Secure Communications via Physical-Layer and Information-Theoretic Techniques

By PHILLIP A. REGALIA, *Fellow, IEEE*
Department of Electrical Engineering and Computer Science
Catholic University of America, Washington, DC 20064 USA
regalia@cua.edu

ASHISH KHISTI
Department of Electrical and Computer Engineering
University of Toronto, Toronto, ON M1B 5P1 Canada
akhisti@ece.utoronto.ca

YINGBIN LIANG, *Member, IEEE*
Department of Electrical Engineering and Computer Science
Syracuse University, Syracuse, NY 13244 USA
yliang06@syr.edu

STEFANO TOMASIN, *Senior Member, IEEE*
Department of Information Engineering
University of Padova, 35131 Padova, Italy
tomasin@dei.unipd.it

I. PROBLEM SETTING

The wireless revolution is rightfully hailed for facilitating massive data exchanges, ranging from conversations, text, and e-mail at the personal level, to financial information, utility resource allocation, support for emergency services, and medical diagnostics at the institutional level. Such connectivity also facilitates security breaches, ranging from passive eavesdropping to active Byzantine attacks, due to the open nature of wireless channels. A future characterized by an explosion of network connected devices, comprising smart grids, smart transportation systems, smart health, and more generally the Internet of Things, opens new doors to potentially disastrous scenarios if security is not built in from the ground up: The allure of instant gratification from anywhere/anytime connectivity must be tempered by the risks of unprotected

This special issue highlights recent advances along with the remaining challenges in the field of physical-layer security.

Digital Object Identifier: 10.1109/JPROC.2015.2473895

exchanges with infected or harmful agents.

Security traditionally relies on encryption via a separation principle in a layered network architecture. The encryption module is based on cryptographic algorithms and abstracts out the underlying communication channel as an ideal bit pipe via error-correction coding. The error-correction module is implemented at the physical layer, by adding redundancy to the information bits in order to combat channel impairments or multiuser interference. The operation of modern cryptosystems is well understood and, if implemented correctly, such systems offer reliable security guarantees.

They likewise have some well-recognized limitations. The first is the strength of the security, which is usually conditioned on an adversary having limited computational resources. While this provides satisfactory security with present-day technology, it is known that Shor's algorithm, running on a quantum computer, can break specific public-key cryptosystems in polynomial time, including the RSA scheme exploiting the hardness of integer factorization, or the Diffie–Hellman or Elgamal schemes exploiting the hardness of discrete logarithms. Given their widespread deployment in key agreement and authentication protocols, the security of today's information infrastructure would be rapidly compromised if quantum computers of nontrivial size should ever become reality. The second limitation concerns the overhead associated with secure key distribution, along with the risks of improper key management once the human-in-the-loop schema is exposed to social engineering. In a rapidly approaching future where large numbers of wireless nodes come and go at random, conventional key distribution schemes and the concomitant trusted infrastructure requirements may not scale well, resulting in a two-tiered network of "haves" versus "have nots" in security protections.

More critically, the separation between coding at the physical layer and cryptography at a higher layer has favored the development of a physical-layer communication infrastructure in which security might be added on in some separate phase, in seeming contempt of the "secure by design" philosophy. The world previously suffered this calamity in the 1990s with the rapid deployment of insecure computer operating systems connected to the nascent Internet, and predictions abound of reiterating past failures with the looming Internet of Things. Indeed, recent demonstrations of security flaws in automobiles and medical devices exposed through wireless connectivity serve as a clear warning of the dangers to come, especially from relative newcomers to the wireless networking field who may foolishly embrace the discredited "security through obscurity" paradigm.

Against this backdrop, an intriguing result by Wyner from the 1970s showed how secure communication may be achieved at the physical layer using coding, by exploiting channel impairments that constitute a physical reality of communication systems. The standard setting is the so-called wiretap channel: This scheme has a sender ("Alice") encode information in a manner that allows the legitimate receiver ("Bob") to reliably decode the message, yet hides information from an eavesdropper ("Eve"). The beauty of the scheme is twofold: 1) it is keyless, in that Alice and Bob may dispense with the need to share a secret key prior to message transmission yet still achieve secure message transmission, even when Eve knows all details about the code employed; and 2) it offers stronger secrecy than standard cryptography, as it appeals to the perfect secrecy condition established by Shannon in the 1940s, sometimes called information-theoretic secrecy. Perfect secrecy, in its simplest terms, is achieved when the intercepted communication conveys no more information on the transmitted message than a random guess. In such a scenario, any computational advantage of an adversary proves irrelevant. This basic result has fueled much recent work reexamining the combination of coding and cryptographic primitives all operating at the physical layer, and appropriately dubbed "physical-layer security." The intent of this special issue is to highlight recent advances in the field along with remaining challenges.

As may be expected, a result as attractive as Wyner's must have a catch. To be sure, the basic result assumes knowledge of channel state information connecting Alice to both Bob and Eve, and in particular that the Eve's channel from Alice is worse than Bob's, giving the so-called degraded channel condition that figures prominently in many treatments: the rate of secure communication is typically limited by the difference in channel capacities connecting Alice to Bob or to Eve. Considerable research has since been devoted to examining the severity of these conditions, and means to overcome them. While various clever schemes have been devised to overcome the degraded channel requirement, the dependence on reliable channel state information remains a recognized obstacle to the widespread deployment of physical-layer security techniques. That being said, these same channel state obstacles have repeatedly reared their ugly heads at every deployment phase of today's wireless backbone infrastructure, and if recent history confirms that necessity is the mother of invention, the observed steady progress in wireless connectivity in the face of unknown channel impairments (albeit without the secrecy constraint) offers a note of optimism.

II. ISSUE OVERVIEW

Following Wyner's seminal result, two essential thrusts form the backbone of physical-layer security: 1) coding schemes that ensure reliable communication between Alice and Bob despite Eve observing their communication; and 2) related techniques to reach secret-key agreement, by

exploiting the same channel impairments that ensure secrecy. The paper by Jorswieck *et al.* provides an overview of the signal processing techniques used in secrecy coding and secret-key agreement at the physical layer. The standard setup assumes known channel characteristics connecting the sender to the legitimate receiver and the eavesdropper. The concomitant problem of code design is known to appeal to so-called "nested" codes, in which one code forms a subset of another, a feature that often intervenes in multiterminal information-theory problems. It turns out that a coherent design procedure for such codes ties in closely with carefully refined definitions of secrecy, as exposed in the excellent treatment by Bloch *et al.* on designing secrecy codes. The paper by Muramatsu *et al.* pursues the related question of protocol design to achieve secret-key agreement by exploiting correlated randomness in sequences observed by players in a game, and related concepts of universal hashing for information-theoretic secrecy are reviewed by Tyagi and Vardy.

A common critique levied against secrecy coding is that the code design must (at present) have accurate channel state information. Assessments of achievable secrecy rates in the face of imperfect channel state information are pursued in the paper by Schaefer *et al.*, favoring models in which the actual channel is chosen from a class of representative channels that seek to capture intrinsic variability; channel uncertainty at the transmitter can be captured by a few popular models, under which the impact of the channel uncertainty on the secrecy capacity of the channel can be characterized. Additional insights are developed by Yener and Ulukus, who review key points learned from judiciously introducing interference to improve secrecy, and who reexamine cooperation with unauthenticated users as a superior alternative to treating eavesdroppers as conventional adversaries. The paper by Fragouli *et al.* treats how to engineer erasure channels, for which so-called "strong" secrecy results are easier to obtain.

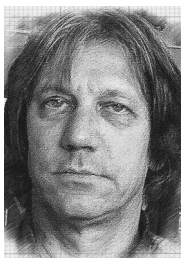
Once multiple users interact simultaneously, many extensions become possible. The special case in which users can naturally be ordered by their channel quality is pursued in the paper by Zou *et al.*, establishing interesting layered results in which users are granted progressively greater access to information or are progressively restricted, based on their channel quality. Xie and Ulukus examine various extensions of channels with additive Gaussian noise interference, seeking secrecy capacities in configurations involving helpers and/or multiple taps, borrowing ideas from powerful interference alignment concepts. The general multiple-input–multiple-output (MIMO) wiretap channel setting is treated in the paper by Oggier and Hassibi, obtaining general capacity expressions that need not assume channel degradedness conditions. The paper by Chan *et al.* provides accessible insights into recent results on secret-key sharing among multiple users, in parallel with connections to multivariate mutual information.

A comprehensive overview of physical-layer techniques applicable to the future Internet of Things is presented by Mukherjee, offering a complementary take on some of the topics visited by Jorswieck *et al.* Building on this framework, Venkitasubramaniam *et al.* examine information-theoretic security in the context of control theory and cyber–physical systems, whose applications span smart grids, networked transportation systems, and even smart and connected healthcare.

III. PERSPECTIVES

The papers of this issue have sought the elusive goal of rendering deep information-theoretic formulations accessible to a broader engineering and mathematical audience, emphasizing operational significance of formulas over algebraic subtleties, and tying them into present and future engineering challenges. While various challenges remain in actual deployments, recent gains in coding theory combined with steady advances in physical-layer communications would appear poised to deliver a future in which secrecy, confidentiality, and authentication can be all accommodated with bottom–up design principles that work hand-in-hand at the physical layer, while providing a keyless future impervious to human-in-the-loop scenarios, and thus freeing security research to pursue bigger game. ■

ABOUT THE GUEST EDITORS



Phillip A. Regalia (Fellow, IEEE) was born in Walnut Creek, CA, USA. He received the B.Sc. (highest honors), M.Sc., and Ph.D. degrees in electrical and computer engineering from the University of California at Santa Barbara, Santa Barbara, CA, USA, in 1985, 1987, and 1988, respectively, and the Habilitation à Diriger des Recherches degree from the University of Paris-Orsay, Paris, France, in 1994.

He has served as Chair of the Electrical Engineering and Computer Science Department, Catholic University of America, Washington, DC, USA, and previously as Chair of the Communications, Information and Image Processing Department, Telecom SudParis, Evry, France. In January 2012, he began a four-year rotation as Program Director with the Directorate for Computer and Information Science and Engineering, U.S. National Science Foundation. His research interests have spanned adaptive system theory, circuit theory, wireless communications, and information theory.

Ashish Khisti received the B.A.Sc. degree in engineering sciences from the University of Toronto, Toronto, ON, Canada, and the S.M. and Ph.D. degrees in electrical engineering from the Massachusetts Institute of Technology (MIT), Cambridge, MA, USA, in 2004 and 2009, respectively.

He is an Associate Professor and a Canada Research Chair in the Electrical and Computer Engineering (ECE) Department, University of Toronto. His research interests span the areas of information theory, wireless physical-layer security, and streaming in multimedia communication systems. At the University of Toronto, he heads the Signals, Multimedia, and Security Laboratory.

Dr. Khisti is a recipient of the Ontario Early Researcher Award from the Province of Ontario as well as a Hewlett-Packard Innovation Research Award.

Yingbin Liang (Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Illinois at Urbana-Champaign, Urbana, IL, USA, in 2005.

In 2005–2007, she was a Postdoctoral Research Associate at Princeton University, Princeton, NJ, USA. In 2008–2009, she was an Assistant Professor at the Department of Electrical Engineering, University of Hawaii, Honolulu, HI, USA. Since December 2009, she has been on the faculty at Syracuse University, Syracuse, NY, USA, where she is an Associate Professor. Her research interests include information theory, wireless communications and networks, and machine learning.

Dr. Liang was a Vodafone Fellow at the University of Illinois at Urbana-Champaign during 2003–2005, and received the Vodafone–U.S. Foundation Fellows Initiative Research Merit Award in 2005. She also received the M. E. Van Valkenburg Graduate Research Award from the Electrical and Computer Engineering Department, University of Illinois at Urbana-Champaign, in 2005. In 2009, she received the National Science Foundation CAREER Award, and the State of Hawaii Governor Innovation Award. More recently, her paper received the 2014 EURASIP Best Paper Award from the *EURASIP Journal on Wireless Communications and Networking*. She is currently serving as an Associate Editor for the Shannon Theory of the IEEE Transactions on Information Theory.

Stefano Tomasin (Senior Member, IEEE) received the Ph.D. degree in telecommunications engineering from the University of Padua, Padova, Italy, in 2003.

He has been doing internships at the IBM Research Laboratory in Switzerland and Philips Research in The Netherlands. In 2005, he joined the University of Padua as an Assistant Professor. Since then he has been visiting for extensive periods Qualcomm in California, the Polytechnic Institute of NYU in New York, and Huawei Technologies in Paris, France. His current research interests include physical-layer security, signal processing and scheduling for wireless communications, and optimization techniques for smart grids.

Dr. Tomasin has been an Editor of both the IEEE Transactions of Vehicular Technologies and the *EURASIP Journal of Wireless Communications and Networking* since 2011.