Journal of Universal Computer Science, vol. 15, no. 2 (2009), 398-400
submitted: 18/12/08, accepted: 10/1/09, appeared: 28/1/09 © J.UCS

Multimedia Security in Communication (MUSIC)

J.UCS Special Issue

Shiguo Lian
(France Telecom R&D (Orange Labs) Beijing, China
shiguo.lian@orange-ftgroup.com)

Yan Zhang
(Simula Research Laboratory, Oslo, Norway
yanzhang@ieee.org)

Stefanos Gritzalis
(University of the Aegean, Mytilene, Greece
sgritz@aegean.gr)

Yu Chen
(State University of New York - Binghamton, USA
ychen@binghamton.edu)

With the rapid development of communication techniques, it becomes more and more practical to talk with anyone anywhere. As an important aspect, multimedia (image, video, audio, etc.) enriches humans' daily life. Nowadays, multimedia communication is in close relation with the activities in entertainment, politics, economics, militaries, industries, etc., which makes it urgent for protecting multimedia security, e.g., confidentiality, integrity, ownership or identity. Generally, multimedia security is different from text/binary data security since multimedia content is often of large volumes, with interactive operations, and requires real-time responses. Additionally, multimedia security is in close relation with the services. Different services require different methods for content transmission or distribution, paying, interaction, etc. Now, various new services arise, such as mobile TV, IPTV, IMS, VoIP, p2p living or download, convergence of mobile and Internet, etc. In mobile TV, the terminal's power should be considered when designing the multimedia protection methods that may be different from traditional means. In p2p living, the distributed architecture requires the protection means different from the server-client mode. Additionally, under the environment of network convergence, the smart means adaptive to different networks are expected.

The aim of this special issue is to present a collection of high-quality research papers that report the latest research advances more on secure multimedia transmission and distribution than on multimedia content protection. In this special issue, we selected 5 papers, which can demonstrate advanced works in this field. It is composed of the papers both selected from normal submissions and from the 2008 International Workshop on Multimedia Security in Communication (MUSIC'08)

(http://www.music-com.org). MUSIC'08 has 16 accepted papers out of 50 submissions, from which 4 were selected to be invited to this special issue. Additionally, 1 paper is selected from 5 normal submissions. All the papers submitted to the special issue were reviewed by at least two anonymous referees each and had two rounds of improvement. A detailed overview of the selected works is given below.

The first article is entitled "On the Superdistribution of Digital Goods" (A. U. Schmidt). The article gives a survey on Superdistribution that is conceptually different from both Digital Rights Management and p2p content sharing, and is regarded as a third field in its own right. From this article, you can get the general structure of Superdistribution networks, the definition of digital goods, the examples for digital good superdistribution, and the properties of Superdistribution (in such lawful, economical, technical and security aspects). Specially, some latest research works (e.g., trusted set-top box, trust-enhanced Control Access Module, online Conditional Access System, and online registration) in secure superdistribution are reviewed. Finally, some open issues and hot topics in superdistribution are provided to researchers or students interested in this field.

The second article is entitled "On the Design of Secure Multimedia Authentication" (J. W. Wang, J. M. Lv, S. G. Lian, and G. J. Liu). The article reviews the existing multimedia authentication algorithms that are used to detect the integrity of received multimedia content, classified them into three categories (i.e., watermarking authentication, signature-based authentication, and content-based watermarking authentication), proposes the principles for design a secure multimedia authentication scheme, and presents an image authentication scheme designed by the proposed principles. It is expected to provide valuable information to researchers or engineers working in multimedia authentication.

The third article is entitled "Stability in Heterogeneous Multimedia Networks under Adversarial Attacks" (D. Koukopoulos). The article studies the stability property of multimedia networks under adversarial attacks. In multimedia networks, a variety of communication protocols are simultaneously running over different hosts, which leads to adversarial attacks that make the networks unstable by some adversarial traffic patterns. The article solves the stability problem with a theoretical model, and also gives an experimental evaluation of the stability behaviour of specific network constructions with different protocol compositions under an adversarial strategy. Some of its results may provide valuable information to multimedia network designers.

The fourth article is entitled "The Topology Change Attack: Threat and Impact" (M. A. Abdelouahab, A. Bouabdallah, M. Achemlal and S. Laniepce). The article reviews the existing attacks on peer-to-peer networks, specially the Topology Change Attack (TCA), proposes the methods to investigate TCA's harms to the Internet Service Provider (ISP). A new cycle-based simulator which simulates eDonkey clients hosted on different ISPs is developed to evaluate and validate the TCA impact. Results indicate that eDonkey and ISPs infrastructure are vulnerable to such attack and demonstrate that server-list file represents a weakness point, which provides some valuable information to peer-to-peer designers or Internet Service Providers.

The fifth article is entitled "Detecting Distributed Denial-of-Service Attack Traffic by Statistical Test" (C.-L. Chen). The article proposes a new detection method

for Distributed Denial-of-Service (DDoS) attack traffic based on two-sample t-test. It first investigates the statistics of normal SYN (Synchronize) arrival rate (SAR) that are confirmed to follow normal distribution. The proposed method identifies the attack by testing the difference between incoming SAR and normal SAR, and the difference between the number of SYN and ACK (Acknowledges) packets. The experimental results show that the possibilities of both false positives and false negatives are very low, and it has the capability of detecting DDoS attack quickly.

In conclusion, this issue of Multimedia Security in Communication (MUSIC) offers a groundbreaking view into the recent advances in multimedia communication and security. This issue offers the latest research works for both academic and industry. Finally, we would like to express our gratitude to the Editor-in-Chief, Prof. Hermann Maurer, for his advice, patience, and encouragements since the beginning until the final stage. Special thanks go to Mag. Dana Kaiser during the production. We thank all anonymous reviewers who spent much of their precious time reviewing all the papers. Their timely reviews and comments greatly helped us select the best papers in this special issue. We also thank all authors who have submitted their papers for consideration for this issue. We hope you will enjoy reading the great selection of papers in this issue.

Shiguo Lian
Yan Zhang
Stefanos Gritzalis
Yu Chen
January 2009