Digital Object Identifier 10.1109/ACCESS.2019.2960171

EDITORIAL

IEEE ACCESS SPECIAL SECTION EDITORIAL: SECURE MODULATIONS FOR FUTURE WIRELESS COMMUNICATIONS AND MOBILE NETWORKS

Security has become an extremely important research topic in wireless networks over the last decade, as it is intimately related to both individual privacy and national security. Directional modulation, as a conventional type of secure modulations, transmits confidential information along the desired directions of legitimate receivers, and artificial noise in other directions, to deliberately confuse eavesdroppers in line-of-sight channels. Recently, artificial noise is also introduced into spatial modulation, leading to a secure spatial modulation strategy. In this Special Section in IEEE ACCESS, secure modulation is defined broadly as any secure modulation method, which includes, but is not limited to, secure directional modulation, secure spatial modulation, and secure index modulation.

Robust approaches, such as minimum mean square error and maximizing signal-to-leakage-and-noise ratio, have been proposed for directional modulation to overcome its performance degradation caused by the estimation error in direction angles. These approaches can significantly improve the performance of directional modulation in terms of achieving a lower bit error rate or a higher secrecy rate.

In the context of directional modulation, multipath artificial noise aggregation caused by multipath propagation significantly degrades the performance of directional modulation systems in multipath fading channels. A current research challenge is how to reduce this performance degradation.

As an enabling technique for physical layer security, secure modulation will work together with routing security and conventional cryptography to provide three-fold protection for future wireless networks. Secure modulation schemes have been viewed as strong candidates for achieving secure, spectral-efficient, and energy-efficient future wireless networks, which can strike a good balance among security, spectrum-efficiency, and energy-efficiency.

Motivated by these observations, this Special Section in IEEE ACCESS aims to capture the state-of-the-art advances in secure modulation concepts (such as secure directional modulation, spatial modulation, and index modulation) and other related research. This Special Section will trigger new research interests in secure modulation from both industry and academia, aiming to solve some challenging problems in the context of secure modulation technology.

Our call for papers received an enthusiastic response with 36 high-quality submissions. Per IEEE ACCESS policy, it was ensured that handling editors did not have any potential conflict of interest with authors of submitted articles. All articles were reviewed by at least two independent referees. The articles were evaluated for their rigor and quality, and also for their relevance to the theme of our Special Section. We considered articles that both proposed solutions tailored particularly for the context of the developing world, and also those that were globally oriented, with solutions that could, by extension, also be applicable in the developing world. After a rigorous review process, we accepted 14 articles to form the Special Section.

The article, ''Secure energy harvesting relay networks with unreliable backhaul connections,'' by Yin *et al.*, studied the effect of unreliable backhaul on the secrecy of an energy harvesting relay network with transmitter selection. In this work, analytical expressions for secrecy outage probability, non-zero achievable secrecy rate, and ergodic secrecy rate were derived under independent Rayleigh fading channels, which can reveal the effect of the number of transmitters and backhaul reliability on the system performance. The authors presented results indicating that energy harvesting time fraction has a huge impact on the system performance, hence, should be optimally designed.

In the article, ''Secrecy rate optimization in wireless multi-hop full duplex networks,'' Tian *et al.* proposed a cross-layer optimization method in wireless multi-hop full duplex networks. Through the cross-layer optimization modeling, formulating, and reformulating, the authors investigated secrecy rate optimization in wireless multi-hop full duplex networks. The numerical results presented in the article validated the proposed methods, which demonstrated that the combination of full duplex and security improved both spectrum efficiency and security of a conventional wireless system.

The article, ''Secrecy outage analysis for distributed antenna systems in heterogeneous cellular networks,'' by Sun *et al.*, proposed two underlay spectrum sharing (USS) schemes, i.e., the interference cancelled opportunistic antenna selection (IC-OAS) and interference-limited

opportunistic antenna selection (IL-OAS), to improve the spectrum efficiency. This is due to the fact that in macro cell, only a single antenna is selected from multiple distributed antennas of macro base station (MBS) to transmit to macro user (MU), while small base station (SBS) directly transmits to small user (SU), leading to low spectrum efficiency. The authors evaluated the secrecy outage probability of their proposed methods, showing that the IC-OAS scheme significantly performs better than the IL-OAS scheme for the macro-cell transmission.

The article, ''Secure connectivity in infrastructure-based one-dimensional networks with the presence of random eavesdroppers,'' by Xiaowei Wang, studied the secure connectivity of infrastructure-based 1-D networks protected by physical-layer security, which consists of three nodes: powerful nodes (PNs), ordinary nodes (ONs), and eavesdroppers. The author establishes an analytical framework by defining *secure segment* and *secure scenarios* to characterize the secure connections in terms of connectivity probability (SCP) and secure segment probability (SSP). The experimental results demonstrated the relations between secure connectivity and system parameters (e.g., the distance between adjacent PNs) of the proposed framework.

In the article, ''Performance analysis of secret precoding-aided spatial modulation with finite-alphabet signaling,'' Wu *et al.* show that the precoding-aided spatial modulation (PSM) is a secrecy-embedded communication scheme when operated in the time-division duplex mode, but experiences security risk under frequency-division duplex mode. Therefore, the authors extend the PSM to a secret PSM (SPSM) that is suitable for operation in any communications scenarios experiencing passive eavesdropping. The authors prove that, for the desired receiver, the SPSM employs all the advantages of the PSM, including low-complexity detection. Relying on the asymptotic analysis, the authors derive the upper and lower bounds for the error performance and secrecy rate of SPSM. Furthermore, the authors study the power allocation between information and interference transmission in order to maximize SPSM's secrecy performance. Their studies result in a range of expressions, which are validated by Monte Carlo simulations, and demonstrate that the analytical formulas are beneficial to the optimization of SPSM systems for maximizing its security performance.

The article, ''Enhancing security of primary user in underlay cognitive radio networks with secondary user selection,'' by Qin *et al.*, investigated the effect of multiuser gain provided by the secondary user selection on the secrecy performance of the primary users, and presented two secondary user selection schemes, named minimal interference-based scheme and maximal jamming rate-based scheme. The authors give a comprehensive analysis of the multiuser gain in secure cognitive communications. For the minimal interference-based scheme, a closed-form lower bound of the achieved ergodic secrecy rate (ESR) is derived and the impact of interference temperature level (I), and peak power of secondary (PS) users on the secrecy performance of the primary users is investigated. For the maximal jamming rate based scheme, the authors provided a closed-form expression of the achievable ESR and showed that it significantly enhances the security of the primary user. The results are presented to demonstrate the multiuser secrecy performance for the primary user, and the maximal jamming rate scheme is also a choice for secure communication for cognitive radio networks.

In the article ''Intrinsic secrecy of EGT and MRT precoders for proper and improper modulations,'' Anjos *et al.* analyzed theoretical information of the intrinsic secrecy level of M-QAM and M-PSK modulation schemes, considering the use of equal gain transmission and maximum ratio transmission precoding techniques. It showed that the proper and improper versions of M-QAM and M-PSK constellations have always associated some intrinsic secrecy when channel coherent precoders like equal gain transmission (EGT) and maximum ratio transmission (MRT) are applied to these modulation schemes. The proper MPSK verifies full secrecy always. For large order constellations, the normalized secrecy level reduces when $M \rightarrow \infty$. For lower values of M, the percentage of information secured by the transmission scheme is large and therefore can be exploited to significantly reduce the entropy of a secret key used to protect the information. Furthermore, a secrecy comparison between the proper and improper constellations showed that the improper case is less secure.

The article, ''Secrecy energy efficiency optimization in AN-aided distributed antenna systems with energy harvesting,'' by Wang *et al.*, studied the secrecy energy efficiency maximization (SEEM) problem for artificial-noise (AN)-aided downlink distributed antenna systems with simultaneous wireless information and power transfer. A double-layer iterative optimization algorithm is proposed. By introducing a tight relaxation variable, the outer layer problem becomes a single variable optimization problem and can be solved using a one-dimensional search algorithm. The inner layer problem is converted to a subtractive form with the Dinkelbach method, and the closed-form expressions for the power of the transmitted confidential signal and the AN power are derived. The simulation results reveal the effectiveness of the proposed algorithm, and the advantage of AN in improving the system secrecy energy efficiency.

In the article, ''Directional modulation with cooperative receivers,'' Xiao *et al.* proposed a secure directional modulation scheme with aided cooperative receivers (DM-CR). By introducing a distortion factor, which is randomly selected from a predefined set into the beamforming vector, the signal in eavesdropper is completely distorted irrespective of the direction or location of the eavesdropper, thus the secure communication can be guaranteed. Furthermore, the authors investigated the average bit error probability of proposed scheme and presented detailed evaluations and simulations to verify the superiorities of proposed method compared with conventional methods.

The article, "Artificial noise aided precoding with imperfect CSI in full-duplex relaying secure communications," by Li, *et al.*, proposed the secure artificial noise aided precoding (ANP) in full-duplex (FD) relay systems with imperfect channel state information (CSI) to enhance the secrecy performance. The authors first derived the closed-form expression of approximate ergodic achievable secrecy rate (EASR) when the number of antennas is arbitrary. Based on this, a closed-form of exact EASR for large-scale antenna array was given. The authors also presented the asymptotic performance analyses of theoretical derivation and simulation to valid the effectiveness and superiority of the proposed ANP combined with FD algorithm in terms of EASR.

The article, "A novel physical layer encryption algorithm based on statistical characteristics of time-selective channels," by Hua *et al.*, proposed a physical layer encryption algorithm for time-selective channels instead of conventional static channels or quasi-static channels in which the time-selectivity of channels can be neglected. The algorithm exploits the channel autocorrelation function and level crossing rate to drive chaos systems to produce the chaos sequence, which is used as the cryptographic key, and then the physical signal is encrypted by the simple scrambling operation. The authors demonstrated the performance of the proposed algorithm through simulations, and the bit error rate results proved that the legal transceiver can decrypt the receiving signal successfully while the illegal eavesdropper cannot recover the original signal due to the channel difference, i.e., the physical layer safety is realized.

In the article, "The security network coding system with physical layer key generation in two-way relay networks," Kong *et al.* presented a security network coding scheme with key generation from multipath channels to enhance the security performance for two-way relay networks. A joint key generation approach is proposed to generate a secret key without key exchange, and an adaptive quantization algorithm is proposed to adaptively choose the quantization method in key generation. The security network coding systems integrate the key generation approaches with the proposed algorithm. Simulation results verify that the proposed schemes are valid and secure against wiretap attacks.

In the article, "A secure waveform format for interference mitigation in heterogeneous uplink networks," Zeng *et al.* developed a system combining a beamforming (BF) technique based on uniform circle array and a frequency-hopping (FH) technique under an orthogonal frequency division multiplex (OFDM) scheme (i.e., OFDM/FH-BF system). In order to improve the reliability of transmission uplinks in HetNet, a modified beamforming receiver structure based on a uniform circle array pattern has been designed for wide-band OFDM/FH signals. The convergence rate of an adaptive BF algorithm was discussed and the impact of the FH parameters and BF parameters (e.g., the number of frequency slots q, the number of interferers K, the number of snapshots N, SNR, and SIR) on system performance, in particular at the cell edge with multiple interferers, were studied via theoretical and numerical simulation analysis. The analysis in this article shows that the proposed OFDM/FH-BF system with adaptive linearly constrained minimum variance algorithm converges in a small number of snapshots N, which implies that the adaptive BF control could be implemented perfectly during the short hopping interval, and can keep up with the direction change of the highly mobile users.

Finally, the article, "Secrecy performance analysis of artificial-noise-aided spatial modulation in the presence of imperfect CSI," by Yu *et al.*, investigated the physical layer security based on the ergodic secrecy rate (ESR) of spatial modulation systems. The authors consider imperfect channel information (CSI) and evaluate the secrecy performance over Rayleigh channels. The ergodic rate and its lower bound for the legitimate receiver and eavesdropper are, respectively, derived. On the basis of these derivations, the authors further derive the system ESR and obtain two approximated expressions. One requires mean computation, and another can provide a closed-form expression. Results show that the ESR exhibits obvious degradation when the estimation error variance is beyond 0.01. Also, after an initial increase, the ESR decreases eventually, with increasing power of the artificial noise. Simulation results align with the theoretical analysis, thereby validating the derived mathematical expressions.

To conclude, we would like to sincerely thank all the authors for submitting their articles to our Special Section, and the large number of reviewers who kindly volunteered their time and expertise to help us curate a high-quality Special Section on this important and timely topic. We also would like to thank the IEEE ACCESS Editor-in-Chief, Prof. Derek Abbott, Margery Meyer and other staff members of IEEE ACCESS for their continuous support and guidance.

FENG SHU, *Guest Editor*
School of Electronic and Optical Engineering
Nanjing University of Science and Technology
Nanjing 210094, China

SHIHAO YAN, *Guest Editor*
School of Engineering
Macquarie University
Sydney, NSW 2109, Australia

DONGMING WANG, *Guest Editor*
School of Information Science and Engineering
Southeast University
Nanjing 210096, China

XIANGWEI ZHOU, *Guest Editor*
Division of Electrical and Computer Engineering
Louisiana State University
Baton Rouge, LA 70803 USA

JIANGZHOU WANG, *Guest Editor*
School of Engineering and Digital Art
University of Kent
Canterbury CT2 7NZ, U.K.

FENG SHU was born in 1973. He received the B.S. degree from the Fuyang Teaching College, Fuyang, China, in 1994, the M.S. degree from Xidian University, Xi'an, China, in 1997, and the Ph.D. degree from Southeast University, Nanjing, China, in 2002. In 2005, he joined the School of Electronic and Optical Engineering, Nanjing University of Science and Technology, Nanjing, where he is currently a Professor, and also a Supervisor of Ph.D. and graduate students. From 2009 to 2010, he held a Visiting Postdoctoral position at The University of Texas at Dallas. He has published about 300 articles, of which over 200 are in archival journals, including more than 60 articles on the IEEE Journals and more than 100 SCI-indexed articles. He holds seven Chinese patents. His research interests include wireless networks, wireless location, and array signal processing. He serves as a TPC member for several international conferences, including the IEEE ICC 2019, the IEEE ICCS 2018/2016, ISAPE 2018, and WCSP 2017/2016/2014. He was awarded with the Mingjiang Chair Professor in Fujian Province. He is an Editor of IEEE ACCESS.

SHIHAO YAN (M'15) received the B.S. degree in communication engineering and the M.S. degree in communication and information systems from Shandong University, Jinan, China, in 2009 and 2012, respectively, and the Ph.D. degree in electrical engineering from the University of New South Wales, Sydney, NSW, Australia, in 2015. From 2015 to 2017, he was a Postdoctoral Research Fellow with the Research School of Engineering, The Australian National University, Canberra, ACT, Australia. He is currently a Research Fellow with the School of Engineering, Macquarie University, Sydney. His current research interests are in the areas of wireless communications and statistical signal processing, including physical layer security, covert communications, and location spoofing detection.

DONGMING WANG received the B.S. degree from the Chongqing University of Posts and Telecommunications, in 1999, the M.S. degree from the Nanjing University of Posts and Telecommunications, in 2002, and the Ph.D. degree from Southeast University, in 2006. He joined the National Mobile Communications Research Laboratory, Southeast University, China, in 2006, where he has been an Associate Professor since 2010. He is currently a Visiting Scholar with the University of California, Davis, CA, USA. His current research interests include turbo detection, channel estimation, distributed antenna systems, and large-scale MIMO systems. He serves as an Associate Editor for *Science China Information Sciences*.

XIANGWEI ZHOU received the B.S. degree in communication engineering from the Nanjing University of Science and Technology, Nanjing, China, in 2005, the M.S. degree in information and communication engineering from Zhejiang University, Hangzhou, China, in 2007, and the Ph.D. degree in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2011. Prior to that, he was a Senior Systems Engineer with Marvell Semiconductor, Santa Clara, CA, USA, from 2011 to 2013. He was an Assistant Professor with the Department of Electrical and Computer Engineering, Southern Illinois University, Carbondale, IL, USA, from 2013 to 2015. Since August 2015, he has been an Assistant Professor with the Division of Electrical and Computer Engineering, Louisiana State University, Baton Rouge, LA, USA. His research interests include wireless communications, statistical signal processing, and cross-layer optimization, with current emphasis on spectrum-efficient, energy-efficient and secure communications, coexistence of wireless systems, and machine learning for intelligent communications. He was a recipient of the Best Paper Award at the 2014 International Conference on Wireless Communications and Signal Processing. He has served as an editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, from 2013 to 2018.

JIANGZHOU WANG (F'17) is currently the Head of the School of Engineering and Digital Arts and a Professor with the University of Kent, U.K. He has authored over 300 articles in international journals and conferences in the areas of wireless mobile communications and three books. His research interests include massive MIMO, Cloud RAN, NOMA, D2D, and secure communications. He is an IET Fellow. He received the Best Paper Award from IEEE GLOBECOM2012. He was an IEEE Distinguished Lecturer from 2013 to 2014. He is the Technical Program Chair of IEEE ICC2019 in Shanghai. He was the Executive Chair of IEEE ICC2015 in London and the Technical Program Chair of IEEE WCNC2013. He was an Editor for the IEEE TRANSACTIONS ON COMMUNICATIONS, from 1998 to 2013. He was a Guest Editor for the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, the *IEEE Communications Magazine*, and the IEEE WIRELESS COMMUNICATIONS.