J Supercomput (2012) 62:1–3
DOI 10.1007/s11227-011-0684-3

Guest editorial: Advances in Digital and Multimedia Convergence

SooKyun Kim · Johnnes Arreymbi · Chia-Chen Lin

Published online: 23 September 2011

Digital and Multimedia convergence is propelled by the advent of digital and multimedia technology. This special issue is intended to foster state-of-the-art research in the area of digital and multimedia convergence (DMC). The DMC offers unprecedented opportunities for various modern multimedia applications and systems, such as ubiquitous computing technology, human-computer interaction, and convergence in multimedia technology, bio-chips, RFID, and multimedia visualization. Its purpose is to solve the various problems of advanced digital and multimedia processing using computer science technology. This special issue focuses on advances in digital and multimedia convergence.

This special issue has become one of the hottest topics in digital and multimedia convergence. This special issue will also serve as a landmark source for digital and multimedia convergence and will provide the reader with the most important state-of-the-art technologies in areas of digital and multimedia processing for DMC. We believe that this special issue will have a high citation in the areas of digital and multimedia convergence.

The first paper, by Sudip et al., proposes a routing algorithm, named *learning automata based fault-tolerant routing algorithm* (*LAFTRA*), which is capable of routing

S. Kim (✉)
Department of Game Engineering, Paichai University, Daejeon, Korea
e-mail: kimsk@pcu.ac.kr

J. Arreymbi
University of East London, London, UK
e-mail: j.arreymbi@uel.ac.uk

C.-C. Lin
National Chiao Tung University, Hsinchu, Taiwan
e-mail: mhlin3@pu.edu.tw

in the presence of faulty nodes in MANETs using multi-path routing. They used the theory of Learning Automata (LA) for optimizing the selection of paths, reducing the overhead in the network, and for learning about the faulty nodes present in the network. The proposed algorithm can be juxtaposed to any existing routing protocol in a MANET. The results of simulation of our protocol using network simulator 2 (ns-2) shows the increase in packet delivery ratio and decrease in overhead compared to the existing protocols.

The second paper, by Wang et al., introduces a class of distributed broadcast algorithms based on variations of Relative Neighborhood Graphs (RNG). Contrasted to the original RNG-based algorithms, the proposed algorithms consider the remaining battery energy of the nodes and the distance between the nodes as criteria for determining the relative neighborhood of a node. Simulations are conducted to demonstrate that the proposed algorithms improve over the original RNG in several aspects, including the reduction of broadcast storms, longer path lifetime, and shorter broadcast latency.

The third paper, by Lee et al., presents secure communication. In internet protocol television (IPTV) broadcasting, service providers charge subscribing fee by scrambling the program with conditional access system (CAS) using control words (CWs). A smart card is used to decrypt the CWs and transfer them back to set-top box (STB) to descramble the scrambled program. Secure communication between STB and the smart card is closely related with the benefit of service providers and the legal rights of users. In addition, secure key exchange with mutual authentication in the communication between STB and the smart card is an essential part of secure communication that will significantly improve the security of the system. To provide secure communication with mutual authentication in IPTV broadcasting, there are several schemes. The schemes proposed a secure and efficient method for the communication between STB and the smart card. Unfortunately, the schemes still have some security flaws. In this paper, we review the previous schemes; they are vulnerable to several attacks. Further, we recommend some modifications to the schemes to correct these security flaws and present a formal analysis about our improved protocol using logic based formal method.

The next paper, “An Ontological Approach to Support Legal Information Modeling,” authored by Wenhuan Lu et al., proposes an ontology-guided approach that provides a semantic primitive representation of legal information with intention perspective. The domain ontology developed is used as a fundamental conceptual framework to maintain the consistency among diverse legal representation.

The fifth paper, by Chao et al., is about SCTP, an emerging transmission protocol providing high availability and increasing reliability. The present study modifies the multi-streaming mechanisms of SCTP and the queue management mechanism of RED, enabling SCTP to use network resources efficiently and providing a differential stream protection for the encoding frame types of MPEG video stream.

The sixth paper, by Muhammad Rizwan Butt et al., says ”In this paper, a lexical routing metric to enable path-wise link quality-aware routing in Wireless Sensor Networks (WSNs) has been proposed. The realization of this routing metric is achieved by applying the indexing techniques of formal language processing in multi-metric route classification and cost evaluation for WSNs. The metric is motivated from the

fact that IEEE 802.15.4 networks are formed on links with highly variable quality, and selection of poor quality links degrades the delivery of the data considerably. We propose LABILE, a composite routing metric that is implemented through modifying RREQ and RREP structures of AODV to capture and convey two-state link information to destination, which in turn is processed through an easy to compute routing lexicon and a corresponding lexical algorithm for path selection in case of availability of multiple paths."

The next paper, An Authentication Protocol offering Service Anonymity of Mobile Device in Ubiquitous Environment, authored by Jong Hyuk Park, suggests the safe authentication method that protects against information exposure by guaranteeing anonymity of service with temporal ID. It provides efficiency because the AAA authentication server is based on the ticket given to a service server without the need of reauthentication when mobile node authorized from the AAA authentication server receives service.

The eighth paper, by Jeong, considers that as an IEEE 802.11-based mobile computing system has been established as the base structure of high-speed wireless network, people's interest in mobility and security of mobile terminal has increased. To reinforce security, 802.1x and 802.11i using EAP were used in standardized instrument. But it was found to be unsuitable for real time multimedia service because of the time delay. In this paper, we suggest a Fast and Secure Handover (FSH) scheme which minimizes time delay in the handover authentication process and prevents from MITM (Man in the Middle) attack. This scheme carries out the re-association process which is necessary for high-speed handover using Inter Access Point Protocol (IAPP) and Old_MSK. To make the existing 802.1x-based user certification procedure suitable for high-speed handover, the terminal and pre-handover-accessed Old_AP make Rough_AP to prevent MITM. To do this, Old_AP uses the Old_MSK-used encrypted method which was used to encrypt MAC information of the mobile terminal and Old_AP. Hereby, FSH has been developed to become a high-speed handover which has the 802.1x-supported security level and the skill of preventing MITM. In this paper, by simulation (NS-2), superiority is confirmed in streaming service such as decreased handover time delay and VoIP.