Jamming Strategies for Physical Layer Security

Yan Huo, Yuqi Tian, Liran Ma, Xiuzhen Cheng, and Tao Jing

Abstract

This article provides a comprehensive overview on jamming strategies in the physical layer for securing wireless communications. As a complement to traditional cryptography-based approaches, physical layer based security provisioning techniques offer a number of promising features that have not been previously available. Among the physical layer security techniques, jamming is an effective way to degrade the channel quality of the eavesdroppers for ensuring security. We start by giving a brief introduction to the fundamental principles of physical layer security and jamming. Then we classify jamming strategies from three different perspectives and explain the major related designs in various scenarios. Finally, we discuss the open issues of jamming that can be helpful to foster future research.

Introduction

The world is rapidly moving to mobile computing, i.e., people use various wireless devices such as smartphones to access information at anytime and from anywhere. Due to the broadcast nature of wireless communications, it is difficult to prevent the transmitted signals from being intercepted by unauthorized receivers (e.g., an eavesdropper). If the quality of the received signals is beyond a certain threshold, unauthorized receivers, regardless of their locations, can decode these signals and extract sensitive information. These characteristics make security provisioning a challenging issue in wireless networks.

To address the pressing security needs, many works have been done in the literature. These works mainly employ cryptographic techniques at the upper layers of the network stack so as to conceal information. However, cryptographic techniques cannot meet the security needs of all network scenarios. For instance, in a body area network consisting of resource-limited sensors, cryptographic techniques may not fit the stringent constraints in terms of computational power, memory, and communication rates. Furthermore, cryptographic techniques may not be able to sufficiently protect the transmitted signals from eavesdroppers when brute-force attacks can be mounted. As a result, an alternative solution is desirable in these scenarios.

Recently, physical layer based measures emerge as an attractive solution because they exploit the channel characteristics to enforce security; that is, the inherent randomness of noise and communication channels are used to limit the amount of information that can be extracted by unauthorized receivers. There have been a number of studies with various proposed techniques, among which jamming is an effective approach with great potential. Traditionally, jamming is regarded as a procedure that generates undesired interference to thwart normal communications [1, 2]. However, it can be beneficial when used in a proper way, that is, jamming at the eavesdroppers with an appropriate strategy. Specifically, a jamming strategy regulates how to transmit an artificial noise signal to eavesdroppers so as to effectively degrade their channel qualities from correct reception.

In this article, we first summarize the existing mainstream jamming strategies and categorize them from the following three different technical perspectives:

- Nonself-cooperative jamming vs. self-cooperative jamming.
- Jamming with perfect or imperfect channel state information (CSI) of the eavesdropper.
- Uniform jamming vs. directional jamming.

Note that a jamming strategy may adopt one or multiple techniques from these categories. We next discuss the security performance of each category, and exemplify the jamming design issues under two scenarios: a simple network and a complicated multiple-input and multiple-output (MIMO) network. Lastly, we discuss a few open research issues so as to further enhance achievable security considering novel techniques and new perspectives.

The rest of the article is organized as follows. We lay out the theoretical foundations of physical layer security and jamming in the following section. Then we present the classifications of jamming strategies and discuss the performance issues of different jamming approaches. Two example jamming strategies employed in different network scenarios are then detailed. We discuss a few open research issues and conclude the article in the final two sections, respectively.

Background

In this section, we give a brief introduction to the theoretical foundations of physical layer security and jamming. We start by introducing Wyner's wiretap channel model, which serves as the foundation of most existing studies on physical layer based security techniques. Then, we outline the underlying theory for jamming strategies.

Digital Object Identifier:
10.1109/MWC.2017.1700015

Yan Huo, Yuqi Tian, and Tao Jing are with Beijing Jiaotong University; Liran Ma is with Texas Christian University; Xiuzhen Cheng is with The George Washington University.

Wyner's Wiretap Channel Model

Consider a wireless network shown in Fig. 1, in which Alice sends a message M to Bob. The message M is coded into signal X before transmission. After transmission, Bob receives a signal Y, and the eavesdropper Eve receives a signal Z through the wiretap channel. This is the classic Wyner's wiretap channel model. Wyner proved that if the quality of the wiretap channel is worse than that of the legitimate channel, the legitimate transmitter and receiver can achieve perfect secrecy by channel coding. Perfect secrecy means that the receiver can decode the received signal Y with negligible errors, but the eavesdropper cannot get any information from Z. It is defined as follows:

$$I(Z;M) = H(M) - H(M|Z) = 0, \quad (1)$$

where $I(Z;M)$ denotes the mutual information between Z and M, and $H(M)$ and $H(M|Z)$ denote the information entropy of M and the conditional information entropy of M after receiving Z, respectively. Here $H(M|Z)$ is also called the equivocation of the eavesdropper.

Under this assumption, Wyner gave the definition of secrecy capacity C_s, which is defined as the difference between the mutual information of the legitimate channel and the wiretap channel:

$$C_s = \max[I(X;Y) - I(X;Z)], \quad (2)$$

where C_s denotes the secrecy capacity of the channel between Alice and Bob, and $I(X;Y)$ and $I(X;Z)$, respectively, denote the mutual information of the channels between Alice and Bob and between Alice and Eve. Secrecy capacity is the maximum achievable rate between the legitimate transmitter and receiver that can guarantee perfect secrecy. It gives the upper bound of the transmission rate subject to constraints of unauthorized users. Many existing works consider secrecy capacity as a performance metric. For example, Wang *et al*. proposed and implemented a practical opportunistic secret communication system over the wireless wiretap channel [3]. Additionally, bit error rate (BER), signal-to-interference-plus-noise ratio (SINR), ergodic secrecy rate (ESR), and secrecy outage probability (SOP), are also performance metrics that have been adopted.

Jamming Basics

Jamming has traditionally been considered as an unfavorable factor in wireless communications. Interference caused by jamming can overlap with the transmitted signal, and thus negatively impact the decoding process at the receiver. However, when jamming (e.g., an artificial noise signal) is targeted at an eavesdropper, it can degrade the channel quality of the eavesdropper. Subsequently, according to the aforementioned wiretap channel model, perfect secrecy may be achieved if the eavesdropper's channel condition is degraded to a certain level (i.e., worse than that of the legitimate receiver).

Hence, jamming can be a practical physical layer based security measure, especially when the transmitted information needs to be protected from passive eavesdroppers whose locations are unknown. The idea was first introduced by Negi and Goel [4], where jamming strategies were investigated for two

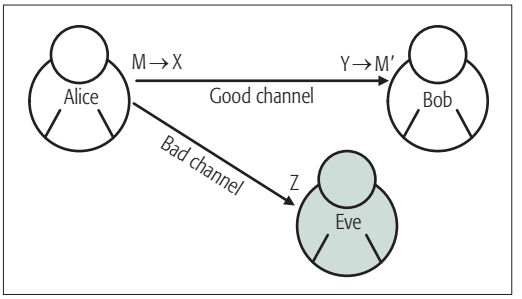

FIGURE 1. The wiretap channel of Wyner.

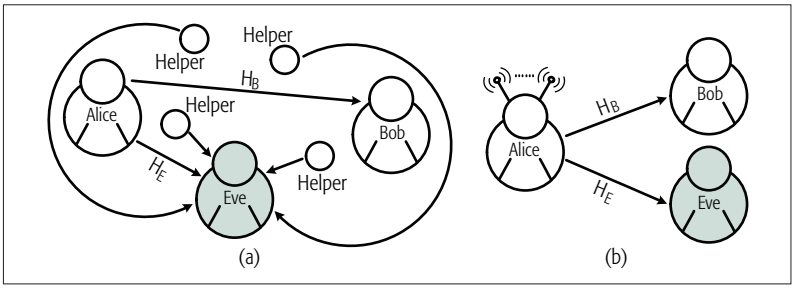

FIGURE 2. Non-self-cooperative vs. self-cooperative: a) non-self-cooperative jamming; b) self-cooperative jamming.

different network scenarios. Since then, a number of studies on jamming strategies have been performed. After an extensive review of these existing studies, we find that the following three factors can influence the design of jamming strategies: whether jammers are nonself-cooperative or self-cooperative, whether the eavesdropper's CSI is perfectly known to the legitimate transmitter, and whether the jamming matrix is designed to be uniform or directional. Thus, we classify jamming strategies from these three aspects, and elaborate on the classification in the next section.

Jamming Strategies

In this section, we introduce our classification of the existing mainsteam jamming strategies, and compare the performance of a few typical jamming schemes.

Nonself-Cooperative vs. Self-Cooperative

Nonself-cooperative jamming refers to the scenario where there is one or more legitimate users in the network besides Alice and Bob. These users can function as helpers to send artificial noise signals to degrade the channel quality of the eavesdropper, as shown in Fig. 2a. The pioneering work from Negi *et al*. proposed a two-stage protocol to achieve nonself-cooperative jamming. Based on this study, a few early investigations were carried out focusing on the design of nonself-cooperative jamming processes, artificial noise generation, and performance analyses. After that, a number of schemes that prioritize different goals were proposed. Some of them consider selecting optimal jammers with the least redundancy so as to achieve more effective jamming with lower overhead, while some others focus on lowering the complexity of power allocation. Recently, Wang *et al*. [5] proposed an opportunistic jammer selection scheme that prefers to select helpers whose channels are nearly orthogonal to the legitimate user's channel as the jammers. This scheme simplifies the signal coordinations among multiple jammers.

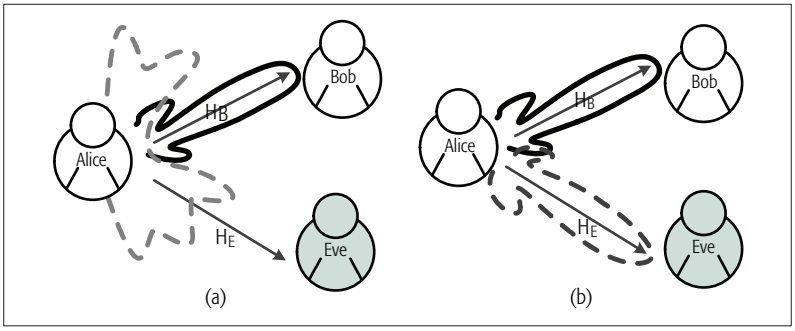

FIGURE 3. Uniform vs. directional: a) uniform jamming; b) directional jamming.

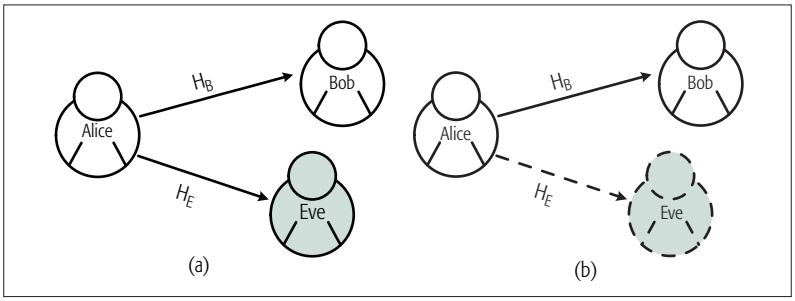

FIGURE 4. Perfect vs. imperfect Eve's CSI: a) perfect Eve's CSI; b) imperfect Eve's CSI.

When there are relays in the network, the design of jamming strategies becomes more complicated. If the relay is trusted, it can act as an ordinary helper and can be chosen as a jammer. In contrast, if the relay is not trustable, it needs to be treated as an eavesdropper. As a result, the receiver needs to help jam the relay when the legitimate signal is transmitted over the air. An example relay-jammer selection scheme was proposed in [6], in which the relay and jammers are selected from multiple friendly intermediate nodes with the objective of optimizing the security performance.

In self-cooperative jamming, there is no potential helper in the network. Instead, Alice or Bob may utilize multiple antennas to transmit artificial noise signals, as shown in Fig. 2b. Studies in self-cooperative jamming mostly focus on antenna allocation and the design of jamming matrices. For the antenna allocation problem, it is important to strike a balance between the transmit power and the number of spatial dimensions available for jamming. A modified water-filling algorithm was proposed in [7] to address this problem. The designs of jamming matrices are often combined with beamforming and pre-coding techniques so as to degrade the channel quality of the eavesdropper more effectively. For instance, Lin *et al.* [8] proposed a generalized artificial noise scheme combined with beamforming for a multiple input, single output, single-antenna eavesdropper (MISOSE) network. This scheme can expand the region with non-zero secrecy rate, and improve the connectivity of the network. When it comes to a network with relay, the considerations are similar to those in the nonself-cooperative jamming case.

Uniform vs. Directional

Uniform jamming means that the transmitter-receiver pair and/or the helpers are equipped with omnidirectional antennas. This strategy is generally used when eavesdroppers are passive, as shown in Fig. 3a. To avoid interfering with the legitimate channel, jamming matrices are often designed in the null space of the legitimate channel. A number of jamming schemes follow this principle. For example, Liao *et al.* [9] proposed a design of artificial noise combined with beamforming, where the artificial noise covariance matrix is in the left null space of the legitimate channel. This scheme optimizes the matrix by minimizing the total transmit power subject to target SINR constraints on the receiver and eavesdroppers, and it achieves better security performance than the one that simply allocates the artificial noise covariance matrix in the left null space of the legitimate channel. In addition, a generalized artificial noise scheme was proposed for a MISOSE network in [8]. Although the proposed scheme may cause leakage of artificial noise at the legitimate receiver, the security performance can still be improved because the covariance matrix of the artificial noise is more flexible than the one selected by Negi and Goel [4].

In directional jamming, artificial noise signals are sent to a specific direction, as shown in Fig. 3b. Obviously, it is more effective compared to uniform jamming. When the location of the eavesdropper is known to the transmitter, directional jamming is more effective and practical. Liu *et al.* [6] and Wang *et al.* [10] independently proposed a directional jamming design, where suitable jammers that can degrade the quality of the eavesdropper's channel to the largest degree are selected based on Eve's CSI. However, when Eve's CSI is unavailable to the transmitter, directional jamming can be a challenge. One possible approach is to concentrate the artificial noise signal on the directions with a higher risk of information leakage. Another possible approach is to analytically define a suspicious area (where eavesdroppers could reside) based on the available information of the geometric locations (described by both the angle of arrival and the distance to the transmitter) of the legitimate receivers and eavesdroppers. Hence, jamming signals can be sent specifically to the suspicious area [11].

Perfect vs. Imperfect Eve's CSI

The channel state information of an eavesdropper is an important factor in jamming strategy design. When Eve's CSI is known to the legitimate users, which indicates that the location of the eavesdropper is known, the jammer can perform targeted jamming. In this case, an optimized power allocation can be achieved. An example work of utilizing the knowledge of Eve's CSI to design jammer selection and power allocation schemes appeared in [10]. Because Eve's CSI is known, the security performance metric can be deduced into a convex optimization problem, which is solvable. With perfect Eve's CSI, security performance is usually high because jamming can be more targeted. On the other hand, with partial or unknown Eve's CSI, security performance is medium or low because jamming can become less effective (Fig. 4).

On the other hand, the information of Eve's CSI is typically incomplete in practice. With this limitation, target jamming and performance optimization are more difficult to achieve. A general approach is to guarantee the robust security performance in the worst case, and design a suboptimal algorithm. For example, Li *et al.* [12] considered the worst-case robust secrecy rate maximization problem with

Scheme	Type	Required information	Application network	Criterion	Security performance	Complexity
[5]	Nonself-cooperative, directional	Perfect Eve's CSI	SISOSE, trusted relay	Secrecy rate	High	Low
[10]	Nonself-cooperative, directional	Perfect Eve's CSI	SISOME	Secrecy rate	High	Medium
[13]	Nonself-cooperative, uniform	Imperfect Eve's CSI (unknown)	MIMO, trusted relay	Secrecy rate	Medium	Medium
[9]	Self-cooperative, uniform	Perfect Eve's CSI	MISOME	SINR	High	Medium
[7]	Self-cooperative, uniform	Imperfect Eve's CSI (partial)	MISOSE	Secrecy rate	Medium	Medium
[6]	Self-cooperative, uniform	Imperfect Eve's CSI (unknown)	MIMO	Secrecy rate	Low	Medium
[8]	Self-cooperative, directional	Perfect Eve's CSI	MIMO, untrusted relay	ESR	High	Medium
[11]	Self-cooperative, directional	Imperfect Eve's CSI (unknown)	Massive MIMO	SOP	High	High

TABLE 1. Performance comparison among jamming schemes.

A nonself-cooperative jamming design depends on whether there exist friendly helpers in the network, while a self-cooperative jamming design depends on whether the transmitter or the receiver has multiple antennas. A directional jamming design is adopted when Eve's CSI is known to the transmitter, while a uniform jamming design is employed when Eve's CSI is imperfect to the transmitter.

incomplete Eve's CSI, and proposed a suboptimal but secure solution to an outage-constrained robust secrecy rate maximization problem. When jointly considering power allocation, many works tended to first allocate enough resources to guarantee a certain quality of service (QoS) of the legitimate channel, and then use the remaining resources to jam the eavesdropper. There are various methods to deal with such cases. For instance, a modified water-filling algorithm was adopted in [7] to balance the required transmit power with the available number of spatial dimensions. This algorithm increases the number of spatial channels available for jamming, and thus leads to a significant increase in secrecy capacity. Huang *et al.* [13] adopted a similar approach to minimize the total transmit power and designed a power allocation scheme for jammers.

Summary and Remarks

In this subsection, we compare a few typical schemes and provide a comprehensive performance analysis in terms of required information, application network scenarios, and security performance. The results are presented in Table 1.

A nonself-cooperative jamming design depends on whether there exist friendly helpers in the network, while a self-cooperative jamming design depends on whether the transmitter or the receiver has multiple antennas. A directional jamming design is adopted when Eve's CSI is known to the transmitter, while a uniform jamming design is employed when Eve's CSI is imperfect to the transmitter. Whether or not Eve's CSI is known to the transmitter influences the design of the optimal algorithm for jamming matrix determination and/or optimal power allocation. On the other hand, the trustworthiness of a relay affects whether or not legitimate users see it as an eavesdropper. Additionally, computational complexity needs to be considered in the jamming design. For a simple network model, computational complexity is relatively low (e.g., [6]), while for a complicated network such as a massive MIMO network, computational complexity can be high. Lastly, it can be seen in Table 1 that a jamming strategy can adopt one or multiple techniques. For example, a nonself-cooperative jamming scheme can also be directional.

Example Jamming Strategy Designs

In this section, we present two examples to demonstrate important jamming design considerations under different network scenarios.

Simple Hybrid Network

We start with the design of nonself-cooperative jamming in a simple hybrid network, which is a single antenna relay network where Eve's CSI is known to all the legitimate nodes. This network model is adopted from [6], where a jamming scheme was proposed for a cooperative wireless network that includes a source (S), a destination (D), an eavesdropper (E), and a set of friendly helpers, as shown in Fig. 5. It is assumed that the source needs a relay to complete its transmission, the eavesdropper is passive, each node has a single omnidirectional antenna, and global CSI information is available, including the eavesdropper's CSI. Since each node has only one single antenna, the jamming signal is easy to design and generate, for example, Gaussian noise can be sufficient. Additionally, because the CSI information of the eavesdropper is known, it is possible to perform targeted jamming toward the eavesdropper. Therefore the main goal of the jamming scheme design is to choose the optimal relay and jammers based on the global CSI.

For instance, the scheme proposed in [6] splits the communication process into two phases. In the first phase, S transmits a weighted combination of the information signal and the jamming signal to the selected relay R. At the same time, the selected jammer J1 cooperates with S to transmit a jamming signal to E. In the second phase, R, using the same

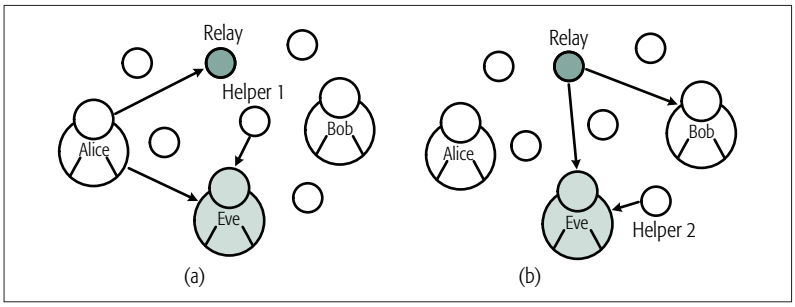

FIGURE 5. The system model in [6]: a) phase 1; b) 9hase 2.

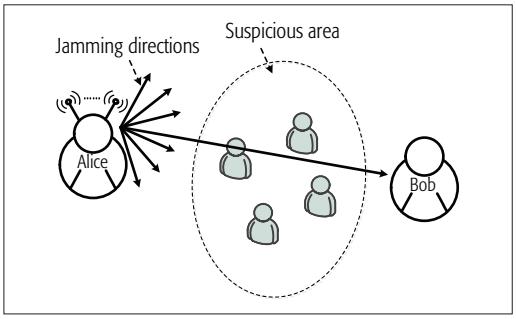

FIGURE 6. The system model in [11].

codebook as S, forwards the data along with the jamming signal to D, while the selected jammer J2 cooperates with R to transmit a jamming signal to E. The optimal R is selected first and then the two jammers are selected. The rationale to choose R is that the ratio of the legitimate channel state to the wiretap channel state is at the maximum while the rationale to choose J1 and J2 is that they can degrade the channel of E the most.

Complicated Hybrid Network

We now move to a complicated scenario of a massive MIMO network. An example work for this type of network (Fig. 6) appeared in [11], where a directional jamming scheme was proposed with the constraint of imperfect global CSI. The proposed scheme assumes that the eavesdroppers are equipped with a large antenna array and are randomly deployed around a legitimate transmitter. It further assumes that all channels follow *Rician* distributions. The SOP was derived based on the combination of a suspicious area (where the eavesdroppers could reside) and its associated secrecy outage region (SOR). The smaller the SOP is, the better security performance can be. This work states that even without knowing the suspicious area, jamming toward different directions also needs to be treated differently. Based on the analysis in [11], one can see that eavesdroppers from different directions (i.e., within different side lobes) can have different impacts on secrecy outage, and jamming should be performed mainly in the two dominating directions in the neighborhood of the line-of-sight (LOS) angle of the receiver. Lastly, the above analysis was extended to multiuser and multi-cell scenarios in [11].

Open Research Issues

In this section, we discuss a few interesting open research issues in jamming design with consideration of novel technical approaches and perspectives.

Game Theory

Game theory studies the interactions between various competing agents, which can be employed to make optimal decisions. The core concept of game theory is to model agents as rational entities whose focus is to maximize their individual gains or payoff functions. From the perspective of physical layer security, users in the network can be seen as rational agents. The interactions between legitimate users and eavesdroppers can be modeled by exploiting the properties of game theory. Thus, there have appeared a number of studies that exploit game theory in jamming schemes. For example, a jamming scheme that models the interactions between the transmitter and the eavesdropper as a two-person zero-sum game was proposed in [14], assuming self-cooperative and uniform jamming, and imperfect Eve's CSI. This work revealed how the transmitter can adjust the jamming scheme according to the eavesdropper's behavior. As claimed by [14], game theory can be a new perspective and a useful tool to facilitate the designs of novel jamming strategies. The challenges may lie in the choice of a suitable game model and the analysis of the Nash equilibrium.

Energy Harvesting

Energy harvesting is not a jamming technique; rather, it is a method to improve the efficiency of energy utilization. The incorporation of energy harvesting into a jamming scheme can help make the jamming scheme more practical and attractive in real world applications. An example of such a combined design was reported in [15], where a jamming scheme with energy harvesting was proposed for a multi-antenna cooperative cognitive radio network. This scheme assumes non-self-cooperative and uniform jamming, imperfect Eve's CSI, and relay-jamming. It employs certain secondary users as helpers to harvest energy. The harvested energy is used by the helpers to generate the artificial noise signal to jam the eavesdropper. This example indicates that the exploitation of energy harvesting introduces more available resources for jamming, and thus provides an opportunity for the system to obtain better security performance. Future studies in this area may need to consider how to generate sufficient harvesting energy to support continuous jamming.

Partial Jamming

Partial jamming represents a novel perspective of jamming design. For all the jamming strategies summarized above, jammers perform jamming in the entire communication process. Nonetheless, it may be possible to design a partial jamming mechanism that is effective enough to achieve the same level of security performance. Intuitively, a receiver may not acquire the transmitted information by just decoding a partial signal, because an eavesdropper needs to receive the entire signal to decode and obtain the information. Based on this idea, it makes sense for a friendly jammer to send interference signals in certain slots to prevent the eavesdroppers from receiving a complete signal. Partial jamming can be very beneficial in a power constraint system. To design a partial jamming strategy, we need to consider challenges such as when to jam, how many signals to send, how to deal with the eavesdroppers' diversity reception

(because they can combine the pieces of received signals via various transmission paths), the potential impacts on the cooperative jamming, and the possible influences on the legitimate receivers.

Jamming in Massive MIMO Networks

Massive MIMO networking was proposed to meet the increasing demand of wireless data services. It exploits an enormous number of antennas at the base station with simple signal processing to serve a comparatively small number of users. As a promising technique for future communication systems, it has become a hot research area in recent years. Massive MIMO technology brings new challenges to jamming design. First, as the number of antennas grows, transmitting artificial noise signals in the spatial null space of the legitimate channel may not be practical since the computational complexity of the null space is extremely high for the large-dimensional channel matrix. Second, random and independent artificial noise may be averaged out because of the availability of the enormous number of antennas, which can make uniform jamming less efficient. Lastly, pilot contamination can negatively affect the channel estimation result, which may lead to improper jamming matrix generation and downgraded security performance. Therefore, new jamming schemes for Massive MIMO networks need to address these challenges.

Conclusion

In this article, we have investigated the jamming strategies applied in physical layer security. We first introduced the basic theories and then provided a literature overview on the existing jamming strategies. We made a classification from three different perspectives and exemplified some jamming strategy designs in hybrid wireless networks. Finally, we discussed a few open research issues on related techniques, addressing new perspectives, opportunities, and challenges of the jamming strategy design.

Acknowledgment

We are very grateful to all reviewers who have helped improve the quality of this article. This work was partially supported by the National Natural Science Foundation of China (Grant No. 61471028, 61572070, 61771289, and 61371069), the Fundamental Research Funds for the Central Universities (2016JBZ003), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No.20130009110015), and the National Science Foundation of the US (Grant No. AST-1443858 and ECCS-1407986).

References

[1] Q. Yan *et al.*, "Jamming Resilient Communication Using MIMO Interference Cancellation," *IEEE Trans. Inf. Forensics Security*, vol. 11, July 2016, pp. 1486–99.
[2] Q. Wang *et al.*, "Jamming-Resistant Multiradio Multi-Channel Opportunistic Spectrum Access in Cognitive Radio Networks," *IEEE Trans. Vehic. Technol.*, vol. 65, Oct. 2016, pp. 8331–44.
[3] Q. Wang *et al.*, "Walls Have Ears! Opportunistically Communicating Secret Messages over the Wiretap Channel: From Theory to Practice." *Proc. Conf. Computer and Commun. Security*, Oct. 2015, pp. 376–87.
[4] R. Negi and S. Goel, "Secret Communication Using Artificial Noise," *Proc. IEEE Veh. Tech. Conf.*, vol. 3, Sept. 2005, pp. 1906–10.
[5] C. Wang *et al.*, "Uncoordinated Jammer Selection for Securing Simome Wiretap Channels: A Stochastic Geometry Approach," *IEEE Trans. Wireless Commun.*, May 2015, pp. 2596–2612.
[6] W. Liu, D. Tan, and G. Xu, "Low Complexity Power Allocation and Joint Relay-Jammer Selection in Cooperative Jamming Df Relay Wireless Secure Networks," *IEEE Int'l. Conf. ASID*, Oct. 2013, pp. 1–5.
[7] A. Mukherjee and A. L. Swindlehurst, "Fixed-Rate Power Allocation Strategies for Enhanced Secrecy in MIMO Wiretap Channels," *Proc. IEEE 10th Workshop on Signal Processing Advances in Wireless Commun.*, June 2009, pp. 344–48.
[8] P.-H. Lin *et al.*, "On Secrecy Rate of the Generalized Artificial-Noise Assisted Secure Beamforming for Wiretap Channels," *IEEE JSAC*, vol. 31, Aug. 2013, pp. 1728–40.
[9] W.-C. Liao *et al.*, "Joint Transmit Beamforming and Artificial Noise Design for QoS Discrimination in Wireless Downlink," *Proc. IEEE Int'l. Conf. Acoustics, Speech and Signal Processing*, 2010, pp. 2562–65.
[10] C. L. Wang, T.-N. Cho, and F. Liu, "Power Allocation and Jammer Selection of a Cooperative Jamming Strategy for Physical-Layer Security," *Proc. IEEE Vehicular Technology Conf.*, May 2014, pp. 1–5.
[11] J. Wang *et al.*, "Jamming-Aided Secure Communication in Massive MIMO Rician Channels," *IEEE Trans. Wireless Commun.*, vol. 14, Dec. 2015, pp. 6854–68.
[12] Q. Li and W. K. Ma, "Spatially Selective Artificial-Noise Aided Transmit Optimization for MISO Multi-Eves Secrecy Rate Maximization," *IEEE Trans. Signal Process.*, vol. 61, Mar. 2013, pp. 2704–17.
[13] J. Huang and A. L. Swindlehurst, "Cooperation Strategies for Secrecy in MIMO Relay Networks with Unknown Eavesdropper CSI," *Proc. IEEE Int'l. Conf. Acoustics, Speech and Signal Processing*, 2011, pp. 3424–27.
[14] A. Mukherjee and A. L. Swindlehurst, "Jamming Games in the MIMO Wiretap Channel with an Active Eavesdropper," *IEEE Trans. Signal Process.*, vol. 61, no. 1, Jan. 2013, pp. 82–91.
[15] Z. Li *et al.*, "Worst-Case Jamming for Secure Communications in Multi-Antenna Cooperative Cognitive Radio Networks with Energy Harvesting," *Proc. 2015 Int'l. Conf. Identification, Information, and Knowledge in the Internet of Things*, 2015, pp. 110–15.

Biographies

Yan Huo (yhuo@bjtu.edu.cn) received the B.E. and Ph.D. degrees in communication and information systems from Beijing Jiaotong University, Beijing, China, in 2004 and 2009, respectively. Since 2011 he has been a faculty member at the School of Electronics and Information Engineering at Beijing Jiaotong University, where he is currently an associate professor. He was a visiting scholar in the Department of Computer Science at The George Washington University from 2015 to 2016. His current research interests include wireless communication theory, security and privacy, cognitive radio and signal processing. He is a member of the IEEE.

Yuqi Tian (yuqi_tian@bjtu.edu.cn) received her B.E. degree from the School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China, in 2015. She is a master student in the Shu Hua Wireless Network and Information Perception Center, Beijing Jiaotong University, China. Her research interests include capacity analysis, spectrum prediction and resource management in wireless networks.

Liran Ma (l.ma@tcu.edu) is currently an associate professor in the Department of Computer Science at Texas Christian University. He received his D.Sc. degree in computer science from The George Washington University in 2008. His current research focuses on wireless, mobile, and embedded systems, including security and privacy, smartphones, smart health, mobile computing, Internet of Things, and cloud computing. It involves building and simulating prototype systems, and conducting real experiments and measurements.

Xiuzhen Cheng (cheng@gwu.edu) received her M.S. and Ph.D. degrees in computer science from the University of Minnesota–Twin Cities, in 2000 and 2002, respectively. She is a professor in the Department of Computer Science, The George Washington University, Washington DC. Her current research interests focus on privacy-aware computing, wireless and mobile security, smart cyber-physical systems, mobile handset networking systems, and algorithm design and analysis. She is a Fellow of the IEEE.

Tao Jing (tjing@bjtu.edu.cn) received his M.S. and Ph.D. degrees from Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, in 1994 and 1999, respectively. He is a professor in the School of Electronic and Information Engineering, Beijing Jiaotong University, China. His research interests include capacity analysis, spectrum prediction and resource management in cognitive radio networks, RFID in intelligent transporting system, and smart phone applications.

Partial jamming can be very beneficial in a power constraint system. To design a partial jamming strategy, we need to consider challenges such as when to jam, how many signals to send, how to deal with the eavesdroppers' diversity reception, the potential impacts on the cooperative jamming, and the possible influences on the legitimate receivers.