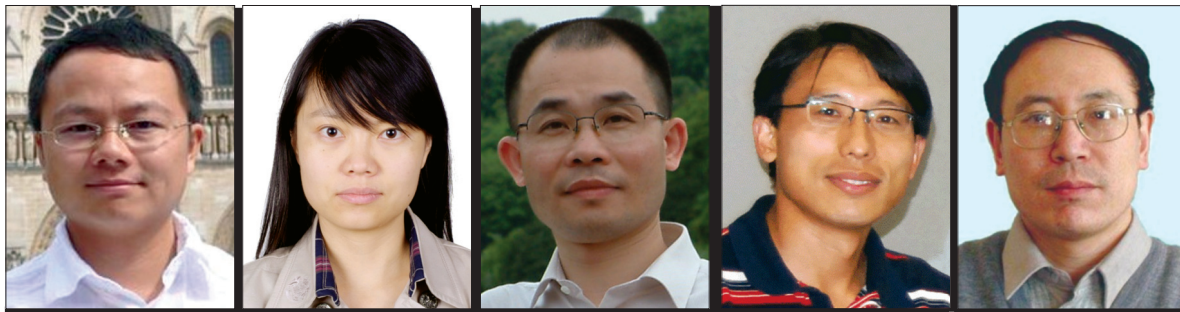


Network Traffic Monitoring, Analysis and Anomaly Detection



Wei Wang

Xiangliang Zhang

Wenchang Shi

Shiguo Lian

Dengguo Feng

Modern computer networks are increasingly pervasive, complex, and ever-evolving due to factors like enormous growth in the number of network users, continuous appearance of network applications, increasing amount of data transferred, and diversity of user behaviors. Understanding and measuring such a network is a difficult yet vital task for network management and diagnosis. Network traffic monitoring, analysis, and anomaly detection provide useful tools for understanding network behavior and determining network performance and reliability so as to effectively and promptly troubleshoot and resolve various issues in practice.

Network traffic monitoring, analysis, and anomaly detection have become a very active research area in the networking community over the past few years. There are several international scientific workshops and conferences as well as projects initiated on this topic. In Europe, for example, the European Commission initiated the FP7 project Decentralized, Cooperative and Privacy-Preserving Monitoring for Trustworthiness (DEMONS) starting in October 2010, aimed at dealing with the major issues of cooperative network monitoring. Network traffic monitoring and analysis is an indispensable tool for various network management activities, such as traffic measurement, pricing and engineering, optimization of network resources, and network planning and design. It also provides a fertile ground for modeling access patterns and network behavior, which is helpful for network performance analysis. Furthermore, network traffic monitoring and anomaly detection provide a sound basis for prevention and reaction in network security, as intrusions, attacks, worms, and other kinds of malicious behaviors can be identified by traffic analysis and anomaly detection.

This special issue is intended to present recent research developments and efforts in addressing major challenges in network traffic monitoring and analysis. In response to the open call, we were pleased to receive 39 submissions from 17 countries. The large number of submissions indicates the high level of interest in network traffic monitoring and analysis. The submissions have been rigorously reviewed, and finally nine articles were selected for publication in this special issue. Due to limited space, five articles are published in this issue (May/June 2011); the other four articles will appear in January/February 2012. The articles provide diverse insights on network traffic monitoring, including experiences, traffic monitoring in traditional networks as well as wireless sensor networks (WSNs), and traffic analysis in the Internet of Things. We hope that all the articles of this special issue will inspire interesting ideas in the research community, and

provide readers with relevant knowledge and techniques on the main issues of network traffic monitoring and analysis.

The first article, “Experiences of Internet Traffic Monitoring with Tstat” by A. Finamore, M. Mellia, M. Meo, M. M. Munafò, and D. Rossi, reports their experiences in engineering and deploying Tstat (TCP Statistic and Analysis Tool), a free open source passive monitoring tool developed by the networking research group at Politecnico di Torino, Italy, over the past 10 years. In this article, the authors discuss the capabilities and internal design of Tstat, and present some examples of measurements collected deploying Tstat at the edge of several European ISP networks in the past years. This article provides general information on and techniques for the design and development of tools for network traffic monitoring and analysis.

With more and more WSNs to be deployed in the real world, monitoring WSNs has become an important issue. The second article, “Packet Traffic: A Good Data Source for Wireless Sensor Network Modeling and Anomaly Detection” by Qinghua Wang, presents a methodology of building behavioral profiles of wireless sensor nodes and networks with packet traffic. Their case studies show that node and network anomalies are detectable by monitoring the evolution of node/network behavioral profiles.

Peer-to-peer (P2P) traffic has grown to be one of the dominant sources of network traffic. The third article, “Measurement and Diagnosis of Address Misconfigured P2P Traffic” by Zhichun Li, Anup Goyal, Yan Chen, and Aleksandar Kuzmanovic, reports a study of the address-misconfigured P2P traffic caused by a large number of peers sending P2P file downloading requests to a target that is never part of the P2P network. By analyzing a very large data set, the authors discover that address-misconfigured P2P traffic is one of the major sources of Internet background radiation and is growing quickly. In the article, in order to measure the address-misconfigured P2P traffic, the authors design and implement a tool called P2PScope that detects and diagnoses such traffic.

The article titled “Dynamic Measurement-Aware Routing in Practice” by Guanyao Huang, Saqib Raza, Srini Seetharaman, and Chen-Nee Chuah proposes dynamic measurement-aware routing (DMR) for network-wide traffic measurement. It overcomes the varying nature of both traffic characteristics and measurement objectives by intelligently routing important traffic sub-populations to some appropriate configured/deployed monitors. The whole procedure thus involves initial assessment of flow importance, flowset configuration and flowset routing with considerations of overall network performances. The article outlines the challenges of implementing DMR in practice

and builds an OpenFlow-based prototype for enterprise networks.

The Internet of Things has become a popular topic in recent years. In the last article, "Multimedia Traffic Security Architecture for Internet of Things" by Liang Zhou and Han-Chieh Chao, a media-aware security framework for facilitating various multimedia applications in the Internet of Things is proposed. The authors present a method of multimedia traffic classification and analysis for handling the heterogeneity of diverse applications. Based on this method of traffic classification, a media-aware traffic security architecture is proposed to enable diverse multimedia services provisioning to the users.

Finally, we would like to thank all those who made this special issue possible: the authors who submitted their work, the peer reviewers who contributed their time and effort to help improve the quality and readability of this Issue; Editor-in-Chief Thomas M. Chen for his continuous support in the development of this special topic; and the staff of publication office for their work in editing. We hope that all the articles accepted for this special issue provide readers with informative and helpful information on network traffic monitoring and analysis.

Biographies

WEI WANG (wei.wang.email@gmail.com) is currently working as a researcher at the Interdisciplinary Center for Security, Reliability and Trust (SnT), University of Luxembourg. He received his B.S. and M.S. degrees from Xi'an Shiyu University, Xi'an, China. He earned his Ph.D. degree in control science and engineering from Xi'an Jiaotong University, Xi'an, China, in 2006. During 2005–2006, he conducted advanced research activities first as a research fellow and then as a postdoc in the Department of Information and Communication, University of Trento, Italy. He was a research engineering expert in the Department of Networks, Security and Multimedia, Telecom Bretagne, France, in 2007. He was a postdoctoral research fellow in 2008 at INRIA, France. He was a European Research Consortium for Informatics and Mathematics (ERCIM) Fellow at the Q2S center, Norwegian University of Science and Technology (NTNU), in 2009 and the SnT Center, University of Luxembourg, in 2010. He has authored or co-authored over 30 peer-reviewed papers in various journals and international conferences. His main research interests and experiences are in various areas of computer and network security, network traffic modeling, and data mining.

XIANGLIANG ZHANG (xiangliang.zhang@kaust.edu.sa) is currently a research scientist in the Division of Mathematical and Computer Sciences and Engineering, King Abdullah University of Science and Technology (KAUST). Prior to this, she was an ERCIM research fellow in the Department of Computer and Information Science, NTNU, during April–August 2010. She earned her Ph.D. degree in computer science with great honor from INRIA-University Paris-Sud 11, France, in July 2010. She was a research engineer at INSERM, France, from September 2009 to March 2010. She received M.S. degree and B.S. degrees from Xi'an Jiaotong University in 2006 and 2003, respectively. She visited the University of Luxembourg during July–August 2010. She has authored or co-authored over 30 refereed papers in various journals and conferences, including SIGKDD, ECML/PKDD, ICDM, and CCGRID. Her main research interests and experiences are in diverse areas of data mining, machine learning, and their applications, such as complex system modeling, computer security, autonomic computing, high-performance computing, large-scale data processing, grid/cloud management, and bioinformatics.

WENCHANG SHI (wenchang@ruc.edu.cn) is currently a professor of computer science at the School of Information, Renmin University of China, Beijing. He is in charge of the Information Security Division, and directing the Systems and Information Security Research Laboratory. He is also a professor in the Graduate University of the Chinese Academy of Sciences, Beijing, China. He received a B.S. degree from Peking University, Beijing, China, and M.S. and Ph.D. degrees from the Chinese Academy of Sciences, Beijing, all in computer science. He is a senior member of the China Computer Federation (CCF) and a member of the IEEE Computer Society. He is a committee member of the CCF Information Security Committee, System Software Committee, and Open System Committee, etc..

Before joining RUC, he was a research professor at the Institute of Software, Chinese Academy of Sciences, Beijing, China. His current research interests include information security, trusted security, cloud computing, computer forensics, and operating systems. He was the chief architect of the Redflag Secure Operating System, which became one of the principal products of Redflag Software Co. Ltd, Beijing, China. He has undertaken a lot of research programs funded by the nation and other organizations, published about 100 academic papers, and won a series of science and technology awards.

SHIGUO LIAN (shiguo.lian@ieee.org) got his Ph.D. from Nanjing University of Science and Technology, China. He was a research assistant with City University of Hong Kong in 2004. Since July 2005 he has been a research scientist with France Telecom R&D (Orange Labs) Beijing. He is the author or co-author of more than 80 refereed international journal and conference papers covering topics of secure multimedia communication, intelligent multimedia services, and ubiquitous communication. He has contributed 15 book chapters and holds 16 filed patents. He authored the book *Multimedia Content Encryption: Techniques and Applications* (CRC Press, 2008) and edited five books. He was nominated for the "Innovation Prize in France Telecom" and "Top 100 Doctorate Dissertations in Jiangsu Province" in 2006. He is a member of the IEEE Communications & Information Security Technical Committee, IEEE Multimedia Communications Technical Committee, IEEE SMCS Technical Committee on Soft Computing, and IEEE Technical Committee on Nonlinear Circuits and Systems. He is on the editorial boards of several international journals. He is the guest editor of more than 10 international journals. He is on the organization committee or TPC of refereed conferences, including IEEE ICC 2008/2009/2010, IEEE GLOBECOM 2008/2009/2010, IEEE CCNC 2009, and IEEE ICCCN 2009. He is also a reviewer of refereed international magazines and journals.

DENGGUO FENG (feng@is.iscas.ac.cn) is currently a research professor at the Institute of Software, Chinese Academy of Sciences. He is director of the State Key Laboratory of Information Security (SKLOIS). His research interest lies in security and privacy issues in computer systems and networks, including areas ranging from software security, networking security, and database security to applied cryptography. He is the recipient of various awards including the National Scientific and Technological Progress Award, the CAS Scientific and Technological Progress Award, and the National Distinguished Young Scholar Award. He is also the author of over 30 books and over 200 refereed papers in conferences and journals.

PacketExpert™ - Quad Port Ethernet Tester



Examine Ethernet Networks using GL's PacketExpert™

- ▶ **Available Interfaces (Quad Port)**
 - ▶ 2 Ports - 10/100/1000 Base-T Electrical Interface
 - ▶ 2 Ports of either 1000 Base-X Optical OR 10/100/1000 Base-T Electrical Interface
- ▶ **Key Performance Indicators**
 - ▶ Bit Error Rate and Count
 - ▶ Sync Loss and Error Free Count/Seconds
 - ▶ Throughput, Frame Loss, Latency
 - ▶ Frame Count, Rate
- ▶ **Supports**
 - ▶ Bi-directional RFC-2544 Tests
 - ▶ Bit Error Rate Tests (BERT) on all 4 ports
 - ▶ Portability & USB 2.0 Interface
 - ▶ Q-in-Q (VLAN Stacking) Capability (BERT only)
 - ▶ MPLS Network Testing (BERT only)
 - ▶ IPV4 & IPV6
 - ▶ Smart Loopback & User-defined Loopback
 - ▶ Error Insertion, Sequence Number Generation
 - ▶ Configure VLAN ID, priority, and various header parameters for MAC, IP and UDP layers
 - ▶ Generates Test reports in PDF and CSV
- ▶ **Coming Soon...**
 - ▶ Carrier & Metro Ethernet Network Testing
 - ▶ S-VLAN and S-MPLS for RFC 2544 and Smart Loopback

GL Communications Inc.

301-670-4784 * info@gl.com * www.gl.com