strain gradient. In addition, we have utilized Piezoelectric Force Microscopy (PFM) and Kelvin Probe Force Microscopy (KPFM) techniques to measure the effective piezoelectric moment and electrical polarization of unstrained α -In₂Se₃.

Key Outcomes

1. **Inducing controlled strain gradient in α -In₂Se₃:** In summer 2023, we successfully developed the technique to induce controlled strain gradient in 2D α -In₂Se₃ as demonstrated in Figure 9. First, we have mechanically exfoliated α -In₂Se₃ on SiO₂/Si substrate. Next, we have prepared pre-stretched polydimethylsiloxane (PDMS) and used plasma treatment to form skin layers. Then we deposited 40 nm gold layer on top of the skin layer. Finally, we use dry transfer technique to pick up the 2D material from SiO₂/Si substrate and transfer onto the gold coated pre-stretched PDMS. Upon releasing the pre-

stretch, the transferred α -In₂Se₃ forms wrinkles. By varying the pre-stretch and gold film thickness, we control the strain gradient.

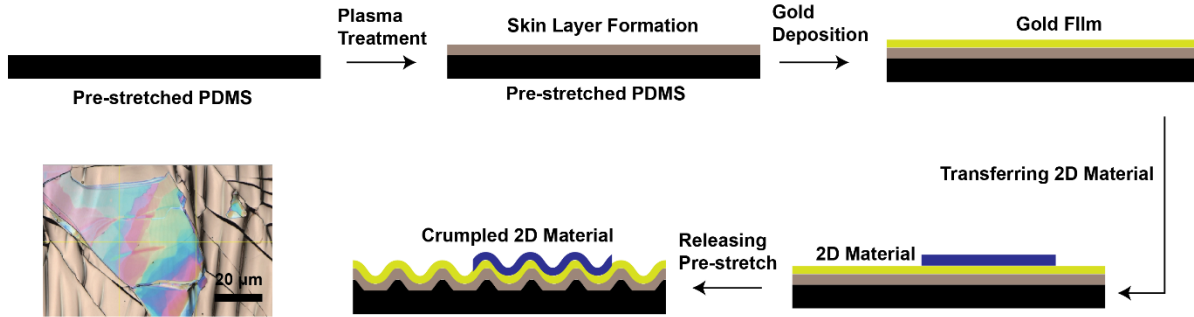


Figure 9. Creating Strain Gradient in α -In₂Se₃ using substrate induced wrinkle formation.

2. **Characterizing the vibrational modes of strained α -In₂Se₃:** Next, we performed Raman spectroscopy on flat and crumpled α -In₂Se₃ to probe the strain effect on the vibrational modes of α -In₂Se₃, as depicted in Figure 10. We observed E², A¹₁, and E⁴ A²₁ modes on the flat sample (Figure 10a). Raman spectroscopy on the wrinkled sample also showed the modes in the similar wavelengths as shown in Figure 10b. Then we performed a line scan on the sample depicted in Figure 10c and plotted the Raman spectra as a function of position (Figure 10d). We do not observe any obvious shift of the Raman peaks, indicating that the strain was not efficiently transferred from the substrate. We hypothesize that the high elastic modulus of the thick sample prevented it from forming conformal wrinkles. Instead, the flake delaminated from the substrate and remained flat.

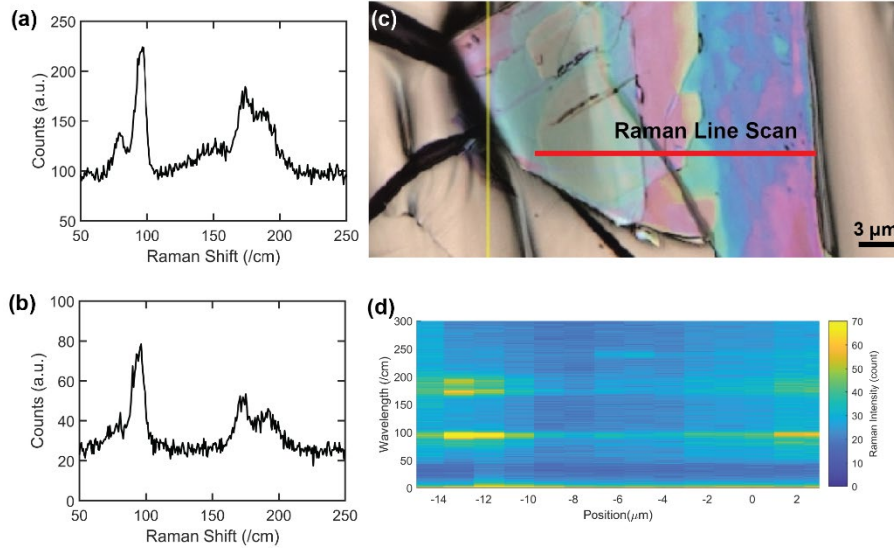


Figure 10. Raman Spectroscopy on (a) flat α -In₂Se₃ exfoliated on SiO₂ and (b) crumpled α -In₂Se₃ on wrinkled gold substrate. (c) Optical image of α -In₂Se₃ on wrinkled substrate. (d) Raman Spectroscopy performed on the marked region of (c).

3. **Characterizing the polarization of α -In₂Se₃ using scanning probe techniques:** We used AFM and KPFM to measure the height and surface potential of α -In₂Se₃ on flat SiO₂ substrate (Figure 11a-b). We used the relation between surface potential (V_s) and polarization (P): $V_s = P t_0 / \epsilon_0 \epsilon_l$ to calculate the polarization of the sample. Here, t is the thickness of the sample and ϵ_0 and ϵ_l are the free space permittivity and dielectric constant of α -In₂Se₃. We also successfully used PFM to measure the effective piezoelectric response from the amplitude image (Figure 11c) and polarization direction from the phase image (Figure 11d).

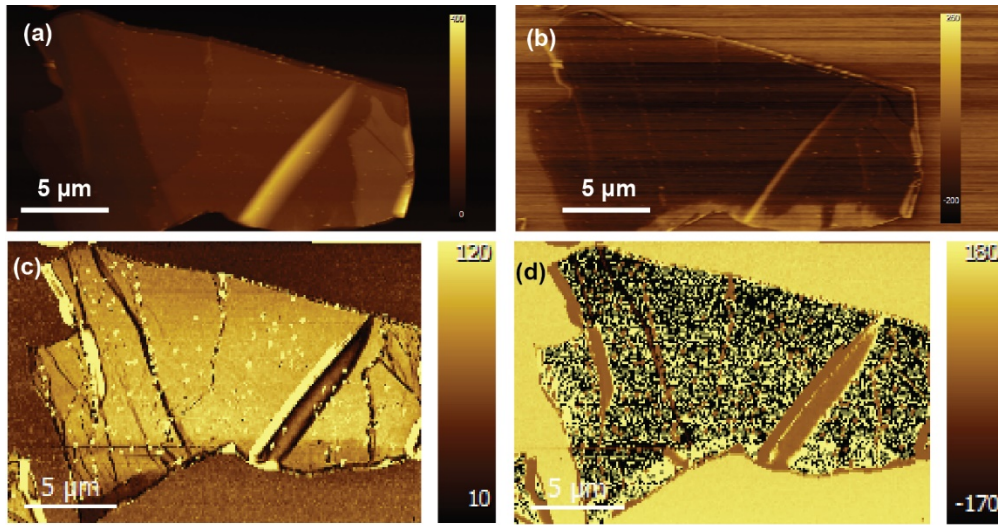


Figure 11. : Scanning probe characterization of α -In₂Se₃ on SiO₂ substrate. (a) AFM topography and (b) KPFM surface potential image of an α -In₂Se₃ flake. (c) PFM amplitude and (d) Phase image of the same flake.

B. Opportunities for Training and Professional Development

This project provided training and professional development opportunities for two undergraduate students, both in Aerospace Engineering at University of Illinois Urbana-Champaign (UIUC). Both students received training on nanoscale materials fabrication and characterization techniques including 2D material exfoliation and transfer, plasma treatment, Raman Spectroscopy, 3D laser scanning profilometer, various scanning probe microscopy and spectroscopy such as atomic force microscopy, piezoelectric force microscopy, and tip enhanced Raman spectroscopy. The students had the opportunity to develop experimental protocols by following published literature. They also learned how to use relevant software and programming language to analyze the collected data. Both students have attended the Advanced Materials Characterization workshop, 2023 (AMC 2023) at UIUC and learned about state-of-the-art micro and nano characterization tools. The students learned about proper scientific methods of research and developed capabilities of conducting research on strain engineering at nanoscale. This project also provided mentoring opportunity for their graduate student mentor who is a 5th year PhD student in the Mechanical Science and Engineering Department, UIUC.

C. Dissemination of Results

Kareef Haque and Ezra Chiou presented their research poster at the Fall Engineering Research Fair in September 2023.

Project 3: Development of Autonomous Drone to Navigate Obstacles Using Depth Camera Technology

A. Goals and Accomplishments

Major Activities

- **ROS System Proficiency:** The students have gained competence in utilizing the ROS system on an Ubuntu platform. They have comprehended the underlying concepts and effectively implemented them by following examples from the official ROS Wiki website.
- **Camera Utilization:** Proficiency has been achieved in working with both the Realsense D435 and T265 cameras. The students have successfully acquired point cloud data from these cameras and applied basic processing algorithms sourced from the Realsense open projects.
- **Xavier Onboard Computer:** The students have acquired the necessary skills to utilize the Xavier onboard computer. They are now capable of compiling projects on arm-based computing platforms.
- **Simulation Software Familiarity:** The students have learned the installation procedures for Unreal Engine and Airsim for drone simulations. While scripts have not yet been tested in the software due to time constraints, testing is planned for the upcoming semester.
- **Basic ML Algorithm Implementation:** The students have learned and implemented basic machine learning algorithms on the Xavier onboard computer. While advanced ML algorithms remain unexplored, plans to delve into these algorithms in the upcoming semester are in place.
- **Drone Algorithm Implementation:** The students rigorously tested the implemented algorithms on the actual drone platform.
- **Advanced ML Algorithm Exploration:** The students explored more intricate ML algorithms to empower them to tackle complex challenges and further refine their understanding of ML techniques.
- **Algorithm Implementation in Simulation Software:** The students applied their knowledge by implementing algorithms not only on the real drone but also within simulation software.

Specific Objectives and Key Outcomes

The students have successfully grasped the usage of the ROS system, depth camera, and perception camera on the Xavier onboard computer. Their foundational understanding of simulation software and basic ML algorithms has been established. The students then initiated

algorithm implementation with the new drone. The hands-on testing provided valuable insights into the real-world applicability and performance of the algorithms.

The dual approach of algorithm implementation on real drone and simulation software enabled students to validate their algorithms under controlled conditions before transitioning to real-world testing.

By aligning these plans with the initial goals and objectives, the students elevated their proficiency and expertise in the autonomous drone project.

B. Opportunities for Training and Professional Development

1. Individualized Robot Training: Students were granted personalized robot training through one-on-one mentoring sessions. This approach enabled them to receive tailored guidance and hands-on experience, fostering a deep understanding of robot-related concepts and techniques.

2. Collaborative Discussion Meetings: Weekly discussion meetings were organized to facilitate open communication among students. This platform promoted the exchange of ideas, problem-solving, and knowledge sharing, contributing to a collaborative and enriching learning environment.

3. Hardware Provision: Hardware resources were made available to students for their robot implementation endeavors. By providing access to necessary tools and equipment, students were empowered to apply theoretical knowledge to practical scenarios, enhancing their technical skills.

These opportunities collectively enhanced the students' competence in robotics and nurtured their ability to work effectively both independently and within a team. The practical experiences gained through mentorship, peer interactions, and hands-on implementation are invaluable for their professional growth and development in the field of robotics.

Benefiting Students' Career Prospects: The project's outcomes also offered a practical benefit to the participating students. By engaging in this project, students gained hands-on experience in a cutting-edge technology area, enhancing their skill set and bolstering their future job applications in the robotics industry.

C. Dissemination of Results

Highlighting Autonomous Drone Implementation: The successful implementation of an autonomous drone holds inherent appeal within the robotics domain. The project's accomplishments were showcased within relevant communities, drawing attention to the innovative aspects of the autonomous drone and its potential implications for the field.

Project 4: Utilization of Audio and Sensing Data for Multi-Factor Authentication and Location-Based Proofs

A. Goals and Accomplishments

The goal of our project is to develop a practical video identification attack, where current video streaming services (e.g., YouTube) use Dynamic Adaptive Streaming over HTTP (MPEG-DASH) to optimize quality of experience (QoE) for their users given dynamic networking conditions. However, due to variable bit rate (VBR), each video has different file sizes, resulting in distinguishable traffic pattern over DASH. Current study ignores the actual user watching behavior (i.e., user may jump or seek during watch session) and assume they watch entire video to establish the video identification attack.

We established a framework to run video sessions with dynamic user behaviors. By collecting the data with tcpdump and logs from website, the results can be used to understand the impact of user behavior on video streaming flows. The framework includes (1) getting QoE information from website browser, (2) dumping every TCP packet information, and (3) running experiment from both servers and clients.

B. Opportunities for Training and Professional Development

The project provided the student to develop a tool to run experiments at scale. This is critical since the performance of deep learning model depends on the quality of the training dataset. Besides, there are many open problems do not have appropriate dataset. This project allows the student to get hands-on experience to collect and analyze the dataset and learn the overall framework of a research project using deep learning models.

C. Dissemination of Results

Nothing to Report

Project 5: Study of Robustness of Machine Learning Models to Semantic Perturbations

A. Goals and Accomplishments

The goal of this project was to examine the robustness of machine learning models regarding their inputs. The Achilles heel of neural networks, as well as associated AI frameworks, is in the difficulty they have with adapting to atypical inputs. Atypical in this sense refers to any significant deviation from those inputs which model was trained on. By computing the derivative range of a given input (in this case, a pixel) with respect to output of the model (or model confidence), we can define a range of possible derivatives for a range of possible pixel values, and from this generate a reliable saliency map for a potentially infinite set of images (“infinite” meaning the domain of real numbers between the upper and lower real bound). The methodology for this process involves a novel combination of dual numbers and interval arithmetic.

Major Activities

We developed an implementation of forward-mode automatic differentiation with interval arithmetic to track bounds on the derivative of the output of a neural network with respect to input pixels as they are propagated forward through a fully connected neural network. The custom dual number and interval arithmetic framework that we implemented gave us a software library to utilize for running our experiments. Furthermore, to emulate the variability that exists

in real-life images, we included epsilon ball abstractions of pixel ranges using our intervals to represent a degree of uncertainty in the pixel's value.

Specific Objectives

Our objective was to visualize the derivative bounds with respect to each pixel in an MNIST image in the form of a heat map. In the heatmap, the color of the pixel can be thought of as indicating the gradient magnitude at each pixel location. Hence darker hues indicate a lower gradient bound for a particular pixel, whereas lighter hues indicate a higher gradient bound.

Findings

What we found was that for images in the MNIST dataset, the derivative magnitudes of the pixels comprising the foreground of the image (the actual writing, or near the actual writing) tended to have higher derivative magnitudes than those comprising the background. In other words, changes in the value of the pixels in the foreground had a larger impact on the model's output. This observation is demonstrated in the heat map in Figure 12.

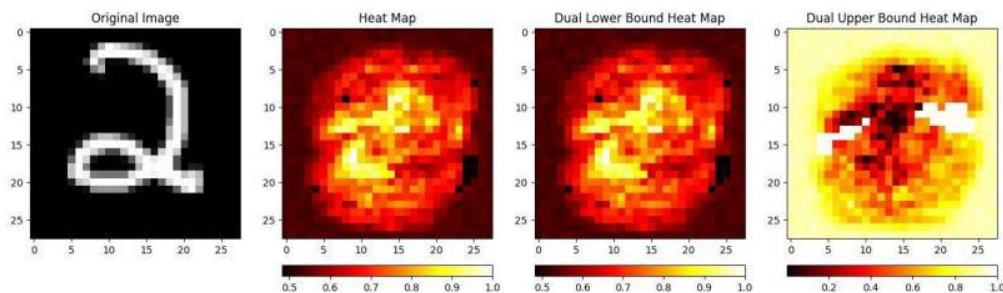


Figure 12. Heat map of a “2” MNIST image

Outcomes

The key outcome of our project is that the undergraduate student has learned the process of formulating a research question as well as how to experimentally validate a proposed research question.

B. Opportunities for Training and Professional Development

The research experience is intended to provide cadets with exposure to state-of-the-art research focusing on the robustness of machine learning algorithms. The experience is designed to teach cadets the skills in how to formulate and solve open-ended research problems.

C. Dissemination of Results

Software was developed for this project to compute provable bounds on gradients. The software is available in a GitHub repository.

Jonah Black presented his research poster at the Fall Engineering Research Fair in September 2023.

Project 6: Improving Trustworthiness of Machine Learning Compilers

A. Goals and Accomplishments

The main goal of the project was to develop techniques needed to build an effective accuracy-aware tensor program compiler. The compiler optimizes tensor programs (such as DNNs) for a target hardware platform using program transformations, including ones that can change the structure of the program and trade off output accuracy for performance. The compiler should automatically find sequence of transformations that give good performance, as what constitutes good choices can vary depending on the input program and target hardware platform. A key step towards this goal is to discover effective transformation techniques that improve the performance of tensor programs.

We examined existing works on individual techniques for tensor program transformations, to find ones that produce good optimization results on a wide range of tensor programs. We identified 1 technique that produces well-optimized programs out of 4 we inspected. This technique, called polarization pruning, reduces the size of tensors in the tensor program to trade off some output accuracy for performance. We found 2 key parameters that polarization pruning depends on and need to be selected manually and try different parameter values to understand how these parameters affect the behavior of polarization pruning. Lastly, we reimplemented this technique in a compiler framework and modified part of the framework to use it together with other program transformations.

B. Opportunities for Training and Professional Development

The graduate student developed supervisory and mentoring skills as he worked one-on-one with the undergraduate student for the summer. He trained the student about toolchains and systems during live coding sessions, and they discussed effective coding practices that help with debugging and producing high-quality code. The undergraduate student also read scholarly articles to build on their knowledge about machine learning compilers.

C. Dissemination of Results

Nothing to Report

Project 7: Cloud Infrastructure for IoT Security

A. Goals and Accomplishments

The major goals of the project were to 1) conduct performance testing of the system, 2) analyze the bottlenecks, and 3) write scripts to monitor the system and alert abnormal events.

Students were able to fully set up the development server for testing purposes, understand the system workflow of how it emulates hardware components, write design spec for performance testing, diagnostic the current circuit configurations, create testing scenarios, and write scripts to measure system performance for major functionalities (runtime latency,

memory and CPU utilization). We were able to fulfill the first goal of the project. Unfortunately, due to the time constraint and the complexity of the system, we were not able to report any major findings at the end of summer. In the fall, the goals were 1) create scripts to mimic realistic client-server traffic loads of our designed IoT system, 2) conduct performance testing against system scalability, and 3) analyze the bottlenecks and propose future improvements.

Previously, our research team was able to diagnose our system's bottlenecks and apply patches for optimization. On top of the optimized system, the student conducted further experiments for cumulative probabilities of compilation time regarding the previous bottlenecks for over 500 instances. We were able to fulfill the first goal of the project and part of the second and third goal. Some graphs were plotted according to the collected results and our research team will continue with the load testing as the next step.

B. Opportunities for Training and Professional Development

The project provided one-on-one training with the graduate student mentor to design research plans and brainstorm experiment ideas and to learn to collaborate with other researchers. The students also learned large scale software engineering development practice.

C. Dissemination of Results

Tomas Sagartz and Daniel Yu presented their research poster at the Fall Engineering Research Fair in September 2023. Daniel Yu presented an updated poster at the Spring Engineering Research Fair in February 2024.

Project 8: Security of Network Functions

A. Goals and Accomplishments

NFV (Network Function Virtualization) is commonly adopted as software components in modern networks, such as firewalls, load balancers, cache proxies, and intrusion detection/prevention systems. As the implementations of these NFVs become more complex, the plane for vulnerabilities and exploits increases accordingly. Since the NFVs are often implemented in general-purpose programming languages and without much standardization, they further complicate modeling of networks for reliability and verification analysis.

This project aimed to

1. Investigate the security of NFVs, including researching and developing the categorizations of NFV vulnerabilities and the limitations of the existing methods.
2. Survey the known vulnerabilities of NFVs based on our vulnerability taxonomy and see which vulnerabilities can affect the network-visible behavior (i.e., any packet forwarding behavior in the data plane that can be affected and changed by the vulnerability).
3. Survey the common practices for testing software NFVs and see what may be improved to catch issues early prior to deployment.

The student who worked on this project was able to achieve all the project goals mentioned above. A written report details most of the survey results and findings. To do so, we hold weekly one-on-one meetings to discuss any project related items, research skills, and to answer any questions the student may have. We also provided a list of publications, websites and online databases for NFV-related vulnerabilities and CVEs (Common Vulnerabilities and Exposures). After the first half of the summer program, the student compiled a list of CVEs and bugs, developed a taxonomy for NFV vulnerabilities, and later in the second half of the program, put together lists of testing methods for NFVs and how different testing methods were used and related to each known bug.

B. Opportunities for Training and Professional Development

The training and professional development opportunities this project provides include weekly one-on-one mentoring sessions, project discussions, code tracing/reviews, and individual study.

C. Dissemination of Results Nothing to Report.

Activities to Guarantee Long-term Sustainability of the Project

We plan to integrate new participants doing research in the areas of cyber and electronic security in the Illinois Scholars Undergraduate Research (ISUR) Program this 2024 – 2025 academic year. We are applying for financial grants from corporate foundations to provide additional funding for the new students. We also plan to submit grant proposals that would expand the topics of interest beyond cyber and electronic security and provide funding for new projects.

Future Plans Post-Award

We will continue our efforts to broaden participation in undergraduate research by engaging the research community in offering undergraduate research experiences that include mentoring of women and students from underrepresented groups in STEM. Mentoring relationships can be life-changing for these groups of students as they foster a sense of belonging, a belief in one's capabilities to produce desired outcomes, and develop a scholar identity.

We plan maintain partnerships with ROTC units, the Merrill Engineering Program, Women in Engineering Program, and key student organizations such as the National Society of Black Engineers and the Society of Hispanic Professional Engineers to promote undergraduate research opportunities and encourage students (undergraduates and graduates) to participate in research.

We continue to collaborate with faculty members and researchers across campus on projects that align with the mission and thrust areas of the Office of Naval Research and plan to submit proposals to relevant funding opportunities.

Products Resulting from the Award - Undergraduate Student Posters

Investigation of Small Array and Reconfigurable Antenna

Joshua Carpenter, Adam Spitzner, Patrick Yim, Kara Maurer, Guilherme Jurgensen, Professor Jennifer Bernhard

Department of Electrical and Computer Engineering, Grainger College of Engineering, University of Illinois at Urbana-Champaign

INTRODUCTION

Antennas are basic electromagnetic devices used for wireless communication of data through the transmission and reception of radio signals. These devices operate on the principle of converting incoming electromagnetic waves into an electrical signal and vice versa when transmitting a signal. Antennas can come in various geometries depending on the application, such as the microstrip patch antenna in a cell phone or complex spiral antenna used for GPS spoofing.

Microstrip Patch Antenna:

Patch antennas are narrowband, wide-beam antennas that consist of rectangular metal patches bonded to dielectric substrates.



Microstrip patch antenna with coaxial port

Reconfigurable Loop Antenna:

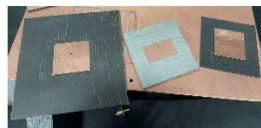
By changing the geometry of an antenna, the radiation pattern can be drastically changed. For example, a hemispherical shaped combined with inductors allows the radiation pattern to be "pointed" in specific directions.



Example of a hemispherical reconfigurable antenna

Objective

The objective of this study is to investigate the behavior of arrayed and reconfigurable antenna through the simulation, fabrication, and performance testing of patch and loop antenna designs.

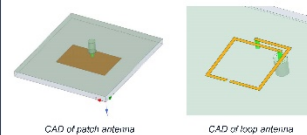


Fabricated Patch Antennas: Rogers Duroid 5670 (left), Rogers Duroid 6006 (middle), Rogers Duroid 5880 (right)

METHOD

Simulation

The patch and loop antennas are designed using Ansys High-Frequency Signal Simulator (HFSS). The simulations provide critical test results that assist in determining antenna geometries and materials.



CAD of patch antenna

CAD of loop antenna

Fabrication

Once the optimal schematics are generated, the antenna designs will be manufactured using the ECE Antenna Lab's CNC milling machine. Presently, only the patch antennas are fabricated.



Milling machine etching out copper-plated antenna on substrate

Resulting patch antenna with milled substrate

Testing

The fabricated antennas are tested using the ECE Antenna Lab's anechoic chamber. The antenna's performance is analyzed by measuring the radiation pattern or antenna gain using a rotating table, and the S_{11} plot of operational frequency (target of 3 GHz).



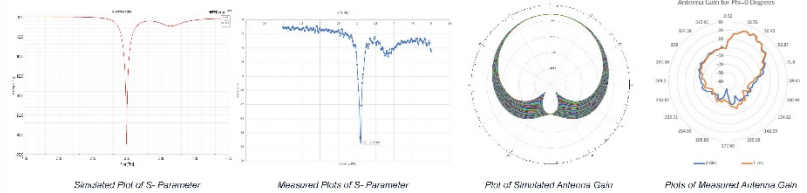
Experimental setup in anechoic chamber

RESULTS

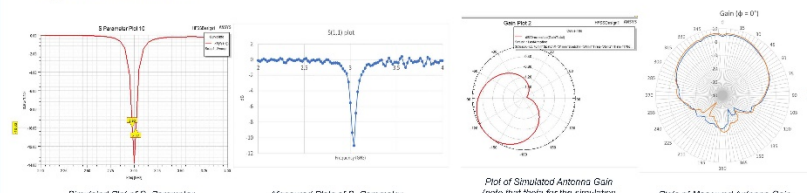
Preliminary Simulation

The simulated and measured radiation pattern and S_{11} parameter of patch antennas are observed through the various plots presented with three different substrates.

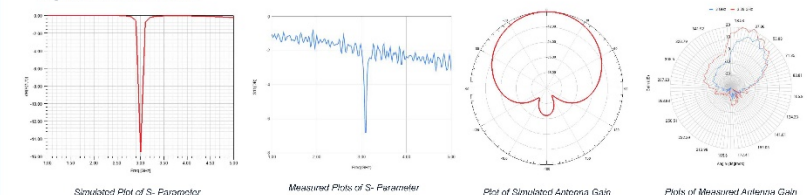
Rogers Duroid 6006 Substrate:



Rogers Duroid 5670 Substrate:



Rogers Duroid 5880 Substrate:



CONCLUSIONS

Feasibility

Minimal variation between the measured experimental results and the ideal simulated antenna characteristics were observed. The plots of the S_{11} parameter indicate that the antennas operate very close to the target frequency of 3 GHz. Additionally, while there is some discrepancy between the ideal and measured radiation pattern, this can be attributed to manufacturing errors such as imprecise milling or faults in the testing setup. Additionally, it was noted that the Rogers Duroid 5670 substrate yielded the most accurate performance. The results indicate that the individual antenna elements perform as intended and have the potential to be implemented into antenna arrays.

Future Work

Future work will focus on manufacturing an array of patch antennas and observing its effectiveness. If successful, the objective will then shift to manufacturing a loop antenna and testing its capabilities to ascertain the potential for producing a reconfigurable loop-arrayed antenna.

REFERENCES

- [1] Alakija, C., and S.P. Stapleton. "A Mobile Base Station Phased Array Antenna." 1992 IEEE International Conference on Selected Topics in Wireless Communications. <https://doi.org/10.1109/ICWC.1992.209727>.
- [2] Huff, G. and Bernhard, J., 2006. Integration of Packaged RF MEMS Switches With Radiation Pattern Reconfigurable Square Spiral Microstrip Antennas. IEEE Transactions on Antennas and Propagation, 54(2), pp.464-469.
- [3] Huff, G., Feng, J., Zhang, S. and Bernhard, J., 2009. A novel radiation pattern and frequency reconfigurable single turn square spiral microstrip antenna. IEEE Microwave and Components Letters, 19(2), pp.57-59.

ACKNOWLEDGEMENTS



ILLINOIS
Electrical & Computer Engineering
Department of Electrical and Computer Engineering

ALERT
Program in Electronic and Cyber Security

ILLINOIS

Microstrip Patch Antennas

Max Damewood, Christelle Seri, Natasha Sherlock, Supervised by Professor Jennifer Bernhard
Department of Electrical and Computer Engineering, Grainger College of Engineering, University of Illinois at Urbana-Champaign



Abstract

For our team's research project, our goal was to create a functioning patch antenna that resonated at 3 GHz. To accomplish this, we first used a computer software program called ANSYS to create a 3D model of the patch antenna. We then used the software's built-in tools to analyze our model and determine its radiation patterns and resonance frequency. Once we tweaked the model to match our given parameters (the dielectric material, the size of the patch, and the resonance) we then moved on to machining and fabricating the physical patch. This process was simple as we only needed to attach a properly sized copper square to a dielectric so that it matches our model, and then drill a hole in order to attach the coaxial port. Our results matched expectations as the experimental data resonated at the same frequency that was modeled, however it did have a lower Q value and smaller peak, showing that it did not resonate as intensely. In conclusion, the model was accurate, and our physical antenna would showcase all the predicted characteristics with a more accurate machining process. When attaching the plates, we used a milling machine to remove the extra copper from the patch. The milling machine was unable to obtain the accuracy of the model, which was compounded in our measured radiation patterns. In the future, I would use a different milling machine or a more precise method of cutting the patch as this is a pivotal part of designing the antenna.

Introduction

We conducted this experiment to demonstrate the simplicity of basic antennas and because of how it demonstrates the relation between dimension and desired frequency in a very easy to understand format. By editing the width of the patch, you are changing the wavelength of the frequency that comes off it in a linear manner and the antenna will emit radiation, or radio waves in all directions broadside to the patch.

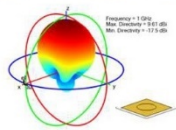


Figure 1: Diagram of the radiation pattern coming from the microstrip patch antenna

Setup

To start the modeling of our patch we had the initial conditions of using a specific dielectric to hold the charge (duroid 5870) making the patch with copper, and having it resonate at 3 GHz.

After creating the HFSS diagram that meets this criteria we then used a milling machine to cut out our path from the dielectric, drilled a hole for the coaxial cable and soldered a coaxial feed on.

Then to collect our the S11 plots for our fabricated patch we ran a current through our coaxial feed which is depicted below and is our final result.



Figure 2: Image showcasing 3 patch antennas with varying dielectrics

Theory

By running an alternating current through the dielectric and copper plate we create a positive and negative electric field on the ends of the system. The radiation the moves outside out the system focusing from the copper plate.

For a rectangular patch, the length can be estimated using

$$\begin{aligned} \text{Patch dimensions} & \quad \text{Ground dimensions} \\ W &= \frac{c}{2f\sqrt{\epsilon_r}} \\ L &= \frac{c}{2f\sqrt{\epsilon_r}} - 2\Delta L \\ L_{\text{eff}} &= L + \Delta L \\ \Delta L &= 0.49 \lambda_d \left(1 - \frac{0.116}{\epsilon_r} \right) \end{aligned}$$

This formula includes a first order correction for the edge extension due to the fringing fields, with:

- L = resonant length
- λ_d = wavelength in PC board
- λ_0 = wavelength in free space
- ϵ_r = dielectric constant of the PC board material

Results

Analytical

The analytical portion of the experiment was all performed in the design program and used electromagnetic theory. The end results of this process generated our patch design (figure 2) and its S11 plot, predicting that the design has the desired output frequency (figure 3)

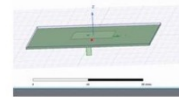


Figure 3: HFSS 3D model of square patch

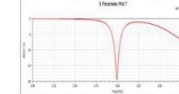


Figure 4: S11 plot depicting peak at 3GHz

Experimental

Using the Patch from figure (1) we attached it to a coaxial cable to get our baseline measurement to ensure our fabric

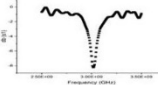


Figure 5: S11 plot based on our experimental data

Upon seeing that figure (5) confirms our results from figure (4) we will be able to determine if our antenna is accurate and we can take more precise measurement with it as described in the setup section.

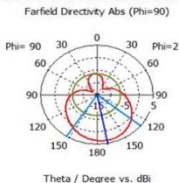


Figure 6: 2D measured radiation pattern of patch antenna

Next Steps

- Mapping out gain of the antenna and figuring out how to improve its natural frequency.
- Creating an array in order to change how the signal is projected

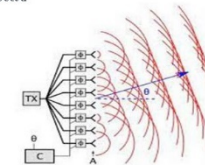


Figure 7: Diagram depicting a phased array

CONCLUSIONS

In conclusion from our preliminary analysis our fabricated model matches well with our analytical S11 graph. One note is that the S11 plot which is the measured reflection coefficient or power reflected does not dip below the benchmark value of -10dB. For these types of antennas having a peak at less than -10dB shows that most of the power is being reflected, and producing a strong signal which is what we want. Some potential reasons for this are that the milling machine scraped off some of the dielectric and scratched part of the copper patch.

References

- Analogic Tips. "The Microstrip Antenna - Part 2: Implementation." Analogic Tips, n.d.
- "Antenna Radiation Patterns - MATLAB & Simulink - MathWorks." MathWorks. The MathWorks, Inc., n.d. Web. 10 Apr. 2023.
- Brown, Arik D. (2021). Active Electronically Scanned Arrays: Fundamentals and Applications. Wiley-IEEE Press.

ACKNOWLEDGMENTS

Professor Bernhard

Graduate students Kara Maurer and Guillelmo Jurgensen

Office of Naval Research, ISUR Program



Stretchable Wrinkled WSe₂ for Tunable Single Photon Emitters

Mary G. Pelzer^{1,†}, Henry Feldhaus^{1,†}, Jin Myung Kim², Yeageun Lee¹, SungWoo Nam^{1,3,*}

¹Department of Mechanical Science Engineering, ²Department of Materials Science Engineering, University of Illinois at Urbana-Champaign, ³Department of Mechanical and Aerospace Engineering, University of California Irvine. [†]These authors contributed equally.

INTRODUCTION

Single Photon Emitters (SPEs)

The development of SPEs is critical to quantum communication and information processing. Atomically-thin transition metal dichalcogenides (TMDs) are a promising method for light extraction, but it is difficult to modulate emission sites and energy.

Strain Engineering

Strain engineering allows precise control of band structure and photon energy of TMDs. Highly stretchable substrates allow for mechanically controlled local strains. Here, we report strain-induced exciton energy modulation and single photon emission of biaxially wrinkled monolayer tungsten diselenide (WSe₂).

Wrinkle Structures

Different biaxial wrinkle structures are functions of skin layer stiffness, substrate pre-strain, and encapsulation layer. Raman, photoluminescence (PL), and absorption imaging are used to demonstrate modulation of PL energy and bandwidth with respect to varying wrinkle topographies.

OBJECTIVES

Tunable TMDs

- Precise control of atomically thin TMD electronic structures (band gap and photon energy) via mechanical strain engineering
- Exciton energy modulation via biaxial strain

Exciton Lifetime

- Stabilization of exciton presence via temperature manipulation on a various wrinkle structures
- Benchmark expected exciton lifetime in biaxially wrinkled TMDs

Degree of Exciton Anti-Bunching

- Identification of wrinkle topography and its effects on electron antibunching

ANALYSIS TECHNIQUES

Techniques

1. Optical Raman imaging
2. Photoluminescence (PL) spectroscopy
3. Photo-induced force microscopy (PIFM)
4. Hanbury Brown Twist (HBT) interferometry
5. Atomic Force Microscopy (AFM)

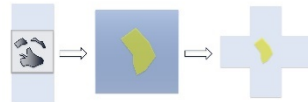
These methods show critical parameters of SPEs:

- Modulation of PL energy and bandwidth with respect to wrinkle topography
- Exciton lifetime
- Degree of exciton antibunching

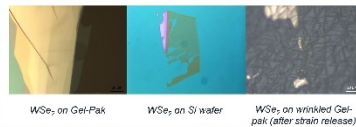
METHOD

Sample Preparation

1. Exfoliate WSe₂ crystal onto Gel-pak substrate using Scotch tape
2. Identify monolayer >10 μm^2
3. Transfer monolayer to peracetic acid (PAA) coated silicon (Si) wafer
4. Pre-strain and plasma clean Gel-Pak substrate
5. Transfer monolayer to pre-strained Gel-pak
 - a. biaxial vs. uniaxial strain
 - b. 10-30% strain
6. Release strain on Gel-pak to create wrinkle structure



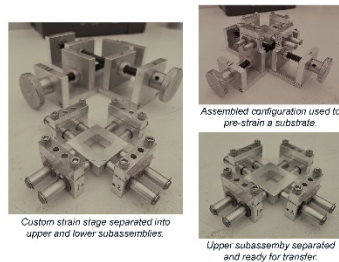
In order: exfoliated crystal on Gel-Pak, monolayer on PAA coated Si wafer, monolayer on pre-strained PDMS (to be released before analysis).



APPARATUS

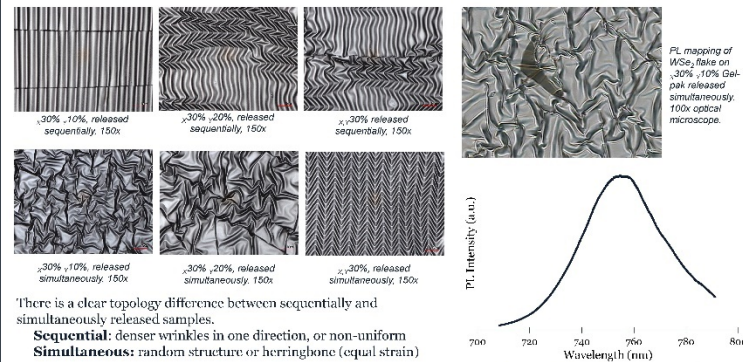
A custom bi-axial strain stage is used to pre-strain and release the Gel-pak substrate. The stage was designed and built to meet various size constraints imposed by other equipment.

The stage splits into two subassemblies. A large lower stage is used to precisely set pre-strain values. An easily replicable, removable upper stage holds a substrate and can maintain strain values anywhere from 0-250%.



ANALYSIS

Laser scanning microscopy yields the following images of wrinkled WSe₂ on a pre-strained Gel-pak substrate. All samples are pre-strained perpendicularly. Variation in the method to release strain produces different results. Sequential release means strain is completely released in one direction before releasing the other direction.



There is a clear topology difference between sequentially and simultaneously released samples.

Sequential: denser wrinkles in one direction, or non-uniform
Simultaneous: random structure or herringbone (equal strain)

NOTE: In all images, x-direction is horizontal, and y-direction is vertical.

RESULTS

Data for this experiment was obtained too recently to present accurate, well-established results. Accurate, representative results will be available within the next two weeks; further, these results will allow for complete conclusions to be made.

CONCLUSIONS

Final conclusions for this experiment are forthcoming. Pending a more in-depth analysis of the results, conclusions will be made about the efficacy of mechanical strain to tune SPEs.

ACKNOWLEDGEMENTS



ILLINOIS

Ultrasensitive Temperature-sensing Intelligent Surfaces for Smart Home

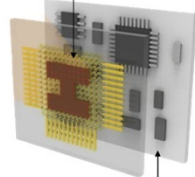
Teague Mitchell, Ezekiel Y. Hsieh, Yixiao Liu, SungWoo Nam, Elizabeth Hsiao-Weckslar

Department of Mechanical Science and Engineering, Grainger College of Engineering, University of Illinois at Urbana-Champaign

INTRODUCTION

With the rise in popularity of “smart homes,” a number of technological innovations are sought to improve them. One thing necessary for many smart homes is a sensor for occupancy and/or motion. Generally, a thermal sensor would be used to accomplish such a task. Existing thermal sensing technologies mostly consist of passive infrared sensors and semiconductor temperature sensors. However, there is a demand for temperature sensors that are more sensitive as well as sensors that are more discreet. This project’s proposed solution is a sensor made from a pectin-graphene composite.

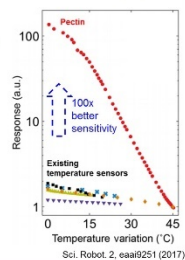
Thermal image sensor



Integrated electronics

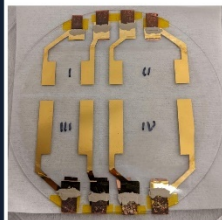
AIM

The primary purpose of this project is to test the capability of a temperature sensor using a pectin-graphene composite. Pectin is a material found in plant cell walls that is exceptionally sensitive to changes in temperature, while graphene is a nanomaterial sheet of carbon atoms. This project hopes to show that combining these two materials can produce a highly effective temperature sensor capable of detecting humans through their body heat.



METHOD

To measure the efficacy of a pectin-based temperature, the first step is to create a sample we can use to collect to data with. For this, we use a gold-pectin-graphene composite and arrange it into a 2x2 lateral conductivity array. We then run electrical currents through this, and can detect changes in temperature when the resistance of the pectin changes. Each pectin sample in the array has different length/width parameters so the effect on its sensing capabilities could be measured. Objects or people can be placed in front of the pectin or removed while an AC current is run through it to detect the changes in temperature.



Au/Pectin/Graphene 2x2 Lateral Conductivity Array

Physical set up for measurement.

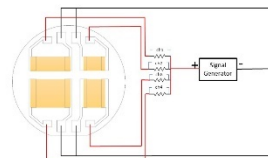
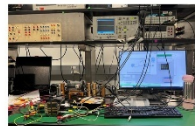
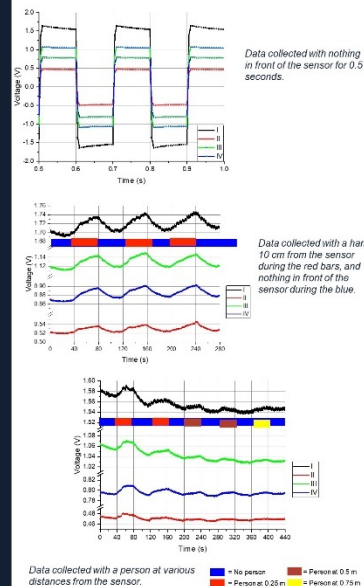


Diagram of set up for measurement

RESULTS

The outcome of these experiments did show the capability of the pectin composite to function as a temperature sensor. A result noticed early on is that the resistance of the pectin degrades over time as a current is run through it due to the build of ions. This can be counteracted by using an AC current, which we do here. We show the results of three tests below, all measured with a 200 hz frequency and using an input signal of 10 Vpp square wave with a 5 hz frequency. Each of the four pixels show sensitivity to incident IR when a heat source is placed in front of the sensor, with greater sensitivity when the heat source is closer. Curiously, pixel one shows greater conductivity than pixel three despite smaller electron width, but the consistency of the results otherwise mean this is likely due to the test conditions. For example, the sample may have been mixed incorrectly or broken.



CONCLUSIONS

The Pectin-graphene composite does show potential for use as a temperature sensor after these tests. Further testing is required to find the ideal construction and methodology of the composite, as well as the limits of the composite, but it has been demonstrated with these tests that the composite is capable of detecting humans at a small distance.

ACKNOWLEDGEMENTS



Human Dynamics and Controls Lab: Pectin-based Temperature Sensors

Grace Zhen, Justin Macatangay, Ashley Saju

Department of Mechanical Science and Engineering, College of Engineering, University of Illinois at Urbana-Champaign

INTRODUCTION

Pectin (Polygalacturonic Acid), is a complex polysaccharide that derives from the cell wall of plants. When individual pectin chains are cross-linked together with ions such as Calcium Chloride, they form pectin networks, where Calcium ions bond with ionized carboxyl groups to form "egg boxes" where the cations are stored.

After dehydrating the pectin networks, the created pectin films display immense temperature response. Increasing temperature on these networks increases the ionic conduction, creating a current or effectively lowering its resistance which can be measured by running an alternating current through the films.

The following three sub projects seek to improve the methods in which pectin films are produced, created, and analyzed.

Altered Vacuum Chamber & Heated Blanket Stand

Goals

- Create a 3D-printed mechanism that allows the vacuum chamber to dry 3 petri dishes at one time on the turntable.
- Power turn tables inside vacuum without use of a battery

Turntable Power

- Cut the wire to charge the turntable in half and connect them to male wires with heat shrink
- Drill two holes in the vacuum
- Put a female-to-female wire in between the hole and glue
- Connect the male wires to the female-to-female wire and power on

Heated Blanket Stand

- Modified existing heated blanket stand to turn on the Z-axis by disassembling the existing stand and putting a larger diameter PVC pipe over the legs
- Clamped the heating blanket on the "arms" of the stand with hair clips
- Clamped an insulating material on the other side of the heated blanket

Future Work

- Create a heating & cooling plate for temperature cycling



Altered Vacuum Chamber assembled



Heated blanket on the stand (left)

Pectin Film Fabrication

Goal

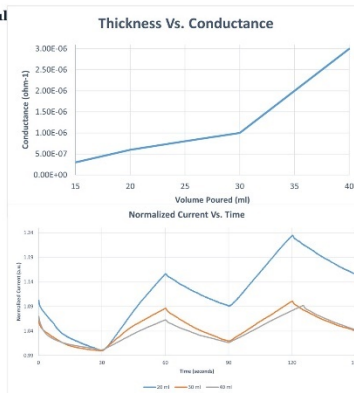
- Investigate ways to modify the fabrication process to improve pectin films' conductance and temperature response

Method



- After CaCl_2 is mixed with pectin, a jellifying period is required for the Ca^{2+} ions to cross-link and form pectin networks.
- Pouring this solution into petri dishes, and drying in a vacuum chamber finalizes production of pectin films with the removal of water.
- Adjusting the volume of solution leads to a change in the thickness of the pectin film once dried
- Measuring different values of thickness, the effect on conduction and temperature can be determined

Result



Future Work

- Continue analysis on how thickness effects the temperature response of pectin
- Investigate the effect of different esterification percentage on temperature response

Sensor Array Testing Controller

Goal

- Change in current of each cell without tester changing location of voltmeter
- Use LabVIEW as the interface for changing which cell is being measured and for data collection

Circuit Specifications

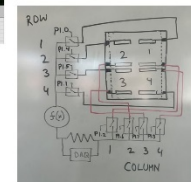
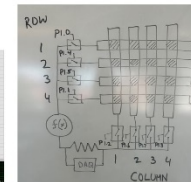
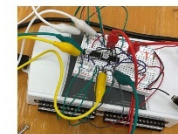
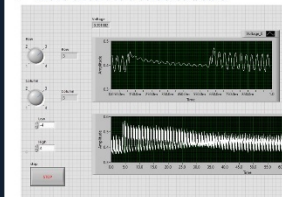
- ADG444 analog switches controlled by digital output from LabVIEW DAQ device (NI-USB 6218) to control current through each cell
- Signal generator (AC) powers sensors, DC from DAQ powers analog switches
- Digital voltmeter from DAQ placed across 22 kOhm resistor to measure changes in ionic conductivity

LabVIEW Program

- Select row and column in LabVIEW for electrically isolated cell sensor array
- Select cell number for both knobs when connected to sensor without electrically isolated cells
- Input lowest and highest voltage analog switch will experience relative to analog ground on DAQ to tune analog chip by DAQ outputting a constant voltage to power analog switch chip
- Outputs file with time, voltage readings, and row and column selection

Future Work

- Move circuit to a soldered board



ACKNOWLEDGEMENTS

These projects were created and funded through the 2023 Accelerated Learning and Engineering Research Training (ALERT) program sponsored by the Office of Naval Research.

I ILLINOIS

Measurement of Flexoelectric Effect in 2D Materials to Engineer Electrical Properties

Kareef Haque, Ezra Chiou, Shahriar Nahid, SungWoo Nam

Department of Materials Science and Engineering and Materials Research Laboratory, Grainger College of Engineering, University of Illinois at Urbana-Champaign

INTRODUCTION

- The **flexoelectric effect**, seen universally in every material, generates electric voltage under mechanical **strain gradients**.
- Previously, the flexoelectric effect was not seen as viable due to high strain gradients being needed and the effect not being prevalent over the piezoelectric effect.
- With **ferroelectric materials** like $\alpha\text{-In}_2\text{Se}_3$, where the effect is more prevalent, and with the ability of **2D materials** to deform under extreme strain gradients, the flexoelectric effect can be observed more pervasively. Because of this, **2D $\alpha\text{-In}_2\text{Se}_3$** is a prime candidate for study.

OBJECTIVES

The primary objective of this research project is to investigate and characterize the flexoelectric effect in ferroelectric materials, with a specific focus on demonstrating flexoelectricity as a universal mechanism of actuation. This research aims to provide valuable insights into the potential of flexoelectricity by breaking the project down into specific objectives.

- Measuring Flexoelectric Coefficient in 2D $\alpha\text{-In}_2\text{Se}_3$:** By accurately determining the **flexoelectric coefficient**, we can gain insights into the material's flexoelectric performance.

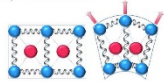


Fig. 4: Flexoelectric effect causing the polarization of a material due to mechanical deformation

- Investigating Strain Gradient-Induced Polarization:** With **different strain gradients**, the flexoelectric properties, such as polarization, can change. Studying different strain gradients can help gain insights into this.
- Comparing Flexoelectricity with Piezoelectric Materials:** By evaluating the **performance of the flexoelectricity relative to established piezoelectric materials**, we can determine its suitability for various actuation applications.

METHODS

Key Methods:

- Developed method for **controlled strain gradients** in 2D $\alpha\text{-In}_2\text{Se}_3$.
- Exfoliated $\alpha\text{-In}_2\text{Se}_3$ on SiO_2/Si substrate.
- Prepared pre-stretched PDMS with SiO_2 skin layers created by plasma treatment and 40 nm gold coating deposited by E-Beam Evaporator
- Transferred $\alpha\text{-In}_2\text{Se}_3$ onto PDMS** and unstretched the substrate to create controlled wrinkles and strain gradients in the sample

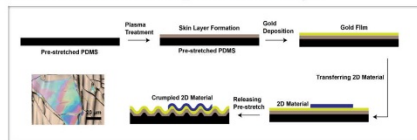


Fig. 2: Creating a strain gradient in 2D $\alpha\text{-In}_2\text{Se}_3$ using substrate-induced wrinkle formation

RESULTS

- Conducted **Raman spectroscopy** on both flat and crumpled $\alpha\text{-In}_2\text{Se}_3$ to investigate strain effects on vibrational modes
- Observed **E^2 , A^1_g , and $E^2A^2_g$ modes** in the flat sample (Fig. 3a) and similar modes in the wrinkled sample (Fig. 3b)
- A line scan was performed on the sample illustrated in Fig. 3c and the resulting Raman spectra was plotted as a position function (Fig. 3d)
- After performing a line scan, **obvious shift in Raman peaks** was anticipated, which would show that the crystal lattice structure of the 2D $\alpha\text{-In}_2\text{Se}_3$ was deformed. No shift in Raman peaks was found.
- Plotted as a function of position, the colormaps would show a clear trend in shifts along the path of the wrinkled sample.
- This would be helpful in determining the strain effect on the sample.
- Due to the inefficiency of **direct exfoliation** on the substrate, no thinner flakes were found, and a thick flake was measured.
- A hypothesis for the outcome would be because the thick flake had a **high elastic modulus**. This would prevent it from forming conformal wrinkles.

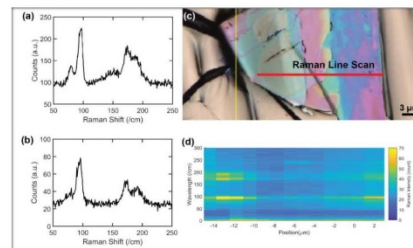


Fig. 3: Raman Spectroscopy on (a) flat $\alpha\text{-In}_2\text{Se}_3$ exfoliated on SiO_2/Si and (b) crumpled $\alpha\text{-In}_2\text{Se}_3$ on wrinkled gold substrate. (c) Optical image of $\alpha\text{-In}_2\text{Se}_3$ on wrinkled substrate. (d) Raman Spectroscopy performed on the marked region of (c).

- For a more conclusive result, a **thinner flake** would be needed. This would have a **lower elastic modulus** that would allow it to deform along with the induced strain gradient, which would allow us to perform PFM (Piezo Force Microscopy) to determine the flexoelectric properties.
- An ideal sample would be over **10 microns** in length and width, with a height of a few layers, such as in Fig. 4

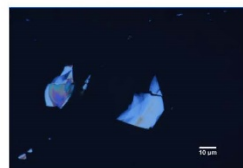


Fig. 4: Few-layer $\alpha\text{-In}_2\text{Se}_3$

FUTURE WORK

- Current dry transfer methods such as direct exfoliation face inefficiencies when transferring $\alpha\text{-In}_2\text{Se}_3$ onto a gold-deposited PDMS substrate, necessitating the introduction of a **more precise transfer station**.
- With direct exfoliation, only thick flakes are being deposited onto the substrate.
- For proper measurement of flexoelectric properties, **thinner flakes** are needed.
- To address this challenge, a **novel probe arm design** (depicted in Fig. 5) is being developed to enhance the precision of material transfers, ensuring the accurate deposition of $\alpha\text{-In}_2\text{Se}_3$ onto the substrate.
- This would allow more material to be deposited onto the substrate, increasing the chance of thin flakes to appear.
- The proposed probe arm will be integrated with a **micro-positioner**, enabling meticulous adjustments and movements of samples. This combination aims to streamline and optimize the transfer process.
- By implementing this **probe arm and micro-positioner setup**, we anticipate achieving more reliable and controlled $\alpha\text{-In}_2\text{Se}_3$ transfers onto the gold-coated PDMS substrate, enhancing the overall effectiveness of experiments.

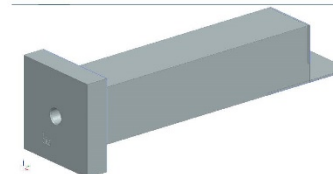


Fig. 5: Current design for transfer station probe arm

ACKNOWLEDGEMENTS



We would like to thank our Graduate Research Mentor, Shahriar Nahid, and our PI, SungWoo Nam, for providing guidance, the Office of Naval Research for providing funding, the Materials Research Laboratory for providing the instruments necessary to conduct our research, and the Office of Undergraduate Research for organizing the ALERT program.

ILLINOIS

Diamond use in Next Generation Power Electronics

Aleksai Herrera, Zhuoran Han, Can Bayram

Department of Electrical and Computer Engineering, College of Engineering, University of Illinois at Urbana-Champaign

INTRODUCTION

The main goal of power electronics is to dissipate the minimum amount of energy possible [1]. Although silicon is most commercially used, other wide band gap materials such as GaN and diamond have properties that could lead to improvements in device size and thermal management. Such properties directly correlate to a materials Baliga's figure of merit, the ratio of ON losses to OFF power. (See Figure 1).

Property	Symbol	Si	4H-SiC	GaN	β -Ga ₂ O ₃	Diamond
Bandgap	E_g (eV)	1.1	3.23	3.45	4.5	5.45
Sat. drift velocity	v_s (10 ⁷ cm/s)	1.0	2.0	2.2	—	1.1
Electron mobility	μ_n [cm ² /(V s)]	1500	1000	1250	300	1000
Hole mobility	μ_p [cm ² /(V s)]	480	100	200	—	2000
Breakdown field	E_{br} (MV/cm)	0.3	3	2	8	10
Dielectric constant	ϵ_r	11.8	9.8	9	10	5.5
Thermal conduct	λ [W/(cm K)]	1.5	5	1.5	0.11	22
BFM (absolute)	(MW/cm ²)	42	2×10^4	8×10^3	1.4×10^5	9.7×10^5
BFM (relative)	(Si = 1)	1	550	190	3200	23000

Figure 1: Properties of Semiconductor Materials [1]

The observed ratio has still not reached the theoretical, meaning we need to investigate into what obstacles are preventing this and how they can be resolved.

AIM

Lowering ON Resistance and Observing Properties

Diamond's relative BFM is still much lower than its absolute due to deep dopant energetic levels stemming from relatively low dielectric constant and high voltage operation of devices with long drift layer causing higher ON resistances. These higher ON resistances can be lowered through unique device structure, and high temperature operation[1]. We observe a device's power efficiency by observing ideality factor and rectification ratio. This can be done through obtaining an IV-curve of our device in forward and reverse bias and taking the ratio of forward over reverse current at a certain voltage and using the diode equation to calculate ideality factor.

METHOD

Power Probe Station

This instrument allows us to measure the IV-Characteristic of our devices, which will then be used to calculate important properties of the device such as breakdown voltage, forward current density, ideality factor, and rectification ratio. The device we will be measuring is a diamond lateral Schottky barrier diode (SBD).

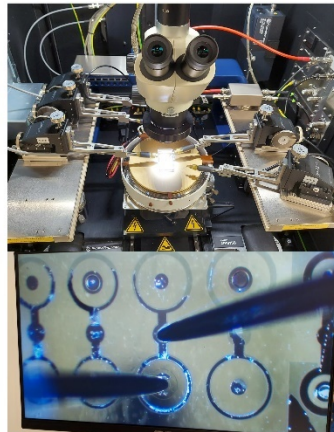


Figure 2: Probe Station Set Up

Procedure

- Prepare sample by placing it in 3M Fluorinert fluid to prevent electrical arcing
- Turn on the vacuum and place the sample in a container on the chuck, align the probes to contact the contacts of the device
- In order to make sure proper contact has been achieved, a forward test is performed
- When performing measurements in the reverse bias, certain settings are recommended to prevent damaging the device. A limit of 100 μ A before stopping measurements, steps of 5V, and a wait time of 1 second between steps
- Once measurements are complete the data can be exported as a .csv file

RESULTS

Analysis of Results

The IV-curves of the SBD in forward and reverse bias operation demonstrate the relation between the voltage applied and current through the device.

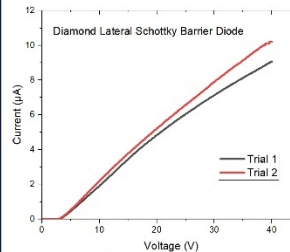


Figure 3: Forward Bias Operation

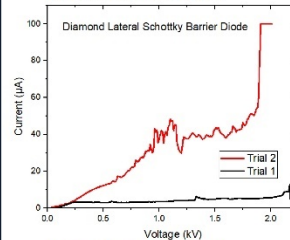


Figure 4: Reverse Bias Operation

Using the known diameter (80 μ m), we can calculate a max forward current density of 1.8mA/mm² at 40V. A rectification ratio of magnitude 10⁶ was calculated. An ideality factor of 12.75 was measured at 5V. Finally, the breakdown voltage was measured to be 2170V on trial 1 and then 2010V before reaching 100 μ A.

CONCLUSIONS

Our results show a breakdown voltage much higher than commercial silicon devices, however the high ideality factor implies the device deviates considerably from ideal diode behavior meaning further improvements need to be made to increase power efficiency. Characterization methods such as XPS can be used measure a sample's composition and surface electronic properties which is especially useful as it is non-destructive [2]. Understanding these properties can lead to more efficient power devices.

References

- [1] S. Koizumi, H. Umezawa, J. Pernot, and M. Suzuki, *Power Electronics Device Applications of diamond semiconductors*. Duxford, United Kingdom: Woodhead Publishing, an imprint of Elsevier, 2018.
- [2] G. Greezyski and I. Hultman, "Publisher's note: 'A step-by- step guide to perform X-ray photoelectron spectroscopy' [J. Appl. phys. 132, 011101 (2022)]," *Journal of Applied Physics*, vol. 132, no. 12, p. 129901, 2022.

ACKNOWLEDGEMENTS



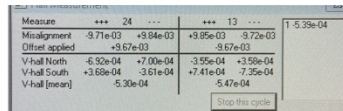
Next Generation Power Semiconductors: Diamond

Victoria Garcia, Zhuoran Han, and Can Bayram

Email: vgarcia9@illinois.edu and cbayram@illinois.edu Group website: icorlab.ece.illinois.edu

INTRODUCTION

Diamond is a new semiconductor, with great potential to improve power electronics. Many tool processes demonstrate sample transformation, analysis, along with how to prepare and test for the perfect diamond semiconductor utilization.



Measure	24	13	1.5.35e-04
Misalignment	-9.71e-03	+9.84e-03	+9.95e-03
Offset applied	+9.67e-03	-9.67e-03	-9.67e-03
V-hall North	-6.92e-04	+7.00e-04	+3.59e-04
V-hall South	+3.68e-04	-3.61e-04	+7.41e-04
V-hall (mean)	-5.30e-04	-5.47e-04	-5.47e-04

Figure 1: Hall Mobility Measurement initial data from software.

BACKGROUND

- In a \$200 billion semiconductor industry, over 50% of electricity in the world is made up by power devices
- Diamonds proven to be supremely superior to other power electronics' semiconductors
- Resistance lowered by 3 orders, breakdown voltage is 500 times larger - allowing for smaller devices, and 3 times larger electron drift - which increases frequency

Research Question

- How can the ALD process be successfully vetted prior to diamond experimental use?

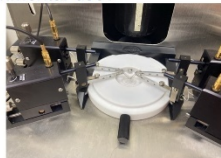


Figure 2: Hall Mobility Measurement Mechanism for which contacts are touched to each corner contact of a sample.

DIAMOND VETTING PROCESS (FIRST USED WITH SILICON)

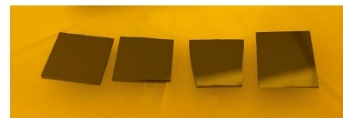
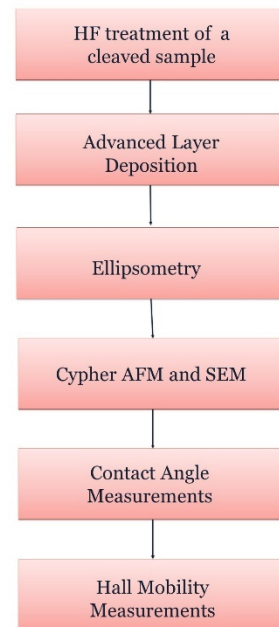


Figure 3: Four cleaved samples of silicon oxide to be used in the diamond analysis vetting process.

METHODS AND RESULTS

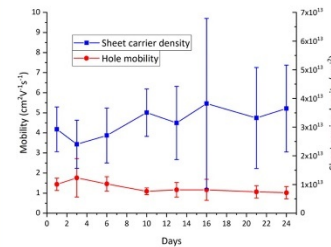


Figure 4: This graph illustrates the relationship between time, mobility, and sheet carrier density as interpreted through the hall measurements on a polycrystalline diamond.

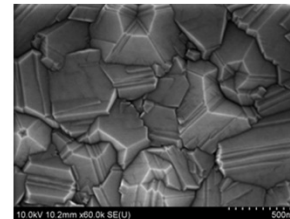


Figure 5: Polycrystalline diamond sample image taken using the SEM Imaging software with the assistance of Ms. Jessica Spear.

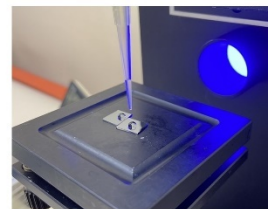


Figure 6: Contact angle measurement with water droplets placed on two samples to measure hydrogenation.

CONCLUSIONS

- Vetting process is best used with silicon oxide as a less expensive and structurally similar sample.
- ALD, followed by analysis with Ellipsometer, Cypher AFM, and SEM would be effective examination of the sample in order to confirm success in terms of energy conductance and use, which can then be replicated with diamond

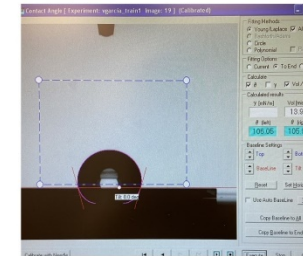


Figure 7: Contact Angle Measurement software in use with angles being measured.

ACKNOWLEDGEMENTS

ACKNOWLEDGMENTS: This material is based upon research supported by, or in part by, the U. S. Office of Naval Research under award number 13235235. Use of the Center for Nanoscale Materials, an Office of Science User Facility, was supported by the U. S. Department of Energy, Office of Science, Office of Basic Energy Sciences, under Contract No. DE-AC02-06CH11357.

Department of Electrical and Computer Engineering,
University of Illinois at Urbana-Champaign, Illinois,
61801, USA

Nick Holonyak, Jr Micro and Nanotechnology Laboratory,
University of Illinois at Urbana-Champaign, Illinois,
61801, USA

I ILLINOIS

Autoencoder Based Intrusion Detection System

Krishna Vasudev, Huichen Li, Professor Bo Li

Department of Physics, College of Liberal Arts and Sciences, University of Illinois at Urbana-Champaign

INTRODUCTION

A malicious network traffic data packet has specific features that set itself apart from normal packets. We use Intrusion Detection Systems (IDS) to detect such data packets. It is essential to detect such attacks because they can cost entities millions in lost revenue, research, or progress. There are three kinds of IDS:

- Signature Based: Utilizes a feature of traffic to predict a class. Hard to generalize to unknown/novel attack classes
- Anomalous Based: Detects deviations from normal learned behaviors. Unable to compensate for changes in everyday operations.
- Hybrid: Combination of the above two approaches

I utilize a Feed-forward Neural Network (NN) to build an effective hybrid IDS. The NN is twofold:

- Part 1: Autoencoder to reduce the dimension of the data packet to something more manageable.
- Part 2: Cross-entropy loss NN to categorize the truncated data packets.

I test multiple learn rates to determine the peak accuracy of my model. Additionally, I prioritize specific kinds of errors over others. I assumed that predicting malicious traffic as the normal class carries the most harmful implications. I utilize a confusion matrix to conclude that my IDS is vulnerable to “back” attacks because my model classifies around 1/3 of those attacks as normal traffic.

DATASET

KDD-NSL attack types:

- Normal: Normal operations; can vary with the policies of the network/company
- R2L: Intruder attempts to gain access to a machine onsite. Does not have previous access.
- DOS: Floods the target system with traffic to initiate a shutdown
- Probe: Gain information from the network (ranges from company proprietary information to a social security number)
- U2R: Normal operator attempting to gain root (super) access to the network

Count of Unsplit Dataset	
Normal	79206
DOS	58617
Probe	16479
R2L	5855
U2R	210

Table 1: Count of each category of attack in unsplit dataset.

METHODS AND EXPERIMENTS

Preprocessing KDD-NSL dataset:

1. One Hot encode categorical variables
 - Protocol type: Set of rules that devices follow within a network to communicate
 - Service: “Purpose” of the connection
 - Flag: Status of the connection. Was the connection reset by the server, rejected, established and or terminated, etc.?
2. Label Encode the ground truth.

Splitting dataset for various tasks:

1. Trained autoencoder on first 100,000 points
2. Following 2,494 data points were used to train the categorization model. Represents 10 points per attack class unless there are less than 10 of that class.
3. Tested overall model on last 30706 data points.

Training Model:

1. Autoencoder-Aims to shrink the data’s vector dimension.
 - The model’s layers gradually shrink from 122 (input layer) to 61 (encoding layer) dimensions (D)
 - The model rebuilds the 122-D vector, learning a concise representation of the dataset
 - The loss function is a mean squared error (MSE) loss between the input and reconstructed datapoint
 - All layers from the input to encoding layer are transferred to the NN categorizer.
2. NN Categorizer-Aims to categorize the encoded form of each data point.
 - Gradually reduces the layer’s size from 61 to 38. The outputs of this model are “raw scores.”
 - I use these raw scores in the CrossEntropy Loss() function. From this function, I obtain the class probabilities of each attack class.

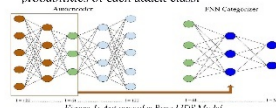


Figure 1: Autoencoder Based IDS Model

Testing Model:

- Send last 30706 points through trained model. Prioritize following errors via confusion matrix:
1. Mistaking an attack for regular traffic
 2. Mistaking attack types with one another (i.e., predicting a DDOS is R2L, etc.)

		Confusion Matrix Example	
		Yes	No
Yes	True Positive - Correctly predicted "Yes"		False Negative - Incorrectly predicted "No"
	False Positive - Incorrectly predicted "Yes"		True Negative - Correctly predicted "No"
No			

Table 2: Confusion Matrix example

RESULTS

Accuracy of Model vs Learn Rate:

1. Tested a range of learning rates (LR) to tune our models carefully
2. Fixed one model at LR = .001, while adjusting the other LR

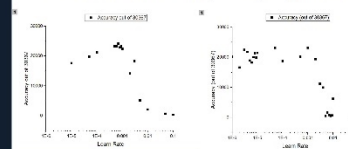


Figure 2: Accuracy vs. Learn rate for Autoencoder (left) and NN categorizer (right)

From Figure 2, I use the most efficient learn rates within my model. Peak accuracy of attack class prediction is ~ 89% during training. ~ 75% during testing:

1. Autoencoder-LR = .001
2. NN Categorizer-LR = .0007

Confusion Matrices with the Above LRs:

		Class Level Confusion Matrix (zoomed in)					
		Predicted					
Truth	normal	0	0	0	4	0	0
	back	0	0	0	448	0	0
	buffer overflow	0	0	0	0	0	0
	ftp_write	0	0	0	0	0	0
	guess_passwd	4	0	0	23	0	0
	http_tunnel	0	0	0	0	0	0
	imap	0	0	0	0	0	0
	ipsweep	0	0	2	0	0	0

Table 3: Class Level Confusion Matrix

From Table 3, we identified a vulnerability with the network:
- Row 5 and Column 19: 448 “back” attack are misidentified as normal traffic.

		Category Level Confusion Matrix					
		Predict					
Truth	Normal	8014	430	1125	1206	334	
	DOS	466	9110	548	83	136	
	Probe	10	68	3828	121	21	
	R2L	23	14	6	4585	154	
	U2R	0	0	0	11	108	

Table 4: Category Level (left) and General Level (right) Confusion Matrix

From Table 4, I conclude the accuracy rate of:

- Distinguishing between attack category is ~ 85%
- Distinguishing between normal and malware traffic is ~ 89%

Back Attack:

Main Characteristics:

1. ~ 50,000 bytes transferred from source to destination
2. ~ 8,000 bytes transferred from destination to source
3. TCP protocol; Http Service; SF or RSTR flag

CONCLUSIONS

Model Accuracy:

Testing various learn rates revealed a peak attack class accuracy of ~ 75% while testing. There is not an exact accuracy because weights are randomly initialized at the beginning of training.

Learn rates of .001 for the autoencoder and .0007 for the NN categorizer are large enough to circumvent local minima on the loss curve, but small enough to converge on the absolute minimum.

Training accuracy with the above learn rates is ~ 89%. The difference between the training and testing accuracies may indicate an overtrained network.

Vulnerabilities:

Testing the most accurate LRs revealed ~ 75% of “back” attacks were misclassified as normal traffic. This was the most severe error my model made. Additionally, we see that ~ 96% of DOS attacks being predicted as normal traffic are “back” attacks being misclassified as normal traffic.

The “back” attack is a DOS attack that sends ~50,000 bytes to the server to overload it. Most of these connections are flagged with normal connection and termination. Finally, the server sends back ~ 8000 bytes of information to the user.

FURTHER ACTIONS

Now that I have found the most effective LRs, I will refrain from changing them further. The future experiments I will run on my model are:

1. Changing the data composition of the NN training dataset to include more “normal” and “back” attacks
2. Experiment with regularization of the weights of my model to reduce overtraining.
3. Experiment with a reduced number of iterations I train my model for.
4. Attempting to build a cluster map of traffic so that it is easier to visualize similarities and differences between normal and malicious traffic.

ACKNOWLEDGEMENTS

I would like to thank the AERT program and the Office of Naval Research for sponsoring this project.



ILLINOIS



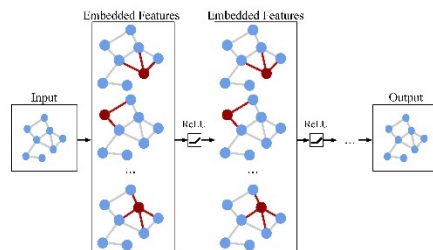
Detecting Anomalous Behaviors for Assured Command and Control

Luke Lalumandier, Ben Candee, Jacob Heglund, Huy Tran



Introduction

A significant factor in planning normal behavior of any traffic system (eg. road traffic, message/communication traffic) is recognizing what abnormal behavior looks like. In the field of machine learning, an abnormal behavior of the network or system being modeled is called an **anomaly**. We cannot predict what any possible anomaly may look like; we can, however, train a machine learning model to recognize unspecified types of anomalies.



Example of Message Traffic Data Structure

Traffic datasets are typically in a time-series graph structure. Some kind of traffic segment (eg. a street, a traffic zone, a census tract) is represented by a node, and these are connected by edges (representing intersections or trips between zones respectively).

Time-Series Graph: A series of graphs, each representing a point in time, consisting of nodes connected by edges.

For traffic data, each node represents some traffic segment, and each node represents an intersection or trip.

To detect anomalies in such data, we analyze both:

- the time-series for the values of features at particular nodes, and
- changes in the graphical structure of the data.

Analyzing a time-series at a particular node is done using similar methods to signal filtering, where we attempt to remove "noise" from the time-series signal to find anomalies. Analyzing changes in the graphical structure involves looking at some decomposition or representation of the graph (such as the spectral decomposition) and seeing when this changes significantly. [1]

- To develop deep learning techniques for unsupervised anomaly detection in dynamic environments
- To identify abnormal behaviors in the operating environment with no prior specification of what those behaviors might look like

We aim to develop a machine learning model which detects anomalous behavior in real time traffic data sets without knowing what the anomalies will look like. To do this, we aim to train our model to analyze time-series graph data by considering both the graph structure and the time-series values of features at each node.

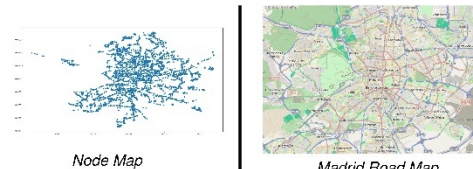
Data Preprocessing

To make our tests valid and replicable, we required a data set:

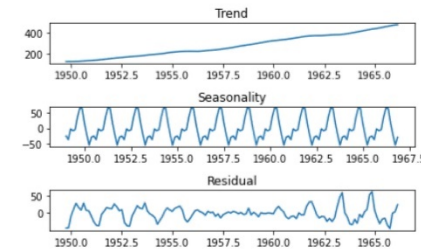
1. with a well-defined graph structure,
2. with anomalies clearly labeled at specific nodes,
3. spanning over a long period of time (eg. 1 year).

To achieve this, we used data from the Madrid City Council open portal [REF]. This website provided us with separate files containing traffic data spanning multiple years (indexed by traffic sensor), locations of traffic sensors (in GPS coordinates), and locations and severities of accidents (by street address).

We used DBSCAN clustering to sort the traffic sensors into nodes, each node representing an intersection or portion of a street segment. We then used a geocoding API to map each accident to a node. This initially presented a challenge as many geocoding APIs are only effective for addresses, not intersections.



The above maps show the results of the traffic sensor clustering compared to a real road map of Madrid. The node locations show a clear picture of Madrid in their structure. We then mapped each piece of accident or traffic data to one of these nodes.



Representation of Node Features

Replication Study

The paper "A Data-Centric Weak Supervised Learning For Highway Traffic Incident Detection" was selected to serve as a baseline to compare against our developed model [2]. This paper did not provide its exact code, so for it to be a baseline, its work must be replicated. The necessity for the baseline creates will allow us to conduct a replication study in the future.

Future Work

Our project partners, Vivek Thatte and Peter Baftoe, will take the step of implementing the neural network itself. The immediate next step is to define a suitable edge structure on the nodes we already have. Then, once the graph structure is defined, we will apply the GNN to the data and compare our model's incident detection accuracy against the methods used in the above replication study.

Acknowledgments

We would also like to thank the US Navy Office of Naval Research (ONR) for their financial support for the Accelerated Learning and Engineering Research Training (ALERT) program.

References

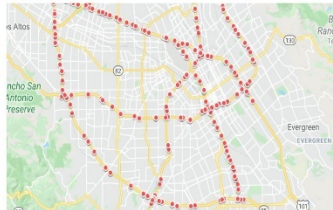
- [1] Akoglu, Leman, Hanghang Tong, and Danai Koutra. 2014. "Graph based anomaly detection and description: a survey." Data Mining and Knowledge Discovery 1, no. 29 (July): 626-688. <https://doi.org/10.1007/s10618-014-0365-y>.
- [2] Yixuan Sun, Tanwei Malik, Prashanna Balaprakash, and Jane MacFarlane. 2021. "A data-centric weak supervised learning for highway traffic incident detection." CoRR, abs/2112.09792. <https://arxiv.org/abs/2112.09792>.

Anomaly Detection in Road Traffic Patterns

Vivek Thatte, Jacob Heglund, Peter Baffoe, Professor Huy Tran
University of Illinois at Urbana-Champaign

Introduction

- Anomaly detection on network-based structures is a problem which has applications in a variety of academic disciplines.
- Our project seeks to develop an anomaly detection algorithm for road traffic patterns, by forming a graph of road traffic sensors, and analyzing changes in the metrics measured by the sensors.
- We base our approach on methods used in [1].

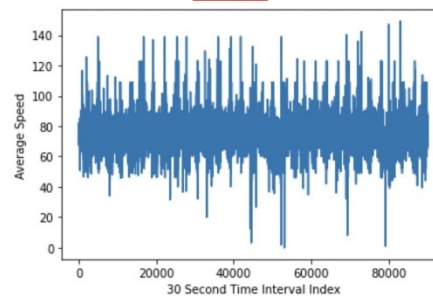


Research Questions

- **Sensor-level approach:** When is an anomaly/accident occurring at a particular traffic sensor?
- **Network-level approach:** Can data from closely related sensors be aggregated to determine when anomalies are occurring at a certain cluster of sensors?

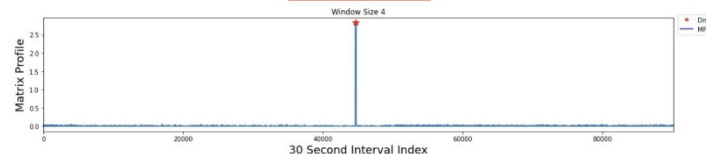


Data



- Data source: Traffic and accident data from the Caltrans PeMS database [2]. We use October 2013 to match [1] to use as a baseline.
- Traffic data: Data includes median velocity readings measured over 30 second intervals from a network of magnetic traffic sensors embedded in California highways.
- Accident data: Data includes accident time, location during the same period as the traffic data.
- Graph structure: Nodes are defined as sensors in same location, but in different lanes, and edges are defined by spatial distance between nodes

Methods



- Matrix profile applied to node-based velocity data over 5 minute intervals
- For each subsequence of a time series, the matrix profile represents the difference of this subsequence with the most similar subsequence to it
- Matrix profile used for anomaly detection through motif and discord identification
- Motifs: Traffic accidents are regularly occurring patterns in the time series.
- Discords: Traffic accidents are data points in the time series which differ significantly from normal patterns.

Summary of Findings

- Preliminary results suggest discord detection is not effective for detecting accidents in traffic data.
- Results suggest accidents may share a common set of patterns.
- Use of matrix profile for unsupervised clustering of network time-series requires further exploration.

Acknowledgements

- University of Illinois ISUR Program
- Office of Naval Research

References

- [1] Y. W. Liyanage, D. -S. Zois and C. Chelmiss, "Near Real-Time Freeway Accident Detection," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp. 1467-1478, Feb. 2022, doi: 10.1109/TITS.2020.3027494.
- [2] *Caltrans Pems*. Caltrans. (n.d.). Retrieved October 25, 2022, from <https://pems.dot.ca.gov>
- [3] Yeh, C.-C. M., Zhu, Y., Ulanova, L., Begum, N., Ding, Y., Dau, H. A., Silva, D. F., Mueen, A., & Keogh, E. (2016). *Matrix Profile I: All Pairs Similarity Joins for Time Series: A Unifying View that Includes Motifs, Discords and Shapelets*. <https://www.cs.ucr.edu/~eamonn/MatrixProfile.html>. Retrieved October 13, 2022. /

I ILLINOIS

Reducing Inertial Sensor Noise Via Physical Adjustments and Filtering

Riley Hudson, Neel Khattri, Kyo Kim
Department of Computer Science, College of Engineering,
University of Illinois at Urbana-Champaign

INTRODUCTION

- As drone usage rapidly grows in warfare, the threat of sensor spoofing also grows
- However, sensors inherently have noise: electronically and mechanically
- High noise would lead to less certainty in its placement in the environment since less certain the vehicle is about its state, more likely an adversary can manipulate the vehicle while evading the detection
- Therefore, we need to minimize the attack surface by minimizing the sensor noise
- We present our work-in-progress to reduce the inertial sensor noise via designing a mount to reduce the vibration as well as using various filters

Goals

- Determine potential causes for the vibration which is causing the IMU noise
- Design a mount to reduce noise in the inertial sensor measurement
- Analyze the effectiveness of the noise reduction under various missions

CURRENT SETUP

Hardware

- Navio 2 + Raspberry Pi 3
 - MPU9250 9DOF IMU
 - LSM9DS1 9DOF IMU
- Drone F450 Frame
- 960kv Motors

Software

- PX4 Autopilot [1]
 - Uses low-pass filters
- Linux

Sources of vibration

- Motors during flight
- Battery not fully fastened
- Mount not fully fastened
- Not optimal placements of shock absorbers

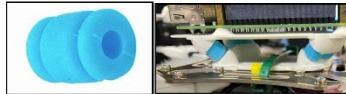


Figure 2. Off-the-shelf rubber shock absorbers to lessen the inertial measurement noise

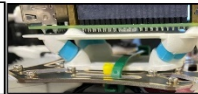


Figure 3. Closeup on the mount

REDUCING VIBRATION

Three approaches are being explored to lower vibrations and reducing the noise of the sensor:

1. Mount for the Navio 2

- Varying the amount of vibration dampeners
- Changing the orientation of the vibration dampeners
- Introducing gasket material to dampen vibration between the Navio 2 mount and the drone frame

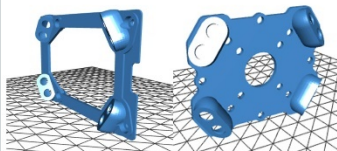


Figure 4. Current version of Navio2 lowerupper mount(2) respectively

2. Mount for the battery

- Current practice is to zip-tie the battery to the frame. A mount will allow easier installation and secure the battery to the frame.

3. Mount for Vicon Balls

- Current practice is to glue the vicon balls, which allow the drone to be detected in the indoor pavilion, to the frame. A mount will decrease the variability in the drone frame and allow a way for the vicon balls to be safely secured during flight.

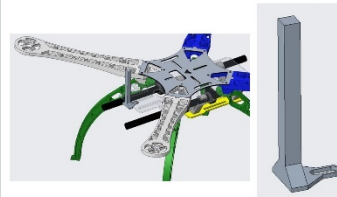


Figure 5. Current version of vicon ball mount

NOISE ANALYSIS

Background Information on Noise Analysis

- Signals can carry extra bandwidth called noise
- Noise makes it harder to analyze and compare signals due to varying amounts of noise for each signal
- SNR (Signal to Noise Ratio) is a measurement of how strong a signal is, therefore, a higher ratio means a stronger signal

$$\text{SNR} = P(\text{signal}) / P(\text{noise})$$

Two Methods to Reduce Noise

- LPEF (Linear Predictor Error Filter)

$$Y(n) = \sum h(n)x(n-k)$$

Works by reducing noise at a set time step intervals.

- ADF (Adaptive Digital Filter)

- Similar to LPEF but involves more precision and ability to distinct between noise and signal by acquiring the noise

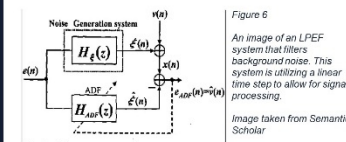


Figure 6

An image of an LPEF system that filters background noise. This system is utilizing a linear time step to allow for signal processing.

Image taken from Semantic Scholar

NOISE REDUCTION

- Two methods above help determine where the noise is and therefore can filter it out from the signal
- Makes it easier to compare signals therefore

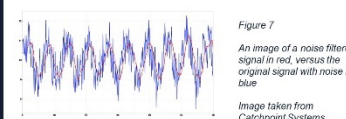


Figure 7

An image of a noise filtered signal in red, versus the original signal with noise in blue

Image taken from Catchpoint Systems

EVALUATION

Missions

- Hover at fixed altitude
- Lateral and vertical movement
- Change in the drone attitude
- Combination of the above

Mount Design

- Test the new mount under various missions
- Compare the noise in inertial sensor data
- Find the type of movements the mount does and does not perform well on

Noise Reduction

- Implement the algorithm in the IMU driver in PX4
- In each mission, test the algorithm with various parameters

FUTURE WORK

- Improving the mount design
- Noise profiling as anomaly detection
- Analyzing the noise reduction performance
- Measure the change in difficulty of the spoofing attacks due to the noise reduction

REFERENCES

1. PX4 Autopilot <https://px4.io>
2. Navio 2 Mount <https://github.com/emlid/hardware>
3. Noise Analysis Algorithms <https://arxiv.org/ftp/arxiv/papers/1110/1110.2267.pdf>

ACKNOWLEDGEMENTS

Natasha Mamaril
ALERT (Accelerated Learning and Engineering Research Training)
ONR (Office of Naval Research)



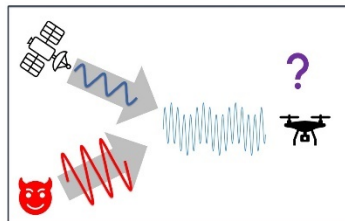
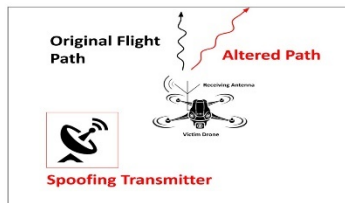
I ILLINOIS

Machine Learning Based Anomaly Detector for GPS Signal Attacks

PRESENTER: Nandika Vuyyuri

INTRODUCTION

- Security measures are crucial for safe operation of UAVs in safety-critical roles
- Commercial UAVs heavily rely on GPS signal for localization
- Dead-reckoning only using IMU results in unbounded position error over an extended period
- Must detect anomalies in the GPS to trigger recovery mechanism



Method

- Find GPS attack dataset and analyze
- Train various ML models to find which ones are more appropriate for the problem
- Compare the model performances
- Implemented in python using sklearn and pytorch libraries

Future Work

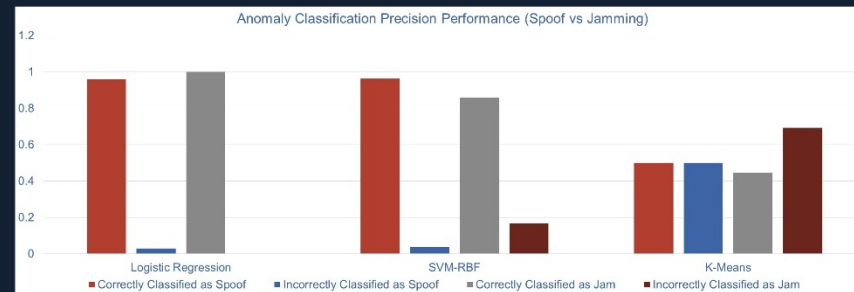
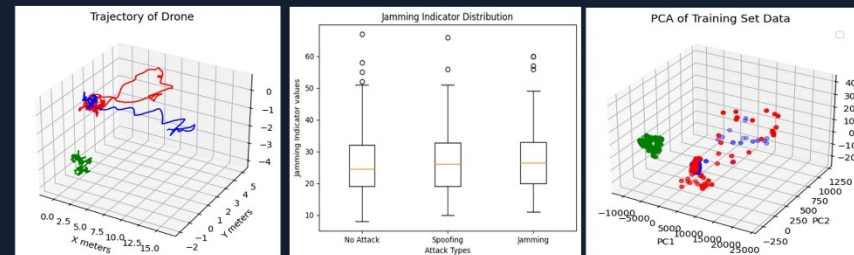
- Measure the model performance on TEXBAT [2]
- Integrating the anomaly detection model to existing flight controller firmware (e.g., PX4)
- Analyzing the overhead of deploy such models

References

- Jason Whelan, Thanigajan Sangarapillai, Omar Minawi, Abdulaziz Almeahdi, Khalil El Khalil, "UAV Attack Dataset," doi: 10.21227/00dp-0et2.
- Lemmenes, Adam, Phillip Corbell, and Sanjeev Gunawardena. "Detailed analysis of the TEXBAT datasets using a high fidelity software GPS receiver." In *Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, pp. 3027-3032. 2016.

Detecting Anomalies in GPS is Important for the Safety of the Autonomous Unmanned Aerial Vehicles

Neural Network Machine Learning Models Performs Well for This Domain

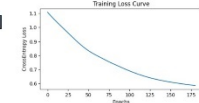


Training Pipeline



GPS Attack Dataset [1]

- Benign
- Spoofing
- Jamming



Pre-Processing

- Removed Features with zero variance
- MinMax Scaling:

$$X_{scaled} = \frac{X - X_{min}}{X_{max} - X_{min}}$$

Models

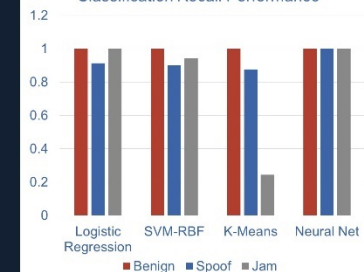
- Logistic Regression
- Support Vector Machine with Radial basis function Kernel
- K-Means Clustering
- 2-Layered ReLU activated Neural Network

Train and Test

- 80/20 split respectively

Detection Performance

Classification Recall Performance



- 2-layered neural network model achieves 100% accuracy on attack classification
- All of the utilized machine learning models can distinguish benign from attack
- Other models are not as good as distinguishing the type of attack compared to the 2-layered neural network model

Nandika Vuyyuri, Emily Grob
Kyo Kim and Sibin Mohan



ILLINOIS

IoT Virtualization: Device Emulation Benchmarking

Tomas Sagartz, Daniel Yu, Gabriella Xue

Department of Computer Science, College of Engineering, University of Illinois at Urbana-Champaign

BACKGROUND & MOTIVATION



OBJECTIVE

The primary goal of this project is to investigate the performance of our IoT virtualization system in order to justify the effectiveness of our virtualized system and to discover potential bottlenecks for our device emulations. We took steps to determine the metrics and scenarios to be applied regarding both software complexity and hardware complexity. We compared our results against the threshold for real-time systems.

Software Complexity - We changed the complexity of programmable code that is put into Arduino emulation. We use C++ compiler to compile our program

Hardware Complexity - We adjusted the (i) number of sensors and (ii) type of sensors that differ by computation requirement to represent different levels of hardware complexity.

We designed scenarios according to the above to analyze system performance.

SYSTEM EVALUATION DESIGN

Scenarios

Scenario 1: Ultrasonic Distance + Air Quality

Scenario 2: GPS + Humidity Sensor

Scenario 3: LDR + LED + Resistor

Scenario 4: GPS + PulseOximeter

Scenario 5: LED + Ultrasonic Distance + Capacitors + Resistors + Battery

Scenario 6: PulseOximeter + Temperature + LED



Metrics



```
1 // Latency, Memory Usage, CPU Utilization
2 // Scenario 1: Ultrasonic Distance + Air Quality
3 // Scenario 2: GPS + Humidity Sensor
4 // Scenario 3: LDR + LED + Resistor
5 // Scenario 4: GPS + PulseOximeter
6 // Scenario 5: LED + Ultrasonic Distance + Capacitors + Resistors + Battery
7 // Scenario 6: PulseOximeter + Temperature + LED
8
9 #include <Arduino.h>
10 #include <Wire.h>
11 #include <Ultrasonic.h>
12 #include <Adafruit_BMP280.h>
13 #include <Adafruit_GPS.h>
14 #include <Adafruit_PulseOximeter.h>
15 #include <Adafruit_Temperature.h>
16 #include <Adafruit_LDR.h>
17 #include <Adafruit_LED.h>
18 #include <Adafruit_Resistor.h>
19 #include <Adafruit_Capacitor.h>
20 #include <Adafruit_Battery.h>
21
22 // Define pins
23 const int trigPin = 9;
24 const int echoPin = 10;
25 const int ledPin = 13;
26 const int ldrPin = 14;
27 const int tempPin = 15;
28 const int pulsePin = 16;
29 const int gpsPin = 17;
30 const int humidityPin = 18;
31 const int capacitorPin = 19;
32 const int resistorPin = 20;
33 const int batteryPin = 21;
34
35 // Define variables
36 unsigned long start_time = 0;
37 unsigned long end_time = 0;
38 unsigned long latency = 0;
39 unsigned long memory_usage = 0;
40 unsigned long cpu_usage = 0;
41
42 // Define functions
43 void setup() {
44   // Initialize pins
45   pinMode(trigPin, OUTPUT);
46   pinMode(echoPin, INPUT);
47   pinMode(ledPin, OUTPUT);
48   pinMode(ldrPin, INPUT);
49   pinMode(tempPin, INPUT);
50   pinMode(pulsePin, INPUT);
51   pinMode(gpsPin, INPUT);
52   pinMode(humidityPin, INPUT);
53   pinMode(capacitorPin, INPUT);
54   pinMode(resistorPin, INPUT);
55   pinMode(batteryPin, INPUT);
56
57   // Initialize sensors
58   Ultrasonic sonar = Ultrasonic(trigPin, echoPin);
59   Adafruit_BMP280 bmp = Adafruit_BMP280();
60   Adafruit_GPS gps = Adafruit_GPS();
61   Adafruit_PulseOximeter pulse = Adafruit_PulseOximeter(pulsePin);
62   Adafruit_Temperature temp = Adafruit_Temperature(tempPin);
63   Adafruit_LDR ldr = Adafruit_LDR(ldrPin);
64   Adafruit_LED led = Adafruit_LED(ledPin);
65   Adafruit_Resistor resistor = Adafruit_Resistor(resistorPin);
66   Adafruit_Capacitor capacitor = Adafruit_Capacitor(capacitorPin);
67   Adafruit_Battery battery = Adafruit_Battery(batteryPin);
68
69   // Initialize variables
70   start_time = millis();
71   memory_usage = 0;
72   cpu_usage = 0;
73
74   // Run the program
75   while (true) {
76     // Measure latency
77     latency = measureLatency();
78
79     // Measure memory usage
80     memory_usage = measureMemoryUsage();
81
82     // Measure CPU usage
83     cpu_usage = measureCPUUsage();
84
85     // Print results
86     Serial.print("Latency: ");
87     Serial.print(latency);
88     Serial.print(" Memory Usage: ");
89     Serial.print(memory_usage);
90     Serial.print(" CPU Usage: ");
91     Serial.print(cpu_usage);
92     Serial.println();
93
94     // Delay
95     delay(1000);
96   }
97 }
```

TESTBED

The emulations are running within Docker containers that uses alpine 3.12 image.

And our test machine is Windows 11 Pro 22H2 (OS Build 22H2.1313.4) with AMD Ryzen 5 7600 6-Core Processor 3.80 GHz; Installed RAM 32.0 GB (31.8 GB usable)

RESULTS & ANALYSIS

Scenario 1: Ultrasonic Sensor + Air Quality Sensor

	Platform Run	Platform Compile
Latency (Seconds)	0.0830	0.718
Memory (Bytes)	50679838	50266112
CPU Usage	8.2%	15.0%

Scenario 2: Humidity + Temperature

	Platform Run	Platform Compile
Latency (Seconds)	0.0228	0.707
Memory (Bytes)	50636680	50330944
CPU Usage	16.31%	14.4%

Scenario 3: LDR + LED + Resistor

	Platform Run	Platform Compile
Latency (Seconds)	0.0385	0.745
Memory (Bytes)	50765920	50847168
CPU Usage	10.4%	15.7%

Scenario 4: Pulse Oximeter + Temperature Sensor

	Platform Run	Platform Compile
Latency (Seconds)	0.0277	0.682
Memory (Bytes)	50659684	50180996
CPU Usage	12.4%	15.1%

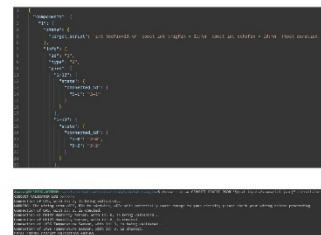
Scenario 5: Ultrasonic + LED + Resistor + Capacitor + Battery

	Platform Run	Platform Compile
Latency (Seconds)	0.0748	0.765
Memory (Bytes)	5074368	50450040
CPU Usage	9.0%	15.4%

Scenario 6: Temperature + Pulse Oximeter + LED

	Platform Run	Platform Compile
Latency (Seconds)	0.0294	0.750
Memory (Bytes)	50678898	50176000
CPU Usage	8.64%	15.0%

Device Validation



ACK.

We wanted to acknowledge our kind and helpful mentor Gabriella and our PI prof. Caesar, and the ALERT program for providing us funding during our time on the research team.

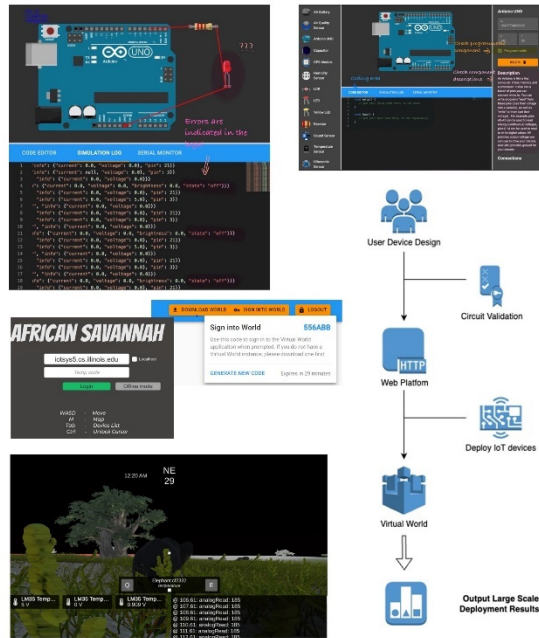


IoT Virtualization: Device Emulation Performance Benchmarking

Daniel Yu, Gabriella Xue

Department of Computer Science, College of Engineering, University of Illinois at Urbana-Champaign

BACKGROUND & MOTIVATION



OBJECTIVE

The primary goal of this project is to investigate the performance of our IoT virtualization system in order to justify the effectiveness of our virtualized system and to discover potential bottlenecks for our device emulations. Over the summer we took steps to determine the metrics and scenarios to be applied regarding both software complexity and hardware complexity. We compared our results against the threshold for real-time systems. Over the Fall we tried to identify the optimal point of scalability with the IoT system in order to more accurately predict possible bottlenecks and scalability issues in the future.

Software/Hardware Complexity - We changed the complexity of programmable code that is put into Arduino emulation. We use C++ compiler to compile our program. We adjusted the (i) number of sensors and (ii) type of sensors that differ by computation requirement to represent different levels of hardware complexity.

Mimic Realistic User Behavior - We wrote scripts to mimic user behaviors including adding and deploying devices to evaluate system performance under realistic settings.

SYSTEM EVALUATION DESIGN

Testing Scenario

Sensors involved: GPS, Humidity, Temperature, Ultrasonic, Air Quality



METHODOLOGY

To evaluate the scalability of the IoT system effectively, we embarked on a comprehensive testing strategy. Our initial focus was on identifying and addressing any potential bottlenecks that might impede the system's performance during a single run. This involved meticulous examination and optimization to ensure the smooth operation of the system.

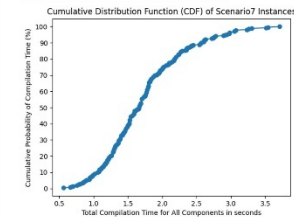
Building on the insights gained from our research conducted over the summer, we recognized that replicating a real use case involving a diverse array of sensors with varying levels of complexity was paramount. This approach allowed us to simulate realistic scenarios, providing a more accurate representation of the IoT system's scalability under diverse conditions which led to the creation of the above test scenario.

In addition to microbenchmarks, we developed client scripts to mimic user behavior for comprehensive end-to-end performance testing. By integrating various types and complexities of sensors, our goal was to replicate the intricacies and variability found in real-world IoT deployments.

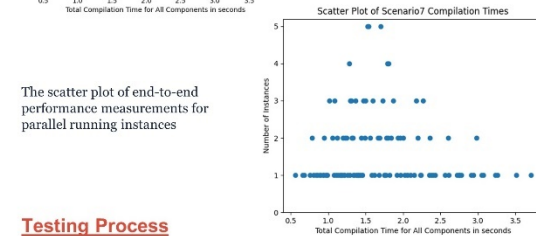
TESTBED

Windows Version: Windows 11 Pro 22H2 (OS Build 22H2.2134)
Processor: AMD Ryzen 5 7600 6-Core Processor 3.80 GHz
Installed RAM 32.0 GB (31.8 GB usable)

RESULTS & ANALYSIS



Among all the instances, 90 percent of them take less than 2.5 seconds to compile



The scatter plot of end-to-end performance measurements for parallel running instances

Testing Process

To test system scalability, we executed 500 instances concurrently to assess how system latency scales with increasing device numbers. We aimed to ensure that our system functions as a real-time system, meaning that device compilation must be completed within our predefined timeframe, without encountering any bottlenecks that could cause spikes. The CDF graph above illustrates the probability distribution of our measured compilation time. Additionally, the scatter plot not only displays the compilation time for each instance but also demonstrates how the number of sensors impacts the overall compilation latency for a device. Besides, we tested to ensure our deployment emulation was faster than 300ms which was determined from Arduino to be the optimal response time for these types of systems.

Lessons Learned

From these tests we were able to determine that while multiple instances of the scenario would create a wider spread of time taken to compile, it did not cause a dramatic spike and most of the times still fell below the 3 second range. This shows that us the circuit validation and deployment of these IoT devices in a large deployable environment should not have a large bottleneck risk. Further testing will need to be conducted to determine the scalability of the communication between IoT devices and back to a centralized database.

ACK.

We wanted to acknowledge our kind and helpful mentor: Gabriella, our PI Prof. Matthew Caesar, and the ALERT program for providing us funding during our time on the research team.

I ILLINOIS

A Study of the Robustness of ML Models to Input Perturbations

Jonah Black, Jacob Laurel, Sasa Misailovic

Department of Computer Science, Grainger College of Engineering, University of Illinois at Urbana-Champaign

INTRODUCTION

Neural networks, despite their powerful predictive capabilities, are difficult to comprehend in their entirety. As such, their internal mechanisms are often viewed as a sort of blackbox from which little information is ever retrieved. However, certain frameworks such as the one proposed here can be leveraged in order to gain insight into the internal mechanisms of deep neural networks. In this project, we employ a technique that combines dual numbers and interval arithmetic to analyze images from the MNIST dataset. This approach allows us to monitor both the upper and lower bounds (the "real part") of an input, as well as its derivative (the "dual part"), at each stage of their propagation through a neural network. In this way we can both provide an output range for a given input interval, and quantify the sensitivity of the model output (model confidence) to input perturbations.

AIM

The goal of this project was to examine the robustness of machine learning models with regard to their inputs. The Achilles heel of neural networks, as well as their derivative "AI" frameworks, lies in their inability to reliably adapt to atypical inputs (atypical in this sense refers to inputs which deviate in some way from the inputs upon which the model was trained). By computing the derivative range of a given input (in this case, a pixel) with respect to output of the model, we can identify a Lipschitz bound (maximum rate of change) for an interval of pixel values, and from this range generate a reliable saliency map for a bounded infinite set of images (defined by the lower and upper real bound). This process involves a novel combination of dual numbers and interval arithmetic, both of which are described in the following section.

METHOD

What are Dual Numbers?

A dual number has the form $a+be$, where a and b are real numbers, and e (epsilon) is a symbol with the property $e^2 = 0$. Dual numbers are distinct from the set of real numbers, and are used to simultaneously represent a function value $f(x)$ and its derivative $f'(x)$.
Ex: Given $f(x) = x^2$, the derivative at $x = 3$ can be computed using $f(3+e) = 9+6e$. The coefficient of e (6 in this case) is the derivative of the function $f(x) = x^2$ at $x = 3$.

What is Interval Arithmetic?

Interval arithmetic is a mode of arithmetic defined specifically for intervals, rather than decimal values. An interval in this context can be represented as $[a, b]$, and arithmetic operations are extended to account for the range.

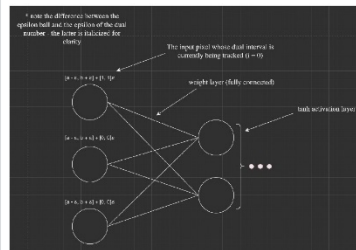
Ex: $[2, 3] + [4, 5] = [6, 8]$.

Epsilon Ball:

Each input pixel's value is perturbed within a tiny ϵ -ball, resulting in intervals representing the range of potential values the pixel can take. This ϵ -ball simulates minor changes to input pixels and captures their combined potential effect on network outputs.

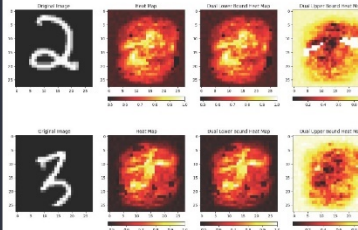
Propagation through Network:

1. Linear Layer: The interval of dual numbers is propagated through a matrix multiplication involving the linear weights, and is supplemented with scalar biases located at each node
2. Tanh Activation Layer: The interval's bounds are propagated through a tanh activation layer, which normalizes the input to the range $[-1, 1]$. However, the nonlinear behavior of the tanh function may contribute to an asymmetric response to positive and negative input perturbations, as illustrated in the following section.



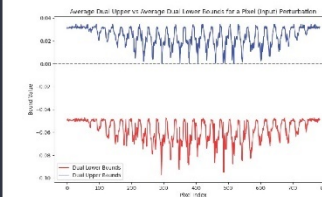
RESULTS

We found that for images in the MNIST dataset, the pixels comprising the foreground of the image (the actual writing, or near the actual writing) tended to have higher Lipschitz constants than those comprising the background. In other words, changes in the value of the pixels in the foreground had a larger impact on the model's output. This is demonstrated with a heat map, provided below:



"100.0" on the heat scale indicates that the pixel has a Lipschitz constant equal to 100% of the maximum Lipschitz constant in a pixel in the image. In general, the color of the pixel can be thought of as indicating the percentage of the max Lipschitz constant that is contained in that particular image. So darker hues indicate a lower Lipschitz constant for a particular pixel, whereas lighter hues indicate a higher Lipschitz constant.

Also notable is the fact that, due to some quirk in the model architecture (likely related to the tanh activation function), the upper and lower bounds of the dual part of the pixel are asymmetric about the y -axis ($y = 0$). To demonstrate this, we averaged the upper and lower dual bounds of each pixel in a training batch (32 images) and graphed them. A visual is provided below:



A graph of the average dual upper and dual lower bounds of the pixels of 32 randomly selected images from the MNIST dataset (784 pixels per image)

CONCLUSIONS

The proposed method provides a robust mechanism to assess the sensitivity of neural network outputs with respect to their inputs. By using interval arithmetic and dual numbers, we can bound the network's behavior and thereby provide a clearer understanding of its mechanisms and vulnerabilities. This work illustrates a potential avenue towards the formation of more coherent and predictable neural networks, important for tasks which mandate precision and reliability.

FUTURE RESEARCH

Although our findings do offer insight into the inner workings of neural networks, the methodology alone is not sufficient to address real-world problems. The process that we've formalized here serves as a diagnostic tool rather than a standalone solution - as such, its real-world utility hinges on its integration with adaptive training paradigms (namely those which leverage reward-penalty frameworks) that can utilize the insights it provides. In this way, one can balance model confidence with model robustness, and therefore ensure better overall model performance.

ACKNOWLEDGEMENTS



ILLINOIS

REPORT DOCUMENTATION PAGE

1. REPORT DATE 20240416	2. REPORT TYPE Final Performance Report	3. DATES COVERED <table border="1"><tr><td data-bbox="989 226 1265 304">START DATE 20210217</td><td data-bbox="1265 226 1549 304">END DATE 20231231</td></tr></table>		START DATE 20210217	END DATE 20231231
START DATE 20210217	END DATE 20231231				
4. TITLE AND SUBTITLE Accelerated Learning and Engineering Research Training (ALERT) Program in Cyber and Electronic Warfare for Undergraduate Midshipmen and Cadets					
5a. CONTRACT NUMBER N00014-21-1-2217	5b. GRANT NUMBER GRANT13235235	5c. PROGRAM ELEMENT NUMBER			
5d. PROJECT NUMBER	5e. TASK NUMBER	5f. WORK UNIT NUMBER			
6. AUTHOR(S) Mamaril, Natasha A.					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) UNIVERSITY OF ILLINOIS BOARD OF TRUSTEES OF THE UNIVERSITY 364 HENRY ADMINISTRATION BLDG URBANA IL 61801 UNITED STATES OF AMERICA		8. PERFORMING ORGANIZATION REPORT NUMBER			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release:distribution is unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT The research training program, Accelerated Learning and Engineering Research Training (ALERT) Program, aimed to train undergraduate midshipmen and cadets to expand and develop their technical and research skills in relation to cyber and electronic warfare. Participants were embedded in a research learning community which integrates research and educational experiences. Through mentored research experiences, students engaged in cutting edge, multidisciplinary, and interdisciplinary research to develop their technical skills and prepare them for more research. Program activities included a fall undergraduate research seminar course, monthly research seminars, and professional development workshops. 37 students from ROTC units and from underrepresented groups in STEM participated in research in a wide range of cyber security related areas, from advanced RF electronics and materials, communications and networking, data science and analytics, electronic warfare, and machine learning, reasoning, and intelligence. Student learning assessment and performance evaluation were conducted throughout their participation in the program. Participants presented their research in the research expo in April. Navy personnel were invited to talk with the students about the projects and naval career opportunities. Students will be tracked longitudinally to determine the effects of research participation on their career choices.					
15. SUBJECT TERMS Accelerated learning, research training, mentored experiences, undergraduate students, cybersecurity, electronic warfare					

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT UU	b. ABSTRACT SAR	c. THIS PAGE SAR	SAR	64 (incl. SF 298)
19a. NAME OF RESPONSIBLE PERSON			19b. PHONE NUMBER <i>(Include area code)</i>	

INSTRUCTIONS FOR COMPLETING SF 298

1. REPORT DATE.
Full publication date, including day, month, if available. Must cite at least the year and be Year 2000 compliant, e.g. 30-06-1998; xx-06-1998; xx-xx-1998.

2. REPORT TYPE.
State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

3. DATES COVERED.
Indicate the time during which the work was performed and the report was written.

4. TITLE.
Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

5a. CONTRACT NUMBER.
Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

5b. GRANT NUMBER.
Enter all grant numbers as they appear in the report, e.g. AFOSR-82-1234.

5c. PROGRAM ELEMENT NUMBER.
Enter all program element numbers as they appear in the report, e.g. 61101A.

5d. PROJECT NUMBER.
Enter all project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

5e. TASK NUMBER. Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

5f. WORK UNIT NUMBER.
Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

6. AUTHOR(S). Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, J, Jr.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES). Self-explanatory.

8. PERFORMING ORGANIZATION REPORT NUMBER.
Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES). Enter the name and address of the organization(s) financially responsible for and monitoring the work.

10. SPONSOR/MONITOR'S ACRONYM(S). Enter, if available, e.g. BRL, ARDEC, NADC.

11. SPONSOR/MONITOR'S REPORT NUMBER(S). Enter report number as assigned by the sponsoring/monitoring agency, if available, e.g. BRL-TR-829; -215.

12. DISTRIBUTION/AVAILABILITY STATEMENT. Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/ restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/ FRD, PROPIN, ITAR, etc. Include copyright information.

13. SUPPLEMENTARY NOTES. Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

14. ABSTRACT. A brief (approximately 200 words) factual summary of the most significant information.

15. SUBJECT TERMS. Key words or phrases identifying major concepts in the report.

16. SECURITY CLASSIFICATION. Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

17. LIMITATION OF ABSTRACT. This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.