Mobile Netw Appl (2012) 17:506–507
DOI 10.1007/s11036-012-0369-z

ACM/Springer Mobile Networks and Applications (MONET) Special Issue on "Collaborative Computing: Networking, Applications and Worksharing"

Songqing Chen · Le Gruenwald · James Joshi · Karl Aberer

Published online: 30 March 2012

Recent advances in computing have contributed to the growing interconnection of our world, including 3 G/4 G wireless networks, web 2.0 technologies, computing clouds, just to mention a few. The potential for collaboration among various components has exceeded the current capabilities of traditional approaches to system integration and interoperability. As the world heads towards unlimited connectivity and global mobile computing, collaboration becomes one of the fundamental challenges. We view collaborative computing as the glue that brings the components together and also the lubricant that make them work together. The 6th *International Conference on Collaborative Computing: Networking, Applications and Worksharing* (*CollaborateCom*) serves as a premier international forum for discussion among researchers and practitioners interested in collaborative networking, technology and systems, and applications.

A total of 62 submissions were received for *CollaborateCom2010*. The Program Committee selected 23 papers (acceptance rate of 37 %) after a rigorous review and a follow up discussion. After further review of the accepted papers immediately after the conference, we have selected four papers that relate to the theme of *CollaborateCom* and mobile computing.

In the first paper titled "Fast Response PKC-Based Broadcast Authentication in Wireless Sensor Networks," Chuchaisri et al. consider two new broadcast authentication schemes, called the key pool scheme and the key chain scheme. Both schemes utilize a Bloom filter and the distribution of secret keys among sensor nodes to create fast and capture-resistant PKC-based broadcast authentication protocols. The experimental results show that the key pool scheme is able to keep forged message propagation to the minimal even when the majority of the nodes have been captured by the attacker. The key chain scheme has smaller transmission overhead than the key pool scheme at the expense of less resistance to node capturing. Authors further present two generic improvements to these schemes.

In the second paper titled "On Security and Reliability using Cooperative Transmissions in Sensor Networks," Aksu et al. present an analytical framework for evaluating when cooperative transmissions may be more beneficial than SISO transmissions in sensor networks with a mix of honest and malicious and/or compromised nodes. Additional parameters such as the path-loss exponent are considered and the framework allows people to evaluate the conditions when cooperative transmissions are better than SISO transmissions.

In the third paper titled "Scaling Group Communication Services with Self-adaptive and Utility-driven Message Routing," Wang et al. identify the inefficiency of geodistance based routing protocols in many existing multicast overlay networks in terms of both resource utilization and group communication efficiency. Basically, they have developed a

S. Chen (✉)
George Mason University,
Fairfax, VA, USA
e-mail: sqchen@cs.gmu.edu

L. Gruenwald
National Science Foundation and University of Oklahoma,
Norman, OK, USA
e-mail: lgruenwa@nsf.gov

J. Joshi
University of Pittsburgh,
Pittsburgh, PA, USA
e-mail: jjoshi@sis.pitt.edu

K. Aberer
EPFL,
Lausanne, Switzerland
e-mail: karl.aberer@epfl.ch

utility-based routing scheme (UDR) that can provide efficient group communication services in a decentralized geographical overlay network. A utility function is defined to refine the geodistance based routing in such a way that the routing path selection can carefully incorporate both geodistance based metric and the network latency. And it is further enhanced with self-adaptive capability by considering the nodes' state and network density. A suite of optimization techniques is also designed to minimize the maintenance cost and computational complexity of the self-adaptive and utility-drive routing scheme.

In the fourth and also the last paper titled "Hardware Security Device Facilitated Trusted Energy Services," Zic et al. describe how to develop a hardware based security solution for a novel, smart-grid enabled energy services system. After background introduction to a new energy services model, authors present how they incorporated a CSIRO developed portable trusted computing platform into a practical, prototype system which assures that all transactions between the energy service company and the consumer are trustworthy, secure and private.

We strongly believe that the selected papers make significant contributions to researchers, practitioners, and students working in the areas of collaborative mobile systems and applications.

We would like to express our sincere gratitude to all the authors for their contributions and to the referees for their hard work in reviewing the papers. Our special thanks also to the editorial board of MONET and Prof. Imrich Chlamtac, the Editor in Chief of this journal, for their support.