Accepted in IEEE Int. Conference on Ubiquitous Wireless Broadband (ICUWB), 2015

A Survey on Cooperative Jamming Applied to Physical Layer Security

Michael Atallah, Georges Kaddoum, Long Kong
Department of Electrical Engineering, LACIME Laboratory
University of Quebec, ETS
Montreal, Canada.
Email: michael.atallah.1@ens.etsmtl.ca, georges.kaddoum@etsmtl.ca, long.kong.1@ens.etsmtl.ca

***Abstract*—Security has always played a critical role in wireless cooperative communication systems design. Eavesdropping and jamming are two common threats to the information security in wireless networks. However, jamming can be used in a cooperative manner to enable a secure communication link between the legitimate transmitter and the intended receiver. This paper presents a comprehensive survey on different jamming methods used to enhance the physical layer security. This survey outlines first the underlying concept and challenges with respect to security in wireless network design followed by a comprehensive literature review and analysis of jamming techniques with their applications in this field. For each jamming protocol, the paper categorizes different techniques within the existing literature by elaborating on their application, and corresponding performances.**

***Index Terms*—Physical layer security, cooperative jamming, beamforming, power allocation, artificial noise, multiple antennas, MIMO, game theory.**

I. Introduction

Wireless communications is playing an integral part in our lives and also has a significant social impact. Privacy and confidentiality with respect to the transmitted information over the wireless medium becomes vital, especially for applications concerning medical information, e-banking, and e-commerce. However, wireless communications are often vulnerable to eavesdropping and signal interception [1]. Many security tasks are involved in wireless networks design, like integrity and confidentiality checks, authentication, spectrum access control [2], [3]. Confidentiality refers to the prevention of unauthorized information disclosure. Integrity ensures that the transmitted information is utilized and modified by the legitimate user. Authentication refers to the identity confirmation of different terminals. Spectrum access control refers to prevention of denial-of-service type attacks. Conventionally, these security tasks are addressed mostly in the upper layers of the network protocol stack using cryptographic encryption and decryption methods. When employing symmetric-key cryptosystems, the two users have to share a common private key to encrypt and decrypt the confidential message [1]. However, for the secret keys sharing, this requires a secure channel or protocol. The difficulties in secret key distribution and management [4] lead to security vulnerabilities in wireless systems. Alternatively, public-key cryptosystems allow the use of a public key for encryption and a separate private key for decryption. The public key is available to all users whereas the private key is known only to the receiver. However, the cryptographic methods rely on the computational hardness on decrypting the message to achieve security when the secret key is not available. As the computational power increases, e.g., with the development of quantum computers, the computational hardness of certain mathematical problems, for which the encryption and decryption are based on, may no longer hold, causing many current cryptosystems to break down [1]. Many coding and signal processing techniques in the physical layer have been developed in the recent years, to support and to further enhance security in wireless systems, many researchers have made contributions to find alternative security solutions to fit the requirements of the current and emerging wireless networks [5]–[8]. Even though the fast channel variations and the wireless medium's broadcast nature may cause additional challenges, physical layer security technique exploits the properties of the wireless transmissions to secure the communication channel in a better way [1].

Interference, in general, is regarded as undesired phenomenon in wireless communications. But in secure communications, interference can benefit the system if it is used in a proper way. The idea is to create an interference and put the eavesdropper in a disadvantage comparing to the legitimate nodes [9]. Several applications use interference to increase the security in the physical layer, one of the security applications that has become a very common and promising technique in the physical security field is the cooperative jamming which is accomplished by the friendly terminals in which one of the legitimate parties sacrifices his entire rate to jam the eavesdropper.

In this paper a continuation and update of the recent achievements in the field of physical layer security is presented with emphasis on different jamming methods and protocols of such schemes. Hence, our contribution can be summarized as follows:

1) Providing a brief overview of physical layer system model and the challenges in this field.
2) Developing a literature review of the different jamming techniques within the existing recent literature with their advantages and disadvantages, followed by a discussion on their subsequent application.

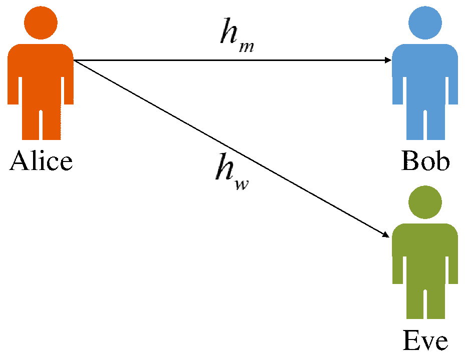

Fig. 1. Wireless wiretap system model

The remainder of this paper is outlined as follows. The concept of physical layer security is depicted in Section II. Cooperative Jamming and techniques to enhance physical layer security via cooperative jamming are presented in section III. Finally, the concluding remarks are given in section IV.

II. Physical Layer Security and Cooperative Jamming

A. Physical Layer Security

As shown in Fig. 1, a generic wireless communication network model which consists of three nodes is taken into consideration: the legitimate transmitter (Alice), the intended receiver (Bob) and the eavesdropper (Eve). The link between Alice and Bob is called the main channel, while the link between Alice and Eve is named as a wiretap channel. This model exemplifies the specific features of most multi-user secure communication systems. The secrecy capacity is defined as the maximum achievable secrecy rate. In [10], the secrecy capacity over additive white Gaussian noise (AWGN) channel $C_{s,A}$ and Rayleigh fading channel $C_{s,R}$ are given by

$$C_{s,A} = \left[\frac{1}{2}\log_2\left(1+\frac{P}{\sigma_m^2}\right) - \frac{1}{2}\log_2\left(1+\frac{P}{\sigma_w^2}\right)\right]^+ \tag{1}$$

$$C_{s,R} = \left[\log_2\left(1+\frac{P|h_m|^2}{\sigma_m^2}\right) - \log_2\left(1+\frac{P|h_w|^2}{\sigma_w^2}\right)\right]^+ \tag{2}$$

where P is the transmitted power, σ_m and σ_w are the noise power of the main channel and wiretap channel. h_m and h_w are the Rayleigh fading coefficients of main channel and wiretap channel respectively. $[x]^+ = \max\{0, x\}$. Also, the received signal-to-noise ratio (SNRs) at Bob and Eve are defined as $\gamma_m = \frac{P|h_m|^2}{\sigma_m^2}$ and $\gamma_w = \frac{P|h_w|^2}{\sigma_w^2}$, respectively.

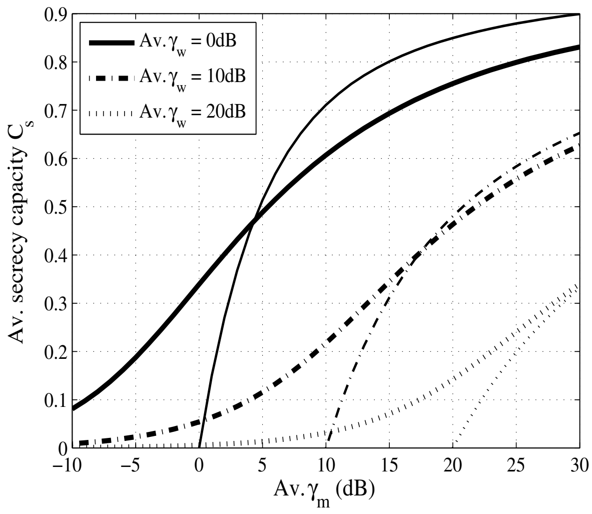

Fig. 2. Normalized average secrecy capacity versus $\overline{\gamma}_m$, for selected values of $\overline{\gamma}_w$. The thicker lines correspond to the normalized average secrecy rate capacity of Rayleigh fading channel while the thinner lines correspond to the secrecy capacity of a Gaussian wiretap channel.

In Fig. 2, an average secrecy capacity of Rayleigh fading channel is compared (equation (2)) with that of Gaussian wiretap channel (equation (1)). Strikingly, one can observe that the secrecy capacity over Rayleigh fading channels is higher than that of an AWGN channel, in other words, we can use the fading property of the physical layer channel to decrease the SNR of wiretap channel. Besides using the fading characteristics of wireless channel, many other methods are applied to improve the secrecy performance of the wireless communication systems. All the existing physical layer security methods in [3] are classified into five major approaches: theoretical secrecy capacity, multiple-input-multiple-output (MIMO) channel, coding schemes (channel coding and network coding), power allocation, and signal design (artificial noise). Additionally, cooperative relay [11]–[13], cooperative jamming [14] and energy harvesting [15] are other useful methods. Among the aforementioned methods, cooperative jamming is a promising technique and has attracted significant attention. It was originally proposed for a multiple access wiretap channel, where multiple legitimate users wish to have simultaneous secure communications with an intended receiver in the presence of an eavesdropper.

B. Cooperative jamming

Cooperative jamming is a special technique where artificial noise is introduced by a helpful interferer to confuse the eavesdropper.

In the following section, we will introduce the cooperative jamming techniques which are used to enhance the physical layer security. To improve the secrecy capacity, we should either increase the legitimate receiver's SNR or decrease the eavesdropper's SNR. A natural approach by which to achieve the latter (decreasing the eavesdropper's SNR) is to introduce interferers into the system.

C. Artificial Jamming Signals types

Cooperative jamming depends on creating the interference at the eavesdropper's side, many artificial jamming signals are used and could be divided into four categories [16]:

1) Gaussian noise: which is the same as the additive noise at the receiver [17]–[19].

2) Jamming signals which are priory known at legitimate receivers, which has an impact only on the eavesdropper's performance. This type of signals is better than the previous one because the jamming signals don't affect the legitimate receiver [20], [21].
3) Random codewords of a public codebook which is known by all the nodes including the eavesdroppers, so the legitimate receiver has the ability to decode and cancel the jamming signals, even though it requires a complicated self-interference cancellation receiver to decode the codewords [22].
4) Useful signals for the other legitimate nodes; like the downlink and the uplink of the neighbouring cells [23], signals of multiple simultaneous source-destination pairs [24], or signals of the invited cognitive ratio users [25] and [26], this type is difficult to apply because of the change of the multiple transmission pairs.

Many applications are used in conjunction with the cooperative jamming strategy to enhance the performance and increase the security, these include the usage of multiple antennas, beamforming, game theory, and power allocation methods.

III. Application of cooperative jamming

A. Cooperative Jamming with Multiple Antennas and Beamforming

Many works apply multiple antennas method with cooperative jamming technique to enhance the physical layer security [15], [27]–[32]. The authors in [27] assume a scenario that the base station has to send multiple independent data streams to multiple legitimate users; during the transmission, many eavesdroppers with multiple antennas have interests in the transmission stream of the base station. The eavesdroppers may collude or not, and maximize the signal-to-interference-plus-noise ratio (SINR) of the desired streams using the beamforming method. The cooperative jammer will work on keeping the SINR at the eavesdroppers below a certain threshold level to guarantee a confidential transmission between the base station and the legitimate users. Another scenario in [29] studies the Gaussian wiretap channel's secrecy capacity aided by an external jammer. Each of the receiver and the transmitter has a single antenna, while the jammer and the eavesdropper are equipped with multiple antennas. The authors in [30] reveal a scenario for secure transmission within a two-hop amplify-and-forward relay network scheme, such that for large number of antennas at the source, the ergodic secrecy capacity (ESC) is independent of the number of antennas; whereas, for a large number of antennas at the destination, the ESC is dependent on the number of antennas.

Beamforming is a very efficient method also when it is used with the cooperative jamming technique. However, these two techniques are adopted separately in most works [11], [12], [32]–[34]. In [12], a scheme with joint cooperative jamming and beamforming is proposed to enhance the security of a cooperative relay network, where part of the nodes uses a distributed beamforming mechanism while the others jam the eavesdropper simultaneously. In [33], another scheme of using the beamforming is proposed; by preventing the eavesdroppers from using the beamformers to suppress the jamming signals. It uses also two orthogonal dimensions for transmitting and receiving signals. A hybrid cooperative jamming and beamforming scheme is proposed in [34] also; the idea is in both cooperative transmission phases, some intermediate nodes relay the signals to the legitimate receivers by adopting the beamforming distribution, while, simultaneously, the other nodes jam the eavesdropper, which eventually leads in protection of the transmitted data. The authors in [11] develop an optimal relay assignment algorithm to solve the secrecy capacity maximization problem, and a smart jamming algorithm is proposed to increase the secrecy capacity of the system.

B. Cooperative jamming with Power Allocation method

Since the system's performance in cooperative jamming depends highly on the jamming strategy as well as the power level of the jamming [9], three power allocation strategies are derived in [9] to minimize the outage probability of the secrecy rate, besides that, three kinds of jamming power allocation schemes are proposed according to the available channel state information (CSI) at the destination to minimize the outage probability. The authors in [28] propose another scenario investigates the MISO channels with power splitting scheme used by the legitimate receiver to split the received signal for both information decoding and energy harvesting. Another power allocation method in [16] is analysed in which the source nodes should send jamming signals as a part of their power instead of hiring extra nodes to jam the eavesdropper. Two types of jamming signals are analysed; a priori known jamming signals at the source nodes, and unknown jamming signals at the source nodes. A major finding reported in this work is that, if the jamming signals are known a priori at the source nodes, the secrecy capacity is improved significantly when compared to the scenario in which the jamming signals are unknown at the source nodes. In [35], a linear precoding scheme is utilized at the base station, which exploits transmit diversity by weighting the information stream, this is studied with the cooperative jamming strategy. An optimal solution is obtained when the number of antennas at the friendly jammer is no less than the total number at the eavesdropping antennas. The authors in [36] propose a sequential parametric convex approximation (SPCA) based algorithms to address the power allocation optimization and maximize the ergodic secrecy rate (ESR) lower bound, and then it is shown that the optimized power allocation tends to allocate more power to the jamming signals to improve the secrecy capacity. An optimal relay selection criterion and power allocation strategy are derived in [37] between the jamming signals and the confidential information for the ESR maximization. Another study in [38] shows that a helper node should allocate its power as a jammer or as a helper depending on the locations of the helper and the eavesdropper.

C. Jamming Policies

Several policies are proposed for relay selection [39]–[41]. In [39], four relay selection policies are proposed and compared, namely random relay and random jammer, random jammer and best relay, best relay and best jammer, and best relay and no jammer; and it characterizes the joint impact of the proposed relay selection policies and the interference power constraint on the secrecy performance by deriving new exact closed-form expressions for the secrecy outage probability; it is shown then that the jammer's absence gives rise to the outage saturation phenomenon. Two relay and jammer selection methods are developed in [41] for minimizing the secrecy outage probability; in both these selection methods, each intermediate node knows its own role while the knowledge of the jammer and relay set is kept secret from all the eavesdroppers. It is shown that maintaining the privacy of the selection result improves greatly the secrecy outage probability performance. This work assumes a decode and forward relay system, in which the source communicates with the destination through many intermediate nodes in the presence of several passive eavesdroppers. The intermediate nodes act as either jammers or as conventional relays to hinder the eavesdroppers from intercepting the signal of interest. The destination broadcasts information that allows the intermediate nodes to determine whether they will serve as relays or jammers, but this information does not allow the eavesdroppers to know the selection result. In [9], a scheme is provided which has a destination, relay and a source; the destination starts to send jamming signals towards the eavesdropper while the source is sending the message to the relay, and the destination then removes the jamming noise perfectly via self-interference cancellation at the second phase. Another scheme in [42] is provided; in the first phase, the source transmits the information bearing signal, simultaneously as it cooperates with the destination in jamming the eavesdropper without interference at the relay. In the second phase, a relay is selected optimally, which transmits the decoded source signal, at the same time, this relay cooperates with the source to jam the eavesdropper without creating interference at the destination. The authors in [43] propose a new transmission scheme, where the relaying group and the jamming group are constructed together, this scheme enables to block the eavesdroppers simultaneously and further increase the signal-to-noise ratio at the destination. In [13], attack strategies are investigated in a multi-relay network that consists of both malicious and cooperative relays, where the malicious relays are given the freedom to listen to the source in the first phase (so that they can send interfering signals in the second phase), or to directly emit jamming signals in both phases. Subsequently, it is shown that the malicious relays should attack in both phases rather than just listening in the first phase and attack in the second phase. On the other hand, the opportunistic cooperative jamming and the opportunistic relay chatting schemes are compared in [44]. It is shown that the chatting scheme is better for implementing the relay nodes to jam the eavesdropper in the both phases comparing with cooperative jamming scheme in which only the eavesdropper jams in the first phase.

Moreover, jamming policies using game theory methods are proposed in [13], [45]–[47]. In [45], a scheme of two user multiple-input-single output Gaussian interference channel is considered, where each transmitter aims to maximize the difference between its secrecy rate and the other's secrecy rate, in this scheme, the weaker link tries to minimize the extra secrecy rate of the other transmitter, while the transmitter with the stronger link tries to maximize it. This paper uses Nash equilibrium strategy as a solution in its scheme. A multi-relay network is considered in [13] that consists of both malicious and cooperative relays, and applies Nash equilibrium game strategy on its scheme, by modelling the cooperative relays set and the malicious relays set as two players in a zero sum game with the maximum achievable rate as the utility. The authors in [46] propose another game-theoretic model, Stackelberg game, with the legitimate parties being spectrum owners acting as a game leader, and the set of the assisting jammers which are constituting the follower. It shows that when the potential jammers' number increases, utility of a chosen jammer for any scheme will start to decrease as the legitimate parties can be more aggressive when leading the game. In [47], a smart jammer can quickly learn the transmission strategies of the legitimate transmitters, then he would adjust his strategy to damage the legitimate transmission. Meanwhile, the transmitters are aware of the existence of the smart jammer. This anti-jamming scenario is modeled as a Stackelberg game, where the leader is the source node and the follower is the jammer. It is shown that the optimal power control strategies obtained from the Stackelberg equilibrium game can decrease the damage caused by the jammer.

IV. Conclusion

Unlike its conventional applications, jamming techniques are used to enhance the security of transmission in wireless communication networks. In this paper, we have surveyed the different challenges related to the physical layer security in wireless networks and we developed a literature review of the different jamming techniques within the existing recent literature with their advantages and disadvantages.

Based on this review we can conclude that there are still many issues to be resolved around jamming techniques applications such as communication architectures for energy harvesting, protocols, and interference management.

Acknowledgment

This work has been supported by the ETS' research chair of physical layer security in wireless networks.

References

[1] Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, *Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems*. Springer Publishing Company, Incorporated, 2013.

[2] W. Lou and K. Ren, "Security, privacy, and accountability in wireless access networks," *IEEE Wireless Commun.*, vol. 16, no. 4, pp. 80–87, Aug. 2009.

[3] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[4] B. Schneier, "Cryptographic design vulnerabilities," *IEEE Comput.*, vol. 31, no. 9, pp. 29–33, sept. 1998.

[5] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[6] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inform. Theory.*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

[7] C. Shannon, "Communication theory of secrecy systems," *The Bell Syst. Technical J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[8] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[9] K.-H. Park, T. Wang, and M.-S. Alouini, "On the jamming power allocation for secure amplify-and-forward relaying via cooperative jamming," *IEEE J. Selected Areas in Commun.*, vol. 31, no. 9, pp. 1741–1750, Sept. 2013.

[10] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory.*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[11] B. Han, J. Li, J. Su, M. Guo, and B. Zhao, "Secrecy capacity optimization via cooperative relaying and jamming for wanets," *IEEE Trans. Parallel and Distributed Systems*, vol. 26, no. 4, pp. 1117–1128, Apr. 2015.

[12] H.-M. Wang, M. Luo, X.-G. Xia, and Q. Yin, "Joint cooperative beamforming and jamming to secure af relay systems with individual power constraint and no eavesdropper's csi," *IEEE Signal Process. Lett.*, vol. 20, no. 1, pp. 39–42, Jan. 2013.

[13] M.-H. Chen, S.-C. Lin, Y.-W. Hong, and X. Zhou, "On cooperative and malicious behaviors in multirelay fading channels," *IEEE Trans. Inform. Forensics and Security*, vol. 8, no. 7, pp. 1126–1139, July 2013.

[14] D. H. Ibrahim, E. S. Hassan, and S. A. El-Dolil, "Relay and jammer selection schemes for improving physical layer security in two-way cooperative networks," *Comput. & Security*, vol. 50, no. 0, pp. 47 – 59, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404815000140

[15] H. Xing, Z. Chu, Z. Ding, and A. Nallanathan, "Harvest-and-jam: Improving security for wireless energy harvesting cooperative networks," in *IEEE Global Commun. Conf. (GLOBECOM).*, Dec. 2014, pp. 3145–3150.

[16] H. Long, W. Xiang, J. Wang, Y. Zhang, and W. Wang, "Cooperative jamming and power allocation with untrusty two-way relay nodes," *Commun. IET*, vol. 8, no. 13, pp. 2290–2297, Sept. 2014.

[17] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1544–1554, Mar. 2013.

[18] X. He and A. Yener, "The role of feedback in two-way secure communications," *IEEE Trans. Inform. Theory.*, vol. 59, no. 12, pp. 8115–8130, Dec. 2013.

[19] R. Zhang, L. Song, Z. Han, and B. Jiao, "Distributed coalition formation of relay and friendly jammers for secure cooperative networks," in *IEEE Int. Conf. Commun. (ICC).*, June 2011, pp. 1–6.

[20] H. Long, W. Xiang, J. Wang, Y. Zhang, and W. Wang, "Cooperative jamming and power allocation in three-phase two-way relaying wiretap systems," in *IEEE Wireless Commun. and Networking Conf. (WCNC).*, Apr. 2013, pp. 4175–4179.

[21] L. Dong, H. Yousefi'zadeh, and H. Jafarkhani, "Cooperative jamming and power allocation for wireless relay networks in presence of eavesdropper," in *IEEE Int. Conf. Commun. (ICC)*, June 2011, pp. 1–5.

[22] A. Pierrot and M. Bloch, "Strongly secure communications over the two-way wiretap channel," *IEEE Trans. Inform. Forensics and Security*, vol. 6, no. 3, pp. 595–605, Sept. 2011.

[23] P. Popovski and O. Simeone, "Wireless secrecy in cellular systems with infrastructure-aided cooperation," *IEEE Trans. Inform. Forensics and Security.*, vol. 4, no. 2, pp. 242–256, June 2009.

[24] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, "Physical layer security from inter-session interference in large wireless networks," in *Proc. IEEE INFOCOM.*, Mar. 2012, pp. 1179–1187.

[25] I. Stanojev and A. Yener, "Recruiting multi-antenna transmitters as cooperative jammers: An auction-theoretic approach," in *Annual Allerton Conf. Commun., Control, and Computing (Allerton)*, Sept. 2011, pp. 1106–1112.

[26] I. Stanojev and A. Yener., "Cooperative jamming via spectrum leasing," in *Int. Symp. Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt)*, May 2011, pp. 265–272.

[27] J. Yang, I.-M. Kim, and D. I. Kim, "Optimal cooperative jamming for multiuser broadcast channel with multiple eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2840–2852, June 2013.

[28] Q. Zhang, X. Huang, Q. Li, and J. Qin, "Cooperative jamming aided robust secure transmission for wireless information and power transfer in miso channels," *IEEE Trans. Commun.*, vol. 63, no. 3, pp. 906–915, Mar. 2015.

[29] L. Li, Z. Chen, and J. Fang, "On secrecy capacity of gaussian wiretap channel aided by a cooperative jammer," *IEEE Signal Process. Lett.*, vol. 21, no. 11, pp. 1356–1360, Nov. 2014.

[30] L. Wang, M. Elkashlan, J. Huang, N. Tran, and T. Duong, "Secure transmission with optimal power allocation in untrusted relay networks," *IEEE Wireless Commun. Lett.*, vol. 3, no. 3, pp. 289–292, June 2014.

[31] K. Banawan and S. Ulukus, "Gaussian mimo wiretap channel under receiver side power constraints," in *Annu. Allerton Conf. Commun., Control, and Computing (Allerton),*, Sept. 2014, pp. 183–190.

[32] S. Vishwakarma and A. Chockalingam, "Mimo decode-and-forward relay beamforming for secrecy with cooperative jamming," in *Nat. Conf. Commun. (NCC)*, Feb. 2014, pp. 1–6.

[33] T. T. Tran and H. Y. Kong, "Csi-secured orthogonal jamming method for wireless physical layer security," *IEEE Commun. Lett.*, vol. 18, no. 5, pp. 841–844, May 2014.

[34] H.-M. Wang, M. Luo, Q. Yin, and X.-G. Xia, "Hybrid cooperative beamforming and jamming for physical-layer security of two-way relay networks," *IEEE Trans. Inform. Forensics and Security.*, vol. 8, no. 12, pp. 2007–2020, Dec. 2013.

[35] J. Yang, I.-M. Kim, and D. I. Kim, "Joint design of optimal cooperative jamming and power allocation for linear precoding," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3285–3298, Sept. 2014.

[36] C. Wang, H.-M. Wang, and X.-G. Xia, "Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 2, pp. 589–605, Feb. 2015.

[37] C. Wang and H.-M. Wang, "Joint relay selection and artificial jamming power allocation for secure df relay networks," in *IEEE Int. Conf. Commun. Workshops (ICC)*, June 2014, pp. 819–824.

[38] H. Deng, H.-M. Wang, W. Guo, and W. Wang, "Secrecy transmission with a helper: To relay or to jam," *IEEE Trans. Inf. Forensics and Security.*, vol. 10, no. 2, pp. 293–307, Feb. 2015.

[39] Y. Liu, L. Wang, T. T. Duy, M. Elkashlan, and T. Duong, "Relay selection for security enhancement in cognitive relay networks," *IEEE Wireless Commun. Lett.*, vol. 4, no. 1, pp. 46–49, Feb. 2015.

[40] L. Sun, P. Ren, Q. Du, Y. Wang, and Z. Gao, "Security-aware relaying scheme for cooperative networks with untrusted relay nodes," *IEEE Commun. Lett.*, vol. 19, no. 3, pp. 463–466, Mar. 2015.

[41] H. Hui, A. Swindlehurst, G. Li, and J. Liang, "Secure relay and jammer selection for physical layer security," *IEEE Signal Process. Lett.*, vol. 22, no. 8, pp. 1147–1151, Aug. 2015.

[42] Y. Liu, J. Li, and A. Petropulu, "Destination assisted cooperative jamming for wireless physical-layer security," *IEEE Trans. Inform. Forensics and Security.*, vol. 8, no. 4, pp. 682–694, Apr. 2013.

[43] M. Lin, J. Ge, and Y. Yang, "An effective secure transmission scheme for af relay networks with two-hop information leakage," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1676–1679, Aug. 2013.

[44] Z. Ding, K. Leung, D. Goeckel, and D. Towsley, "Opportunistic relaying for secrecy communications: Cooperative jamming vs. relay chatting," *IEEE Trans. Wireless Commun.*, vol. 10, no. 6, pp. 1725–1729, June 2011.

[45] S. A. A. Fakoorian and A. L. Swindlehurst, "Competing for secrecy in the miso interference channel," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 170–181, Jan. 2013.

[46] I. Stanojev and A. Yener, "Improving secrecy rate via spectrum leasing for friendly jamming," *IEEE Trans. Wireless Commun.*, vol. 12, no. 1, pp. 134–145, Jan. 2013.

[47] Y. Li, L. Xiao, J. Liu, and Y. Tang, "Power control stackelberg game in cooperative anti-jamming communications," in *Int. Conf. Game Theory for Networks (GAMENETS)*, Nov. 2014, pp. 1–6.