In this issue: Debris-phobic Coatings, Women's Technology Leadership Group

ISSUE 02 - AUG 2017

HRL HORIZONS

Future Proofing the Internet

HRL Science in Cybersecurity

HRL® LABORATORIES

HRL HORIZONS STAFF

Creative Director
Michele Durant

Technology Writer
Shaun A. Mason

Contributing Writers
Parney Albright
Leslie Momoda
Son Dao

Photos
Dan Little
Bryan Ferguson
Julian Grijalva
Geoff Ramos
Getty Images

HRL HORIZONS Online
Bryan J. Ferguson

HRL HORIZONS
is a publication from HRL Laboratories, LLC's Multimedia and PR Department

Printed in the USA - August 2017

MS16524 - TICR 17-178

About HRL

HRL is the largest employer in Malibu, California with over 500 employees on our campus overlooking the Pacific from the Santa Monica Mountains. Although all HRL scientists and engineers are U.S. persons, 43% were born in other countries. Among them, 99% hold advanced degrees and 82% have doctorate degrees. Our diversity is a strength that enriches our organizational growth and development and ensures a breadth of perspectives from around the world with wide-ranging technical knowledge. Since 1960, HRL scientists and engineers have led pioneering research and provided real-world technology solutions for defense and industry. We are recognized for our world-class physical science and engineering research laboratories as well as our significant contribution to national defense.

HRL PHOTO COURTESY OF GEOFF RAMOS

CONTENT

05 A WORD FROM SON DAO

HRL's leader of computer science research opens our 2nd issue with thoughts on the growing cyber ecosystem and the challenges our scientists face in securing information from current and future threats.

06 A LOOK BACK

A fun trip into HRL's past with stops every ten years all the way back to Howard Hughes' original idea for a research and development laboratory.

08 **FEATURE: Future-proofing the Internet**

HRL researchers tackle the toughest problems facing the future of our advancing computer-dominated society, including biometric encryption, autonomous vehicle security, and quantum networking.

07 HIGHLIGHTS

Exciting news features and items of historical importance since our last issue.

14 DEBRIS-PHOBIC COATINGS

Scientists from HRL's Sensors and Materials Laboratory use nanotechnology to combine disparate materials into coatings with amazing new properties.

16 NEW AMPLIFIER CIRCUIT

As defense technology becomes more advanced, HRL's new amplifier will help keep communications clear through cluttered radio signals and jamming attempts.

18 WOMEN'S TECHNOLOGY LEADERSHIP GROUP

In this issue, A Look Inside examines HRL's efforts to support leadership among its women scientists and its outreach to middle school students to spark interest in STEM careers.

22 INTELLECTUAL PROPERTY

A look at the technologies described in this issue and what lies beyond.

23 WHAT'S NEXT

HRL Vice President Leslie Momoda concludes the issue with a forward-looking roundup of current HRL programs and research successes we hope to see in coming years.

HRL Laboratories, LLC, Malibu, California (www.hrl.com) is a corporate research-and-development laboratory owned by The Boeing Company and General Motors specializing in research into sensors and materials, information and systems sciences, advanced electromagnetics, and microelectronics. HRL provides custom research and development and performs additional R&D contract services for its LLC member companies, the U.S. government, and other commercial companies.


HRL LABORATORIES

A WORD FROM SON DAO

Director, Information
and Systems Sciences Laboratory

The Internet of Everything (IoE) describes the online world of all our connected devices, not just our computers and phones, but vehicles, appliances, buildings and even infrastructure. The IoE grows more autonomous and complex every day. HRL researchers are developing new technologies in computer network resiliency and user verification to take cybersecurity to the new level made necessary by IoE expansion.

The cybersecurity ecosystem comprises computer hardware, software to control the hardware, and humans who program the software. Because of unsafe computing habits and programming errors, the human factor is the primary source of system vulnerability. With these increasingly interdependent cyberphysical systems, maintaining the current paradigm of software development and analysis will result in highly insecure, unreliable, and brittle systems. As systems are deployed that operate more autonomously, cybersecurity resilience and safety remain research challenges, particularly in mixed environments with humans or older human-operated systems. Safe autonomous decision making will require methods that use control algorithms that are mathematically verified.

Securing the cyber ecosystem is no longer just a matter of building higher and higher walls around programs to keep out attackers. Hence, new tools are needed to make software resilient to attacks from outside their networks and to human programming errors within their networks. Future software will need to be machine-checkable and human-friendly, with demonstrable resilience and security assurances. Tools are also needed that can analyze complex system architectures and provide guarantees on performance of subsystems as the architecture is being designed and integrated. Software development toolchains need to be able to mix software components of different security assurance levels without introducing potential weaknesses into the system.

User-friendly, secure codes that are mathematically provable to be secure are needed to withstand attackers with ever-increasing computing capabilities. Secure, privacy-aware infrastructure and software will be key competitive advantages in coming decades for those desiring to enter the IoE marketplace. As a practical matter, there will be a need for over-the-air software updates, software patch authentication and verification, IoE sensor and mobile data logging, and cloud-assisted storage and computation. Infrastructure and software platforms need strong cryptography to ensure confidentiality, integrity, and non-repudiation of stored and communicated data at rest and in transit.

We also are exploring the huge research space of using algorithms to protect users regardless of their vulnerability to manipulation. Some attackers target people by exploring interests and passions mentioned in their visible social media accounts. An attacker might use an individual's interests to capture critical organizational information. Many large cyberattacks have been initiated through these types of smaller social media engineering attacks. This has created a need for proactive behavior analysis tools that incorporate social, political, economic, cultural and other principles to protect the human connected to the social media account.

In the ensuing pages of *HRL Horizons* we will discuss in greater detail many of these issues. As the world moves toward ever greater connectivity, HRL is meeting the associated challenges head-on. ■

A LOOK BACK

HRL's story reaches back through the history of innovation and technology to the glory days of 20th century aviation when men like Howard Hughes were setting speed and endurance records in the latest propeller-driven aircraft. Jumping back a decade at a time, this brief tour of HRL history reveals many fascinating and exciting discoveries that have made life better through science.

70 years ago

In 1948, The Electronics and Guided Missile department of Hughes Aircraft Corporation branches off to create Hughes Research and Development Laboratories. Headquartered in Culver City, Ca., Hughes R&D employs 150 people. Its founding mission is to upgrade microwave systems by developing better travelling wave tube transmitters, ultra-low-noise microwave maser receivers, and improved radar display devices. Former Caltech classmates Simon Ramo and Dean Woolridge serve as co-directors.

60 years ago

In 1957, Hughes researchers work on an atomic clock using an ammonia maser oscillator. With improvements in size, weight and power of atomic clocks they eventually become key to global navigation satellite systems and global positioning systems. In later years, atomic clocks become key to internet applications that require accurate frequency and times standards and long-baseline interferometry, an important investigative technique in radio astronomy.

50 years ago

In 1967, ultra-high-energy ion implantation is developed for integrated circuits in gallium arsenide, gallium nitride, and indium phosphide devices. These circuits enable greatly enhanced targeting radar for fighter planes. Two years before, Robert Bower invents the self-aligned gate field-effect transistor (SAGFET), the device soon to become the basis for all modern integrated circuits.

40 years ago

In 1977, Hughes Research Laboratories develops gallium arsenide solar cells, which are highly efficient for satellites and military applications. Kamath and Mitchell invent liquid phase epitaxy of mercury cadmium telluride (HgCdTe) for manufacture of semiconductors for infrared sensors, which becomes the industry standard for the next 20 years.

30 years ago

In 1987, Building 254 is completed. R.W. Schumacher and colleagues pioneer the crossatron, a high-power modulator device that combines the best features of thyratrons, vacuum tubes, and power semiconductor switches. The DARPA-funded Autonomous Land Vehicle (ALV) becomes the first cross-country map and sensor-based autonomous robotic vehicle. ALV team members Mike Daily & Dave Payton help develop some of the first algorithms to analyze lidar sensors.

20 years ago

On December 17, 1997, the Hughes Research Laboratories facility is legally renamed HRL Laboratories, LLC. The Hughes Research Laboratories' Xenon Ion Propulsion System (XIPS) program completes 30 years of research culminating in the launch of the first NASA satellites with ion propulsion thrusters. Ion thrusters are many times more fuel efficient than chemical rockets.

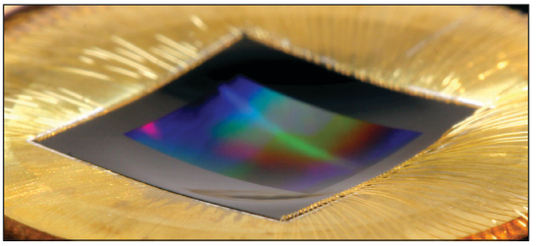
10 years ago

In 2007, HRL achieves its 300th issued patent since becoming a limited liability company in 1997 and receiving its first issued patent in 2000. HRL releases SwarmVision, a video content analysis software package that consists of modules installable on PCs running Windows 2000 or XP. Encompassing many applications, it includes visual object recognition and tracking, video analysis without motion or background estimation, and behavior recognition. HRL scientists publish their first paper on self-propagating photopolymer microlattice material. HRL launches the Advanced Electromagnetics Laboratory with Dan Sievenpiper as its first director.

In 1987, Building 254 is completed.

HIGHLIGHTS

A look at the year's biggest achievements and news



HRL Creates Breakthrough Curved Camera Sensor

HRL, with research support from Microsoft, created a prototype curved-sensor camera that surpasses the sharpness of larger professional camera systems, while improving image uniformity and illumination. This work may lead to compact cameras with excellent performance in low light.

Given HRL Laboratories' extensive experience in electronics fabrication and integration, Microsoft sought their collaboration for an innovative, low-cost process that transforms current flat sensor dies from high-volume silicon foundries into highly curved sensors. "The sensor has increased sensitivity, full-field resolution, and reduced packaging weight and volume," Dr. Geoff McKnight said. "This technology will enable a whole new class of lenses that weren't possible before. It can be applied to virtually any existing image sensor, so there is no costly redesign or new material development required."

Promising Transcranial Stimulation Featured at Conference

Dr. Praveen Pilly represented HRL at the 3rd Annual Brain Initiative Investigators meeting with his presentation entitled *Improving Memory Performance by Augmenting Consolidation with Transcranial Stimulation* in the plenary session on "Applications of BRAIN Technologies." The conference was sponsored by the National Institutes of Health members who are participating in the White House BRAIN Initiative and the National Science Foundation, the Intelligence Advanced Research Projects Activity (IARPA), and Defense Advanced Research Projects Agency (DARPA).

As part of DARPA's RAM Replay program, a multipronged approach was tested for accelerating skill acquisition, learning, and memory consolidation through transcranial electrical stimulation during learning and sleep. The team is also focused on understanding neurophysiological mechanisms underlying enhancement of sleep consolidation with noninvasive brain stimulation.

3D-printed high-strength aluminum

SML researchers Hunter Martin and Brennan Yahata are first to successfully use additive manufacturing (3D printing) to create parts from high-strength aluminum. Besides aluminum alloys desirable in automotive and aircraft engineering, the technique —nanoparticle functionalization— can be applied to any metal, can be used with current 3D printing equipment, and can make any unweldable metals weldable.

This revolutionary technology will enable additive manufacturing of aluminum alloys with more than double the strength of the most commonly produced additive aluminum alloy.

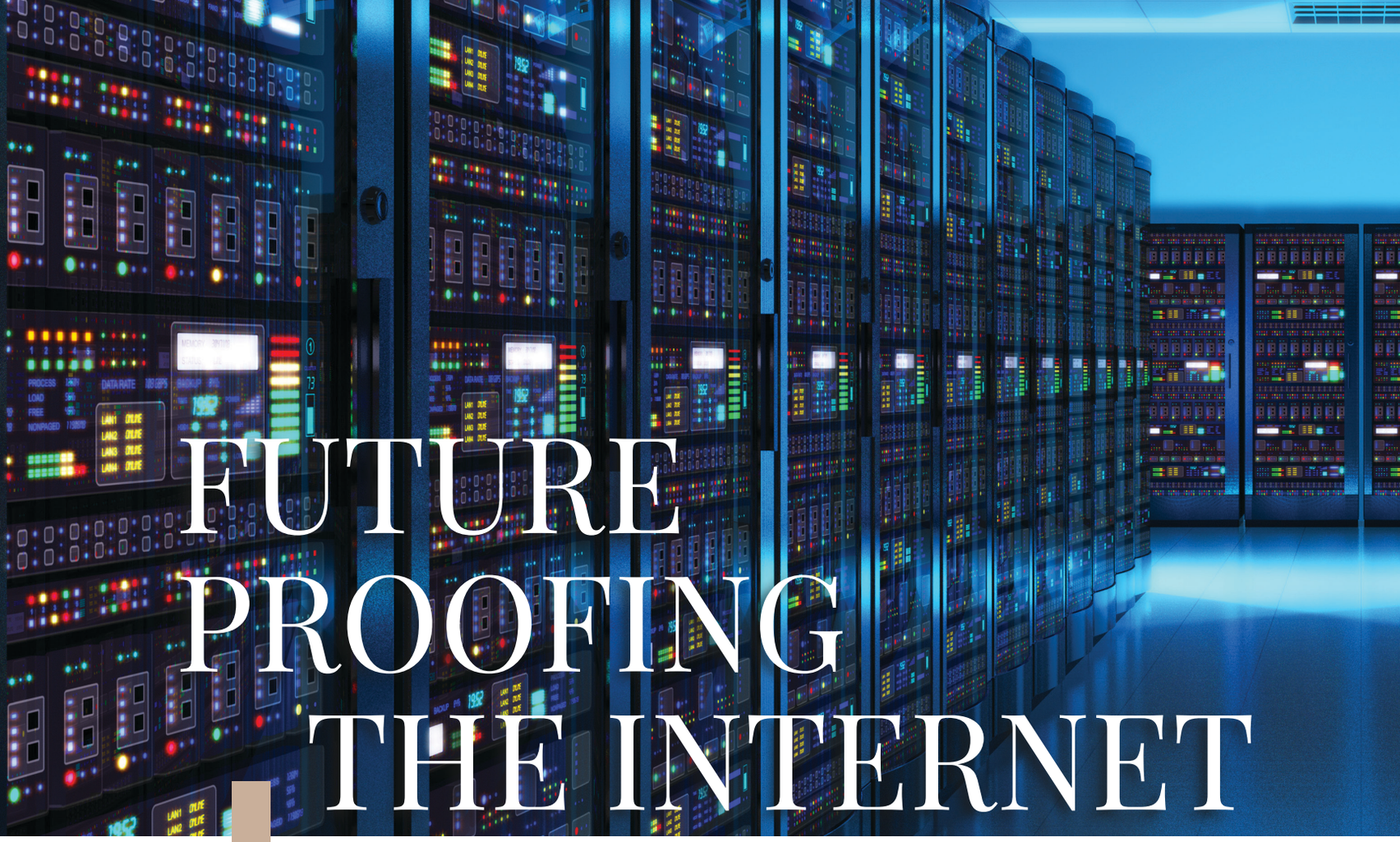
HRL Team Receives IEEE Best Paper Award

Deepak Khosla, David Huber and Yang Chen from HRL's Information & Systems Sciences Laboratory, received the Best Paper Award at the 2017 IEEE Homeland Security Symposium. The paper was entitled *Automated scheduling of radar-cued camera system for optimizing visual inspection and detection of radar targets.*

Authors: Deepak Khosla (top), David Huber (left), Yang Chen (right)

MITRE adds Paul Kaminski to Board

MITRE Corp. said this week it has added HRL Board Chairman and former Pentagon official Paul Kaminski to its board of trustees. Kaminski was Undersecretary of Defense for Acquisition, Technology and Logistics from 1994 to 1997 and was chairman of the Defense Science Board from 2009 to 2014. Until recently, he was chairman of RAND Corp.'s board of trustees. MITRE is a not-for-profit company operating multiple federally funded research and development centers.



FUTURE PROOFING THE INTERNET

HRL Science in Cybersecurity

As the 21st century turned, cybersecurity was a young but growing concern among industry and government computer experts. In 2009, HRL launched its first cybersecurity research project, which was the beginning of a continuing concentrated effort to solve problems in cybersecurity. The number of HRL projects, and funding for them, grew rapidly from that point as HRL teams took a long hard look at the need for immediate cybersecurity approaches as well as how future difficulties would be met. HRL Laboratories' world-class scientists were already at the forefront of computing technology, microelectronics, and software development, and this new area became a primary focus of HRL research.

Within the cybersecurity ecosystem, approaches focused on setting up perimeter defenses and discovering and patching known vulnerabilities have been found to be inefficient and ultimately ineffective for securing computer networks. Tools are needed by software engineers to set up defenses and mitigate the damage caused by the constant threat of cyberattack, regardless of its manifestation. HRL scientists are developing new approaches to this technology that soon will be available to the public to improve global online security. HRL Laboratories has brought its world-class core competencies to bear on several of these areas.

A fast-growing threat

When William Gibson coined "cyberspace" in his 1984 novel Neuromancer—presciently describing an environment in which the world was connected by a computer network—only ARPANET existed. It was a small network of university computers constructed by the Advanced Research Project Agency (ARPA) to test and share computer resources. Gibson had no idea that his then-speculative term would become one of the

most commonly used words of the 21st century, nor did ARPA scientists anticipate that their small communications experiment would grow within a generation to become the electronic infrastructure on which world communications, commerce, finance, and defense depends.

The internet is a technology for which the speed of adoption and pervasiveness of reach have few comparators throughout human history. It was a revelation, and the very definition of a paradigm change. The life-changing ability to share all information with anyone at the touch of a fingertip, to conduct commerce globally in an instant, and to connect people who would never have had the chance to meet surprised everyone. And nearly the last question asked by almost anyone building or using the internet was how to keep this amazing, ever-expanding network secure. Early on there were not even reasons to consider internet security. From the very beginning, the internet was designed to facilitate access with no consideration toward preventing electronic mischief, network vandalism, or data theft.

The first cyberattackers were seen by many as antihero outsiders—nerd buccaneers who demonstrated their prowess by showing up the establishment with internet pranks. The image of the lone-wolf malcontent living in his mother's basement is still the stereotype many people conjure when they think of cyberattacks. The reality is far more chilling. Real-world cyberattackers can be large organized criminal enterprises, government-sponsored operators, or military personnel—deployed in great numbers with powerful resources by nation-states—who go online attempting to undermine social and economic stability of targeted countries, ultimately threatening their national security. The country under cyberattack more than any other is the United States.

Large-scale cyberattacks against health systems, retailers, corporations, and governments have become commonplace in the second decade of the 21st century. The Department of Homeland Security's Office of Cybersecurity and Communications recorded 350,000 attacks between October 2013 and May 2014, 120,000 more than the full 12 months before. Among stolen data were sensitive personal information, valuable intellectual property and trade secrets, and information to diagram industrial control systems for future attacks. Keeping our computerized world safe has moved to the fo-

> Researchers have demonstrated their ability to electronically attack cars [...]. Resiliency will be an absolute necessity as vehicle designs eventually rely completely on software for safety and decision making.

MAST TEAM (L TO R): Srinivas Nedunuri, Pape Sylla, Alexei Kopylov, Alexander Graber-Tilton, Nick Brument, Michael Warren, Kevin Martin, Gavin Holland, Aleksey Nogin, and Darrel Van Buer. Not pictured: Alana McRoberts

Mixed Assurance Technology

Tools to Build Secure Autonomous Vehicle Software

Software that controls critical systems in vehicles needs to have high assurance of resilience against malicious attacks or malfunctions caused by programmer errors. DARPA embarked on the High-Assurance Cyber Military Systems (HACMS) program after several breakthroughs enabled construction of certain high-assurance software components. HRL's challenge was to make a high-assurance system using these technologies.

Not all software components are equally important to a system, and some are more difficult to achieve high assurance for. Thus, HRL researchers compiled a development toolchain that can build software with a hierarchy of multiple assurance levels. This makes a resilient overall systwem, but does not require the same full resilience for every component, based on a component's importance or difficulties in making some less important components secure.

Systems built this way make partial progress towards high-assurance for some components (medium assurance), and none for others (low assurance) based on their importance to the system. The challenge becomes integrating the assurance levels so the low-level components do not become an avenue for cyberattackers to compromise the higher assurance software.

The Mixed-Assurance Software Toolchain (MAST) enables combining the resiliency of higher-assurance components with full functionality of the easier-to-create lower-assurance ones. The high-assurance components protect the lower assurance components from outside attack and internal programming errors. The lower assurance components function normally and are prevented from becoming an avenue of attack against the higher ones. With this toolchain, all components need not be high-assurance, while the overall system requires less effort to remain highly resilient overall. Through integration of mixed assurance software components, MAST can be used to build software that solves many problems inherent in autonomous vehicle cybersecurity.

MAST was assembled from individual tools into a coherent toolchain by the HRL team led by Aleksey Nogin and funded as part of DARPA's HACMS program. It enables software to be engineered to keep cyberattackers out of the system.

DARPA's goal was to demonstrate that this level of assurance was achievable on real systems, so the HRL team was provided with a self-driving heavy equipment transport (HET) truck to test MAST on. Large autonomous vehicles are of great help to the military, allowing chains of driverless trucks to convoy across hostile landscapes where they might be attacked. Soldiers that do not have to drive vehicles can shoot back, or do not have to be in danger at all. If cyberattackers gain control of one or more of such vehicles, they could become destructive weapons that are very difficult to stop.

The HRL team was able to make the HACMS software work on the HET, preventing a team of computer experts from successfu-

refront of national defense and HRL research, and is a high priority for good reason. The US government defines cybersecurity as:

Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.

Clearly, the vastness of the effort to create a safer internet is beyond the scope of any single company, research institution, or government agency. Ultimately, one key to cybersecurity may be a people problem, requiring us to change our habits and accept more stringent access points to reduce the possibility of leaving a door open for a cyberattacker. This may especially be true of social media, through which some perpetrators of major cyber break-ins have revealed as their pathway to corrupting large networks.

In the early decades of internet connectivity, information was sent back and forth from client servers, but now data is distributed across multiple locations such as cloud servers and peer-to-peer networks. The development of the internet of things—including smart factories, retail stores, healthcare systems, and critical infrastructure—makes cybersecurity a vastly greater undertaking than simply protecting stored data. Disruptions could affect public safety and put lives at risk.

After fingerprints are taken, the fuzzy extractors are used to extract a random string of data from the digitized fingerprints.

Protecting biometric data

The value of HRL cybersecurity research became more obvious when the 2015 cyberattack on the US Office of Personnel Management (OPM) resulted in theft of personal data of millions of government employees and security clearance applicants, including nearly 6 million sets of fingerprints. Some identity data such as names, addresses, and even social security numbers can be changed, but not fingerprints. This type of biometric information can always be used to identify its owner. If that owner has a security clearance, the frightening implications of this type of theft by an adversary are obvious.

With typical digital fingerprint storage systems, even when data is encrypted it can be stolen as part of a back-end data theft, such as the one at OPM. The fingerprints can be decrypted later, especially if the cyberattackers are able to steal the decryption key along with the data, as is often the case with much current data storage methods.

A team of researchers in HRL's Information and Systems Science Lab (ISSL) are using cryptographic algorithms to protect biometric data. Algorithms called fuzzy extractors enable the researchers to extract a cryptographic key from any biometric or physical trait—such as fingerprints—that is used for authentication or access control.

"After fingerprints are taken, the fuzzy extractors are used to extract a random string of data from the digitized fingerprints. The random string is the only reference to the fingerprints stored in the database," said Chong Ding, the ISSL researcher leading the team. "To authenticate someone's identity based on the fingerprints, their prints are taken again, and with computer processing the random strings can be used to verify that the new fingerprints match those from which the strings were extracted."

With this technology in place, biometric identification could be completely protected from exposure by cyberattack, even if it is stolen. If thieves obtain the data, the HRL mathematical proofs show they cannot decrypt the random strings to recreate the fingerprints. Although in early development, the fuzzy extractor concept should be expandable to any other digitally stored biometrics, which could include corneal scans, full hand prints, or eventually facial recognition.

lly assuming control and doing damage to obstacles with the HET. The autonomous truck followed its initial instructions without glitches and could not be commandeered. The final successful HACMS demonstration was completed in April 2017.

HRL will continue with the next steps, which include a MAST tutorial for the United States Army Tank Automotive Research, Development, and Engineering Center (TARDEC), teaching them how to use the MAST tools. HRL will also begin a new project to apply HACMS technology to a Navy system. Although not yet fully available to the public, significant parts of MAST not created by HRL are available as open-source software.

With the MAST project, the HRL Laboratories team showed that given tools they had never used before and platforms they were not familiar with, they were able to developing a working cybersecurity platform in a relatively short time that determined cyberattackers could not penetrate. ■

Autonomous vehicle security

With full vehicle autonomy on the horizon, engineers and others are integrating more smart technology into current designs. Vehicles are more connected to each other through the internet of things and their systems are becoming more reliant on software than mechanics. Military and civilian cars and trucks are becoming veritable computer networks on wheels. With expanding connectivity comes vulnerability and greater need for attack resilience. Fully and partially autonomous vehicles are complex because they combine artificial intelligence and machine learning with sensor arrays for control, which makes them vulnerable to cyberattack.

ISSL senior researcher Aleksey Nogin and his colleagues are focused on projects to make cyberattacks ineffective against software for any cyberphysical system, including vehicle autonomy systems. To be thorough, the team must consider two types of concerning attacks against vehicular software. As with non-vehicle software systems, the cyberphysical software can be vulnerable to network attacks in which enemies send malicious messages trying to confuse the electronic network and disable or control the vehicle, but software in a cyberphysical system must also be prepared for more direct physical attacks. In those situations, enemies might try to spoof or disable the vehicle's many sensors, such as deploying obstruction decoys to confuse radar, sonar, and lidar or fooling cameras with bright lights or lasers.

Nogin's team has assembled software development tools into one toolchain as part of the High-Assurance Cyber Military System (HACMS) project funded by the Defense Advanced Research Project Agency (DARPA). HACMS mathematical tools can be used to build software that is resilient to both types of cyberphysical attacks. The HACMS team uses formal methods to produce mathematical proofs of the software's resiliency. With the HACMS tools, software is engineered to maintain its original function and do nothing else, regardless of network interference or attempts to fool its integrated sensor arrays. This allows developers to trust the assurance of the mathematics, not a human programmer or tester. Humanity is often the weak link in network security.

"Instead of trying to plug holes in a dam as they appear, the HACMS tools are used to build a dam that from the beginning cannot be penetrated. Despite attempts in a very wide range of attack behaviors, the system still works. Unlike antiviral programs, the software does not actively repel particularly identified attacks, it is designed from the outset to do the right thing—according to its initial programming—no matter what happens," Nogin said. "This enables a system that is far more robust than one that must always play catch-up to repel the latest evolving malware. The software built with the HACMS tools keeps going and ignores attack attempts."

> "Our technologies will enable creation of autonomous functionality that is highly attack-resilient."

Nogin and colleagues were originally tasked by DARPA to test some of the tools by making resilient software for a passenger vehicle. Using a 2013 model year American-made vehicle they successfully demonstrated a highly attack-resilient controller. The test vehicle was not fully self-driven, but had adaptive cruise control and some autonomous capability. This HACMS proof-of-concept testing showed that the controller kept track of vehicle speed and it knew when to slow down if there was an obstacle in the road.

"Our technologies will enable creation of autonomous functionality that is highly attack-resilient. The software we create comes with a mathematical proof that under certain assumptions the software will do exactly what it is supposed to and nothing else. That means there is an absence of a very broad class of bugs in the system, and that it will continue operating correctly when someone tries to mess with it," Nogin said. Nogin also said that in modern cars, drivers are mostly just telling the software what to do to control the vehicle, so whether the vehicle's system is guided by computer or human, resilience to cyberattack is critical. Researchers have demonstrated their ability to electronically attack cars in ways that disable the brakes, for example. Resiliency will be an absolute necessity as vehicle designs eventually rely completely on software for safety and decision making. Because of the safety issues involved, it is DARPA's and HRL's goal to make the output from the HACMS project open-source.

Policing the cloud

Any distributed computer system with internet connectivity over an extended period can and probably will be attacked and compromised. No business or government is completely safe and for many institutions cyberattacks are

relentless. Large institutions like the US government are on defense at all times against nation-state armies of organized cyberattackers.

Focused, skillful cyberattacks on one computer in a network can eventually break into nearly any system. HRL's Cloud Control Operations Plane (CloudCOP), is a network defense approach that operates with this type of attack in mind.

CloudCOP exploits the attackers' speed limit for compromising multiple computers and gaining network control with a distribution system that maintains full network availability and confidentiality even when a fraction of the computers has been compromised. CloudCOP protocols offer two separate defenses. First they prevent cyberattackers from doing any damage until they can control at least 25-30% of all the computers in a CloudCOP-protected conglomerate. Second they enable periodic wiping and rebooting of every computer in the conglomerate, proactively cleaning them. This means that attackers can no longer creep up slowly to gain the 25-30% control threshold. Unless they can attack with unlikely speed, taking over many computers in quick succession, they lose any footholds they might have gained from successful attacks. Thus, they never achieve the threshold needed to do any damage.

Consider a very powerful cyberattacker that can compromise a hypothetical 15% of computers in a system in the time it takes CloudCOP to refresh. The data is scattered on multiple computers, and will look indistinguishable from random noise to an attacker that does not reach the 25%-30% threshold. If an attacker is able to steal 15% of system data in one attack, the system refreshes before another 15% can be stolen. The data from the first theft are not compatible with the data from the second, so despite repeated attempts, the attacker will never reach the threshold to compromise the network.

Although this type of system has been used with small networks of a few computers, HRL's CloudCOP project has significantly improved the cryptographic protocols to achieve success in networks using hundreds of computers. This enables system users to hide data for a particular job by randomly rotating it from one computer to another across the network. If a cyberattacker intends to compromise a particular computer that has a desired set of target data on it, they will not be able to distinguish it from all the computers on the network. Even if a powerful cyberattacker gets lucky and hits the right computer, the data refresh will render their initial theft incompatible with the subsequent data, and therefore useless. CloudCOP also continues working according to its initial programming regardless of attacks. CloudCOP cybersecurity tunability makes it possible to maintain protection without having to use maximum effort at all times.

> "Quantum networks provide a way of transmitting cryptographic data across public networks without risk of cyberattack."

THADDEUS LADD AND JIM HARRINGTON

Quantum networking

"Quantum networks provide a way of transmitting cryptographic data across public networks without risk of cyberattack," said HRL researcher Thaddeus Ladd. "Such networks enable communication between parties without the worry of eavesdropping."

Ladd and fellow researcher Jim Harrington lead an HRL team exploring quantum communications networks that exploit a quantum state called entanglement. When two particles, such as photons, are entangled, they share their quantum information identically over distance. Using an encryption method called quantum key distribution, two parties may choose a truly random key to encrypt communication to each other without revealing the key. Any attempt to tap into such a network creates noise in the signal, revealing the cyberattack attempt and exactly what information was compromised, through statistical analysis. The communicating parties are then able to stop and take informed action.

The quantum entangled information can be transmitted to another photon farther down the line through a process called teleportation. Teleportation does not transport the actual photon particle, but all of its information to the receiving particle. With teleportation, information

Continued on page 22

HRL Scientists Use Nanotechnology to Create Durable Coatings

MAKING CARS & AIRPLANES *DEBRIS-PHOBIC*

The Scaled Nanotechnologies Group in HRL's Sensors and Materials Lab develops durable coatings that can be sprayed on and have unprecedented properties, such as eliminating adherence of insect debris or ice, for aircraft and automobile exteriors.

"The goal of our group is to use nanotechnology to create coating materials with extraordinary performance that are very durable," said Adam Gross, the group's lead researcher. "Rather than make small samples of successful materials, we scale them up to a size that will cover a car door or an airplane wing."

Gross emphasizes that combining durability with performance usually is an engineering trade-off. Materials with desirable properties such as repelling water or debris do not last long and can even be wiped off, and materials with high durability do not provide these types of properties.

"Our approach for obtaining durability and performance is based on finding materials with very different properties and combining them at the right scale to get the best of both properties, not a poor average, which is the usual outcome," Gross said. "Durability and scalability result from the material choices and structure."

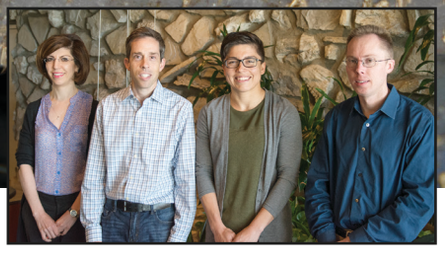
Airplane and car designs rely on aerodynamics to make vehicles as "slippery" as possible as they move through air. Whether flying or driving, a vehicle's interaction with the air flowing over it can affect fuel efficiency. Drag on a vehicle can reduce maneuverability, especially at higher speeds. A vehicle fighting wind resistance requires more power to maintain the same speed as a more aerodynamic vehicle, thus consumes more fuel per distance traveled.

Although modern vehicle designs are painstakingly tested for maximum reduction of drag and wind resistance, the environment a vehicle travels through can adversely affect aerodynamics in many ways. Besides precipitation, ice can also build up on wings, hoods, covers, and headlights.

Coatings to lessen environmental effects require highly dissimilar materials combined to attain properties that no single material has. "High-performance next-generation coatings require combinations of highly contradictory properties that need to be expressed at the surface. You can't get this type of performance with traditional materials," said Andy Nowak, a researcher with the group. "We combine elements that don't play well together into a single material that gives us novel performance."

For example, by combining antifreeze type materials with nonstick Teflon-like materials, a coating can be made that is "ice-phobic," designed to delay freezing and prevent ice from adhering to a surface such as an airplane wing. With these properties combined in one substance, even if ice forms on the coated wing, it is easily shed from the non-stick surface by motion or wind. Mud, dust, and slush can also roughen air flow, as well as obscuring head and tail lights. These problems are accentuated as the world moves toward a future with autonomous vehicles, which have multiple arrays of cameras and sensors that can be fouled and obscured by the elements.

In warmer climates with large insect populations, cars and airplanes can become inundated with detritus as bugs splatter against them at high speeds. For "bug-phobic" materials, a nonstick element is combined with a lubricating element that draws in water from its



The goal of our group is to use nanotechnology to create coating materials with extraordinary performance that are very durable. Rather than make small samples of successful materials, we scale them up to a size that will cover a car door or an airplane wing."

SCALED NANOTECHNOLOGIES TEAM MEMBERS Maryam Behroozi, Adam Gross, April Rodriguez and Andrew Nowak.

environment to make a coating that stays very slick on its surface. This combination of properties repels debris of splattering insects, preventing it from building up and affecting vehicle performance.

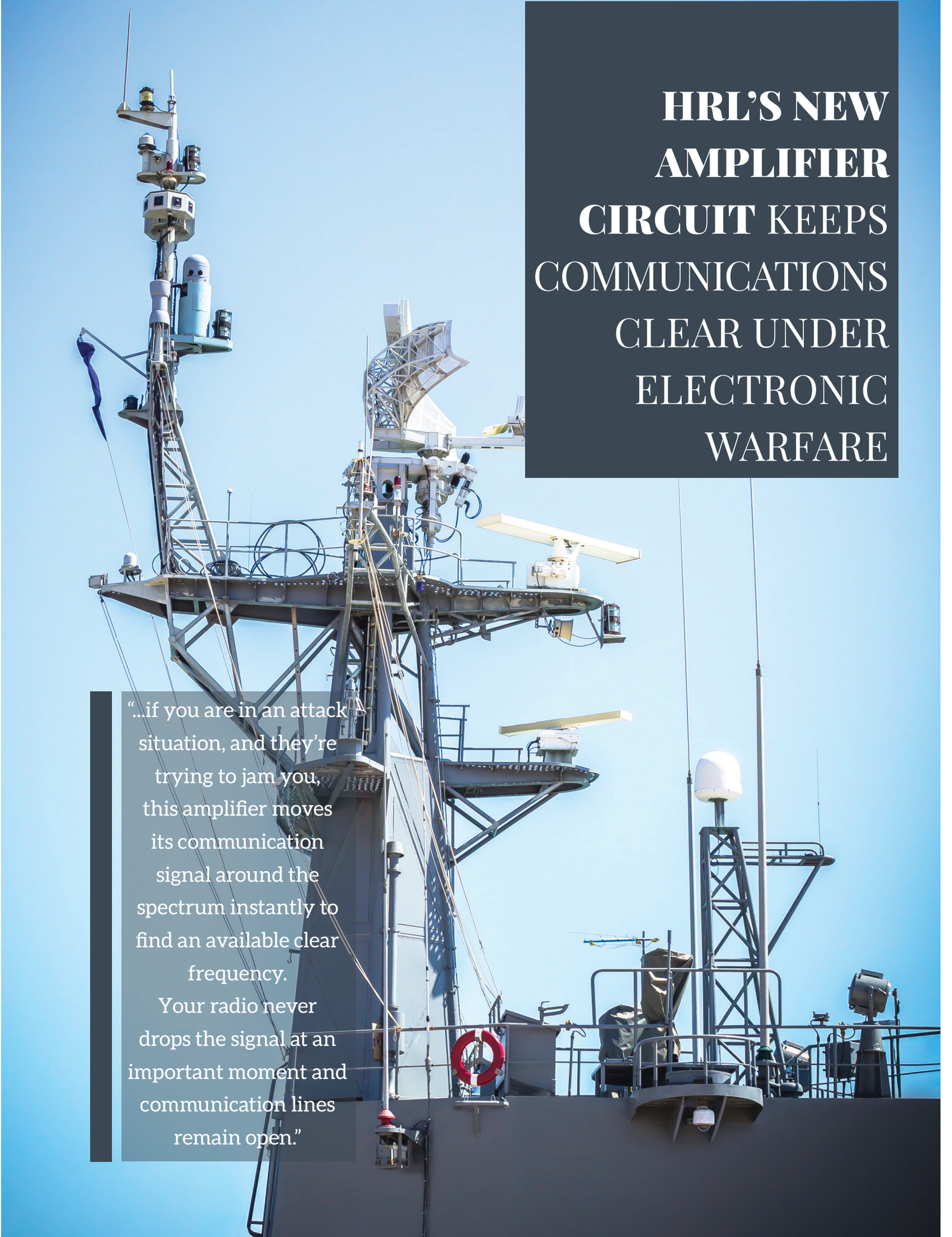
Testing for this coating is done with a "bug cannon" apparatus that uses compressed air to launch anaesthetized crickets and fruit flies against a coated surface at speeds up to 125 miles per hour. This material also is showing promise for repelling mud and road salt slush.

"So far results have been very positive for ice-phobic and bug-phobic coatings," said researcher April Rodriguez. "Our team hopes to expand our debris-phobic toolkit to include anti-mud, anti-corrosion, and anti-smudge coatings. These types of coatings could greatly lessen or eliminate the need to wash your car or wipe off your smartphone."

Getting the disparate materials to combine when they normally would repel each other is the core the of the Scaled Nanotechnology Group's focus. As their name suggests, they are not attempting to mix materials in the common way, but are bonding them at the molecular level and letting forces present between materials assemble into larger length scale structures. This means they begin by combining molecularly bonded precursors into more useable blocks of material. For example, using organic polymers that normally would not mix, they build a microstructure with one polymer around the other that makes a new material with the desired properties of both. They then increase the scale of the material to coat an exterior surface.

"We don't want to do a new process for every project," Gross said. "We'd like to have a toolbox that is agnostic to the type of material. This way we can simply choose the properties we want and combine separate materials with those properties to get the desired coating."

The other members of the Scaled Nanotechnologies Group are Maryam Behroozi, Shanying Cui, Michael Gervasoni, Jason Graetz, Sharon Guan, Russell Mott, Ashley Nelson, Elena Sherman, Adam Sorensen, Souren Soukiazian, John Vajo, and Shuoqin Wang. ■



HRL'S NEW AMPLIFIER CIRCUIT KEEPS COMMUNICATIONS CLEAR UNDER ELECTRONIC WARFARE

"...if you are in an attack situation, and they're trying to jam you, this amplifier moves its communication signal around the spectrum instantly to find an available clear frequency. Your radio never drops the signal at an important moment and communication lines remain open."

Defeating Signal Jammers with Wide Band of Frequencies

Scientific discoveries are often driven by defense requirements in a world that relies every day on leading-edge electronics systems needed by the armed forces to negotiate daily life in a high-technology society. The US Navy of the 21st century needs communications systems that are reliable in extremely adverse conditions. HRL engineers working with the Office of Naval Research (ONR) are constantly exploring emerging technologies to help meet the demands of a modern maritime force.

Exemplifying that effort, a team from HRL's Microelectronics Lab (MEL) led by Jeong-Sun Moon has developed a linear wideband distributed amplifier circuit to enable clear, consistent communication between systems operating in some of the world's most difficult situations. Measuring 2mm x 3mm, this tiny but powerful circuit can amplify a communications signal with very high spectral purity and dynamic range for transmission or reception with greatly reduced harmonic distortion. Funded by the ONR, this work was presented in 2016 and 2017 at the annual IEEE Radio & Wireless Week Conference.

"What makes the circuit special is that it operates on a wide band of frequencies," Moon said. "In electronic warfare with very cluttered electromagnetic environments, dynamic spectrum access is very important. For instance, if you are in an attack situation, and they are trying to jam you, this amplifier moves its communication signal around the spectrum instantly to find an available clear frequency. Your radio never drops the signal at an important moment and communication lines remain open. Also, in complex situations when many people may be communicating simultaneously, radio frequency signals mix. This causes distortion to all signals and the overall communication quality drops. The signal purity of this linear wideband amplifier keeps communication clean and clear at all times."

Building a wide-band linear amplifier has been a difficult goal sought by many researchers leading to this discovery. Moon and his colleagues used high electron mobility transistors made from gallium nitride (GaN) because they enable transmissions with more power than other commonly used radio frequency transistors such as gallium arsenide (GaAs) devices. Because of the extreme linearity requirement over wideband operation, the HRL team had to develop a new approach to making the amplifier chain more linear, the key to achieving the desired purity of its amplified radio signal.

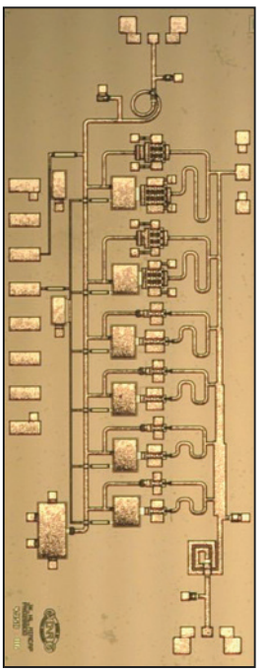
"Our amplifier's architecture has the wide-band distortion cancellation scheme built into it," Moon said. "This means that our patented circuit reduces harmonic distortion. We tested the clarity of the amplifier on 4G cellular systems and they came out very clean."

The applications of the amplifier are wide ranging as well. The amplifier could improve communication between ground forces, ships, aircraft, and even unmanned aerial vehicles (UAVs). As autonomous UAVs become more pervasive in combat scenarios, often in large swarms, the need for communication between them to coordinate missions grows exponentially. Because such drones can attain proximity to an enemy that would be extremely hazardous for human soldiers, the need for clear radio signals is paramount. Maintaining a clean radio frequency despite jamming attempts would be a clear advantage under combat conditions.

As with much defense technology, there is possible civilian use for the linear wideband amplifier as well. The technology is extremely relevant to base stations that want to cover as many cellular bands from as many carriers as possible. The electronic warfare radio frequency spectrum is wider than the cellular phone spectrum, thus the amplifier could easily be suited for cellular use.

"It's possible that in cell phones, because the spectrum would be narrower, we could make the amplifier more efficient, less expensive, and an easy fit into their power usage requirements," Moon said.

HRL's MEL continues to strive on the cutting edge of science for its customers and to bring new technology to the United States and the world. Other researchers on the linear wideband amplifier team were Jongchan Kang, Robert Grabar, Helen Fung, Peter Chan, Haw Tai, and Dave Brown. ■



CIRCUIT DIAGRAM OF NOVEL GAN POWER AMPLIFIER that demonstrated linear amplification over 100 MHz to 6 GHz for agile spectrum access.

A LOOK INSIDE

Women's Technology Leadership Group

HRL Laboratories' Women's Technology Leadership Group (WTLG) was developed for female members of the technical staff (MTS) with the specific goal of increasing diversity in the technical leadership at HRL.

Research shows that diversity in the workplace can increase productivity and have competitive advantages in the market.

Morale is higher in a diverse environment, with increased employee desire to succeed, thus work harder. Companies can offer more solutions for their customers because of new ideas that derive from a diverse and inclusive workforce.

The founding membership of WTLG was launched by HRL Vice President Leslie Momoda, who also serves as a leadership role model for the group. However, the fact that she stands out as a woman leader at HRL highlights the diversity problem. "I was director of the Sensors and Materials Lab at HRL, my predecessor was Mary Young, and the HRL vice president at the time was a woman, but that was it," Momoda said. "We've occasionally had women department managers, but not many. We asked ourselves why that was and what we could do about it, and the WTLG came about as a way for us to focus on mentoring women with leadership training and encouraging women to aspire to leadership roles."

HRL leadership saw that cultural and interpersonal concerns were elements that sometimes hamper ambition in women scientists. Women often perceive that success requires them to be more aggressive in business situations. Many women also can believe that unless they've had a tailored leadership experience, they will not be considered for leadership positions.

"When we looked for people we were interested in developing into leadership positions and who are promotable, there were not many women," HRL CEO Parney Albright said. "There are of course many factors involved, including the generally lower number of women in certain scientific disciplines, such as computer science. Most of the people who are promotable in senior management jobs now would have started 15 or 20 years ago, when it was still tough for women to get into the engineering and science disciplines, so the pool is smaller, but there are also cultural issues within society and within the scientific community that can discourage women from believing in themselves."

One WTLG approach is inviting outside speakers to talk to the group about what the models of success are and how one gets a place in the pool for leadership positions. Momoda stresses the importance of women seeing themselves in leadership roles, so many invited speakers are women leaders from

WTLG GUESTS have included executives from Boeing and General Motors, and NASA astronaut Dr. Mary Ellen Weber (shown above, top row, fifth from the left).

science and industry. Such guests have included executives from Boeing and General Motors, and NASA astronaut Dr. Mary Ellen Weber. "Mentors for women do not always need be female," Momoda also emphasized. "My mentors were always male, and there was never a point at which I couldn't understand what they were saying or felt that my gender affected their attitude toward guiding me. I don't think gender matters for mentoring as much as some people worry that it does, but it does help when young ambitious women can talk to a successful female leader about her journey."

Albright and Momoda hope the WTLG will give MTS women a toolset to help them assert themselves and let their ambitions motivate them without fear of pushback. The WTLG also serves as a forum for female employees to talk about challenges and problems in the workplace. They can help each other with problems unique to women in an atmosphere of understanding. Momoda and Albright emphasize the importance of work/life balance for career scientists and acknowledge that women scientists have problems that aren't shared by everyone, although many career challenges are the same regardless of gender.

"I think it's true that you can define a lot of your personal satisfaction and how you want to make a mark on the planet through your job, but at the same time recognize that you have a family and that is part of the mark you're making on the planet as well. Everyone has to decide what that balance is to ensure their own happiness and well-being," Albright said.

"It's a place where you can find a mentor if you need one," said Ashley Nelson, a WTLG member from HRL's Sensors and Materials Laboratory. "There are women who have only been here a couple of years, like me, and those who have been here for many years who are willing to discuss concerns you might not feel comfortable bringing up in a work setting. The WTLG gives us a relaxed atmosphere where we can interact with female collegues who listen and advise each other. Our conversations are wide open and can include back and forth dialogue such as 'oh yeah, I've thought about that too.' Or 'I haven't seen that, explain it some more.' It's a great network that inspires a feeling of community between scientists who don't always work together directly."

In trying to understand the factors that affect work/life balance, the WTLG members can turn to each other for advice, and to Momoda as a leadership model. "I offer the group my experience with

> "When we looked at our succession plans, there were not many women"

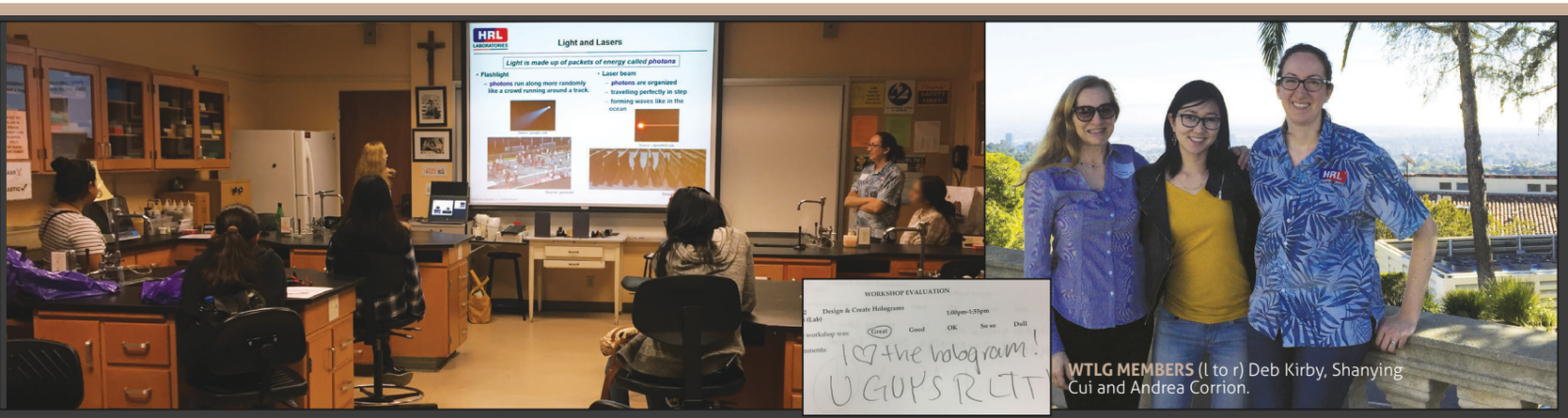
what has worked best for me over the years. Of course everyone's situation is different," Momoda said. "For instance, I believe that when you can't work a lot of extra hours, you become more efficient, and if you're here late, it's at the expense of your family time. That is obviously a concern. I remember on my first maternity leave my boss, Mary Young, told me 'your children are only this age for so long, please do not miss this.' She was always very accommodating. She would often say 'leave, you've been here too late, go home.' she was very family-centric and we want to ensure that everyone at HRL has access to that kind of concerned mentoring, so I hope they feel they can turn to the WTLG for such guidance."

"Leslie is the facilitator for the group. It sounded like a good idea to me because one issue that women, or underrepresented groups in general, run into is social isolation," said HRL researcher and WTLG member Andrea Corrion. "When I started at HRL, there were only a couple of women in my department, and the WTLG was a way for me to meet other women across the company and make new friends, which I think is important for people to enjoy their jobs."

Corrion also was encouraged by the way the WTLG pulls together a subset of people from all four labs to increase the scientific discussion across disciplines, and it is not intended to be exclusionary. "What this group is not is a forum to air grievances," Corrion said. "I'd like to see it be something that men and women can benefit from. Parney has told us he finds our meetings very useful to better understand what is happening at HRL at the ground level, and he has led many discussions about providing growth opportunities. This type of group could also inspire other institutions to form similar groups."

Corrion pointed out that aside from the fact that women are in the minority at HRL in the workforce, they are also underrepresented within the cultures of HRL's customers. "Our largest customer is US government science and technology, so there aren't an equal number of women working there either," Corrion said.

"Leslie brings in guests to talk with us who can serve as role models, like female leaders from General Motors, so we can get perspectives from different companies," Nelson said. "We have discussions with the guests, there is no lecture involved, they introduce themselves and we



WTLG MEMBERS (l to r) Deb Kirby, Shanying Cui and Andrea Corrion.

HRL Scientists Reach Out with STEM Education

Introducing Adolescent Girls to Science Can Have Lifelong Benefits

As part of HRL's Women's Technology Leadership Group (WTLG) community outreach, HRL scientists Andrea Corrion, Shanying Cui, and Deb Kirby participated in a volunteer workshop sponsored by Expanding Your Horizons, a nonprofit volunteer organization that promotes science, technology, engineering, and mathematics (STEM) education to middle-school girls. The workshop featured many participatory programs and projects that allowed the students to interact directly with professional women working in STEM.

The HRL scientists devised a lecture presentation combined with a hands-on project-building exercise entitled Build Your Own Hologram. First the scientists instructed the students on the basic physics of light and lasers. They then showed the girls how holograms are made and viewed, and the students made their own holographic projections of objects and toys using kits the scientists provided.

"One of the girls' mothers came and spoke with me at length about what the job prospects were for someone getting a PhD in engineering. You could see it dawning on her that her daughter could follow that track, and she was getting a little excited about it. So we were 'expanding the horizons' not just of the kids, but of the parents too." Corrion said.

The workshop was held at Mount Saint Mary's University near Brentwood, California. The participants were Los Angeles inner-city students recruited by a program called *Gaining Early Awareness*

ASHLEY NELSON, a WTLG member from HRL's Sensors and Materials Laboratory

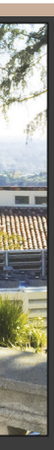
are free to ask about how they got where they are and how their organization's culture works, to compare it with our own experience. We learn about each other and what it means to be a woman in a technical field. We also talk about what made us want to be scientists, which helps us think of ways to increase STEM influence on younger girls."

The WTLG also has a participatory goal in mind with community outreach. The group hopes to encourage employee participation in bringing knowledge and information about STEM education to underrepresented groups, specifically women. HRL's leadership hopes WTLG will establish mentorships that inspire girls, particularly middle- and high-school- aged girls, to pursue careers in STEM. Data shows that university computerscience and electrical engineering programs are graduating fewer women than many other sciences, and nothing near an amount equal to male graduates.

"I definitely think that girls don't see themselves as engineers and scientists enough. If you look at popular representations of scientists in the media they are almost always men. We hope to reach out to girls in their formative years and present ourselves as scientists with faces that they might identify with as closer to their own," said Corrion.

Begun in 2015, the WTLG meets often. By inspiring students as early as possible in their STEM pursuits, the long-term goals of the group include increasing the number of women with post-graduate degrees in the physical applied sciences.

Albright and Momoda agree that there is more to leadership than attaining a position as a manager or lab director. Being a leader means assertiveness in leading projects, having a positive, encouraging impact on peers, and being seen as a leader by peers. They hope to expand the HRL culture that values inspiration for scientists to be creative and take pride in showing they can deliver whatever their customers need. The WTLG is an example of how HRL is focusing on diversity and helping female MTS obtain some of the tools that will help them attain any goals they set for themselves. ■



and Readiness for Undergraduate Programs (GEAR UP http://www.castategearup.org/), which is funded by the US Department of Education. Expanding Your Horizons hopes to spark interest in STEM activities and careers by having girls engage with female STEM role models and participate in hands-on activities. Cui pointed out that her previous science outreach volunteering opportunities were in relatively affluent communities or at state-level science fairs, which down-selected students who did well. She found it refreshing to interact with girls who began the workshop with varying degrees of interest in science and have most of them leave with a sense of wonder and excitement.

"I certainly would have loved a workshop like this when I was in middle school," Cui said. "I loved hearing the collective 'whoa!' and 'cool!' as each girl saw her hologram revealed. The most rewarding part for me was being able to interface with these kids who aren't already predisposed to science through their parents or environment."

Kirby agreed that the student's fascination grew as the workshop progressed. "In particular, I enjoyed observing the girls' excitement as they ran from one station to the next to check on each other's holographic artistic creations." Kirby said. "Each group made two or three holograms, and were inspired to be progressively more creative."

> "Corrion, Cui, and Kirby could easily see themselves in the places of the students at the same age, and each scientist agreed that they would have loved to have an event such as the workshop available to them as middle-school students."

"I participated in a couple of science events as a middle-schooler and they had a big impact on me," Corrion said. "I won first prize in Science Olympiad's Name that Organism competition in 7th grade. Experiences like that helped me realize that I wanted to go into science, but I still didn't have a good idea of what that meant, other than potentially becoming a science teacher, since I certainly didn't know any scientists at that age. Introducing young female students to professional women working in science is a goal of the WTLG, as well as a rewarding experience for us."

"We each told a short story of how we became involved in science and what captures our interest on a daily basis," Kirby said. "Our mission was to motivate them by showing a fun perspective of science through our stories and the hologram workshop. It was rewarding to be a part of developing the girls' curiosity and encouraging them to reach for STEM goals that they had maybe not yet considered."

The students were extremely positive in their after workshop evaluations and exuberant in their comments. A common thread among them was their fascination with the science, and their inspiration from getting to interact with and learn from women scientists. Corrion, Cui, and Kirby hope to continue the WTLG's successful relationship with Expand Your Horizons and that more HRL scientists will participate. So far the WTLG's educational outreach effort is off to a great start. ■

FUTURE PROOFING THE INTERNET

Continued from page 13

can be transmitted through public fiber optic cables safely.

Because of the nature of quantum signals, dissipation that always happens over distance (e.g., photons lost from optic fiber) can cause complete loss of quantum information. While classical signals can be amplified to extend signal distance, quantum signals instead require teleportation to solve this problem. Devices called quantum repeaters enable extension of the distance of quantum networks using teleportation, eliminating a possible unencrypted access point.

Quantum networks enable information protection that does not rely on assumptions that the code is a very difficult mathematical solution, being built instead on quantum mechanical properties that are truly random. A faithful copy of quantum information cannot be made because the copying process inevitably changes that information. Quantum networks that use entanglement will reveal if a message is interrupted or intercepted between communicating parties. Quantum networks do not guarantee uninterrupted communication, but they do detect any interference.

When communication can be delivered with absolute assurance it was not interfered with, secrecy is then guaranteed and the cyber communication is secure. "Quantum cryptography may be extended beyond peer-to-peer cryptography to offer protocols for improved secure network capabilities such as voting or auctions," Ladd said.

"For one protocol we developed, our approach was that if we have eight parties sharing entanglement, we can use the entanglement to verify distribution of the entangled state to all the parties," Harrington said. "Even if one of the parties is acting maliciously, we can still get all our randomness transmitted without biasing the result. Or we could have up to two of the shared parties with errors in their measurements, i.e., noise in their signals and we would be able to detect the noise immediately and throw out those measurements."

An unending battle

Cybersecurity has become a large, ever-expanding component of national security, and protecting global communications from harm by bad actors is an effort that goes beyond borders and political ideologies. The massive importance of computer connectivity across the world is pushing technology companies and government organizations to extend it to every corner of the planet.

As that effort continues, HRL Laboratories will expand its focus on advancing the technology of materials, algorithms, sensors, microelectronics, and wireless antennas and amplifiers that have been there since the beginning of global wireless connectivity. Going forward securely will mean learning from the oversights, however understandable, that occurred at the internet dawn. Staffed with top scientists and engineers, HRL Laboratories will remain a vigilant key contributor to communications technology experimentation, innovation, and discovery. ■

IP

64 PATENTS ISSUED SINCE JANUARY 2017

9,531,571 AGILE RADIO ARCHITECTURE • Xu, Zhiwei A.; Kuan, Yen-Cheng; Li, James Chingwei; Hitko, Donald A.; Jensen, Joseph F.

9,535,151 CODED APERTURE BEAM ANALYSIS METHOD AND APPARATUS • Lynch, James J.

9,536,114 SECURE MOBILE PROACTIVE MULTIPARTY COMPUTATION PROTOCOL • El Defrawy, Karim; Lampkins, Joshua D.

9,546,280 STRUCTURAL COATINGS WITH DEWETTING AND ANTI-ICING PROPERTIES, AND COATING PRECURSORS FOR FABRICATING SAME • Nowak, Andrew P.; Gross, Adam F.; Bartl, Michael H.

9,559,012 GALLIUM NITRIDE COMPLEMENTARY TRANSISTORS • Chu, Ronming; Cao, Yu

9,646,248 MAPPING ACROSS DOMAINS TO EXTRACT CONCEPTUAL KNOWLEDGE REPRESENTATION FROM NEURAL SYSTEM • Benvenuto, James; Bhattacharyya, Rajan

9,643,379 MICROSTRUCTURED RECONFIGURABLE COMPOSITE MATERIAL • McKnight, Geoffrey P.; Henry, Christopher Paul; Herrera, Guillermo

9,680,702 NETWORK OF NETWORKS DIFFUSION CONTROL • Ni, Kang-Yu; Keegan, Matthew S.

9,697,462 SYNAPTIC TIME MULTIPLEXING • Cruz-Albrecht, Jose M.; Srinivasa, Narayan; Petre, Peter; Cho, Youngkwan; Nogin, Aleksey

9,705,201 CAVITY-BACKED ARTIFICIAL MAGNETIC CONDUCTOR • White, Carson R.; Gregoire, Daniel J.

WHAT'S NEXT

by Leslie Momoda, Vice President

As cybersecurity challenges become more immediate, sophisticated, and pervasive, HRL is creating new approaches to protecting computer networks based on a wider view of the internet as a cyber ecosystem.

These new methods are flexible, adaptable, and enable quick threat detection. HRL scientists are at the forefront of software design that in the near future will be resistant to attack from its very inception, using tools that are adaptable to any size network.

HRL's expertise in custom microelectronics and algorithms that emulate the brain and human thought processes enable unprecedented methods of threat detection and decision-making. Like the brain, HRL's demonstrated neuromorphic chips are very energy efficient. They can analyze complex data using very low amounts of power to quickly identify anomalies in the cyber ecosystem and react to them.

One of our unique artificial intelligence capabilities—on-chip learning—enables computer systems that think and react on their own, adapting instantly to changing threats. We continue to push the state-of-the-art in hardware and software to further lower the amount of energy needed and to increase computing power for systems. Investigations are underway in novel memory-based computing elements (memristors) as well as unique low-power physics-based computing paradigms and implementations of probabilistic computing, both of which allow more efficient processing of very complex sensory tasks such as imagery and acoustics.

Building provable secure cyberphysical systems with detection embedded in them is also a focus area. We are expanding our work on the HACMS program (described in this issue) to address secure computing in a cloud-based environment and other multiparty interaction scenarios by developing self-healing methods for compromised systems as well as tools to audit them.

We are investigating using signals already present in functioning hardware systems to find impending faults as well as using our graph-based, large-scale data analytics tools to detect and predict catastrophic events. We are exploring more fundamental use of advanced mathematics to design highly complex, interactive systems that are resilient to disruption.

As HRL pushes the forefront of these technology areas, we remain focused on implementation of these innovations. From ideas to demonstrations, we create paths that maximize mission impact and ease system insertion. We look forward to describing these successes in future editions of *HRL Horizons.* ■

"HRL's expertise in custom microelectronics and algorithms that emulate the brain and human thought processes enable unprecedented methods of threat detection and decision making."

...

www.hrl.com

LinkedIn.com/hrl-laboratories

Facebook.com/HRLlaboratories

HRL Horizons
HRL LABORATORIES, LLC
3011 Malibu Canyon Road
Malibu, CA 90265