Guest Editorial: Signal Processing for Wireless Physical Layer Security

Eduard Jorswieck, Lifeng Lai, Wing-Kin Ma, H. Vincent Poor, Walid Saad, and A. Lee Swindlehurst

THE ONGOING advances in wireless technologies (e.g., cognitive radio, device-to-device communications, social networking services, etc.) have introduced new security challenges in next-generation networks. Despite the proven efficiency of cryptographic techniques, the associated overhead and complexity make it difficult to implement encryption algorithms in future large-scale, heterogeneous, and distributed wireless networks. Indeed, the emergence of highly decentralized wireless architectures without an infrastructure that supports key management and authentication imposes new challenges on classical security measures such as cryptography. Motivated by these issues, substantial recent research has been dedicated toward seeking novel information-theoretic techniques that can secure wireless networks without the computational overhead that accompanies standard cryptographic techniques. The main idea of this work is to exploit physical characteristics of the wireless channel such as fading or noise, traditionally seen as impediments, to improve the transmission reliability against eavesdropping attacks with relatively low computational overhead. This approach is known as wireless *physical layer security*. At the heart of this formalism lies the concept of a *secrecy capacity* which is defined as the maximum wireless transmission rate that achieves perfect secrecy - the eavesdropper cannot do better than a guessing-based exhaustive search for data detection and, thus, it achieves the worst-case bit error rate during signal detection. Indeed, if well designed, physical layer security mechanisms can provide a robust solution for boosting wireless security and can act as either an alternative or as a complement that can strengthen traditional encryption techniques.

The emergence of physical layer security as a potential technique for securing wireless transmission has significantly captured the attention of researchers in both the signal processing and communications communities. In this context, developing advanced signal processing techniques for optimizing and enhancing the secrecy rate of wireless links has become an issue of considerable interest in the design and analysis of future wireless networks. As is the case with any novel technology, reaping the benefits of physical layer security is contingent upon meeting several key challenges. The main goal of this special issue is to gather state-of-the-art contributions that address such challenges as they pertain to the design, analysis, and optimization of physical layer security in next-generation networks. In particular, the selected papers are aimed at addressing the following challenges in physical layer security: 1) design of multiple antenna and cooperative techniques for maximizing the achievable secrecy rate, 2) development of new signal processing techniques that exploit channel randomness for secret key generation, 3) development of advanced algorithms at the physical layer for treating security primitives such as authentication and privacy, 4) waveform and signal designs for boosting the secrecy rate and combatting active and passive eavesdropping, 5) novel coding techniques that are tailored toward physical layer secrecy, and 6) fundamental limits and novel optimization approaches for wireless secrecy.

The special issue begins by focusing on contributions that address physical layer enhancements, such as multiple antenna and cooperative techniques, that are tailored toward improving secrecy rate. One fundamental problem in this area is to develop secrecy-enhancing transmission techniques in dense networks with multiple antennas at the transmitter and, possibly, at the receivers. The related contributions include fundamental results on optimal secrecy-achieving precoding techniques, novel beamforming schemes for optimizing secrecy rates, and relay-assisted cooperative schemes for characterizing and optimizing secrecy rates in a variety of multi-antenna settings.

Wireless physical layer security is not limited to characterizing and optimizing secrecy rate, but also extends to utilizing channel characteristics for developing novel authentication and key extraction techniques. In this respect, the next group of papers address the major problems in secret key generation and authentication using physical layer techniques. The contributions encompass solutions to several open problems such as deriving fundamental results for extracting secret keys from various wireless channels (reciprocal, frequency selective, etc.), key agreement schemes in multiple access channels, and a number of physical layer-based authentication

E. Jorswieck is with the Electrical and Computer Engineering Department, TU Dresden, Dresden, Germany (e-mail: eduard.jorswieck@tu-dresden.de).

L. Lai is with the Electrical and Computer Engineering Department, Worcester Polytechnic Institute, Worcester, MA, USA (e-mail: llai@wpi.edu).

W.-K. Ma is with the Department of Electronic Engineering, The Chinese University of Hong Kong, Hong Kong (e-mail: wkma@ee.cuhk.edu.hk).

H. V. Poor is with the Electrical Engineering Department, Princeton University, Princeton, NJ, USA (e-mail: poor@princeton.edu).

W. Saad is with the Electrical and Computer Engineering Department, University of Miami, Coral Gables, FL, USA (e-mail: walid@miami.edu).

A. L. Swindlehurst is with the Electrical Engineering and Computer Science Department, University of California, Irvine, CA, USA (e-mail: swindle@uci.edu).

P. Cosman is the J-SAC board representative for this issue of IEEE Journal on Selected Areas in Communications.

Digital Object Identifier 10.1109/JSAC.2013.130901

protocols for different applications that include body area networks as well as more traditional wireless systems.

Next, the special issue focuses on signal designs for enhancing wireless secrecy and combatting eavesdroppers with various capabilities. Indeed, exploiting different properties at the eavesdropper's side such as receiver characteristics or eavesdropper behavior (active/passive) can provide interesting dimensions for optimizing secrecy. The papers in this group cover diverse topics such as the use of non-linear conversion operation at an eavesdropper's receiver to maintain a positive secrecy capacity, the derivation of fundamental results on the ergodic secrecy capacity under partial channel state information at the transmitter, and the development of new signal processing techniques for optimizing secrecy under two scenarios: the presence of active and passive eavesdroppers as well as in the case of multicasting.

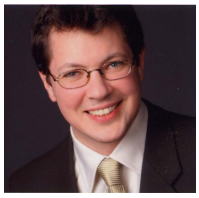
In order to deploy and operate physical layer security mechanisms, it is necessary to understand the prospective performance and potential limitations of these techniques. This is important for both key generation and secrecy optimization. In this regard, the next collection of papers focuses on fundamental results pertaining to modeling and analysis of wireless physical layer security scenarios. These results are expected to enhance our understanding of the performance of physical layer security mechanisms, subsequently providing the much needed theoretical foundations for such protocols. These contributions include the development of foundational measures for characterizing the performance of physical layer-based secret key generation mechanisms, the introduction of novel coding and performance analysis techniques, as well as the derivation of fundamental information-theoretic bounds and metrics for characterizing and analyzing physical layer secrecy and its limits.

Last but not least, this special issue provides two papers that focus on cross-layer approaches to combining physical layer secrecy with higher layer performance measures. To this end, the first paper introduces novel control-theoretic techniques that neatly link evading eavesdropping at the physical layer and networking issues such as packet arrivals, queuing, and admission control. Then, the final paper in this special issue develops a detection-theoretic method for optimizing packet reordering at routers or proxy servers, so as to prevent eavesdroppers from tracking the flow of packets, under both throughput and memory constraints.

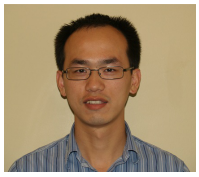
In a nutshell, despite the significant advances in physical layer security that accompanied the past decade, this special issue provides novel solutions to a variety of open physical layer security problems that have emerged in the past few years, particularly from the signal processing and optimization perspectives. We believe that these contributions will also provide a solid basis for future research developments towards introducing physical layer security schemes in practical scenarios.

ACKNOWLEDGEMENTS

The guest editors would like to thank the large number of people who significantly contributed to this special issue, including the authors, reviewers, and JSAC editorial staff.



Eduard Jorwieck received his Diplom-Ingenieur (M.S.) degree and Doktor-Ingenieur (Ph.D.) degree, both in electrical engineering and computer science from the Technische Universitt Berlin, Germany, in 2000 and 2004, respectively. Since 2008, he has been the head of the Chair of Communications Theory and Full Professor at Dresden University of Technology (TUD), Germany. Eduard's main research interests are in the area of signal processing for communications and networks, applied information theory, and communications theory. He has published two monographs, 7 book chapters, more than 55 journal papers and some 170 conference papers on these topics. Dr. Jorswieck is senior member of IEEE. He is member of the IEEE SPCOM Technical Committee (2008-2013). Since 2011, he acts as Associate Editor for IEEE TRANSACTIONS ON SIGNAL PROCESSING. Since 2008, continuing until 2011, he has served as an Associate Editor for IEEE SIGNAL PROCESSING LETTERS. Since 2012, he is Senior Associate Editor for IEEE SIGNAL PROCESSING LETTER. Since 2013, he serves as Associate Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. In 2006, he received the IEEE Signal Processing Society Best Paper Award.



Lifeng Lai (M'07) received the B.E. and M. E. degrees from Zhejiang University, Hangzhou, China in 2001 and 2004 respectively, and the PhD degree from The Ohio State University at Columbus, OH, in 2007. He was a postdoctoral research associate at Princeton University from 2007 to 2009, and was an assistant professor at University of Arkansas, Little Rock from 2009 to 2012. Since Aug. 2012, he has been an assistant professor at Worcester Polytechnic Institute. Dr. Lai's research interests include information theory, stochastic signal processing and security.

Dr. Lai is a co-recipient of the Best Paper Award from IEEE Global Communications Conference (Globecom) in 2008, the Best Paper Award from IEEE Conference on Communications (ICC) in 2011 and the Best Paper Award from IEEE Smart Grid Communications (SmartGridComm) in 2012. He received the National Science Foundation CAREER Award in 2011, and Northrop Young Researcher Award in 2012. He served as a Guest Editor for IEEE Journal on Selected Areas in Communications, Special Issue on Signal Processing Techniques for Wireless Physical Layer Security. He is now serving as an Associate Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS.

Wing-Kin Ma (M'01-SM'11) received the B.Eng. (first-class honors) degree in electrical and electronic engineering from the University of Portsmouth, Portsmouth, U.K., in 1995, and the M.Phil. and Ph.D. degrees, both in electronic engineering, from The Chinese University of Hong Kong (CUHK), Hong Kong, in 1997 and 2001, respectively. He is currently an Assistant Professor with the Department of Electronic Engineering, CUHK. From 2005 to 2007, he was also an Assistant Professor with the Institute of Communications Engineering, National Tsing Hua University, Taiwan, R.O.C., where he is still holding an adjunct position. Prior to becoming a faculty member, he held various research positions with McMaster University, Canada; CUHK; and the University of Melbourne, Australia. His research interests are in signal processing and communications, with a recent emphasis on MIMO communication, convex optimization, and blind signal processing.

Dr. Ma is currently serving or has served as Associate Editor and Guest Editor of several journals, which include IEEE TRANSACTIONS ON SIGNAL PROCESSING, IEEE SIGNAL PROCESSING LETTERS, and IEEE SIGNAL PROCESSING MAGAZINE. He is currently a Member of the Signal Processing Theory and Methods (SPTM) Technical Committee. Dr. Ma's student has won an ICASSP 2011 Best Student Paper Award, and he is co-recipient of a WHISPERS 2011 Best Paper Award.

H. Vincent Poor (S'72, M'77, SM'82, F'87) received the Ph.D. degree in EECS from Princeton University in 1977. From 1977 until 1990, he was on the faculty of the University of Illinois at Urbana-Champaign. Since 1990 he has been on the faculty at Princeton, where he is the Michael Henry Strater University Professor of Electrical Engineering and Dean of the School of Engineering and Applied Science. Dr. Poor's research interests are in the areas of stochastic analysis, statistical signal processing and information theory, and their applications in wireless networks and related fields including social networks and smart grid. Among his publications in these areas are the recent books *Smart Grid Communications and Networking* (Cambridge University Press, 2012), and *Principles of Cognitive Radio* (Cambridge University Press, 2013).

Dr. Poor is a member of the National Academy of Engineering and the National Academy of Sciences, a Fellow of the American Academy of Arts and Sciences, an International Fellow of the Royal Academy of Engineering (U. K), and is a Corresponding Fellow of the Royal Society of Edinburgh. He is also a Fellow of the Institute of Mathematical Statistics, the Optical Society of America, and other organizations. In 1990, he served as President of the IEEE Information Theory Society, and in 2004-07 he served as the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY. He received a Guggenheim Fellowship in 2002, the IEEE Education Medal in 2005, and the Marconi and Armstrong Awards of the IEEE Communications Society in 2007 and 2009, respectively. Recent recognition of his work includes the 2010 IET Ambrose Fleming Medal for Achievement in Communications, the 2011 IEEE Eric E. Sumner Award, and honorary doctorates from Aalborg University, the Hong Kong University of Science and Technology, and the University of Edinburgh.

Walid Saad received his B.E. degree in Computer and Communications Engineering from the Lebanese University in 2004, his M.E. in Computer and Communications Engineering from the American University of Beirut (AUB) in 2007, and his Ph.D degree from the University of Oslo in 2010. Currently, he is an Assistant Professor at the Electrical and Computer Engineering Department at the University of Miami. Prior to joining UM, he has held several research positions at institutions such as Princeton University and the University of Illinois at Urbana-Champaign.

His research interests include wireless and small cell networks, game theory, wireless security, network science, and smart grids. He has co-authored one book and over 70 international conference and journal publications in these areas. He was the author/co-author of the papers that received the Best Paper Award at the 7th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), in June 2009, at the 5th International Conference on Internet Monitoring and Protection (ICIMP) in May 2010, and at IEEE WCNC in 2012. Dr. Saad is a recipient of the NSF CAREER Award in 2013.

A. Lee Swindelhurst received the B.S., summa cum laude, and M.S. degrees in Electrical Engineering from Brigham Young University, Provo, Utah, in 1985 and 1986, respectively, and the PhD degree in Electrical Engineering from Stanford University in 1991. From 1986-1990, he was employed at ESL, Inc., of Sunnyvale, CA, where he was involved in the design of algorithms and architectures for several radar and sonar signal processing systems. He was on the faculty of the Department of Electrical and Computer Engineering at Brigham Young University from 1990-2007, where he was a Full Professor and served as Department Chair from 2003-2006. During 1996-1997, he held a joint appointment as a visiting scholar at both Uppsala University, Uppsala, Sweden, and at the Royal Institute of Technology, Stockholm, Sweden. From 2006-07, he was on leave working as Vice President of Research for ArrayComm LLC in San Jose, California. He is currently a Professor and Associate Chair of the Electrical Engineering and Computer Science Department at the University of California Irvine. His research interests include sensor array signal processing for radar and wireless communications, detection and estimation theory, and system identification, and he has over 230 publications in these areas.

Dr. Swindlehurst is a Fellow of the IEEE, a past Secretary of the IEEE Signal Processing Society, past Editor-in-Chief of the IEEE Journal of Selected Topics in Signal Processing, and past member of the Editorial Boards for the EURASIP JOURNAL ON WIRELESS COMMUNICATIONS AND NETWORKING, IEEE SIGNAL PROCESSING MAGAZINE, and the IEEE TRANSACTIONS ON SIGNAL PROCESSING. He is a recipient of several paper awards: the 2000 IEEE W. R. G. Baker Prize Paper Award, the 2006 and 2010 IEEE Signal Processing Societys Best Paper Awards, the 2006 IEEE Communications Society Stephen O. Rice Prize in the Field of Communication Theory, and is co-author of a paper that received the IEEE Signal Processing Society Young Author Best Paper Award in 2001.