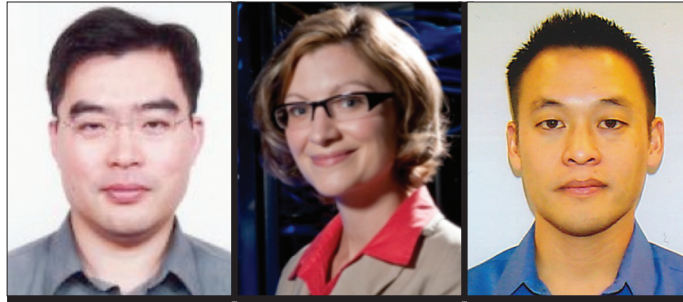


## NETWORK TESTING SERIES



Ying-Dar Lin

Erica Johnson

Eduardo Joo

Slightly different from the previous two issues, this issue consists of one contribution from open calls, on reusing simulated code onto the experimented wireless platforms, and two invited contributions from National Chiao Tung University Network Benchmarking Laboratory (NCTU-NBL), on false positive/negative analysis of intrusion detection, and the University of New Hampshire InterOperability Laboratory (UNH-IOL), on interoperability testing of the emerging Ethernet-centric data center bridging. These two laboratories are directed by two of the editors of this series. The invited submissions also went through the review process to check and improve their quality. The major reason we invited our colleagues to submit to this series was based on an observation made in the last issue: Soliciting highly industry-oriented submissions from the test laboratories and test equipment providers might be more promising than soliciting from the manufacturers. Although we do not rule out the possibility of submissions from manufacturers, our experiences have indicated us they are either too busy to write at the quality we require or reluctant to leak test results on their own products. The open calls for future issues are still valid, with two due dates on June 1 and December 1 every year. But we shall continue to invite contributions from the leading test laboratories and test equipment providers. The inputs from NBL and IOL in this issue serve as the first move and also an example in soliciting these types of input.

The invited contributions from our colleagues did not disappoint us. The article from UNH/IOL (“Testing Challenges of Data Center Bridging Networks”) first gives a tutorial on Ethernet-centric data center bridging (DCB), where the same Ethernet interconnects storage, processors, and general data networking. In an effort to replace the currently predominant Fibre Channel technology, Ethernet itself needs extensions to avoid congestion and hence frame loss in bridging the increasingly heavy traffic inside data centers with iSCSI over DCB. The congestion scenario in data centers could be more severe than the gener-

al data networking due to the long transfer patterns to and from the storage devices. Four extensions to Ethernet were defined or are being developed under DCB in the IEEE 802.1 Data Center Bridging Task Force: priority-based flow control, enhanced transmission selection, congestion notification, and data center bridging exchange. The article discusses the challenges in testing these four mechanisms, and how conformance testing and interoperability testing could complement each other. Based on their 13 interoperability test events (named “plugfests”) over three years, the authors present the results, revealing the interoperability issues that decreased gradually from over 100 in one plugfest event to a few tens.

The article from NCTU-NBL (“Statistical Analysis of False Positives and False Negatives from Real Traffic with Intrusion Detection/Prevention Systems”) analyzed over 2000 false positive (FP) and false negative (FN) cases collected in 16 months from the campus beta site of NCTU and the packet trace library of NBL. It first reviews the methodology that leverages “multiple” commercial intrusion detection/prevention systems to capture intrusions in the real traffic of the beta site. When these multiple systems have different opinions, some of them would be diagnosed as false positives or false negatives. These collected real but false cases serve as the basis for this study. Some interesting findings are reported:

- There are 13 times more FPs than FNs because many signatures are so short that they would match some benign traffic.
- 91 percent of FPs are not related to security issues but to policy management configured for access control.
- The classic buffer overflow, SQL server attacks, and worm slammer attacks account for 93 percent of FNs, which mean variations of intrusions still sneak past many intrusion detection/prevention systems.

Detailed case studies and analysis further reveal some insights in which manufacturers or researchers of this area would be interested.

The only open call article in this issue (“CommonCode:

A Code-Reuse Platform for Wireless Network Experimentation”) evolves an interesting idea of reusing simulated code onto experimented platforms. The virtue of this approach is combining the ease of implementation in simulations and the realistic PHY/MAC channel conditions in a well controlled repeatable environment. The authors tried to resolve the challenges of achieving an ideal code reuse platform by developing three mechanisms:

- Hardware adaptor to configure the PHY/MAC parameters of simulations into hardware platforms
- Real-time event schedule to transform the simulation event time to the real event time
- Debugging platform to run and compare the common code (CC) on both simulation (CC-sim) and experimentation (CC-exp)

It shows the effectiveness of this promising approach by a series of simulations and experiments.

### BIOGRAPHIES

YING-DAR LIN (ydlin@cs.nctu.edu.tw) is a professor of computer science at National Chiao Tung University (NCTU) in Taiwan. He received his Ph.D. in computer science from the University of California at Los Angeles (UCLA) in 1993. He spent his sabbatical year as a visiting scholar at Cisco Systems in San Jose in 2007–2008. Since 2002 he has been the founder and director of the Network Benchmarking Laboratory (NBL, [www.nbl.org.tw](http://www.nbl.org.tw)), which reviews network products with real traffic. He also cofounded L7 Networks Inc. in 2002, which was later acquired by D-Link Corp. His research interests include design, analysis, implementation, and benchmarking of network protocols and algorithms, quality of services, network security, deep packet inspection, P2P and mesh networking, and embedded

hardware/software co-design. His work on multihop cellular has been cited over 500 times. He is currently on the editorial boards of *IEEE Transactions on Computers*, *IEEE Computer*, *IEEE Network*, the Network Testing Series of *IEEE Communications Magazine*, *IEEE Communications Surveys and Tutorials*, *IEEE Communications Letters*, *Computer Communications*, *Computer Networks*, and *IEICE Transactions on Information and Systems*. He recently published a textbook, *Computer Networks: An Open Source Approach* ([www.mhhe.com/lin](http://www.mhhe.com/lin)) with Ren-Hung Hwang and Fred Baker (McGraw-Hill, 2011), which is the first textbook interleaving open source implementations with protocol designs.

ERICA JOHNSON ([erica.johnson@iol.unh.edu](mailto:erica.johnson@iol.unh.edu)) is director of the University of New Hampshire InterOperability Laboratory. In this role, she manages and oversees over 20 different data networking and storage technologies providing all aspects of administration, including coordination of high-profile testing events, coordination with different consortia, and working with various industry fora. She is also a prominent member of organizations both internally and externally. She enjoys a powerful mix of technology and business related activities. At the University of New Hampshire she participates in the UNH Steering Committee for Information Technology, the Senior Vice Provost for Research Working Group, and the Computer Science Advisory Board. In the industry, she was appointed the technical representative of North America for the IPv6 Ready Logo Committee and was also chosen to be an IPv6 Forum Fellow. Passionate about the laboratory and its possibilities, she continues to work with many industry fora, commercial service providers, network equipment vendors, and other universities in order to further the InterOperability Laboratory's mission.

EDUARDO JOO ([ejoo@empirix.com](mailto:ejoo@empirix.com)) is a software project leader at Empirix, Inc., in Bedford, Massachusetts. He received his Master of Science in computer system engineering, computer communications and networks, from Boston University in 2006. He joined Empirix, Inc., in 2001 and has led the successful development of network testing and emulation systems, including PacketSphere Network Emulator, PacketSphere RealStreamer, Hammer NxT, and Hammer G5. He is currently leading the development of next-generation mobile broadband data network monitoring and testing tools. His areas of interest include voice and data protocols, and wired, wireless, and mobile network communications.



*Run Ahead of the Curve!*

**IEEE COMMUNICATIONS SOCIETY**

Global Community of Communications Professionals