Department of Electrical Engineering and Computer Science

COL Andre Sayles, Ph.D.
Professor and Head,
Department of Electrical Engineering and Computer Science

The mission of the Department of Electrical Engineering and Computer Science is to educate cadets to be Army officers who understand, develop, and exploit current and future technologies. We ensure that our highly productive research programs support our curriculum, enhance the professional development of both cadets and faculty, and contribute to the fields of science and engineering important to the Department of Defense. Our more than 50 faculty members have superb qualifications in computer science, electrical engineering, information systems engineering, and information technology. The Photonics Research Center and the Information Technology and Operations Center have an outstanding track record of finding research opportunities that best support our mission. This year, due to the increasing importance of network science in many disciplines, we have taken necessary steps to establish a Network Science Center. These centers establish funding programs and invite faculty to support projects of choice without overhead requirements or administrative burdens. This approach to department research has resulted in 100% faculty participation and up to 100 publications and presentations in a given year. At the same time, we are making a difference throughout the Defense community as well as in the Federal Government. Of particular note are our contributions to smart pixel technologies, optical and oversampled analog to digital conversion, image processing, novel semiconductor lasers, information assurance, science and engineering education, diversity, officer education needs in network-centric warfare, information technology, advanced technology classrooms, high speed communications, fiber optics, and the science and engineering underpinning numerous Army battlefield and automation systems. The quality of our scholarship and service is recognized by peers nationally and internationally.

Through the efforts of the Department, the Information Technology and Operations Center (ITOC) and the NSA Fellow, USMA is a Center of Academic Excellence in Information Assurance Education as designated by the National Security Agency (NSA). The Military Academy was the first-ever undergraduate institution to be so designated and was re-designated this past year. The ITOC also continues to be the driving force behind the annual Cyber Defense Exercise. The Cyber Defense Exercise challenges cadets from all five service academies to design, implement, and protect a sophisticated computer network from attack by a NSA-led red team. The winning academy is awarded the NSA Information Assurance Director's Trophy. In 2007 the Academy's Team took first place. The CDX program has significantly raised the level of Information Assurance education and understanding for all participants and is being used as the model for both a multi-national Department of Defense exercise and a competition for civilian universities. Additionally, the ITOC serves as the lead agency for the Annual IEEE Information Assurance Workshop, which brings together over 150 representatives from academia, industry and the federal government. The electrical engineering and computer science efforts in the Photonics Research Center continue to be singled out for excellence during reviews by outside agencies. Our cadets, staff, and faculty continue to work as a team to achieve the best possible research experience while supporting the needs of our primary customer—the United States Army.

Information Technology Operation Center Projects:
Center Director: LTC Ron Dodge, Ph.D.

Information Operations

Ancile
LTC Fernando Maymi

Sponsor: Program Manager, Ground Combat Command and Control

The Ancile project designed and constructed a PDA prototype device that can, in combination with GPS technology, provide increased survivability of dismounted soldiers by correlating location information with indirect fire data. Ancile is intended as a complementary system to FBCB2 and potentially, Land Warrior. Ancile has been successfully tested under 81mm mortar live-fire conditions at Yuma Proving Ground, AZ, and is currently undergoing commercial productization.

Voice Over IP Integration Assessment
COL Jeff Girard, Ph.D.

Sponsor: ITOC

A Voice Over Internet Protocol (VoIP) network is a network which sends both typical data packets and voice packets in the same network through the same hardware (cables, routers, hubs, etc). The network server contains call manager software, which is the source of the setup for the voice portion of the network. This allows for the addition of new phones and the initial setup of these phones. The Academy will move to implement VoIP for all telephone services at USMA. This project will serve to provide installation and management considerations for the future deployment of VoIP At USMA.

J. Girard, "VoIP Security" presented at the American Bar Association, Honolulu, Hawaii, June 2006.

Information Assurance

Military Academy Attack/Defense Network Simulation
LTC Ronald Dodge, Ph.D. and LTC John Hill, Ph.D.

Sponsors: National Science Foundation, Defense Information Systems Agency

This complete application simulates all facets of building and managing an information system; combining them into a seamless application that provides an integrated, engaging, challenging, and competitive information assurance learning environment. The goal is to build an information assurance simulation that integrates all the complexities involved in maintaining an information system infrastructure, including hardware configuration, service requirements, "sizing" the system to the correct capacity, administrative support and security configuration. MAADNET has been adopted by the Defense Information Systems Agency as an education tool for user, manager, and technician education.

R. Dodge and J. Hill, Military Academy Attack/Defense Network Simulation NSF Technical Report, May 2006.

UNICODE Stenographic Exploitation
Dr. Frank Mabry and Dr. John James

Sponsor: Department of Defense/National Security Agency

In the simpler days of the not too recent past, an English-speaking computer user could view a message and intuit the underlying digital representation of the characters without error. In this idyllic past the characters had few places to hide. The distance between the pixels on the display and the internal character representation was measured by a reference table in the back of the display adapter's manual. As the use of Unicode has become more prevalent, sufficient understanding of character representation, storage, transmission and rendering has become very complex and less than intuitive. The complex interpretation process needed for Unicode application programming provides an ever expanding "landscape of details" in which

steganographic exploits can be hidden. In this project we explain (1) basic concepts and definitions associated with Unicode, (2) general concepts from steganography, (3) the description of an example exploit embedded in the first paragraph of the Declaration of Independence, (4) overview of the implications of this exploit for Military messaging systems, (5) description of a solution architecture which addresses these concerns and (6) some implications for other application environments.

Email Phishing
LTC Ron Dodge, Ph.D.

Sponsor: ITOC

User security education and training is one of the most important aspects of an organizations security posture. Using security exercises to reinforce this aspect is frequently done by education and industry alike; however these exercises usually enlist willing participants. We have taken the concept of using an exercise and modified it somewhat to evaluate a users propensity to respond to email phishing attacks.

R. Dodge, C. Carver, and A. Ferguson, "Phishing for user security awareness," Computers and Security, Computers & Security, Volume 26, pages 73-80, February, 2007.

Mobile Device Security
LTC Grant Jacoby, Ph.D.

Sponsor: National Reconnaissance Office

Although mobile devices are globally omnipresent, security developments for these devices have not kept pace with their technological advancements. Thus, mobile devices are increasingly vulnerable to intrusions and malicious attacks. Gibraltar combats these growing threats by monitoring demands placed on battery current (mA) as well as correlating power and event activities, such as processes, open ports, and registry keys. This combination serves as an early warning tripwire-like sensor for mobile hosts, blocking as well as identifying attacks. The end state for this program is to provide a totally host-based proactive form of intrusion detection systems (IDS) that can be easily integrated into current network IDS to provide an enhancement in detecting, alerting and responding to various intrusions. This research outlines the design, test, and build methodologies used to resolve attack-sensing and warning research problems and discusses lessons learned.

G. A. Jacoby and N. J. Davis IV, "Mobile Host-Based Intrusion Detection and Attack Identification," IEEE Wireless Communications Journal, Fall 2006.

G. A. Jacoby and N. J. Davis IV, "Achieving Mobile Host-Based Security," ACM Transactions on Information and System Security Journal, 2006.

G. A.Jacoby, R. Marchany, and N. J. Davis IV, "Using Battery Constraints Within Mobile Hosts To Improve Network Security," IEEE Security & Privacy Magazine, September 2006.

G. A. Jacoby and J. S. Ransbottom, "Effective Reporting (ER) for Mobile Host-based Security and Forensics", (published in) Proceedings of the IEEE Consumer Communications & Networking Conference (CCNC) 2007, Las Vegas, Nevada, January 11-17, 2007.

G. A. Jacoby, J. S. Ransbottom, CDT T. Hickman and CDT M. Potasknik, "Screening Mobile Devices to Examine Network Health", Hawaii International Conference on System Sciences (HICSS) 2007, Waikoloa, Hawaii, January 3-6, 2007.

J. S. Ransbottom and G. A. Jacoby, "Monitoring Mobile Device Vitals for Effective Reporting (ER)", (published in) Proceedings of the IEEE Military Communications (MILCOM) 2006, Washington DC, October 23-25, 2006.

J. S. Ransbottom and G. A. Jacoby, "Mobile Triage in Support of Effective Reporting (ER)," Military Communications Conference (MILCOM06), 23-25 October 2006.

G. A. Jacoby, CDT T. Hickman, CDT S. P. Warders, CDT B. Griffin, CDT A. Darensburg, and CDT D. E. Castle, "Mobile Intrusion Protection," Proceedings from The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing, June 2006.

T. K. Buennemeyer, G. A. Jacoby, R. C. Marchany, and J. G. Tront, "Battery-Sensing Intrusion Protection System," Proceedings of the 7th IEEE SMC 2006 Information Assurance Workshop, June 2006.

Honeynets

LTC Ronald Dodge, Ph.D., LTC Kevin Huggins, PhD., and MAJ Tanya Markow

Sponsor: 1st Information Operations Command

Honeynets are an ideally suited security tool for detecting new attacks and catching advanced attackers. They reveal the attacker's identity, tools, and means of communication. Data collected from honeynets contribute to the prevention of future attacks. The systems designed at West Point are being used as the model for development of Army and DoD systems. The ITOC is engaged with DoD honeynet development efforts and with the open source honeynet alliance. In June and July 2006, cadets on AIAD's at Universities in Paris, Panama, and Santiago worked in collaboration with local students to deploy similar honeynets with the goal of analyzing the distributed honeynets to detect commonalities in attack vectors.

R. Dodge, Chapter Title: "Configuring and Deploying Honeynet Systems," Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues, Idea Group Publishing, 2006.

R. Dodge, "The Virtual Guide to Honeynet Deployments", www.honeynet.org.

Network Cognizance
Dr. John James and Dr. Frank Mabry

Sponsor: ITOC

This project is focused on the development of an analytical approach for network cognizance and the implementation of a prototype demonstration of applying the analytical technique. We will design an interface for construction of an overlay interface for visual display of the status of a power generation and distribution system and an associated network. The intent is to attempt to resolve the differences between those values predicted by a given model and those values observed as system parameters shared over a network Supervisory Control And Data Acquisition (SCADA) system. The model used for prediction of system values will be a PowerWorld model of the same complexity as the implementation of a Matlab/Simulink model of a two-generator, three-bus network with 700 kilometers of transmission lines which is unstable without proper feedback control implementation (i.e. a Power System Stabilizer (PSS)). A model of this complexity is expected to provide an initial demonstration of the validity of the approach for objective-driven-evidence-accumulation-and-analysis.

RFID Vulnerability Analysis
LTC Ronald Dodge, Ph.D. and Mr. Jeff Bonner

Sponsor: ITOC/Department of Defense/National Security Agency

The Global Information Grid (GIG) has been designated as the de facto mode of operation for combat and control in the next decade. A current enabling technology employed by DoD on the GIG is Radio Frequency Identification (RFID). RFID is used from supply chain management to battlefield sensors (for example, Ultra-Low Power Battlefield Sensor Communication Systems, ULPBSCS). In supply chain management, RFID technology is engaged to track and log movement of parts and equipment. One logical management system used by the Army is the Battlefield Combat Service Support System (BCS3). The system uses RFID technology to track each item in the supply system beginning at entry into the Army system. Items are scanned by an RFID interrogator at transit locations to track its movement. The application allows you to display the location of an item by tracking number or to select an area on the digital map and all tagged items will be displayed. This capability provides an information confidentiality risk by allowing an adversary to interrogate supply vehicles from a concealed stand-off location and discover all supply items (repair parts, end items, ammunition…) entering a given area of operations. Furthermore, the application delivering the supply information to the user is available on the NIPRNET which adds additional security considerations.

The objective of this research is to examine the RFID protocol to discover potential vulnerabilities introduced to the GIG. The potential vulnerabilities include unaccounted for access points into the GIG, loss of information, and data integrity. Additionally, the characteristics of a stand-off device will be evaluated from a power and size perspective for a series of distances. Finally, an assessment using the MORDA framework of the security risks associated with using the NIPRNET for use in the DoD supply management.

Hacking and Innovation
LTC Gregory Conti, Ph.D.

Sponsor: ITOC

This research covers the passionate and independent-minded global community of highly skilled technical experts that frequently functions outside the mainstream of computer product development and conventional technology research. Sometimes called the hacker community, these experts are responsible for innovation that pushes the limits of technology, sometimes in unintended or uncomfortable ways, as well as for prescient warnings about the threats of both technology and the government's technology-related policy and regulations. Computer scientists have much to learn about innovation and nontraditional problem solving by listening to and working with them.

G. Conti (guest editor), "Hacking and Innovation," Communications of the ACM (CACM), June 2006.

Web-based Information Disclosure
LTC Edward Sobiesk, Ph.D., LTC Gregory Conti, Ph.D.

Sponsor: ITOC

Virtually every Internet user on the planet uses the powerful free tools offered by a handful of information service providers in many aspects of their personal and professional lives. As a result, users and organizations are freely providing unprecedented amounts of sensitive information in return for such services as Internet search, email, mapping, blog hosting, instant messaging and language translation. Traditional security measures, such as cryptography and network firewalls, are largely ineffective because of the implicit trust paradigm with the service provider. In this research, we directly address this problem by providing a threat analysis framework of information disclosure vectors, including fingerprinting of individuals and groups based on their online activities, examine the effectiveness of existing privacy countermeasures and clearly outline the critical future work required to protect our corporate, organizational and individual privacy when using these services.

G. Conti, "Googling Considered Harmful;" New Security Paradigms Workshop; October 2006.

G. Conti, "Web Search Privacy Issues," International World Wide Web Conference, May 2007.

G. Conti, "Googling: I'm Feeling (un)Lucky," DEFCON, July 2006.

E. Sobiesk and G. Conti, "The Cost of Free Web Tools;" IEEE Security and Privacy, May/June 2007.

Visualization of Security Data

LTC Gregory Conti, Ph.D.

Security analysts and network administrators are faced with tremendous amounts of security related data. Unfortunately current tools quickly overwhelm us with too much or the wrong type of information. This research explores solutions to this problem using carefully crafted security visualization systems that produce insightful images, animations and movies of security data. If properly constructed, the results can be dramatic and will help you quickly perform analysis and better communicate results to clients, management and other analysts.

G. Conti, Security Data Visualization, No Starch Press, September 2007.

Information Assurance Education

Information Warfare Analysis and Research Lab
LTC Ronald Dodge, Ph.D.

Sponsor: ITOC

The Information Warfare, Analysis, and Research (IWAR) Lab represents six LAN segments consisting of approximately 200 nodes. It provides an "enterprise" appearance to the users of the network by running many operating system versions and multiple similar services on various hardware architectures. The network segments contain both "vulnerable" and "hardened" targets. These systems are used in support of Information Assurance education and training at USMA. The lab also serves as the resource center for computing assets supporting sponsored research. New technologies and applications are integrated into the IWAR network as appropriate, adding to the complexity and realism of the network.

Virtual Information Assurance Network
LTC Ronald Dodge, Ph.D.

Sponsor: National Security Agency, Microsoft

The Virtual Information Assurance Network (VIAN) project at USMA uses new technologies to allow for robust testing on a single platform. The VIAN solution has been demonstrated to several Federal Agencies and is currently in use by the 1st Information Operations Command and the State Department. The agencies use the system for both live exploit experimentation and for education. VIAN provides a "real" network using only one machine. In this machine, virtual networks can be rapidly configured. The project provides the Army with the capability to analyze malicious Virus/Trojan/Worms in mobile isolated environments.

R. Dodge, and D. Ragsdale, " Remote Virtual Information Assurance Network," Proceedings of the 22nd IFIP International Information Security Conference, Sandton, South Africa, May 2007.

Network Routing and Switching Fundamentals and Advanced Training
LTC Ronald Dodge, Ph.D.

Sponsor: ITOC

The emerging need for facilities and curriculum to prepare students and practitioners to understand, anticipate, and investigate malicious activity conducted using Internet based services and infrastructure is emerging as a high interest area and increasing in importance. Curriculum development focusing on host forensics has been discussed and written about frequently in the recent past. However the area of network forensics has largely not been included. The objective of this research is to create a physical laboratory and describe the integration of practical, example based network focused curriculum.

Seventh Annual IEEE Information Assurance Workshop
LTC Ronald Dodge, Ph.D., LTC John Hill, Ph.D., Dr. John James

Sponsors: IEEE Systems, Man and Cybernetics Society, National Security Agency

The Department of Electrical Engineering and Computer Science, with support from the IEEE and the National Security Agency, has initiated a national-level series of workshops to provide a forum for discussion of information-assurance-related issues and publication of information-assurance-related research. The EE&CS Information Technology and Operations Center has hosted highly regarded workshops on Information Assurance topics since 2000. The proceedings have been published on compact disk and in book form.

Proceedings of the Seventh Annual IEEE SMC Information Assurance Workshop, West Point, NY. June 15-17, 2006.

International Cyber Defense Workshop 2006
LTC Ron Dodge, Ph.D. and LTC Fernando Maymi

Sponsor: ITOC

The Information Technology and Operations Department of the United States Military Academy (USMA), in conjunction with the Office of the Assistant Secretary of Defense for Networks and Information Integration Information Assurance Directorate (OASD (NII)/IA Directorate), create and execute a Cyber Defense Workshop and Exercise to provide an opportunity for participants to work in a collaborative environment to address various technical security issues regarding the identification and remediation of computer security vulnerabilities. Topics covered include wireless technologies and their various reconnaissance and attack technologies, network reconnaissance and attack methods and tools, and hands-on exercises to provide training on the topics discussed. The topics are introduced in seminar style with field experts invited to present current trends. Hands-on training/exercise labs are used to reinforce discussions.

Participants are broken down into several teams to compete in the situational training exercises (STX).

Cyber Defense Exercise 2007
LTC Ron Dodge, Ph.D, MAJ Damon Becknel

Sponsor: National Security Agency

The inter-academy Cyber Defense Exercise (CDX) is a hands-on, competitive real-life learning experience initiated and implemented by faculty and cadets of the US Military Academy, with funding and direction provided by the National Security Agency. The concept of "defending the network" was derived to evaluate cadet skills and the effectiveness of the Information Assurance (IA) education at West Point. The CDX served as the final project for senior-level Computer Science majors enrolled in the IA course. All five service academies competed in 2007. A team of analysts from the National Security Agency served as the Red Team. Remote access was provided to each participating school's Cyber Defense Network (CDN) via a Virtual Private Network configured to provide authentication and encryption of all traffic. The team verified the student's efforts to provide security to the CDN while ensuring the predetermined services and applications were available, with a baseline set of network resources and operating systems provided by the DoD Public Key Infrastructure Program Management Office. The Red Team then, based on predetermined assessment criteria, designated the school with the strongest information assurance posture the winner of the exercise.

T. Augustine and R. Dodge, "Cyber Defense Exercise: Meeting Learning Objectives thru Competition," 10th Colloquium for Information Systems Security Education, pages 61-67, Adelphi, MD, June 5-8, 2006.

G. White and R. Dodge, "The National Collegiate Cyber Defense Competition," 10th Colloquium for Information Systems Security Education, pages 68-74, Adelphi, MD, June 5-8, 2006.

Classroom XXI
MAJ Duane Fairfax

Sponsor: TRADOC

This project provides technical expertise and maintains the test-bed laboratory for the TRADOC multimedia classroom of the 21st Century. In addition, it evaluates and recommends proposed technologies. The researcher performs test and acceptance of Classroom XXI implementations and conducts courseware development training. Objectives include:

Determine benefits and limitations of student computer management tools;
Evaluate collaborative tools and other methods to enhance student learning;
Evaluate and test hardware, software, and audio-visual equipment for possible use in future Classroom XXI implementations; and

Assess knowledge/learning management systems to enhance school administrator ability to conduct soldier Human Capital Management.

Information Assurance Education and Curriculum Development

LTC Ronald Dodge, Ph.D., LTC Fernando Maymi, and COL Daniel Ragsdale, Ph.D.

Sponsor: ITOC

Our nation's economy and our military are becoming increasingly dependent on information systems. Assuring the confidentiality, integrity, and availability of these systems is a national security issue. A significant effort is being expended to develop information assurance curriculum for use in undergraduate programs. Objectives include:

- Develop consistent IA curriculum criteria for all undergraduate universities to employ;
- Share advances in IA education with other universities as well as industry by facilitating technology transfer;
- Work with the NSA and other organizations to continue to expand cadet and faculty internships;
- Ensure IA education is conducted employing a multi-disciplinary approach; and
- Identifying means for universities resource bounded to include IA into existing curriculum.

Photonics Research Center Projects:

Photonic Analog-to-Digital Conversion and Image Processing Applications of the Error Diffusion Neural Network

COL Barry L. Shoop, Ph.D., COL Eugene K. Ressler, Ph.D., Dr. Thomas D. Wagner, Dr. Jean R. S. Blair, LTC Robert W. Sadowski, Ph.D., COL Andre H. Sayles, Ph.D., Dr. Wenli Huang, Department of Electrical Engineering and Computer Science
Dr. Pankaj K. Das, University of California at San Diego, La Jolla, California
Dr. Liu Jaing, Dr. Joseph N. Mait, Dr. George Simonis, U.S. Army Research Laboratory, Adelphi, Maryland

Sponsors: Army Research Office and Defense Advanced Research Projects Agency

Since the majority of signals encountered in nature are continuous in time and amplitude, the analog-to-digital (A/D) interface is generally considered to be the most critical and challenging part of any signal acquisition and processing system. Because of the difficulty in achieving

high-resolution and high-speed A/D converters, this A/D interface has been and continues to be a barrier to the realization of high-speed, high-throughput systems. As a result, photonic-based systems have received increased emphasis because of their high-speed switching capability and the inherent parallelism that comes with a 2-D photonic system.

This research investigates photonic-based A/D conversion employing oversampling and spectral noise shaping techniques. In these applications, a low-resolution quantizer is embedded in a feedback architecture in an effort to reduce the quantization noise through spectral noise shaping. Here a large error associated with a single sample is diffused over many subsequent samples and then linear filtering techniques are applied to remove the spectrally shaped noise thereby improving the overall signal-to-quantization noise ratio of the converter. A two-dimensional extension of this concept diffuses error spatially using an error diffusion neural network realization for digital image halftoning and image processing applications.

Applications under consideration include high-speed, high-resolution photonic A/D conversion, photonic-based digital image halftoning, and data reduction and classification of multispectral and hyperspectral imaging systems.

Eugene K. Ressler, Wenli Huang, Barry L. Shoop, "Three-Dimensional Error Diffusion For Color Halftoning," Conference presentation in Frontiers in Optics 2006 OSA Annual Meeting, Rochester, NY, 8-12 Oct 2006.

Wenli Huang, Eugene Ressler, Barry Shoop, "Error Diffusion for Color Halftoning Using Three-Dimensional Neural Interconnects", Proceedings in The 3rd International IEEE EMBS Conference on Neural Engineering, pp. 553-556, Kohala Coast, HI, 2-5 May 2007.

Mixed Signal Applications of Smart Pixel Technology

LTC Robert W. Sadowski, Ph.D., COL Barry L. Shoop, Ph.D.,
COL Andre H. Sayles, Ph.D., and Dr. Wenli Huang
Department of Electrical Engineering and Computer Science
Dr. Pankaj K. Das, University of California at San Diego, La Jolla, California
Dr. George Simonis, US Army Research Laboratory, Adelphi, Maryland

Sponsors: Defense Advanced Research Projects Agency and Army Research Office

Smart pixel technology is a relatively new field that integrates electronic circuitry with optoelectronic devices in an effort to improve overall performance of existing applications and enable new applications not previously envisioned with either single technology. Smart pixels leverage the functionality and programmability of established electronic circuit technology and the high-speed switching and parallelism of arrays of optoelectronic devices. A smart pixel hardware implementation of the error diffusion neural network has been investigated and experimentally characterized. This hardware approach to the error diffusion neural network provides the ability to perform real-time image halftoning for applications such as xerography, laser printing, and facsimile.

Previously, we designed and fabricated proof-of-concept smart pixel circuits that realize the error diffusion filter. The earlier 5 × 5 CMOS-SEED implementation demonstrated correct functionality, however the design was not optimal. We then initiated a VLSI circuit design, modeling, simulation and testing program using the MOSIS foundry for our precision analog circuits.

As device features shrink to sub-micron scales, available transistor models fail to accurately predict their operation. Most external research focuses on modeling digital circuitry at these dimensions. Analog CMOS circuits offer particular challenges at the sub-micron level because current simulation tools fail to accurately predict their behavior. We initially conducted statistical analysis of extracted run parameters to see how we can minimize device mismatch from run-to-run parameter variations. Using these matching guidelines, we explored a variety of different topologies to implement the smart pixel neuron. As a result, we have developed a neuron topology that overcomes many of the inherent limitations of the proof-of-concept circuit. The key element of the new neuron is a modified current starved inverter. The modification consists of a novel loading scheme that allows us to effectively determine the quantizer slope independent of the transistor parameters. This means that run-to-run variations should not adversely effect the neuron operation. We are using MOSIS foundry runs to validate our design and the initial results look very promising.

R.W. Sadowski, M. C. Ballmann, and B.L. Shoop, "A Neural Network CMOS Circuit Implementation for Real-Time Halftoning Applications," 49th International IEEE MW Circuits and Systems Symposium, Image Processing II, C2L-E, IEEE, Aug 2006.

M. C. Ballmann and R.W. Sadowski, "Experimental Validation of a CMOS Circuit Implementation for Real-Time Halftoning Applications Using an Error Diffusion Neural Network," Accepted for Presentation at the National Conference of Undergraduate Education, April 2007.

Biologically Motivated Analog-to-Digital Conversion

COL Eugene K. Ressler, Ph.D. and COL Barry L. Shoop, Ph.D.
Department of Electrical Engineering and Computer Science
Dr. Pankaj K. Das and Dr. Brian Watson
University of California at San Diego, La Jolla, California

Sponsors: Defense Advanced Research Projects Agency and Army Research Office

Biologically-motivated analog-to-digital conversion considers the coordinated neuronal firings of biological systems to allow for the low-noise processing and transmission of analog signals through a network of coupled neurons. The inherently high noise levels associated with biological neurons has been found to be mitigated over a specific frequency range using a network of interconnected neurons. These neural interconnections cause statistical temporal patterns in the summed output of the network which result in spectral noise shaping and improved signal to noise ratio performance.

Photonic Crystal Vertical-Cavity Surface-Emitting Lasers

LTC James J. Raftery, Jr., Ph.D., LTC Gregory R. Kilby, Ph.D., CPT David J. Chang, Ph.D., and LTC Robert W. Sadowski, Ph.D.
Department of Electrical Engineering and Computer Science
Prof. Kent D. Choquette, University of Illinois at Urbana-Champaign, Urbana, IL

Sponsor: Army Research Office

The incorporation of a two-dimensional (2D) photonic crystal (PhC) lattice containing a lattice defect into a distributed Bragg reflector (DBR) of a vertical-cavity surface-emitting laser has proven to be effective for introducing a precisely controlled index step for lateral optical beam confinement leading to single mode device operation. Such devices are desirable for short-haul optical communication systems, as well as other applications such as light sources for very compact atomic clocks. PhC VCSELs with a single lattice defect have demonstrated single fundamental mode operation at high power (> 3 mW) and at high speed (> 9 Gb/s).

Creating multiple defects in the PhC lattice of a PhC VCSEL has lead to coherently coupled arrays of vertically emitting microcavities producing both out-of-phase and in-phase far field radiation patterns. It has been found that the phase difference between these emitting defect cavities can be tuned with injection current, and can result in an electronically steerable beam as observed in the far field radiation pattern. Coherently coupled 2D arrays of vertically emitting lasers offer the potential of extended area coherent sources with high spectral purity, useful in a variety of applications, such as electronically steerable laser sources for spectroscopic sensing or navigation vision systems for unmanned ground systems.

A. C. Lehman, J. J. Raftery, Jr., P. S. Carney, and K. D. Choquette, "Coherence of Photonic Crystal Vertical Cavity Surface Emitting Laser Arrays," IEEE J. Quantum Electron., vol. 43, no. 1, pp. 25-30 (2007).

A. C. Lehman, J. J. Raftery, Jr., and K. D. Choquette, "Photonic Crystal Vertical Cavity Surface Emitting Laser Arrays," Journal of Modern Optics, vol. 53, nos. 16-17, pp. 2303-2308 (2006).

P. O. Leisher, A. J. Danner, J. J. Raftery, Jr., D. Siriani, and K. D. Choquette, "Loss and index guiding in single mode proton-implanted holey vertical-cavity surface-emitting lasers," IEEE J. Quantum Electron., vol. 42, pp. 1091-1096 (2006).

J. J. Raftery, Jr., A. C. Lehman, A. J. Danner, P. O. Leisher, A. V. Giannopolous, and K. D. Choquette, "In-Phase Evanescent Coupling of Two-Dimensional Arrays of Defect Cavities in Photonic Crystal Vertical Cavity Surface Emitting Lasers," Appl. Phys. Lett., vol. 89, p. 081119 (2006). (see also Virtual Journal of Nanoscale Science & Technology, vol. 14, no. 10, 2006).

K. D. Choquette, J. J. Raftery, Jr., and A. C. Lehman, "Beam Steering in Photonic Crystal Vertical Cavity Semiconductor Laser Arrays," IEEE Aerospace Conference Proceedings (2006).

J. J. Raftery, Jr., A. C. Lehman, A. J. Danner, P. O. Leisher, A. V. Giannopoulos, and K. D. Choquette, "Coherent Transverse Coupling in Photonic Crystal Vertical Cavity Lasers," C. Lei and

K. D. Choquette, Editors; Proc. SPIE 6132, Vertical-Cavity Surface-Emitting Lasers X, 61320I (2006).

J. J. Raftery, Jr. and G. R. Kilby, "A Modified Single Defect Cavity Study for Coherent Coupling in Photonic Crystal VCSELs," Frontiers in Optics the 90th OSA Annual Meeting/Laser Science XXII, Rochester, NY, USA (Oct. 2006).

J. J. Raftery, Jr., G. R. Kilby, A. C. Lehman, K. D. Choquette, "Coherent Coupling in Photonic Crystal VCSELs," APS/AAPT NYSS 2007 Spring Meeting, West Point, NY, USA (Apr. 2007).

G. R. Kilby and J. J. Raftery, Jr., "Photonic Crystal VCSEL Characterization," APS/AAPT NYSS 2007 Spring Meeting, West Point, NY, USA (Apr. 2007).

Additional Department Research

Book Chapters:

R. Burk, N. Goerger, B. Gates, C. Blais, J. Nagel and S. Goerger. "Knowledge Representation for Military Mobility Decision-Making by Humans and Intelligent Software: The Mobility Common Operational Picture Data Model and Ontology." Published in *Extending the Horizons: Advances in Computing, Optimization, and Decision Technologies* (edited by Baker, Joseph, Mehrota and Trick). Springer 2007, New York.

Journal Publications:

J. Guo, C. You, M. Chu, P. Curran, J. Diao, B. Goda, P. Jin, J. McDonald, "Silicon Germanium Programmable Circuits for Gigahertz Applications," IET Circuits, Devices, and Systems, pp. 27-43, (Feb 2007).

E.K. Ressler, S.J. Ressler, C. Bale, "Engineering an Engineering Design Contest," *Computers in Education Journal*, vol. 17, no. 2, pp. 90–103 (April-June 2007).

S. K. Schwartz and E. M. Kowalski, "Collaborative Teaching Across Freshman Information Technology and Chemistry Courses," Journal of College Science Teaching, vol. XXXVI, No. 5, pp. 34-39 (Mar/Apr 2007).

C. You, J. Guo, R. Kraft, M. Chu, B.Goda, J. McDonald, " A 12Bb/s Demux Implemented with SiGe High Speed FPGA Circuits," Transactions on Very Large Scale Integration, (March 2007).

J. M. Zara, .l E. Patterson, "Polyimide amplified piezoelectric scanning mirror for spectral domain optical coherence tomography", *Applied Physics Letters*, 89, 263901 (2006).

Conference Presentations and Proceedings:

W. J. Adams, "Role-based Information Customization," presented at the Information Assurance Workshop, Orlando, FL, 12–15 February 2007.

M. Ades, M. Chinni, J. Hamilton, Jr., J. Hill, H. Rajaei, and C-H. Wu. Proceedings of the 2007 Spring Simulation Multiconference (SpringSim'07), Volume II. Norfolk, VA ISBN 1-56555-314-4, 26-28 March 2007.

D. T. Bennett, "Teaching Style vs. Student Learning Style and Performance – Does it Matter?" American Society for Engineering Education Midwest Section Conference, Kansas City, MO, September 2006 (Awarded Best Paper).

J. R. S. Blair, D. Fairfax, B. Goda, K. Huggins, M. Lemanski, W. Suchan, "Faculty Development in Information Technology Education", SIGITE 2006, Minneapolis, MN, 18-20 October 2006.

R. Burk and R. Burk. "Comparing Organic vs. Assigned UAV Support to the Maneuver Company", *NATO Research and Technology Symposium on Platform Innovations and Systems Integration for Unmanned Air, Land and Sea Vehicles*, Florence, Italy, May 2007.

D. J. Chang. and E. K. Morlok, 2006, "Review of Network Flexibility", *Proceedings of 11th International Conference of Hong Kong Society for Transportation Studies*, December 2006.

C. M. Chewar, K. L. Huggins, and J. R. S. Blair. "Avoiding the Pratfalls of Program Assessment." SIGCSE Bulletin (inroads), Vol 38, No. 4, December 2006. pp. 29 - 33.

R. DeCoste, K. L. Huggins, "Teaching Discrete Math for the First Time." ACM SIGCSE Bulletin. Vol 38, Issue 4. ACM Press. New York, NY, December 2006.

R. Dodge, and D. Cook, "Out of the Box Forensics," Proceedings of the 40th Hawaii International Conference on System Sciences - 2007, Kona, Hawaii, January 3-6, 2007.

J. C. Giordano and J. S. Ransbottom, "Diversity in Uniform: An Approach to Teaching Introductory Information Technology," (published in) Proceedings of American Society of Engineering Education (ASEE) 2007, NJ, March 2007.

W. Huang, F.C. Jain, "Pseudo Quantum Dot Behavior in InGaN-AlGaN Quantum Wire Lasers having Excitonic Transitions," Proceedings of *Connecticut Symposium on Microelectronics and Optoelectronics*, Yale University, New Haven, CT, March 2007.

W. Huang, F. Jain, "Reduced dependency of threshold current density on temperature in InGaN-AlGaN quantum wire lasers due to excitonic transitions," Conference presentation at *APS meeting*, West Point, NY, April 2007.

J. Nagle, C. Blais, R. Burk, B. Gates, N. Goeger and P. Richmond. "The Mobility Common Operational Picture Data Model: A Foundation for Conceptual Interoperability in the Domain of Ground Vehicle Mobility and Maneuver." *Fall Simulation Interoperability Workshop* conference proceedings 2006 (nominated for Recommended Reading List).

P. E. Patterson, J. M. Zara, "Real-time high-displacement amplified bimorph scanning mirror", *Proceedings of the SPIE, Optomechatronic Actuators, Manipulation, and Systems Control*. volume 6374, Boston, MA. 63740B, 2006.

P. E. Patterson, M. Dubey, J. Pulskamp, R. Polcawich, L. Currano, and J. Zara, "Piezoelectric polyimide scanning micromirror" *Proceedings of The 14th Annual Army Research Laboratory/United States Military Academy Technical Symposium*, November 2006.

E. Ressler, J. R. S. Blair, T. Markow, "Catch that Speeding Turtle: Latching onto Fun Graphics in CS1," SIGAda Conference, Albuquerque, NM, November 2006.

C. W. Reynolds, "Engineering the Information Technology Curriculum with Pervasive Themes," ACM SIGITE'06, Minneapolis, MN, October 2006.

B. A. Ring, J. S. Ransbottom, J. Giordano, "Problem Solving Through Programming: Motivating the Non-Programmer" Eastern Conference of the Consortium for Computing Sciences in Colleges, Patchogue, NY, October 2007.

A. Rodriguez, P. Yarlagadda, F. Alomoody, F. Papadimitrakopoulos, W. Huang, J. Ayers, and F. Jain, "Characterization of Cladding and Core Strain and Thicknesses in ZnCdSe-ZnSe Cladded Quantum Dots Using Wide Angle X-ray Diffraction and PL Data," Proceedings of *Connecticut Symposium on Microelectronics and Optoelectronics*, Yale University, New Haven, CT, March 21, 2007.

L. Shay, K. L. Huggins, J. Blair, B. Shoop, "Increasing the Efficiency of an Effective Outcome Assessment Process: Perspectives from an Electrical Engineering and a Computer Science Program" submitted to the International Journal of Engineering Education.

E. Sobiesk, J. R. S. Blair, J. Cook, J. C. Giordano, B. Goda, and C. W. Reynolds, "Designing an Interdisciplinary Information Technology Program," in *Proceedings of the ACM Special Interest Group for Information Technology Education (SIGITE) Conference*, October 2006.

W. Suchan and E. Sobiesk, "Strengthening the Weakest Link in Digital Protection," *IEEE Security and Privacy*, vol. 4, no. 6, pp. 78-80, Nov/Dec, 2006.

W. Suchan, J. R. S. Blair, D. Fairfax, B. Goda, K. L. Huggins, M. Lemanski, "Faculty Development in Information Technology Education," ACM Special Interest Group for Information Technology Education 2006 Conference (SIGITE 2006), Minneapolis, MN, October 19-21, 2006.

P. Stanton, Unit Immersion in Mosul: Establishing Security in Transition, *Military Review: The Professional Journal of the U.S. Army*, pp. 60-70, July-August, 2006.