1. Introduction

Mobile Internet technology has moved the digital world frontiers much far beyond what was even imaginable a few years ago. Such unprecedented revolution affected many sectors of modern society, ranging from business, culture, education, and social life, by also significant enhancing productivity for both public and private organizations. In particular, the convergence of mobile communications technologies and ubiquitous Internet coverage is introducing alternative business models, together with new applications, devices services, protocols, and security/performance issues. Day-to-day activities and operations in many areas ranging from healthcare to energy and transportation management can be significantly influenced by the availability of cheap, high-performance ubiquitous connections to the Internet. In addition, mobile broadband technologies such as WiFi, LTE, and WiMax together with advances in cheap sensor equipment and energy-efficient processing devices are fostering the integration of the Internet with an ever increasing quantity of smart objects deployed around us, leading to a new convergence between physical space and cyberspace. This also implies a shift in communication dynamics from person-to-person to machine-to-machine, resulting in the emerging Internet of Things paradigm, where the emerging active objects will largely outnumber (of several orders of magnitude) the actually connected devices, with the obvious consequences in terms of address space requirements and the need of new IPv6-based mobility services.

The evolution of mobile Internet will have as its most significant follow-up much more than improving the Web surfing or mobile access experience: new networking architectures, protocols, and paradigms such as software defined and cognitive networks are incessantly emerging, with obvious effects on a wide range of Internet-enabled services, activities, and transactions. The diffusion of these new network services, models, and architectures opens new security challenges to be faced by using flexible and effective methods that should be able to operate with very different and heterogeneous devices and technologies.

All the above issues are now considered as topics of paramount importance for research/academia, industry, and government as well as policy makers. Clearly this implies increased investments, enhanced productivity, and more job opportunities. Accordingly, this special issue is intended to foster the dissemination of state-of-the-art research in the aforementioned scenario, ensuring that the above technologies could reach their full potential, so that all the digital citizens can fully experience the benefits made possible by the mobile broadband economy. Original research articles have been selected by covering several aspects of innovative mobile Internet technologies, including emerging services and applications, theoretical studies, and experimental prototypes.

2. Special Issue Contents

This Special Issue is composed of five contributions, carefully selected according to their subject and accepted based
on merit contents. These works cover a variety of topics, including mobile IPv6, advanced network architectures and services, and, finally, communications security.

In the new service environments empowered by mobile Internet connectivity Proxy Mobile IPv6 (PMIPv6) emerged as a promising network-based mobility management protocol, which does not need any participation of the involved Mobile Nodes. In this scenario, the contribution presented by L. Wang et al. proposed two efficient PMIPv6 based mobile multicast sender support schemes, namely, PMIP bidirectional tunneling (PMIP-BT) and PMIP direct routing (PMIP-DR), that can transparently support the multicast sender mobility in PMIPv6 networks.

Furthermore, the contribution presented by M. Song et al. proposes several cost-optimized mobility management schemes based on pointer forwarding for PMIPv6 networks with the aim of reducing the overall network traffic due to mobility-related signaling and packet delivery. When the MN moves in both intradomain and interdomain handoff, their schemes can reduce high-signaling overhead by using pointer chains to connect the local mobility anchor (LMA) and the mobile access gateway (MAG). All the schemes are independent, dynamical, and per-user-based, taking into account the optimal threshold of the forwarding chain length, as well as the mobility of each user, and the service patterns for minimizing overall network traffic.

From a completely different perspective, the article authored by G. Sato et al. introduces a disaster resilient network integrating various wireless networks into a cognitive network that can be used as an access network to the Internet in presence of severe disaster occurrence. We designed and developed such a disaster resilient network based on software defined network (SDN) technology in order to automatically select the best network link and route among the possible access resources to Internet by periodically monitoring their operating status.

On the other hand, the article by L.-F. Huang et al. presents a synchronous cognitive MAC protocol (distributed-antenna based heterogeneous cognitive wireless network synchronous MAC protocol), exploiting CSMA/CA mechanism in the 802.11DCF, for heterogeneous cognitive radio networks, aiming at combining the advantages of cognitive radio and distributed antennas to fully utilize the licensed spectrum and broaden the communication range. The use of distributed antennas to sense spectrum and transmit data significantly improves the sensing performance and increases network throughput.

Regarding security issues, the work by G. Vitello et al. proposes a novel embedded automatic fingerprint authentication system (AFAS) for mobile devices improving the performance of standard AFAS hardware implementations in order to enable its deployment in mobile architectures. The system exhibits an interesting trade-off between the needed resources, authentication time, and accuracy rate.

Finally, the contribution from K. Singh and P. Rangan presents an improved construction for lattice based universal reencryption scheme that can replace the existing universal reencryption schemes used in postquantum cryptography to ensure location privacy in mobile system.

We are sure that the experiences presented in this Special Issue may significantly contribute to the literature and the efforts conducted by academic people, industry professionals, and everyone interested in the covered areas, by also inspiring readers to find sources of new innovative insights that will benefit their future research.

**Acknowledgments**

We would like to express our sincere appreciation of the valuable contributions made by all the authors and our deep gratitude to all the highly qualified anonymous reviewers who have carefully analyzed the assigned papers and significantly contributed to improve their quality.

Ilsun You
Francesco Palmieri
Leonard Barolli