PROCEEDINGS OF SPIE

Disruptive Technologies in Sensors and Sensor Systems

Russell D. Hall
Misty Blowers
Jonathan Williams
Editors

11–12 April 2017
Anaheim, California, United States

Sponsored and Published by
SPIE

Volume 10206

Proceedings of SPIE 0277-786X, V. 10206

Disruptive Technologies in Sensors and Sensor Systems, edited by Russell D. Hall, Misty Blowers, Jonathan Williams,
Proc. of SPIE Vol. 10206, 1020601 · © 2017 SPIE · CCC code: 0277-786X/17/$18 · doi: 10.1117/12.2270680

The papers in this volume were part of the technical conference cited on the cover and title page. Papers were selected and subject to review by the editors and conference program committee. Some conference presentations may not be available for publication. Additional papers and presentation recordings may be available online in the SPIE Digital Library at SPIEDigitalLibrary.org.

The papers reflect the work and thoughts of the authors and are published herein as submitted. The publisher is not responsible for the validity of the information or for any outcomes resulting from reliance thereon.

Please use the following format to cite material from these proceedings:
Author(s), "Title of Paper," in *Disruptive Technologies in Sensors and Sensor Systems*, edited by Russell D. Hall, Misty Blowers, Jonathan Williams, Proceedings of SPIE Vol. 10206 (SPIE, Bellingham, WA, 2017) Seven-digit Article CID Number.

ISSN: 0277-786X
ISSN: 1996-756X (electronic)

ISBN: 9781510609136
ISBN: 9781510609143 (electronic)

Published by
SPIE
P.O. Box 10, Bellingham, Washington 98227-0010 USA
Telephone +1 360 676 3290 (Pacific Time) · Fax +1 360 647 1445
SPIE.org

Printed in the United States of America.

Publication of record for individual papers is online in the SPIE Digital Library.

SPIE. DIGITAL LIBRARY
SPIEDigitalLibrary.org

Paper Numbering: *Proceedings of SPIE* follow an e-First publication model. A unique citation identifier (CID) number is assigned to each article at the time of publication. Utilization of CIDs allows articles to be fully citable as soon as they are published online, and connects the same identifier to all online and print versions of the publication. SPIE uses a seven-digit CID article numbering system structured as follows:

- The first five digits correspond to the SPIE volume number.
- The last two digits indicate publication order within the volume using a Base 36 numbering system employing both numerals and letters. These two-number sets start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B … 0Z, followed by 10-1Z, 20-2Z, etc. The CID Number appears on each page of the manuscript.

Contents

Authors

Numbers in the index correspond to the last two digits of the seven-digit citation identifier (CID) article numbering system used in Proceedings of SPIE. The first five digits reflect the volume number. Base 36 numbering is employed for the last two digits and indicates the order of articles within the volume. Numbers start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B...0Z, followed by 10-1Z, 20-2Z, etc.

Conference Committee

Symposium Chair

Donald A. Reago Jr., U.S. Army Night Vision & Electronic Sensors Directorate (United States)

Symposium Co-chair

Arthur A. Morrish Raytheon Space and Airborne Systems (United States)

Conference Chairs

Russell D. Hall, Northrop Grumman Corporation (United States)
Misty Blowers, Air Force Research Laboratory (United States)
Jonathan Williams, Air Force Space Command (United States)

Conference Program Committee

Gustave W. Anderson, Lockheed Martin Corporation (United States)
Howard A. Blair, Syracuse University (United States)
Christophe Bobda, University of Arkansas (United States)
Harsha Chenji, Ohio University (United States)
George E. Corbin, BAE Systems (United States)
Erik Einarsson, University at Buffalo (United States)
John F. Federici, New Jersey Institute of Technology (United States)
Josep Miquel Jornet, University at Buffalo (United States)
Wei-Shinn (Jeff) Ku, Auburn University (United States)
Georgiy M. Levchuk, Aptima, Inc. (United States)
Chen Liu, Clarkson University (United States)
John A. Marsh, State University of New York Institute of Technology (United States)
Daniel M. Mittleman, Brown University (United States)
Val A. Red, Air Force Research Laboratory (United States)
J. David Schaffer, Binghamton University (United States)
Ngwe Thawdar, Air Force Research Laboratory (United States)
Christopher Thorn, Texas A&M University (United States)

Session Chairs

Sensors and Communication I
Josep Miquel Jornet, University at Buffalo (United States)

Sensors and Communication II
Ngwe Thawdar, Air Force Research Laboratory (United States)

Internet of Things/Cyber Physical Systems
Val A. Red, Air Force Research Laboratory (United States)

Innovation in Cyber Operations
James Sidoran, Air Force Research Laboratory (United States)

Sensor M&S
Stephen Kozacik, EM Photonics, Inc. (United States)

Computing M&S
Susan Harkrider, U.S. Army Night Vision & Electronic Sensors Directorate (United States)

Spectrum
Aaron L. Paolini, EM Photonics, Inc. (United States)

Introduction

The Chairs of the Disruptive Technologies in Sensors and Sensor Systems conference would like to thank the SPIE organizers, speakers, expert panelists, session chairs, and students that made this conference such a great success. This was the first year this conference was offered as an evolution of our prior year's conference on Machine Learning and Bio-Inspired Computation.

Dr. Raju Namburu from the U.S. Army Research Laboratory kicked the event off with an insightful presentation on the current and future direction of network operations and advanced computer hardware architectures. Dr. Mike Fanto from the Air Force Research Laboratory provided a second keynote presentation on new methods for enabling quantum computing with photonics.

Dr. Josep Jornet and his team of students from University at Buffalo maintained a huge presence while they captivated the audience with discussions on nanotechnologies, bio-sensing, blockchain technologies, and autonomous systems.

The conference featured a student panel that resulted from a competitive selection process in which students from multiple universities submitted topics they felt represented the most disruptive technologies of the future. Sponsorship for these students was provided by a global consulting firm called ICF. There were numerous submissions from 8 different universities. The four winning students covered topics on machine learning, blockchain technology, quantum, and bio-technologies.

An expert panel led by Lt. Val Red from the Air Force Research Laboratory provided engaging discussions on the future of cyber security for cyber physical systems and the internet of things.

Two sessions focused on innovation for cybersecurity. Cybersecurity will be redefined in the next decade as more and more devices become connected to the World Wide Web. Sensor technological advancements will vastly improve our capacity for observation and data collection. Talks demonstrated the growing demand for improvements to processing speeds, advanced algorithmic approaches, robust architectures, and resilient system security that can only be realized by breaking the mold on conventional thought and technologies.

Sessions on advancements in modeling and simulation provided insight into the next generation of interfaces and computer based systems to help operators and analyst improve their understanding and representation of the outside world and

simulate real world systems. Modeling and simulation allows intrinsic views into the behaviors of many types of systems and can often help to minimize ill-intended effects upon deployment.

Contributions from ICF, Northrop Grumman, Air Force Space Command, Air Force Research Laboratory, U.S. Army Research Laboratory, University at Buffalo, EM Photonics and over 30 speakers made this conference a resounding success. This new conference for 2017 was the place where we looked to the future to discover the technologies that will be game changers when considering the next generation of sensors and sensor systems.

Russell D. Hall
Misty Blowers
Jonathan Williams

Student Panel Presentations

The 2017 SPIE conference on Disruptive Technologies for Sensors and Sensing Systems featured a student panel that resulted from a competitive selection process in which students from multiple universities submitted topics they felt represented the most disruptive technologies of the future. Sponsorship for these students was provided by a global consulting firm called ICF. There were numerous submissions from 8 different universities and the winning entries are shown below. The four winning students served as expert panel members fielding questions on their respective topics from the research community. They also presented posters on their topics in the poster session over two nights. This was a fantastic opportunity for these students to build their resumes and to attend a globally recognized conference providing both networking and career opportunities.

Title: Bitcoin and Blockchain Technology
Author: Kyler Harrington, University at Buffalo

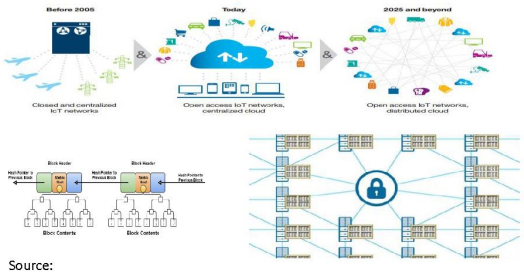
ICF *Student Sponsored*

Blockchain technology

Description

- Blockchain technology is the backbone of bitcoin but has many other uses
- Extremely secure system for transferring ledgers through a distributed network
- Modification is the keyless signature infrastructure used in Electronic-Estonia (E-Estonia)
- Infrastructures secured by blockchain technologies will provide the needed transaction transparency to ensure tamper when transferring important information

Blockchain Operational Concept



Source:
https://www.theregister.co.uk/2016/02/18/ibm_open_sources_blockchain_code/
https://www.linkedin.com/pulse/blockchain-device-democracy-manav-gupta

Advantage Over Current State

- For future operational environments to be scalable they need to break away from their dependence on a centralized cloud/management platforms
- Decentralization of trust can occur in architectures equipped with basic cryptographic tools and security functions like those found in the blockchain architecture

Student Name and Affiliation

University at Buffalo
School of Engineering and Applied Sciences

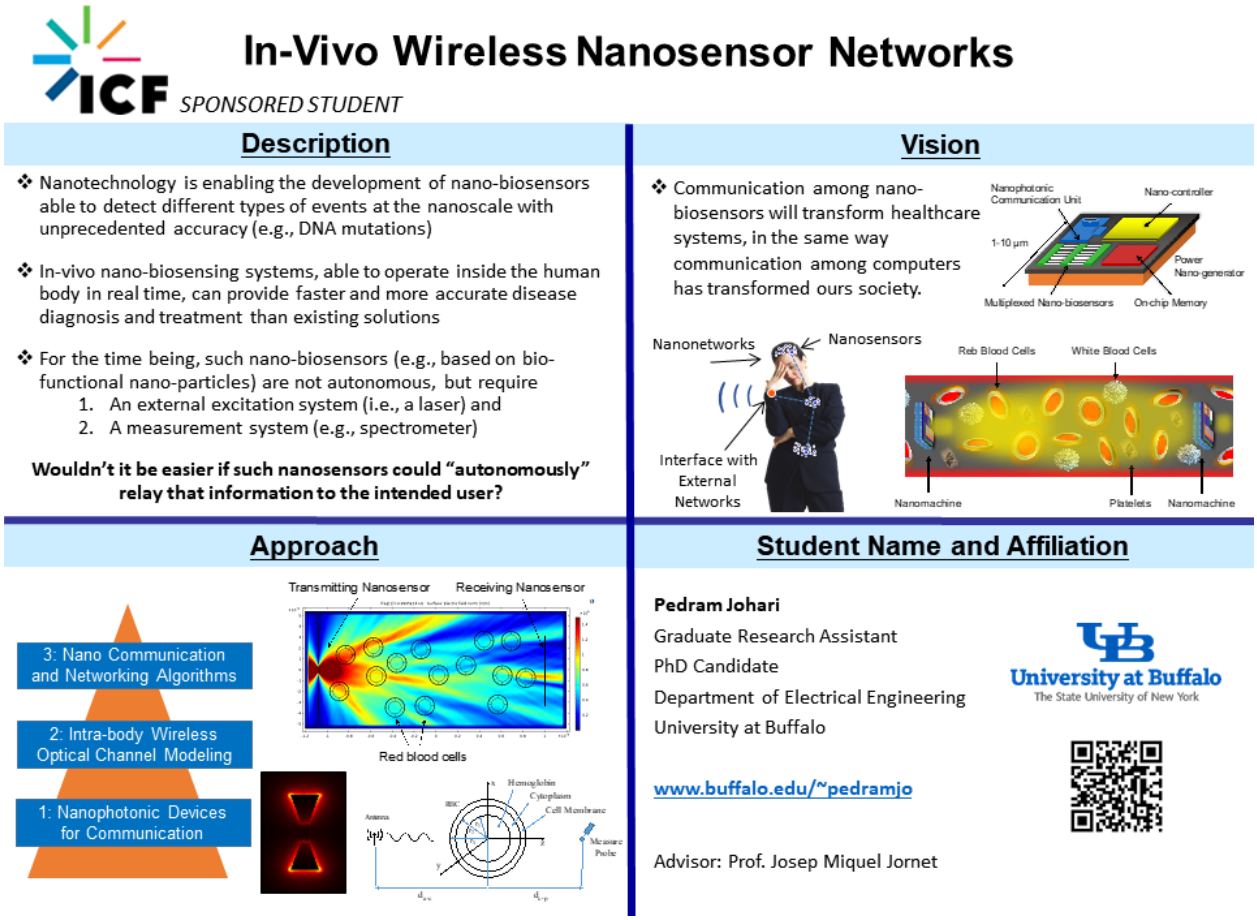
Kyler Harrington
University at Buffalo
kylerhar@buffalo.edu
https://www.linkedin.com/in/kylerharrington

There's a lot of hype in technical journals about blockchain technology. A recent World Economic Forum report predicts that by 2025 10% of GDP will be stored on block chains or a type of distributed ledger system which is the underlying architecture for blockchain related technology. Blockchain technology is gaining momentum in both government and the private sector. In the past few years, variations of block chain type secure information transfer systems have been implemented in countries around the world as a means to secure information transfer and enabled digital societies. Estonia is an example of a country that has taken a step towards a more secure digital system with transaction

transparency. Estonia's digitized societal infrastructure has demonstrated a transformation of the systems people rely on today. It shows how we can evolve into a radical new world of revolutionized banking infrastructures and information transfer that is reliable and sustainable. The Estonian government has demonstrated how information can be managed and transferred with blockchain technology to preserve security and reliability.

Blockchain technology can provide both government and private agencies a secure network to share data and securely complete transactions without fear of security compromises due to the transparency of transaction history. It could lead to new network and software architectures for online banking ensuring that our economy will be less vulnerable to hacking threats. In time, more people around the world will realize the potential of blockchain technology to secure their sensitive data and improve our security with so many networked devices. This will lead to more countries of the world to adopt a digital infrastructure like Estonia. When the world embraces blockchain technology, there will be hope for greater government efficiency and transparency. Imagine an election systems where there is no threat of voter fraud or election tampering. If blockchain is implemented into the global economy the world will become a much more secure and reliable place for ensured flow and trust of data that is transmitted across a chaotic and often unreliable network of computer systems and connected devices.

Title: In-Vivo Wireless Nanosensor Networks
Author: Pedram Johari, University at Buffalo



With the recent progress in nano-bioscience, it is not beyond imagination that within a few years we will see the emerging nano-bio devices in our daily life with remarkable applications ranging from healthcare monitoring wearables and intra-body microfluidic nanosensors to brain-machine interface (BMI) implants. Independently of the specific application, one of the most important challenges in this area is the communication between these devices, which is the interest of a part of our research group. More specifically, we are working on different aspects and layers of communication networks, namely: the development of novel optical plasmonic nano-antennas; the characterization of the channel for both nanoscale intra-body and wireless on-chip communications; the development of new modulation schemes and protocols tailored to these networking paradigms; and system-level design for this new technology. The objective of our research is to pave the way for development of unprecedented applications among which the following can be mentioned as our current focus:

- Optical plasmonic communication among autonomous in-vivo nano-bio-sensors, which can operate inside the human body in real time, and have been recently proposed as a way to provide faster, low-cost, and more accurate disease diagnosis and treatment than traditional technologies.
- Establishing the foundations of distributed neuronal activity monitoring with cooperative nano-devices for next-generation nanophotonic brain-machine interfaces.
- Create an ecosystem (hardware + software) able to provide wireless connectivity to on-body wearable medical devices which act as an interface between intra-body information sources (e.g., nanosensors, biological processes) and a user's personal device (e.g., cellphone, tablet).

Title: Quantum Key Distribution
Author: Rushui Fang, Binghamton University

Quantum Key Distribution

ICF *SPONSORED STUDENT*

Description

- Quantum cryptography is a disruptive technology that applies quantum mechanics properties to cryptographic techniques.
- Quantum key distribution (QKD) provides a secure way to transmit key, which is used to encrypt messages when the bit error rate is reasonable.
- Traditional key distribution depends on complexity of computation but it's vulnerable at the presence of quantum computers or advance algorithms.
- QKD relies on photon's natural properties such as uncertainty principle and no-cloning theorem as its advantages. It's also one-time pad, which is considered as provably secure.
- The experimental bit rate and transmission distance have been constantly improved, and QKD has great potential to be more widely commercialized.

Pictorial Representation of Concept

Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↑	↖	→	↑	↑	→	→	↖	↗	↑	↖	↗	↗	↑
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION	Can be done through classical channel such as broadcast radio or internet														
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
Remaining shared secret bits			1					0				1			1

Quantum transmission using protocol BB84[1]

Advantages Over Current State

- The Heisenberg uncertainty principle: the very act of observing would change the properties of photons. (ex. Choose a base to measure photos' polarizations)
- No-cloning theorem: it's impossible to copy quantum states because of the superposition principle[2], making QKD more robust to intercept-resend attack.
- One-time pad: QKD can generate truly random sequence of bits as the cryptographic key which is the same length with the plaintext.
- QKD doesn't require much computation algorithms.

References are included in another sheet

Student Name and Affiliation

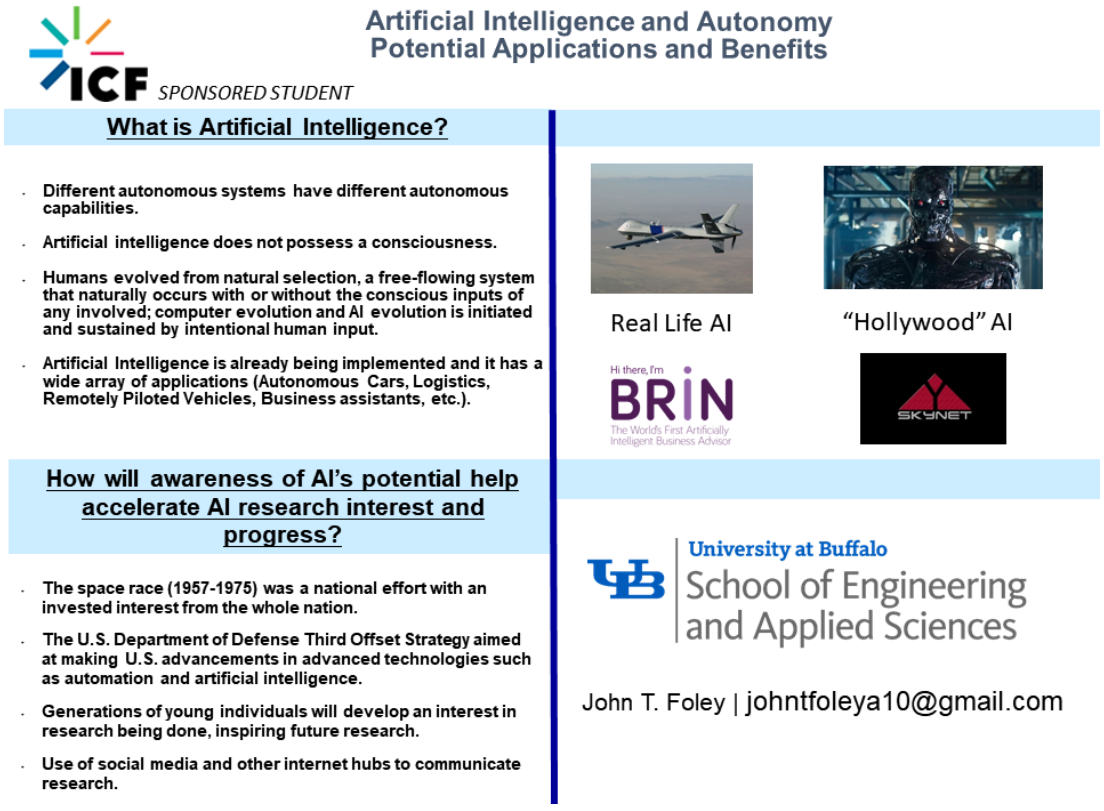
Rushui Fang
Electrical Engineering
Binghamton University
rfang4@binghamton.edu
https://www.linkedin.com/in/rushuifang

BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK

In the next 10 years, cyber security will still hold a significant place because organizations and individuals require their information to be safe from unauthorized access. While traditional cryptography has various ways to scramble or substitute letters, quantum cryptography encrypts states of bits by photon's different properties such as polarization and has theoretically better secure performance. According to the uncertainty principle, the very act of observing a photon changes its properties. During the quantum key distribution process, the information holder would notice if a third party once tried to eavesdrop the information. This technique is facing a practical problem that photons loss through a quantum channel. A solution could be a relay station between two nodes so the 60 miles maximum transmission distance can be extended. Information transmission would be unbreakable when this one-time pad technique is applied on the market. The benefits of Quantum Cryptography are highlighted below:

- Quantum cryptography is a disruptive technology that applies quantum mechanics properties to cryptographic techniques. Quantum key distribution (QKD) provides a secure way to transmit key, which is used to encrypt messages when the bit error rate is reasonable.
- Traditional key distribution depends on complexity of computation but it's vulnerable at the presence of quantum computers or advance algorithms.
- QKD relies on photon's natural properties such as uncertainty principle and no-cloning theorem as its advantages. It's also one-time pad, which is considered as provably secure.
- The experimental bit rate and transmission distance have been constantly improved, and QKD has great potential to be more widely commercialized.

Title: Artificial Intelligence and Artificial Autonomy
Author: John Foley, University at Buffalo



A large part of scientific research entails effective communication between the researcher, the investor, and the consumer. It becomes difficult to accomplish things in the laboratory when there is no support coming from the people who will be funding you and the people who will be utilizing your product or service. The major challenge for computer scientists and electrical engineers in the next decade will be effectively communicating the details and premises of their work to onlookers of their projects. I will look specifically at the topic of artificial intelligence to emphasize my point. As of today, there is a large misconception of what artificial intelligence is. What needs to be understood is that there is a major difference between "intelligence" and "autonomy" in the world of computer science. Here, Intelligence involves the ability to gather and relay data and information that is often considered complex and vast. Artificial intelligence with such intelligence is already beginning to be implemented today. Let's look at "autonomous" cars as an example. "Autonomous" cars are computers that are designed to make a series of decisions through a programmed series of calculations and measurements based on a number of statistics gathered from the car's sensor systems. It is also true that these cars expand their repertoire of knowledge through exposure and experience to real-life traffic. Google has its own self-driving car project known as Waymo and since 2009 they have accumulated nearly 3 million miles in driving on public roads with test drivers, creating an enormous repertoire of traffic situations for the car to learn from. When the Google car's creators decided to expose the car to real traffic and the car learned how to deal with it, the car gained a level of autonomy enabled with artificial intelligence.

Artificial intelligence is also being applied to help small businesses grow and prosper. An app known as BRiN, founded by Dale Beaumont, is the world's first AI-powered business advisor. Within seven days of its release, BrIN had 3,000 new users. Such systems are again not autonomous in that they don't have a consciousness. That being said, there are branches of artificial intelligence that are exploring the realms of machine learning and autonomous decision making in computers. In conclusion, it needs to be made known that what these scientists are doing is both exciting and controlled. People fear the unknown and most people don't understand artificial intelligence. Science Fiction movies have contributed largely to scientific research but movies such as "Terminator" have made people hesitant to put their trust in scientists. The idea that computers will have the ability to override and outsmart their creators is a far stretch and people need to understand that machines and computers will only have the ability to do what they are intended to do by their creators. Artificial intelligence has a wide array of applications and investors and consumers need to be made aware of the work scientists and engineers are doing behind "closed doors". Within the next ten years, communication between computer scientists/electrical engineers and investors/consumers will need to be increased and improved if progress is to be made.