Center for Embedded Systems for Critical Applications

VirginiaTech
Invent the Future

CESCA Newsletter
Center for Embedded Systems for Critical Applications

CESCA • 302 Whittemore Hall • Dept. of ECE • Virginia Tech • Blacksburg • 24061 • USA

October 2015• No.013

The **Center for Embedded Systems for Critical Applications** is a research center within the Bradley Department of Electrical and Computer Engineering. CESCA addresses the major challenges in the conception, the design, and the implementation of next-generation embedded systems. CESCA bundles the efforts of eight faculty and their students in a cross-disciplinary setting. CESCA generates know-how, expert advice, and skilled researchers who tackle the needs of tomorrow's industry and academia.

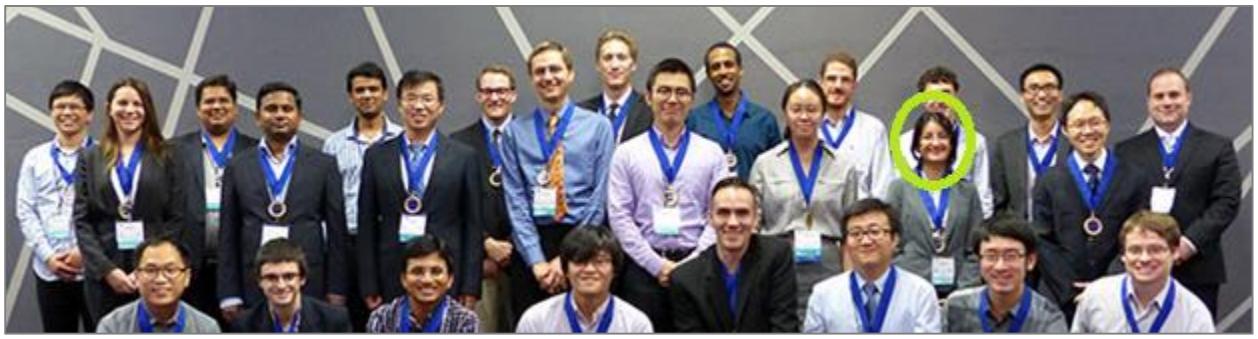
From the Director's Desk

CESCA is now on Twitter. If you have a twitter account, we invite you to follow us! If do you do not have a twitter account, you may still view our news feeds on twitter.com/vt_cesca . We plan to make regular updates on twitter. However, we will still send out regular newsletters at a lower frequency.

In this newsletter, you will find some of the new projects that have started, as well as the achievements and placement of our students, whom we are both proud and fortunate to have the opportunity to work with. We hope you enjoy the newsletter and we always welcome your comments as we attempt to improve on communicating with you.

Michael Hsiao
CESCA Director

Award



Best-in-Session Award at SRC TECHCON

Nahid Farhady Ghalaty (circled in green on the picture) received a Best-in-Session Award for her presentation at SRC TECHON 2015 in Austin, TX. Her presentation, "FAME: Fault-Attack Awareness using Microprocessor Enhancements," describes recent progress in the SRC-sponsored research project on Fault-attack Aware Microprocessor Design.

In the talk, Nahid discussed common fault injection mechanisms, and common fault analysis techniques. From these observations, she derived a set of guidelines and techniques for fault-attack resistant design. The main message of the talk was to describe fault-attack resistant design and differentiate it from fault tolerant design, a set of techniques based on redundancy.

This research was supported through the National Science Foundation Grant 1441710, and through the Semiconductor Research Corporation.

New Projects

Schaumont to Start New Project on PCB Authenticity

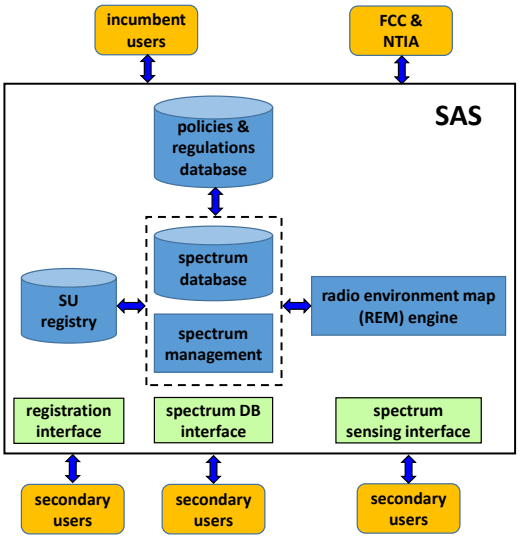
Dr. **Patrick Schaumont** is supported by CISCO on a new project on PCB Authenticity. This project investigates an application of the low level physical properties of digital components. Physical Unclonable Functions (PUF) are constructions that can convert those device-unique properties into stable and unique digital identifiers. In this project, Schaumont will apply PUF technology for an integrity protocol. In the resulting setup, a server will collect a set of challenge/response from a PUF integrated in a device. After deployment of the device in the field, the server will test the device authenticity by testing its ability to regenerate an earlier generated response. In a collaboration between NICT, Google and Virginia Tech, a team of researchers including Schaumont recently demonstrated the feasibility of designing and implementing such a protocol, under the additional constraint that preserves the device's privacy*.

The specific research objectives of the project are threefold: (a) We plan to evaluate if the authentication protocol we have developed can be applied to test PCB integrity; (b) We plan to evaluate how well known PUF technology is suitable to identify the origin (place of manufacture) of a component; and (c) The third objective in this project is to capture the results of the experiments in a protocol for physical proofs.

* A. Aysu, E. Gulcan, D. Moriyama, P. Schaumont, M. Yung, "End-to-end Design of a PUF based Privacy Preserving Authentication Protocol", Proc. of the IACR Workshop on Cryptographic Hardware and Embedded Systems (CHES 2015), September 2015.

Park Received NSF Grant on Incumbent Protection Zones

Dr. **Jerry Park** is the PI of an NSF grant titled "Collaborative research: Dynamic exclusion zones: Balancing incumbent protection and spectrum utilization efficiency" with a total budget of $731K. This is a collaborative research project between Park (lead investigator) and W. Lehr (at MIT).



The primary goal of the project is to develop a framework for implementing Incumbent Protection Zones that take advantage of the network of SAS (Spectrum Access System) databases and spectrum sensing data to adjust the geo-contours of exclusion zones dynamically. This will expand opportunities for Secondary Users to co-exist with Incumbent Users without causing harmful

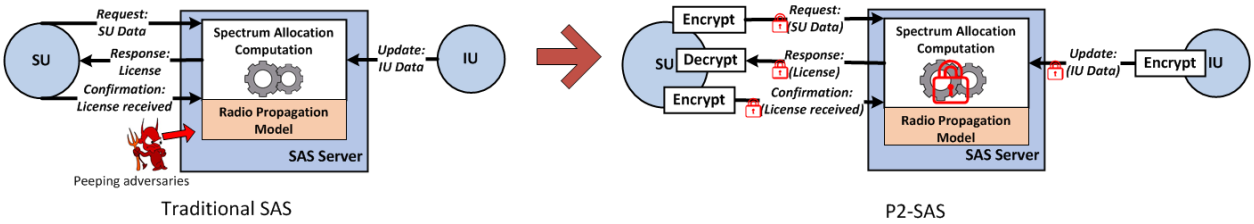
interference. This research is intended to provide a practical framework that is both technically and economically viable for implementing incentive-compatible dynamic sharing solutions as part of the SAS framework.

Yang Granted an NSF project on Dynamic Spectrum Access

Dr. **Yaling Yang** is the PI of an NSF project titled "Collaborative Research: Preserving User Privacy in Server-driven Dynamic Spectrum Access System" of $750k total budget. This is a collaborative project with Kui Ren (University at Buffalo).

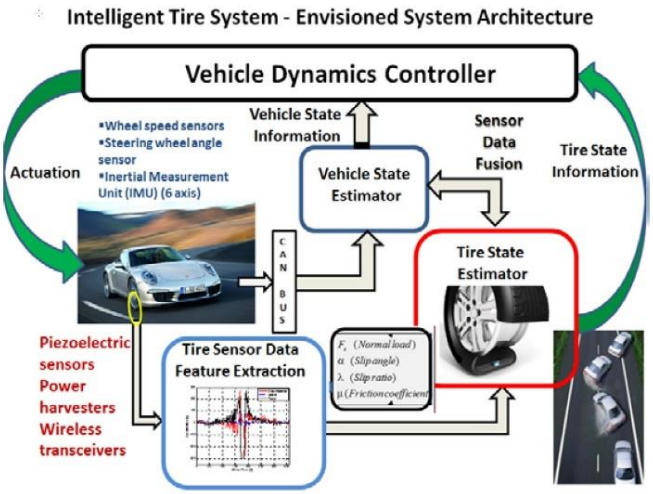
Dynamic spectrum access (DSA) technique enables wireless devices, which is called secondary users (SUs), to use spectrum that are allocated to licensed incumbent users (IUs) as long as they do not interfere with IUs' operation. It has been widely accepted as a crucial solution to mitigate the spectrum scarcity problem for wireless communications. As a key form of DSA, US government has proposed to release more Federal spectrum for sharing with commercial wireless users. It has also recommended a spectrum access system (SAS) database to govern the spectrum sharing between IUs and SUs. However, the flourish of SAS-driven Federal-Commercial sharing hinges upon how privacy issues are managed. In current SAS schemes, the operation data of both federal IUs and commercial SUs need to be shared with the SAS database for it to decide if sharing is permitted. Yet, operation data of federal IUs are often classified information and SU operation data may also be commercial secret. Since SAS is not necessarily operated by a trusted third party and can potentially be breached by attackers, these current schemes threaten the privacy of both IUs and SUs. To address this privacy issue, this project will develop a **p**rivacy-**p**reserving SAS (P^2-SAS), which ensures that the SAS system can still accurately decide whether spectrum sharing among IUs and SUs are permitted while it learns nothing about the operation data of IUs and SUs.

This project is the first to be able to successfully realize privacy-preserving spectrum allocation in SAS. It will address regulators' concerns with DSA's privacy issue and hence greatly help the development of the entire nation's broadband networks. The project will also provide a blueprint on how privacy-preserving mechanisms can be integrated in many other communication systems beyond DSA.



The project realizes its privacy preserving spectrum allocation using secure homomorphic computation. In P^2-SAS, IUs and SUs share only ciphertexts of their operation data with the SAS Server. SAS Server then performs secure homomorphic computation directly over these ciphertexts, so that none of the IU/SU operation data would be exposed to any snooping party, including the SAS itself. The project is able to convert complex spectrum allocation computation and certification procedures into the limited homomorphic computation types provided by efficient Paillier cryptosystems. Leveraging the unique characteristics of spectrum allocation computation, various refining techniques are explored to significantly reduce the computation and communication overhead of P^2-SAS and prevent potential attacks on the system.

Park Awarded an NSF Grant on Wireless Transmission of Safety Data



Dr. **Jerry Park** is a co-PI of a major NSF grant titled "Advanced materials manufacturing, sensing, and wireless controls for intelligent automobile environments" with a total budget of $1.15M. This project will involve research collaboration between Prof. Park, Prof. S. Taheri (VT's Dept. of Mechanical Engineering), Prof. M.R. Hajj (VT's Dept of Biomedical Engr. and Mechanics), Prof. S. Priya (VT's Dept. of Mechanical Engineering), and Prof. S. Trolier-McKinstry (Penn State Univ.).

In intelligent vehicles envisioned to be manufactured in the near future, safety-critical components, such as tires and seat belts, play critical roles in the development of intelligent controls as they can provide information on the most relevant parameters such as friction, slip, pressure, and driver conditions. The overall goal of the project is to actively monitor those parameters through embedded sensors based upon piezoelectrics and dielectrics. Park's group will take the lead in the design and implementation of the mechanisms and protocols needed to enable reliable, secure, and efficient wireless transmission of the sensor-collected data.

Abbott started a multidisciplinary project

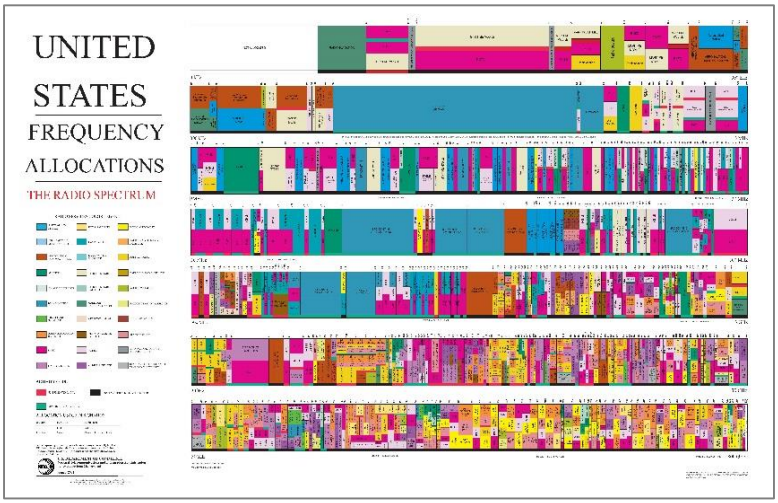
Dr. **Lynn Abbott** is co-PI of a new project, "Developing an Automated Emotion Training System." The work is funded by NIH, and the PI is Dr. Susan White, from VT's Dept. of Psychology. This multidisciplinary team is developing a computer-based system that uses a Kinect sensor and computer-vision techniques in an attempt to recognize human facial expressions automatically. Example emotions being recognized are happiness, fear, and anger. This novel system is expected to have clinical utility for treatment of children with Autism Spectrum Disorder (ASD) and other neurodevelopmental disorders characterized by impaired emotion expression. An interactive, prototype version of the system is currently being tested with human subjects. The long-term goal of this effort is to develop an interactive, computer-assisted system to help children develop appropriate emotional recognition and expression skills.

Park Hosted Workshop on Enhancing Access to the Radio Spectrum (EARS)

Dr. Jeff Reed (PI) and Dr. **Jerry Park** (co-PI) have been awarded a grant by NSF to organize a major workshop on Enhancing Access to the Radio Spectrum (EARS). This EARS Workshop was held on October 19-20, 2015 in Arlington, VA.

At this workshop, an interdisciplinary group of highly-visible academic researchers, relevant government officials, and industry stakeholders gathered to discuss technologies and polices that will enable us to unlock the true potential of the spectrum while respecting the needs of incumbent users. This group created a vision for future spectrum use, identifying the problems

to be overcome, the research needed to overcome these problems, and the financial and human capital resources necessary to support this vision.



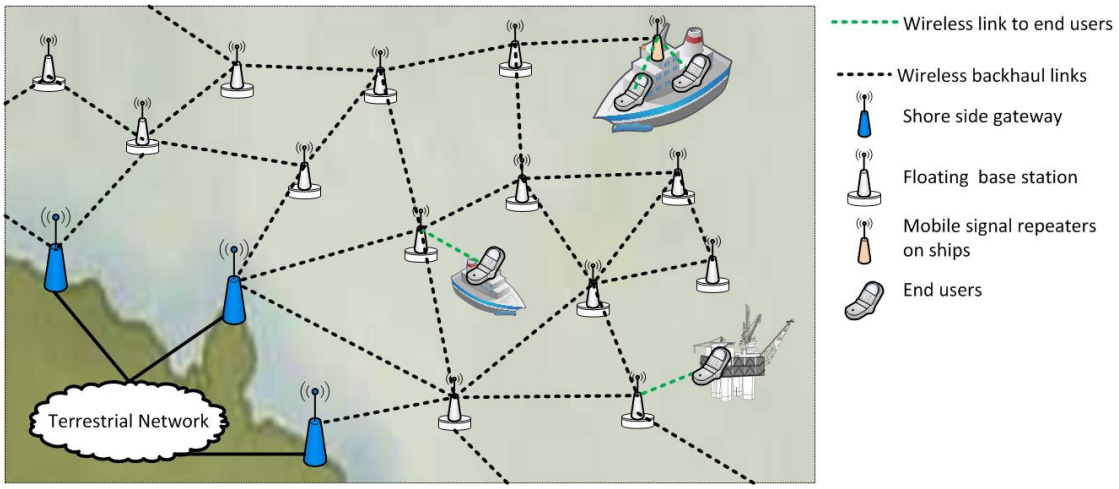
Yang to Start Collaborative Project for Improving Ocean Communication

Dr. **Yaling Yang** is the PI of a NSF project titled "NeTS: Small: Long-range Ocean Communication Links Powered by Energy Harvesting" of 200k total budget. This is a collaborative effort with Prof. Majid Manteghi (ECE, VT) and Prof. Lei Zuo (ME, VT).

Advancements in maritime communications are severely lagging behind its land counterpart. Existing marine communication technologies usually have very limited capacity and are extremely expensive to operate. Novel solutions are demanded to meet the imminent requirements for broadband marine mobile wireless access. The purpose of this project is to fill the void of marine broadband wireless communications by developing long-range self-powered ocean wireless communication links. The ocean wireless link is composed of compact, maintenance-free and low cost floating wireless base stations (BS) that can be simply dropped into the water. Once in the water, the BSs start to harvest energy from ocean waves and establish communication links with each other. Users' broadband traffic, then, can be delivered to the Internet through these links. This project will bring revolutionary change to the maritime communications. New maritime networked applications and operation scenarios that are infeasible but highly desirable in the past can be enabled by this technology. It can have significant impact on all aspect of ocean related industry, such as fishing, recreational boating, marine transportation, oil and gas industry, ocean scientific study, and national security and defense.

The project will focus on two thrust areas: Thrust 1 is about ocean wave energy harvesting. For a BS to provide large coverage range and high capacity links to its users and other BSs, the BS must consume a large amount of energy. It is nontrivial to design such an energy-harvesting unit while staying low-cost, compact and maintenance-free. Existing technologies are too large in size and hence are expensive and hard to be stabilized in rough ocean states and require frequent maintenance. This project solves this critical challenge by a novel power takeoff mechanism. This design enables the researchers to build an ocean wave energy harvester that can effectively harvest tens watts of power on typical ocean states with a floating buoy of less than 1 meter diameter. Thrust 2 is about building the high capacity marine communication links. The constantly moving ocean waves can affect the capacity, stability and range of the backhaul

links among BSs. In this project, we will study how to analyze and model the channel and design antenna and radio hardwares to handle the complex channel of ocean communication links. The researchers will also study the unique features of ocean communication links and their potential beneficial and/or harmful impact on network communications.



Park Received Grant from Cisco on Anonymity-Preserving Authentication

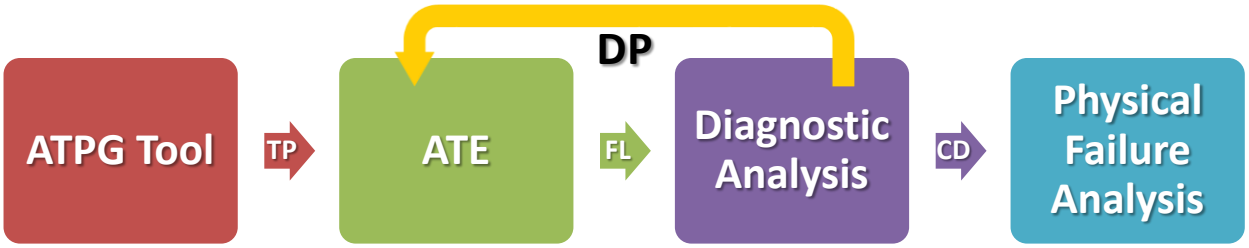
Dr. **Jerry Park** (PI) has been awarded a grant from Cisco entitled "Anonymity-Preserving Authentication for Large Networks". In many network applications, we need to be able to authenticate the data while, at the same time, protect the anonymity or privacy of the data source—in other words, *anonymity-preserving authentication* (APA) is needed. APA schemes are needed in applications where the receivers (or verifiers) of data should not learn the actual identity of the data sender (or source of data), and are willing to accept tokens of authentication that are verifiably linked to an anonymous user, knowing that the sender's identity can be revealed by a trusted third party, if disputes need to be resolved. Examples of applications that require APA include identity escrow schemes, digital auctions, e-cash protocols, remote attestation of computing platforms, safety applications in vehicular networks, and a number of Internet-of-Things (IoT) applications. The conventional approach for authenticating entities and messages in large networks is to employ digital signatures. However, the concept of digital signatures conflicts with the notion of privacy, especially in terms of the signer's anonymity and unlinkability of the issued signatures.

To achieve both authentication and privacy, it is necessary to decouple the information that uniquely identifies the signer from the signature verification procedure. APA schemes enable this decoupling. Existing approaches for APA have limited utility in large networks due to their high computational complexity and/or high communication overhead. Park and his team will investigate novel approaches for APA and study the performance and security requirements of a number of important applications which require APA.

Hsiao Receives a New Intel Project on Defect Diagnosis

Dr. **Michael Hsiao** recently received a new project on defect diagnosis by Intel. Semiconductor companies rely on effective tests to distinguish the good parts from

those defective ones. For those defective chips, it would be desirable to investigate the reason behind the failures, especially if the defect(s) are due to a fixable cause. Diagnosis tools play a key role here, by identifying the source of the underlying defect. In general, the diagnosis tools' goal is to produce a (ranked) list of potential defect locations. Not all defective chips are equal. This is to say that some bad parts may be easier to diagnose than others. The overall research question that this project aims to address is: Is there inherent knowledge embedded in the failing and passing vectors from the tester that can be utilized for diagnosing the error on the fly without resorting to the traditional off-line diagnosis that requires a full netlist? If so, it could significantly reduce the diagnosis costs.



Student News & Highlights

New Students

- Akash Agrawal, M. Eng student (Advisor: Michael Hsiao)
- Shravya Gaddam, MS student (Advisor: Patrick Schaumont)
- Chinmay Deshpande, MS student (Advisor: Leyla Nazhandali)
- Prachi Joshi, PhD student (Advisor: Haibo Zeng)
- Qingyu Liu, PhD student (Advisor: Haibo Zeng)
- Harsha Mandadi, MS student (Advisor: Patrick Schaumont)
- Gaurang Naik, PhD student (Advisor: Jerry Park)
- Yecheng Zhao, PhD student (Advisor: Haibo Zeng)

Summer Interns

- Akash Agrawal, Intel Corporation, Hillsboro, OR, (Advisor: Michael Hsiao); internship in summer and fall
- Mahmoud Awadallah, Bihrle Applied Research, Hampton, VA (Advisor: Lynn Abbott)
- Pooja Harekoppa, Intel Labs, Santa Clara, CA (Advisor: Lynn Abbott)
- Ahmed Ibrahim, Provost Office, Virginia Tech (Advisor: Lynn Abbott)
- Markus Kusano, NEC Laboratories, Princeton, NJ (Advisor: Chao Wang)

- Sarmad Tanwir, Intel, Santa Clara, CA (Advisor: Michael Hsiao)

Recent Graduates

- Vineeth Acharya (MS, Advisor: Michael Hsiao) joined National Instruments, Austin, TX
- Sharad Bagri (MS, Advisor: Michael Hsiao) joined Intel, Santa Clara, CA
- Michael Dsouza (MS, Advisor: Michael Hsiao) joined Synopsys, Mountain View, CA
- Hassan Eldib (Ph.D., Advisor: Chao Wang) became a postdoc at Rice University
- Ege Gulcan (MS, Advisor: Patrick Schaumont) joined Accenture in Istanbul, Turkey
- Sepideh Khoshnood (MS, Advisor: Chao Wang) joined Microsoft, Redmond, WA
- Branden Marcellino (MS, Advisor: Michael Hsiao) joined Northrop Grumman
- Prateek Puri (MS, Advisor: Michael Hsiao) joined CISCO, San Jose, CA
- Zeying Yuan (MS, Advisor: Michael Hsiao) joined Apple

Publications

Please click a title **in blue** to view the abstract.

- V. Acharya, S. Bagri, and M. S. Hsiao, "Branch guided functional test generation at the RTL," *Proceedings of the IEEE European Test Symposium*, May 2015
- K. Adhikari, J. Street, C. Wang, Y. Liu, and S. Zhang, "Verifying a Quantitative Relaxation of Linearizability via Refinement," *Springer International Journal on Software Tools for Technology Transfer (STTT)*, 2015.
- Z. Al-Bayati, Y. Sun, H. Zeng, M. Di Natale, Q. Zhu, and B. Meyer. "Task Placement and Selection of Data Consistency Mechanisms for Real-Time Multicore Applications." *Proceedings of the 21st IEEE Real-Time and Embedded Technology and Application Symposium (RTAS)*, April 2015.
- S. Aly, A. Trubanova, A. L. Abbott, S. W. White, and A. Youssef, "VT-KFER: A Kinect-based RGBD+Time Dataset for Spontaneous and Non-Spontaneous Facial Expression Recognition," *Proceedings: 8th IAPR International Conference on Biometrics* (ICB-2015), Phuket, Thailand, May 2015.
- S. Bhattarai, A. Ullah, J. Park, J. Reed, D. Gurney, and B. Gao, "Defining incumbent protection zones on the fly: Dynamic boundaries for spectrum sharing," *2015 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*, Sweden, Sep.–Oct. 2015.
- R. Bloem, B. Konighofer, R. Konighofer, and C. Wang, "Shield Synthesis: Runtime Enforcement for Reactive Systems," *Proceedings: International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS 2015)*. April 2015.

- P. Deng, F. Cremona, Q. Zhu, M. Di Natale, and H. Zeng. "A Model-based Synthesis Flow for Automotive CPS." *Proceedings of the 6th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, April 2015.
- Y. Dou, K. Zeng, Y. Yang, D. Yao, "MadeCR: Correlation-based Malware Detection for Cognitive Radio," *2015 IEEE Conference on Computer Communications (INFOCOM)*, April 26 – May 1 2015.
- H. Eldib, C. Wang, M. Taha, and P. Schaumont, "Quantitative Masking Strength: Quantifying the Power Side-Channel Resistance of Software Code," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 2015.
- K. Gent and M. S. Hsiao, "Abstraction-based relation mining for functional test generation," *Proceedings of the IEEE VLSI Test Symposium*, May 2015.
- S. Guo, M. Kusano, C. Wang, Z. Yang, and A. Gupta, "Assertion Guided Symbolic Execution of Multithreaded Programs," *Proceedings: ACM Symposium of the Foundations of Software Engineering (FSE 2015)*, Aug 2015.
- S. Khoshnood, M. Kusano, and C. Wang, "ConcBugAssist: Constraint Solving for Diagnosis and Repair of Concurrency Bugs," *Proceedings: International Symposium on Software Testing and Analysis (ISSTA 2015)*, July 2015.
- S. Kim, J. Park, and K. Bian, "PSUN: An OFDM Scheme for Coexistence with Pulsed Radar," *2015 Int'l Conference on Computing, Networking, and Communications (ICNC)*, California, USA, Feb. 2015, 5 pp.
- V. Kumar, H. Li, J. Park, K. Bian, and Y. Yang, "Group signatures with probabilistic revocation: A computationally-scalable approach for providing privacy-preserving authentication," *2015 ACM Conference on Computer and Communications Security (CCS)*, Denver, USA, Oct. 2015.
- M. Kusano, A. Chattopadhyay, and C. Wang, "Dynamic Generation of Likely Invariants for Multithreaded Programs," *Proceedings: IEEE/ACM International Conference on Software Engineering (ICSE 2015)*, May 2015.
- B. Mak, M. Chen, G. Zhang, L. Huang, and H. Zeng. "Online energy management strategy for Hybrid Electric Vehicle." *Proceedings of the 6th International Conference on Future Energy Systems (ACM e-Energy)*, Poster/Demo, July 2015.
- I. Munagani, M. S. Hsiao, and A. L. Abbott, "On the Uniqueness of Fingerprints via Mining of Statistically Rare Features," *Proceedings: IEEE International Symposium on Technologies for Homeland Security* (HST 2015), Boston, MA, Apr. 2015.
- P. Puri and M. S. Hsiao, "Fast stimuli generation for design validation of RTL circuits using binary particle swarm optimization," *Proceedings of the IEEE International Symposium on VLSI*, July 2015.
- P. Puri and M. S. Hsiao, "SI-SMART: functional test generation for RTL circuits using loop abstraction and learning recurrence relationships," *Proceedings of the IEEE International Conference on Computer Design*, October 2015.

- M. Saleh, A. L. Abbott, and G. W. Flintsch, “3D Pavement Surface Spherical Representation and Reconstruction,” to appear in *Proceedings: 95th Annual Meeting of the Transportation Research Board*, Washington, D.C., Jan. 2016.
- A. Sarkar, A. L. Abbott, and Z. Doerzaph, “Assessment of Video Magnification for Nonintrusive Heart Rate Measurement,” to appear in *Proceedings: IEEE First International Conference on Control, Measurement and Instrumentation* (CMI 2016), Kolkata, India, Jan. 2016.
- A. Sarkar, A. L. Abbott, and Z. Doerzaph, “ECG Biometric Authentication Using a Dynamical Model,” *Proceedings: IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems* (BTAS 2015), Arlington, VA, Sept. 2015.
- S. Tanwir, S. Prabhu, M. S. Hsiao, and L. Lingappan, "Information-theoretic and statistical methods of failure log selection for improved diagnosis," *Proceedings of the IEEE International Test Conference,* October 2015.
- A. Ullah, S. Bhattarai, J. Park, J. Reed, D. Gurney, and B. Bahrak, “Multi-tier exclusion zones for dynamic spectrum sharing,” *2015 IEEE Int’l Conference on Communications (ICC)*, London, UK, June 2015.
- C. Wang, Z. Gu, and H. Zeng. “Integration of Cache Partitioning and Preemption Threshold Scheduling to Improve Schedulability of Hard Real-Time Systems.” *Proceedings of the 27th Euromicro Conference on Real-Time Systems (ECRTS)*, July 2015.
- J. Xiong, D. Wu, H. Zeng, S. Liu and X. Wang. “Impact Assessment of Electric Vehicle Charging on Distribution Systems at Neighborhood Levels.” *Proceedings of the 28th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, May 2015.
- Q. Yi, Z. Yang, S. Guo, C. Wang, J. Liu, and C. Zhao, “Post Conditioned Symbolic Execution,” *Proceedings: IEEE International Conference on Software Testing, Verification and Validation (ICST 2015)*. April 2015.
- Q. Yi, Z. Yang, J. Liu, C. Zhao, and C. Wang, “Explaining Software Failures by Cascade Fault Localization,” *ACM Transactions on Design Automation of Electronic Systems (TODAES)*, 2015.
- Q. Yi, Z. Yang, J. Liu, C. Zhao, and C. Wang, “A Synergistic Analysis Method for Explaining Failed Regression Tests,” *Proceedings: IEEE/ACM International Conference on Software Engineering (ICSE 2015)*. May 2015.
- L. Zang, A. Chattopadhyay, and C. Wang, “Round-Up: Runtime Verification of Quasi Linearizability for Concurrent Data Structures,” *IEEE Transactions on Software Engineering (TSE)*, 2015.
- H. Zeng and M. Di Natale. “Computing periodic request functions to speed-up the analysis of non-cyclic task models.” *Real-Time Systems Journal*, 51(4): 360-394, July 2015.

- N. Zhang, M. Kusano, and C. Wang, "Dynamic Partial Order Reduction for Relaxed Memory Models," *Proceedings: ACM Conference on Programming Language Design and Implementation (PLDI 2015)*. June 2015.
- Q. Zhao, Z, Gu, and H. Zeng. "Resource Synchronization and Preemption-Thresholds within Mixed-Criticality Scheduling." *ACM Transactions on Embedded Computing Systems (TECS)*, 14(4): 1-25, October 2015.