

CALL FOR PAPERS

IEEE Journal on Selected Areas in Communications Special Issue on Advances in Digital Forensics for Communications and Networking

Computer and Internet crimes are on the rise due to the fast-paced development of computer and Internet technology. Information security in Internet communications and electronic business is essential, and as such, techniques to combat these crimes are required more and more on a daily basis. Network forensics has been an emerging research area for IT-related professionals, researchers, and practitioners since the turn of the century. Crimes committed using data embedding/mining systems, computer systems, network communications, or system detections pose a great threat to information security. Another area of focus in network forensics is how to collect and analyze digital evidence in an existing communication and network environment.

Digital forensics has many challenges, including effective evidence collection and efficient forensic procedures in data mining for evidence trace, custody of evidence chain, digital evidence management and data/image authentication and forensics, cryptography and cryptanalysis in forensics, and network forensics. The interest in digital forensics in network systems can be seen in industrial and standardization efforts accomplished in the last years. Examples include basic forensic tools, such as commercial integrated forensic tools developments, the standardization efforts of text-interface to graphic interface to facilitate evidence mining and speed up investigations, and forensic procedures in communication and network systems.

The proposed special issue will give a state-of-the-art overview of problems and solution guidelines emerging in communication and network systems, thus completing the panorama of current digital forensic research efforts. A wide variety of topics of interest to the J-SAC audience will be addressed, from the physical views such as 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, such as effective management of seized evidence and diverse system operations, to user views - in security issues such as 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 aspects of the forensics and security areas in communications and networks that are distinctively different from security protocols in computer and network systems in general, including information and communication technologies, law, social sciences and business administration.

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

- Web services/XML forensics
- Integrity of digital evidence and live investigations
- Forensic analysis and tracing traitors
- Cyberstalking investigations in network activities
- Formal methods in network forensic computing
- Social networking forensics
- Network forensics case studies
- Multimedia analysis for forensics
- Network forensics
- Custody of evidence chain in networking systems
- Incident response and investigation in communications
- Digital forensics surveillance technology and procedure
- Security and privacy in forensics and communications
- Legal, ethical and policy issues in network forensics
- Steganography and steganalysis in network forensics
- Data mining for evidence trace in networks
- Communication protocols in network forensics
- Phishing and online fraud prevention in communications

Prospective authors should follow the IEEE J-SAC manuscript format described in the information for authors. All papers should be submitted in PDF format via email to Prof. Shih-Jeng Wang, sjwang@mail.cpu.edu.tw, according to the following timetable:

- Full manuscript due: August 1, 2010
- Acceptance notification: February 1, 2011
- Final manuscript due: April 1, 2011
- Publication date: 3rd Quarter 2011

Shih-Jeng Wang Central Police University, Taiwan sjwang@mail.cpu.edu.tw	Javier Lopez University of Malaga, Spain jlm@lcc.uma.es	Hamid R. Arabnia The University of Georgia, USA hra@cs.uga.edu
Yi Mu University of Wollongong, Australia ymu@uow.edu.au	Binod Vaidya Inst. of Telecom./Univ. of Beira Interior, Portugal bnvaidya@mail.co.it.pt	Jongsung Kim Kyungnam University, Korea jongsung.k@gmail.com