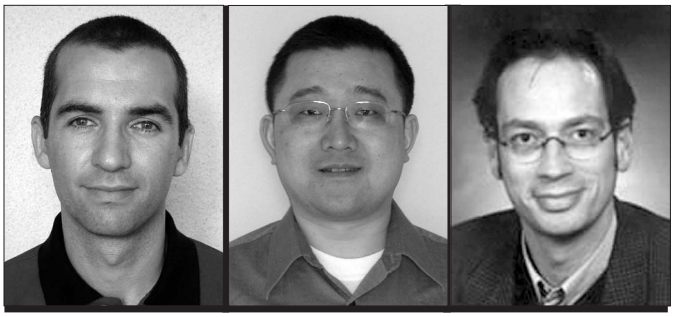
DEPENDABILITY ISSUES WITH UBIQUITOUS WIRELESS ACCESS



ALBERT BANCHS DAJI QIAO DIRK WESTHOFF

Recent years have witnessed a proliferation of the number of wireless technologies available to access the Internet, ranging from wireless local area networks to cellular and broadcast systems, and ad hoc and mesh networks. While the emergence of these new technologies can enable truly ubiquitous Internet access, it also raises issues with the dependability of the Internet service delivered to users. Dependability in this context refers to the ability of a wireless access system to deliver specified services on which users can rely.

When compared to traditional wired access solutions, wireless Internet access is more prone to security attacks and less predictable in terms of the quality of service (QoS) experienced by users. This poses serious challenges to the provisioning of a dependable Internet service that meets the users' requirements in terms of security, QoS, reliability, and availability, among others.

In order to meet the above requirements for dependability, new solutions such as security and QoS mechanisms need to be designed for wireless Internet access. Several issues need to be addressed in the design of such dependable wireless solutions, including the following:

- The open nature of radio communications provides serious exposure to security attacks. In this context, solutions are needed in order to counter denial-of-service attacks as well as to provide privacy-aware dependable operations, among others.
- The limited capacity and shared nature of the wireless medium complicate the provisioning of QoS. Predictable shared medium access mechanisms are needed to provide dependable service.
- Inherently unpredictable wireless channel characteristics make it hard to guarantee availability. In order to ensure that wireless Internet access will always be available, adequate coverage is needed. Additionally, availability can be improved by combining different wireless technologies.
- Exploitation of resources due to selfish and malicious behavior is difficult to prevent. Techniques are therefore required to identify and control selfish users that take advantage of the nature of the wireless medium to gain a greater share of resources.
- The emergence of new paradigms, such as opportunistic spectrum usage and self-organizing networks, promise improvements but introduce new challenges for dependability. New solutions are required to provide dependable service in these emerging contexts.

While some of the above have already received attention from the research community and related standardization bodies, many challenges are yet to be addressed to provide truly dependable wireless Internet access. The aim of this special issue of *IEEE Wireless Communications* is to highlight some of these challenges and present possible solutions. A total of 28 articles were submitted to the special issue, of which five could be accepted, yielding an acceptance rate of about 18 percent.

The articles in this special issue cover different aspects of QoS and security in wireless access. They are organized as follows. The first article is "MAP: A Scalable Monitoring System for Dependable 802.11 Wireless Networks" by Sheng *et al.* This article introduces the MAP project, which includes a scalable 802.11 measurement system that can provide continuous monitoring of wireless traffic to quickly identify threats and attacks. The authors discuss the MAP system architecture, design decisions, and evaluation results from a real testbed.

The second article is "Quality of Service Assessment of Opportunistic Spectrum Access: a Medium Access Control Approach" by Pawelczak *et al.* Opportunistic spectrum access (OSA) is a promising new spectrum management approach that allows coexistence of licensed and opportunistic users. This article investigates the QoS of the opportunistic users as a function of the tolerance of licensed users in OSA, and concludes that opportunistic users can achieve good QoS as long as licensed users are not highly active.

The third article, "Toward Dependable Networking: Secure Location and Privacy at Link Layer," is authored by Matos *et al.* Although many existing network-level architectures provide location privacy features, they leave open the privacy problem of nodes in the same link layer domain. This article fills this gap by proposing an improved approach to location privacy at the link layer.

The fourth article, "Optimal Admission Control in Multimedia Mobile Networks with Handover Prediction," is by Martinez-Bauset *et al.* It studies the problem of optimizing admission control policies in mobile multimedia cellular networks when predictive information regarding the movement of mobile terminals is available. The authors show that the performance gain is a function of the anticipation time with which the admission controller knows the occurrence of handovers, and they also show that an optimal anticipation time exists.

The last article is entitled "Identity-Based Key Management in Mobile Ad Hoc Networks: Techniques and Applications" and is authored by da Silva *et al.* This article presents a survey of the most important ID-based key management

schemes in MANETs, discussing their approaches, strengths, weaknesses, and comparing their main features. The article also discusses the main ID-based key management application fields in MANETs.

The guest editors would like to thank all authors and reviewers for their valuable contributions to this special issue. We would also like to thank Abbas Jamalipour, Editor-in-Chief, for his invaluable help and advice in preparing this special issue.

BIOGRAPHIES

ALBERT BANCHS (banchs@it.uc3m.es) received his M.Sc. and Ph.D. degrees in telecommunications from the Technical University of Catalonia, Barcelona, in 1997 and 2002, respectively. His Ph.D. received the national award for best thesis on broadband networks granted by the Professional Association of Telecommunication Engineers. He worked for the International Computer Science Institute, Berkeley, California, in 1997, for Telefonica I+D, Madrid, in 1998, and for NEC Network Laboratories, Heidelberg, from 1998 to 2003. Since 2003 he has been with University Carlos III of Madrid. He has published over 50 articles in international conferences and journals. He is an Associate Editor of *IEEE Communications Letters* and has been a member of the Technical Program Committees of several conferences and workshops, including ICC, GLOBECOM, and INFOCOM. His current research interests include resource allocation, QoS, and performance evaluation of wireless and wired networks.

DAJI QIAO (daji@iastate.edu) received his Ph.D. degree in electrical engineering: systems from the University of Michigan, Ann Arbor. He joined Iowa State University in May 2004 and is currently an assistant professor in the Department of Electrical and Computer Engineering. His research interests include wireless local area networks, wireless sensor networks, wireless mesh networks, and cross-layer design and optimization. He has published more than 35 papers in the field of wireless and mobile networks in various prestigious conferences and journals such as ACM MobiCom, IEEE INFOCOM, *IEEE/ACM Transactions on Networking*, and *IEEE Transactions on Mobile Computing*. Since 2004 he has been invited to serve on the Technical Program Committees of several international conferences and workshops, including IEEE INFOCOM, IEEE SECON, IEEE ICCCN, IEEE WCNC, and IEEE GLOBECOM, among others.

DIRK WESTHOFF [M](dirk.westhoff@netlab.nec.de) received a Ph.D. degree in computer science in 2000, and in 2007 his postdoctoral lecture qualification was entitled "Security and Dependability Solutions for 4G Wireless Access Networks," both from the Distance University of Hagen. Since 2001 he has been at NEC Europe Ltd. R&D Network Laboratories, Heidelberg, Germany, currently as a chief researcher. Recently he has been strongly involved in the definition and launching phases of the European projects UbiSec&Sens, SENSEI, and WSAN4CIP. He is co-founder of the European Workshop on Security in Ad Hoc and Sensor Networks series published by Springer. He has more than 50 peer-reviewed publications in network security and distributed systems security, and holds six patents. He has been involved in the Technical Program Committees of several ACM and IEEE workshops and conferences, and is a member of the Steering Committee of the ACM WiSec. His research interests include wireless security, ad hoc and sensor network security, and many other security and privacy aspects of distributed mobile communication.