Mobile Information Systems 7 (2011) 165–167
DOI 10.3233/MIS-2011-0122
IOS Press

Guest Editorial

Emerging Wireless and Mobile Technologies

Fang-Yie Leu[a], Ilsun You[b] and Feilong Tang[c]
[a]*Department of Computer Science, TungHai University, Tunghai, Taiwan*
[b]*School of Information Science, Korean Bible University, Nowon-gu, Seoul, South Korea*
[c]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China*

Recent advances in wireless and mobile technologies have led to a new paradigm of the high-tech society and people's daily life. Accordingly, wireless and mobile technologies have been gaining tremendous attentions from researchers all over the world in recent years. However, a lot of new challenges, which go much beyond conventional network systems, still need to be solved for advanced applications. To further improve the quality of the modern communication, new techniques need to be continuously explored and developed. This special issue looks for significant contributions and high quality research results on wireless and mobile technologies in theoretical and practical aspects, especially on QoS routing, distributed authentication mechanism, automatic security assessment, fast handover security mechanism, enhancing MISP with Fast Mobile IPv6 and applications in wireless mobile networks, as well as ad-hoc networks.

This special issue grew out of selected best papers from the Fifth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA 2010), held in Fukuoka, Japan, and the 4th International Workshop on Intelligent, Mobile and Internet Services in Ubiquitous Computing (IMIS 2010), held in Krakow, Poland. This event was an effort to take up the challenges and to bring together an international community in the area.

The first paper [1], "QoS Routing in Ad-hoc Networks Using GA and Multi-Objective Optimization" from Admir Barolli, Evjola Spaho, Leonard Barolli, Fatos Xhafa and Makoto Takizawa, proposes a QoS routing in ad-hoc networks. Distinguishing from existing works related to routing in ad-hoc networks, this paper designs a QoS-guaranteed solution based on Genetic Algorithms (GAs) and multi-objective optimization. In particular, the authors implemented a search space reduction algorithm, which reduces the search space for GAMAN (GA-based routing algorithm for Mobile Ad-hoc Networks) to find a new route.

In the second paper [2], Inshil Doh, Jiyoung Lim and Kijoon Chae propose a "Distributed Authentication Mechanism for Secure Channel Establishment in Ubiquitous Medical Sensor Networks", in which bio-data is collected and delivered to the server system through mobile devices or gateways. This scheme adopts candidate devices, which act as the intermediary when the original device cannot function properly. In this way, bio-data of patients can be sensed and collected to monitor their body status uninterruptedly.

The next paper [3] entitled "Design of a secure RFID authentication scheme preceding market transactions" by Chin-Ling Chen, proposes a RFID mutual authentication protocol for market application

systems. In order to achieve mutual authentication, the proposed scheme integrates fingerprint biometrics, cryptology and a hash function mechanism to ensure the security of transmitted messages. The proposed scheme can resist tag impersonation attack, replay attack, trace attack and forgery attack. Also, it maintains privacy protection and achieves mutual authentication, anonymity and forward secrecy.

In the fourth paper [4] entitled "Automatic Security Assessment for Next Generation Wireless Mobile Networks", Francesco Palmieri, Ugo Fiore and Aniello Castiglione design an active third party authentication, authorization and security assessment strategy. In this strategy, the infrastructure automatically detects incoming devices and analyzes whether they are secure or not. If a device is found to be insecure, it is immediately taken out from the network and denied further access until its vulnerabilities have been fixed. As the fundamental component of the security assessment strategy, the security assessment module takes advantage from a reliable knowledge base containing semantically-rich information about mobile nodes. Consequently, this scheme supports for the secure protection of wireless and mobile networks through automatic and real-time security/risk evaluation to some extend.

The fifth paper [5] with the title "A Handover Security Mechanism Employing Diffie-Hellman Key Exchange Approach for IEEE802.16E Wireless Networks" from Yi-Fu Cioua, Fang-Yie Leua, Yi-Li Huanga and Kangbin Yim, proposes a handover authentication mechanism, called handover key management and authentication scheme (HaKMA) to protect sensitive information delivered through wireless channels. The HaKMA provides a fast and secure key generation process for handover. The three-layer architecture in the HaKMA simplifies key generation flows compared to related work. Moreover, the authors also design two levels of handover mechanisms to minimize service disruption time (SDT), guaranteeing secure bidirectional connections between a mobile station and a base station. The analyses in this paper demonstrate that the HaKMA can effectively provide user authentication, and balance data security and system performance during handover with a low cost.

In the last paper [6] "Enhancing MISP with Fast Mobile IPv6 Security", Ilsun You, Jong-Hyouk Lee,Yoshiaki Hori and Kouichi Sakurai proposes a secure fast handover scheme that combines the advantages of *MISP* and *Fast Mobile IPv6* (*FMIPv6*). The MISP, a combination of MIS and MISAUTH protocols developed by Mobile Broadband Association, provides secure and fast connection for wireless access networks but suffers from denial-of-service attacks due to its weak session key. The proposed scheme in this paper improves the MISP through making full use of the fast handover approach of FMIPv6 and minimizing an involvement of the authentication server. The formal analyses in this paper show that the proposed scheme is robust against session key, off-line dictionary, DoS attacks while reducing handover latency compared with the existing schemes.

We would like to thank the authors of above papers published in this special issue, and regret that more papers could not be included. We appreciate all reviewers for their time and effort with reviewing assigned papers on time and providing invaluable comments and suggestions for authors for improving their papers. We also want to thank Professor David Taniar, Editors-in-Chief of *Mobile Information System*. His generous help and support have made this special issue a reality.

Hopefully, this special issue will bring forth advancements in science and technology as well as improve practices and applications of wireless and mobile technologies.

References

[1] A. Barolli, E. Spaho, L. Barolli, F. Xhafa and M. Takizawa, QoS Routing in Ad-hoc Networks Using GA and Multi-Objective Optimization, *Mobile Information System* (*MIS*), 2011.

[2] I. Doh, J. Lim and K. Chae, Distributed Authentication Mechanism for Secure Channel Establishment in Ubiquitous Medical Sensor Networks, *Mobile Information System* (*MIS*), 2011.

[3] C.-L. Chen, Design of a secure RFID authentication scheme preceding market transactions, *Mobile Information System* (*MIS*), 2011.
[4] F. Palmieri, U. Fiore and A. Castiglione, Automatic Security Assessment for Next Generation Wireless Mobile Networks, *Mobile Information System* (*MIS*), 2011.
[5] Y.-F. Cioua, F.-Y. Leua, Y.-L. Huanga and K. Yim, A Handover Security Mechanism Employing Diffie-Hellman Key Exchange Approach for IEEE802.16e Wireless Networks, *Mobile Information System* (*MIS*), 2011.
[6] I. You, J.-H. Lee, Y. Hori and K. Sakurai, Enhancing MISP with Fast Mobile IPv6 Security, *Mobile Information System* (*MIS*), 2011.