


Special Issue Call for Papers (draft one)



IEEE JOURNAL ON
**SELECTED AREAS IN
COMMUNICATIONS (J-SAC)**

*Special Issue on
Advances in Forensics and Security for Communications and
Networks*

Computer and Internet crimes are on the rise due to the fast paced development of computer and Internet technology and the techniques to combat these crimes are required more and more on a daily basis. Therefore, with the focus on subjects related to information security, Internet communications and electronic business security become very essential. In other words, network forensics has been an emerging research area for IT-related professionals, researchers, and practitioners since the turn of the century. When either data embedding/mining systems, computer systems, network communications, or system detections are applied on crimes committed, it poses a great threat to the safeguarding of information security. However, the one branch of majorities in network forensics is also to focus on “after the commitment”, namely how to collect and analyze digital evidence in an existing communication and network environments.

Digital forensics have recently raised relevant interest in both the academic and the industrial research communities as one of the most promising study and application fields for information security and cyber-crime in communication and network systems. As a matter of fact, the studies of digital forensics pose challenges such as effective evidence collections and efficient forensic procedures in data mining for evidence trace, custody of evidence chain, digital evidence managements and data/image authentication and forensics, cryptography and cryptanalysis in forensics, network forensics.

The interest in digital forensics in network systems is also shown by the relevant industrial and standardization efforts accomplished in the last years in this wide area, from the basic forensic tools, the commercial product of integrated forensic tools developments to a number of academic research projects about network forensics for customized designs in needs, from the standardization efforts of text-interface to graphic interface to facilitate the evidence mining and speed up the investigations to forensic procedures in communication and network systems.

Notwithstanding the relevance of the addressed topic, to the best of our knowledge, the IEEE J-SAC has not devoted yet any special issue to the theme of network forensics, even if partial security analysis in data recovery of related articles have been already published in the magazine/journal. The intensive topics of digital forensics and evidence approval investigated in the usage of working systems have not been more aggressively covered by magazines/journals. Accordingly, the proposed special issue intends to give state-of-the-art overview of problems and solution guidelines emerging in the communication and network systems., thus completing the panorama of current digital forensic research efforts, which are widely inherent to topics of high interest for the J-SAC reader audience, from the physical views-sophisticated techniques for forensic developments in computer and communication-link environments to logical views-programming of interface connections and testing of forensic tools, from conceptual views- effective managements of seized evidence and diverse system operations to user views- in security issues such authentications, forensic procedures, and ethical and policy issues related to network forensics.

The goal of this special issue is to report on cutting-edge research achievements covering those aspects of the forensics and security areas in communications and networks including information and communication technologies, law, social sciences and business administration that are distinctively different from security protocols in computer and network systems in general.

Papers on practical as well as on theoretical topics and problems are invited. Topics include (but are not limited to):

- Electronic mail security
- Web services/XML forensics
- Investigations of packet flows in internet traffic
- Forensic analysis and tracing traitors
- Cyberstalking investigations in network activities
- Formal methods in network forensic computing
- Social networking forensics
- TCP/IP layer security
- Custody of evidence chain in linked-encryption communications
- Incident response and investigation in communications
- Mobile and wireless network security
- Security and privacy for emerging technologies in communications
- Denial-of-service attacks and countermeasures
- Peer-to-peer network security

- Network forensics case studies
- Privacy solutions to web services
- Network forensics
- Detection and protection in internet firewall systems
- Security of GSM/GPRS/UMTS systems
- Key managements in communication channels
- Security protocols in network applications and services
- Phishing and online fraud prevention
- Denial of service and intrusion in network forensics

Schedule

Full manuscript due: **August 15, 2010**

Acceptance notification: **December 20, 2010**

Final manuscript due: **March 1, 2011**

Publication date: **Summer or Fall, 2011 (Tentative)**

Submission Procedure

Prospective authors should follow the IEEE J-SAC manuscript format described in the Information for Authors under <http://www.jsac.ucsd.edu/>. Authors MUST submit their manuscripts through the EDAS peer review website.

Manuscript Submission Due: Aug. 15, 2010 (Tentative)

Guest Editors:

Shiuh-Jeng Wang (corresponding editor)
Central Police University, Taiwan
Email: sjwang@mail.cpu.edu.tw

Javier Lopez
University of Malaga, Spain
Email: jlml@lcc.uma.es

Hamid R. Arabnia,
The University of Georgia, USA
Email: hra@cs.uga.edu

Yi Mu,
University of Wollongong, Australia
Email: ymu@uow.edu.au

Binod Vaidya,
Inst. of Telecom./Univ. of Beira Interior, Portugal
Email: bnvaidya@mail.co.it.pt

Jongsung Kim,
Kyungnam University, Korea
Email: jongsung.k@gmail.com