Critical Communications and Public Safety Networks, Part 2: Technical Issues, Security, and Applications

Mehmet Ulema

Alan Kaplan

Kevin Lu

Niranth Amogh

Barcin Kozbe

As we mentioned in the Guest Editorial of Part 1 of this Feature Topic, which was published in March 2016, due to a high number of high quality submissions, we divided the accepted papers into two parts. While the articles in Part 1 focused on general topics such as overview, spectrum policies, and economics, the articles of Part 2 in this issue of the magazine focus on more technical issues and solutions.

Technologies used in public safety networks and critical communications networks today are going through a transformation from narrowband technologies to broadband-communications-based technologies (mainly Long Term Evolution, LTE) due to its superior support for higher bandwidth multimedia applications, and the ubiquitous, standardized, and cost-effective availability of equipment. To realize the promises of broadband technologies for critical communications and public safety networks, many obstacles in designing, deploying, and operating these kinds of systems need to be overcome. The Feature Topic articles in this issue are intended to provide an in-depth overview of the technical issues and solutions related to evolution, critical communications, performance, security, and reliability aspects as well as application challenges in environments other than public safety agencies.

The first article in this series is "Group Communication over LTE : A Radio Access Perspective," co-authored by Juyeop Kim, Sang Won Choi, Won-Yong Shin, Yong-Soo Song, and Yong-Kyu Kim. This article provides an analysis of how the current LTE system can support group communication and demonstrates how each LTE-enabled radio access method can efficiently support group communication. In addition, they propose a new multicast transmission scheme, which shows more scalable and resource-efficient support of group communication by the LTE system.

The second article, "Public Safety Networks Evolution towardNew Technologies: Sharing Infrastructures and Spectrum with Commercial Systems" co-authored by Romano Fantacci, Francesco Gei, Dania Marabissi, Luigia Micciullo, focuses on critical issues that impact migration toward new technologies and describes possible evolution steps, including advanced solutions.

The third article, "Aerial Base Stations with Opportunistic Links for Next Generation Emergency Communications," co-authored by Karina Gomez, Sithamparanathan Kandeepan, Macià Mut Vidal, Vincent Boussemart, Raquel Ramos Ramos, Romain Hermenier, Tinku Rasheed, Leonardi Goratti, Laurent Reynaud, David Grace, Qiyang Zhao, Yunbo Han, Salahedin Rehan, Nils Morozs, Tao Jiang, Isabelle Bucaille, Philippe Charpentier, Tom Wirth, Roberta Campo, and Tomaž Javornik, describes the main outcomes of the ABSOLUTE project, which focuses on designing, prototyping, and demonstrating a high-capacity IP mobile data network with low latency and large coverage suitable for many forms of multimedia delivery including public safety scenarios.

The fourth article, "Enhanced Interworking of LTE and Wi-Fi Direct for Public Safety," co-authored by Rajavelsamy Rajadurai, Karthik Srinivsa Gopalan, Mayuresh Patil, and Suresh Chitturi, provides an overview of the PS related efforts in the Third Generation Partnership Project (3GPP), interworking aspects of LTE and Wi-Fi, and their application to public safety, and provides a mechanism to enhance the interworking between the two technologies to deliver an effective solution for mission-critical communication and applications.

The fifth article, "Cloud-Centric Multi-Llevel Authentication as a Service for Secure Public Safety Device Networks," co-authored by Ismail Butun, Melike Erol-Kantarci, Burak Kantarci, and Houbing Song, also focuses on the security aspects of public safety networks with an emphasis on cloud-centric multi-level authentication as a service approach that addresses scalability and time constraints.

The sixth article, "LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation," co-authored by Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, and Jeffrey H. Reed, investigates the extent to which LTE is vulnerable to RF jamming, spoofing, and sniffing, and assesses different physical layer threats that could affect next-generation critical communication networks. In addition, the authors examine how sniffing the LTE broadcast messages can aid an adversary in an attack and establish an overall threat assessment of LTE to jamming and spoofing.

The final article in this Feature Topic, "Mission-Critical Mobile Broadband Communications in Open-Pit Mines," by Luis G. Uzeda Garcia, Erika P. L. Almeida, Viviane S. B. Barbosa, George Caldwell, Ignacio Rodriguez, Hernani Lima, Troels B. Sorensen, and Preben Mogensen, introduces fundamental concepts behind open-pit mining, which poses unique challenges to traditional network planning and optimization techniques. The authors also present an integrated framework to support continuous environmental awareness and autonomous adaptation of the network infrastructure.

We hope that you find these articles interesting, informative, and challenging, and that they encourage further research and development, leading to more advanced solutions. Again, we would like to thank all the authors who submitted their articles to this Feature Topic and the reviewers, who have given their time generously to provide valuable feedback and comments on the articles and thus make this Feature Topic a reality.

BIOGRAPHIES

MEHMET ULEMA (mehmet.ulema@manhattan.edu) is a professor with Computer Information Systems at Manhattan College, New York. Previously, he was with AT&T Bell Laboratories, Bellcore, Daewoo Telecom, and Hazeltine. He also serves as the Director of Standards Development in ComSoc. He was the TPC Chair of GLOBECOM 2009 and General Co-Chair of NOMS 2016. He is on the Editorial Boards of *IEEE Journal of IoT* and *Springer Journal of Network and Services Management*. He received his Ph.D. from Polytechnic University, Brooklyn, and his B.S. and M.S. from Istanbul Technical University.

ALAN KAPLAN (kaplana@ieee.org) is CTO of Drakontas, developing software for public safety agencies. He was formerly with Panasonic Princeton Research Lab, Clemson University, and Flinders University of South Australia. He holds Ph.D. and M.S. degrees in computer science from the University of Massachusetts Amherst and a B.S. in computer science from Duke University. He is also currently a lecturer in the Department of Computer Science at Princeton University.

KEVIN LU (klu@ieee.org) is an adjunct professor of electrical and computer engineering at Stevens Institute of Technology. He is a member of the IEEE Standards Association (IEEE-SA) Standards Board and is the IEEE-SA contact for the Global Standards Collaboration task force on emergency communications. He was a chief scientist and executive director at Telcordia applied research until 2012. He received his D.Sc. in systems science and mathematics from Washington University in St. Louis.

NIRANTH AMOGH (namogh@huawei.com) is a principal researcher at the Huawei India R&D Center at Bangalore. He is responsible for the wireless networks research within the organization. His research areas include broadband critical communications, M2M/IoT, SDN/NFV, and NGSON. He has filed several patents in his research areas and holds leadership positions in several SDOs in India and globally. In critical communications standardization, he is actively contributing to the 3GPP SA6 (Mission-Critical Applications) WG.

BARCIN KOZBE (kozbe@yahoo.com) is currently a senior consultant at NGen Solutions. Prior to joining NGen Solutions, he was a technical solutions manager at Ericsson Inc. He has been working in the field of computer science, specializing in information technology for telecommunications, for 20 years. He received his M.Sc. degree in computer engineering from Chalmers Technology University in Sweden. His research interests include public safety networks, network management systems, software defined networks, and cloud computing.