To Avoid or Not to Avoid CSI Leakage in Physical Layer Secret Communication Systems

Ta-Yuan Liu, Pin-Hsun Lin, Shih-Chun Lin, Y.-W. Peter Hong, and Eduard Axel Jorswieck

ABSTRACT

Physical layer secrecy has attracted much attention in recent years due to its ability to ensure communication secrecy with the use of channel coding and signal processing techniques (and without the explicit use of secret keys) in the physical layer. It serves as a promising technique for highly dynamic or ad hoc systems such as device-to-device and machine-type communication systems. However, the achievable secrecy performance depends highly on the level of CSI at the transmitter, the receiver, and the eavesdropper. In this article, we discuss how different levels of CSI resulting from conventional and unconventional ways of performing training and channel feedback may affect the confidentiality in terms of the information-theoretic (perfect) secrecy rate. The conventional approach refers to the emission of pilot signals from the transmitter and explicit channel feedback from the receiver. This approach is backward compatible with existing systems and allows the receiver to obtain accurate knowledge of the CSI, but may suffer from CSI leakage toward the eavesdropper. Unconventional approaches capitalize on reverse training to prevent CSI leakage and are shown to achieve significant improvements over conventional schemes in certain cases. For example, in a system with four transmit antennas and a single antenna at both the receiver and the eavesdropper, a secrecy rate gain of approximately 0.8 b/channel use at transmit SNR of 16 dB is observed over the full CSI case by providing CSI only to the transmitter (but not the receiver and the eavesdropper).

INTRODUCTION

Security in wireless communications has always been a major concern due to the broadcast nature of wireless transmissions. Conventionally, these issues have been addressed in the upper layers of the network protocol stack using cryptography-based solutions, which typically rely on the use of confidential secret keys to seal the transmitted messages. However, with the rapid growth of the number of wireless devices, the secret key distribution and management that are required to maintain these operations are becoming increasingly difficult, and are introducing larger overhead and latency to the system. For example, in the Long Term Evolution Advanced (LTE-A) system, the authentication and key agreement (AKA) process takes up to several hundreds of milliseconds for key computations and distribution. The latency and the additional burden on the backhaul may increase even more rapidly with the introduction of machine-type communications and the Internet of things (IoT).

Interestingly, recent information-theoretic studies of the wiretap channel have demonstrated the possibility of achieving secrecy in the physical layer with the sole use of channel coding and signal processing techniques (i.e., without the explicit use of secret keys). However, many of these fundamental studies make ideal assumptions on the channel state information (CSI) at the transmitter, the receiver, and/or the eavesdropper, and ignore the practical issues of training and channel feedback. However, in practice, CSI cannot be obtained for free and is often subject to imperfections. For example, in LTE-A, a downlink pilot time slot (DwPTS) is allocated for the emission of pilot symbols by the base station to enable channel estimation at the user equipment (UE), and a physical uplink control channel (PUCCH) is utilized for CSI feedback from the UEs to facilitate closed-loop transmissions when the coherence time is sufficiently long. Even with the dedicated resources for training and feedback, CSI at the receiver and the transmitter is never perfect due to channel estimation errors and limited feedback bandwidth. These issues must be taken into consideration when employing physical layer secrecy techniques in practice.

In this article, we first discuss how different levels of CSI at the transmitter, which result from conventional ways of performing training and channel feedback, may impact the confidentiality in terms of the information-theoretic (perfect) secrecy rate. We show that the conventional approach of having the transmitter emit the training signal and having the receiver feed back the estimated channel to the transmitter is compatible with existing systems, and allows the receiver

Ta-Yuan Liu and Y.-W. Peter Hong are with National Tsing Hua University.

Pin-Hsun Lin and Eduard Axel Jorswieck are with Technische Universität Dresden.

Shih-Chun Lin is with National Taiwan University of Science and Technology.

0163-6804/15/$25.00 © 2015 IEEE

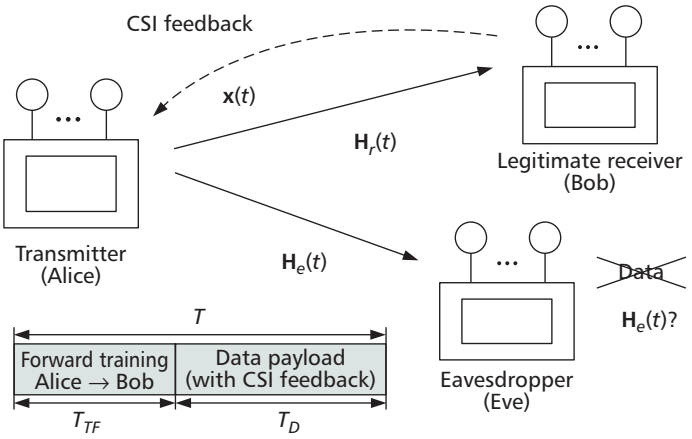

Figure 1. The wiretap channel consists of a transmitter, a receiver, and an eavesdropper with conventional training-based transmission where there is only forward training for Bob to estimate channel state information.

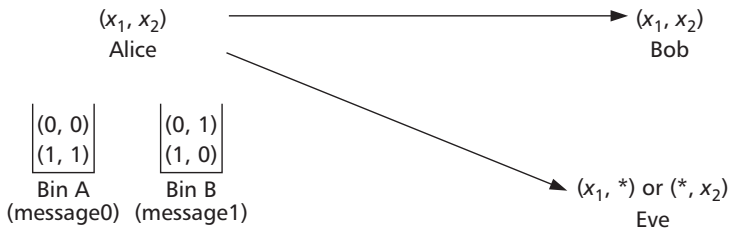

Figure 2. An illustration of secrecy binning.

and the transmitter to obtain accurate knowledge of the CSI. However, this approach does not prevent the eavesdropper from obtaining CSI, and in order may reduce the achievable secrecy rate. To avoid CSI leakage, we then review several novel techniques proposed in the literature that capitalize on the use of reverse training, that is, training with pilot signals emitted by the receiver. Reverse training enables channel estimation directly at the transmitter, but does not benefit estimation of the transmitter-to-eavesdropper channel at the eavesdropper. Finally, numerical simulations are provided to demonstrate the gains that can be obtained with the prevention of CSI leakage in terms of the achievable secrecy rate. However, it is worthwhile to note that the schemes which avoid CSI leakage may not be suitable for all scenarios due to their need for the use of reverse training and artificial noise. Moreover, by assuming that perfect CSI is available at the eavesdropper, schemes that do not avoid CSI leakage can be viewed as worst-case schemes which can be used when the level of CSI at the eavesdropper is uncertain.

Overview of Physical Layer Secrecy

A basic secret communication system (often referred to as the wiretap channel in the information theory literature) consists of three terminals: a transmitter (Alice), a legitimate receiver (Bob), and an eavesdropper (Eve), as illustrated in Fig. 1. For the above channel, the seminal works [1, 2] (and many works that follow) proved the existence of channel codes that can be used to send confidential messages from the transmitter to the receiver with arbitrarily low error probability while ensuring asymptotically zero information rate at Eve (i.e., perfect secrecy). The transmission rate achievable under these conditions is referred to as the secrecy rate, and the maximum of such rates is the secrecy capacity.

Let $\mathbf{x}(t)$ be the symbol vector sent by the transmitter in the tth coherence block, and let

$$\begin{aligned} \mathbf{y}_r(t) &= \mathbf{H}_r(t)\mathbf{x}(t) + \mathbf{z}_r(t), \text{ and} \\ \mathbf{y}_e(t) &= \mathbf{H}_e(t)\mathbf{x}(t) + \mathbf{z}_e(t), \end{aligned} \quad (1)$$

be the received signals at Bob and Eve, respectively, where $\mathbf{H}_r(t)$ and $\mathbf{H}_e(t)$ are the corresponding channel matrices in block t, and $\mathbf{z}_r(t)$ and $\mathbf{z}_e(t)$ are the corresponding additive white Gaussian noise (AWGN) vectors. We assume that the channel is block fading with coherence time T, with a value that depends on whether the channel is fast or slow fading. The ergodic secrecy rate is considered as the main performance criterion throughout this article.

To ensure confidentiality without secret keys, a coding technique called "secrecy binning" is employed at the heart of many physical layer secrecy techniques. The key idea is to insert additional randomness into the codeword of each confidential message to increase the uncertainty at Eve. The amount of randomness required to achieve perfect secrecy is often proportional to the capacity of the eavesdropper channel (Alice-Eve). An example is given as follows.

Example 1[1]: We consider the wiretap channel in Fig. 2 with input $\mathbf{x} = (x_1, x_2)$ being a vector of binary entries, that is, $x_1, x_2 \in \{0,1\}$. The channel outputs at Bob and Eve are $\mathbf{y}_r = (x_1, x_2)$ and $\mathbf{y}_e = (x_1, *)$ or $(*, x_2)$, respectively, where $*$ denotes an erasure. The reception at Bob is perfect, but that Eve may have an erasure in one of the two entries. To transmit a secret binary message to Bob, Alice constructs two secrecy bins corresponding to message bits 0 and 1: Bin A and Bin B, respectively. Bins A and B consist of codewords $\{(0, 0), (1, 1)\}$ and $\{(0, 1), (1, 0)\}$, respectively. During each transmission, Alice randomly sends a codeword from the bin corresponding to the secret message. The message can be successfully decoded by Bob since the main channel is noiseless, but cannot be decoded by Eve since Eve receives only one entry of the codeword. By randomly choosing codewords within a bin, Eve faces one bit of uncertainty. This one bit is equal to the capacity of the eavesdropper channel, and is exactly the amount needed to prevent eavesdropping at Eve.

Notice that the efficiency of the secrecy binning technique depends on the discrepancy between the quality of the main and eavesdropper channels. Therefore, to enhance secrecy, signal processing techniques have been employed on top of the secrecy-binning-based coding schemes to further enlarge the channel quality discrepancy by artificially generating a better channel for Bob than for Eve. For example, with multiple antennas at the transmitter, one can employ the so-called secrecy beamforming tech-

[1] Please refer to S. El Rouayheb, E. Soljanin, and A. Sprintson, "Secure Network Coding for Wiretap Networks of Type II," *IEEE Trans. Info. Theory*, vol. 58, no. 3, Mar. 2012, pp. 1361–71.

nique where the message-bearing signal is directed toward a spatial dimension that yields a better channel quality for Bob than for Eve. Secrecy beamforming is known to maximize the secrecy capacity of the multiple-input single-output channel when perfect CSI is available at all terminals [3, 4]. Under non-ideal CSI assumptions, artificial noise (AN) [5] can be super-imposed on top of the message-bearing signal in an appropriately chosen signal subspace to cause additional interference at Eve. In the following sections, we discuss how different CSI assumptions resulting from conventional and unconventional ways of doing training and channel feedback may impact the achievable secrecy rate, especially through the prevention of CSI leakage (or lack thereof).

Physical Layer Secrecy without Protection against CSI Leakage

In this section, we discuss the impact of CSI assumptions that result from conventional training and channel feedback schemes. Conventionally, training is performed in the forward direction by having Alice emit pilot signals at the beginning of each coherence interval to enable channel estimation at Bob. Channel feedback is then sent from Bob to Alice. This approach can easily be applied to current wireless standards without major modifications of the signaling mechanism since it adheres to the traditional frame structure, as illustrated in Fig. 1. Moreover, since these schemes make no attempt to prevent CSI leakage to Eve, they are often devised by assuming perfect CSI at Eve, and thus are suitable for worst-case scenarios.

In the following, we first consider cases where perfect CSI is available at both Bob and Eve (due to perfect forward training), and further categorize the results according to three different assumptions on the CSI at the transmitter (CSIT). The CSIT assumptions are consequences of perfect (without delay), delayed, and partial feedback operations from Bob. Then, by taking into consideration the channel estimation errors, we further discuss the trade-off between training and secret data transmission in the conventional setting.

Secrecy with Perfect Main-Channel CSIT

In this subsection, we consider the case where perfect main-channel (Alice-Bob) CSIT is available instantaneously (without delay), which requires sufficiently large feedback bandwidth from Bob to Alice. Ideally, when perfect eavesdropper-channel CSIT is also available, secrecy beamforming accompanied by the Gaussian (secrecy) binning codebook is known to be secrecy-capacity achieving in a multiple-input single-output multiple-eavesdropper (MISOME) channel [4]. Alice can choose a beamforming direction that maximizes the difference between the capacity of the main channel and that of the eavesdropper channel (i.e., the achievable secrecy rate). The optimal beamforming vector is the generalized eigenvector of the two CSITs when the power is sufficiently large.

With only partial or no eavesdropper-channel CSIT, secrecy beamforming can still be performed if long decoding latency is allowed. The uncertainty of the Alice-Eve channel is averaged out by channel coding over multiple coherent blocks. Usually, the beamforming direction cannot be determined to maximize the instantaneous channel quality difference in each block, and AN is used to help suppress the reception quality at Eve. The AN is often placed in the null space of the main channel to avoid interfering Bob. In this case, the achievable secrecy rate of the AN-assisted beamforming scales with the transmit power at a rate similar to that of the optimal secrecy beamforming with full CSIT [4]. Interestingly, placing AN in the null space of the main channel may not always be optimal since embedding AN partially in the main channel may cause more harm to Eve than to Bob [6]. For the case where allowed decoding latency is short, the so-called secrecy outage probability is considered, which denotes the probability that the target rate cannot be achieved. The optimal beamformer in terms of secret outage probability is shown to be a linear combination of the maximal ratio-combining and zero-forcing beamformers with weight adjusted according to the available CSIT [7]. Finally, if only the set of possible eavesdropper channel realizations is known (instead of the distribution), a secrecy beamformer maximizing the worst-case secrecy rate can be chosen.

To ensure confidentiality without secret keys, a coding technique called "secrecy binning" is employed at the heart of many physical layer secrecy techniques. The key idea is to insert additional randomness into the codeword of each confidential message to increase the uncertainty at Eve.

Secrecy with Delayed Main-Channel CSIT

In some scenarios, CSIT may be outdated due to insufficient feedback bandwidth, causing the main-channel CSIT in coherence block t to consist of only the past channel matrices $\mathbf{H}_r(t-1), \ldots, \mathbf{H}_r(1)$. In this case, it is beneficial to utilize messages and AN transmitted in past blocks as common randomness between Alice and Bob to help secure the message in the current block. This is demonstrated in the following example from [8], where it is assumed that the past CSI of Eve, that is, $\mathbf{H}_e(t-1), \ldots, \mathbf{H}_e(1)$, is also available at the transmitter.

Example 2 [8]: Let us consider a wiretap channel with two transmit antennas at Alice and only a single antenna at both Bob and Eve. The 1×2 channel vectors of the main and eavesdropper channels in coherence block t are denoted by $\mathbf{h}_r(t)$ and $\mathbf{h}_e(t)$, respectively. To utilize the delayed CSIT, this example shows an achievable scheme where Alice transmits two independent message-carrying symbols over three coherence blocks, as illustrated in Fig. 3. This scheme is optimal at high signal-to-noise ratio (SNR); thus, we assume that the reception is noiseless for ease of exposition. In the first time slot, only AN is transmitted by Alice and is received by Bob as $y_r(1)$. In the second slot, Alice is able to obtain the knowledge of $\mathbf{h}_r(1)$ (and, thus, $y_r(1)$) through delayed feedback and transmits a linear combination of $y_r(1)$ and the two message signals x_1 and x_2 to Bob. Here, $y_r(1)$ is treated as common randomness between Alice and Bob that can help secure the message signals. By removing $y_r(1)$ at Bob, one linear equation of x_1 and x_2 is obtained. In the third time slot, Alice utilizes the knowledge of $\mathbf{h}_e(2)$ to reconstruct Eve's past signal $y_e(2)$ and transmits it to provide Bob with

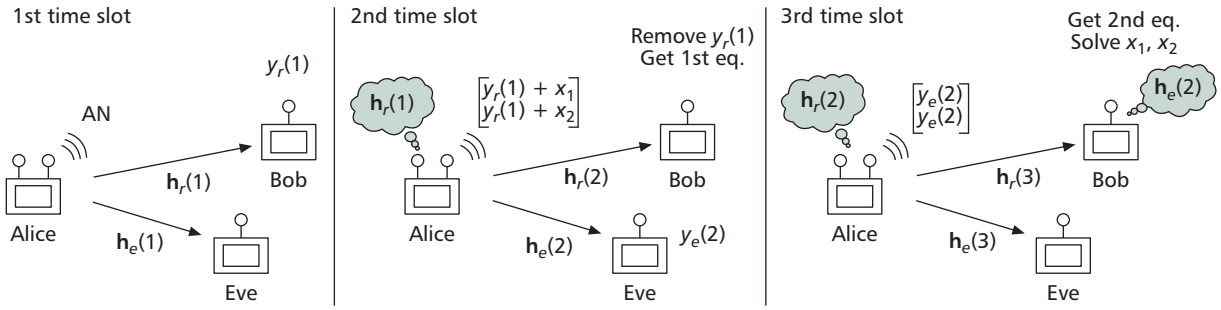

Figure 3. An illustration of the transmission scheme for wiretap channels with delayed CSIT.

the second linear equation needed to solve for x_1 and x_2.

The aforementioned transmission scheme can be modified to incorporate cases without the eavesdropper-channel CSIT [8]. In these cases, Alice will not be able to reconstruct and retransmit Eve's signal in the third time slot. However, the first two time slots can still be employed with only one message transmitted in the second time slot. The delayed CSIT $y_r(1)$ is similarly used as the common randomness to secure the message transmission in slot 2. Even though the above scheme performs well, its optimality is still unknown.

Secrecy with Partial Main-Channel CSIT

In this subsection, we consider the case with instantaneous but partial CSI feedback from Bob and no CSI feedback from Eve. This is most often the case in practical systems, such as LTE-A, where CSI is first quantized, and only the index of the quantized vector is fed back to the transmitter through the PUCCH. In this case, AN-assisted secrecy beamforming can be performed by Alice based on the quantized main-channel CSIT [9, 10]. However, the uncertainty of the CSIT, caused by the quantization noise, will result in the AN leakage problem. That is, the AN placed in the null space of the quantized main channel will leak into the actual main channel causing interference to Bob. To limit the secrecy rate loss due to AN leakage, one can scale logarithmically the number of quantized bits with respect to the transmit SNR.

In the extreme case where no (or infrequent) feedback is provided, Alice may only be able to obtain statistical knowledge of the CSI. In this case, beamforming can still be performed by directing the message-bearing signal toward dimensions that are most likely favorable to Bob. However, when both channels are Gaussian with entries that are independent and identically distributed (i.i.d.), it is optimal to emit signals evenly in all directions. This concept can also be applied to cases with general Nakagami fading channels [11].

Trade-off between Training and Secret Data Transmission

In the previous subsections, we assumed that forward training is perfect, which implies the need for infinite resources for training and channel feedback. However, the cost of utilizing these resources and the trade-off with the amount of resources that can be utilized for a data transmission period is not considered. In fact, when more resources are allocated to training, less resources are left for data transmission, and vice versa.

Let P be the total average power constraint over coherence time $T = T_{TF} + T_D$ so that

$$T_{TF}P_T + T_DP_D \le PT, \tag{2}$$

where P_T and P_D are the powers utilized for training and data transmission, respectively, and T_{TF} and T_D are the durations of the respective phases. By utilizing the minimum mean square error (MMSE) estimator in the training phase and the AN-assisted secrecy beamforming in the data transmission phase, the power allocation between training and data transmission was examined in [12] at high SNR. With conventional training, and by setting T_{TA} equal to the number of transmit antennas, it was shown that to maximize the achievable secrecy rate, the power ratio P_T/P_D should scale as $\sqrt{T_D}$ as the coherence time increases. This is due to the fact that as the coherence time increases, time and energy resources are sufficient for data transmission, and thus more resources should be devoted to obtaining better channel estimates. Moreover, in data transmission, approximately half the power should be used for the message-bearing signal and half for AN.

Physical Layer Secrecy with Protection against CSI Leakage

Traditional training and channel feedback procedures were often designed without secrecy considerations, and schemes such as forward training and insecure channel feedback may also provide Eve with sufficient CSI to enhance its eavesdropping capability. Therefore, by capitalizing on training in the reverse direction (i.e., from Bob to Alice), several techniques have been proposed in the literature to prevent such (Alice-Eve) CSI leakage.[2] Reverse training can be viewed as an intelligent way to perform channel estimation and feedback simultaneously without benefiting the eavesdropper. By assuming that the Bob-Eve channel is independent of the main (i.e., Alice-Bob) and eavesdropper (i.e., Alice-Eve) channels, as done in [12–14], no

[2] Notice that leakage of the main-channel CSI to Eve may also impact the secrecy performance. In fact, this has also been considered in [3–11] by assuming perfect main-channel CSI at Eve and in [12–15] by assuming that Eve has the same level of main-channel CSI as Bob.

information regarding the latter two channels is revealed to Eve through the reverse training. To adopt reverse training, it is necessary to partition the training phase into two phases: the reverse and the forward training phases, as illustrated in Fig. 4.

Secrecy with Suppressed CSI at Eve

An interesting scheme that utilizes reverse training to suppress the CSI at Eve is the so-called two-way discriminatory channel estimation (DCE) scheme [13]. In this scheme, reverse training is first performed to enable channel estimation directly at Alice. Under the channel reciprocity assumption (e.g., in a time division duplex system), this estimate can be used to directly infer knowledge of the forward channel matrix $\mathbf{H}_f(t)$. Then, in the forward training phase, an AN-assisted training signal, which consists of a pilot signal plus AN in the null space of the estimated main channel, can be transmitted to facilitate channel estimation at Bob while preventing that at Eve. With sufficiently reliable estimation in the reverse training phase, AN can be placed accurately in the desired subspace to avoid interference at Bob. However, under a total power constraint, this reduces the power that can be used for forward training and data transmission. Therefore, a trade-off exists in terms of the resources that should be allocated to reverse training, forward training, and data transmission.

Let P be the average total power constraint over the channel coherence time $T = T_{TF} + T_{TR} + T_D$ so that

$$T_D P_D + (T_{TR} + T_{TF})P_T \le PT, \quad (3)$$

where P_T and P_D are again the powers utilized for training and data transmission, respectively, and T_{TR}, T_{TF}, and T_D are the durations of the respective phases. By considering again the MMSE estimator in training and the AN-assisted secrecy beamforming scheme in data transmission, the optimal power allocation derived in [12] shows that, compared to the conventional case discussed above, more power should be allocated to training since DCE helps construct a better secrecy channel for data transmission and less power should be utilized for AN in data transmission since the channel quality has already been successfully discriminated through training. This concept can also be extended to non-reciprocal channels as discussed in [13].

Secrecy with Only Main-Channel CSIT and No CSI at Bob and Eve

In this subsection, we consider the case where only reverse training is applied, that is, $T_{TF} = 0$. The key idea is that, since forward training is always performed at the risk of CSI leakage, why not avoid it completely? This can be achieved by employing only reverse training and no forward training, but comes at the price of also not being able to provide CSI to Bob. Conceptually, this can be viewed as a wiretap channel with perfect main-channel CSIT, but no CSI at Bob and Eve [14]. In the wireless scenario, having CSIT allows

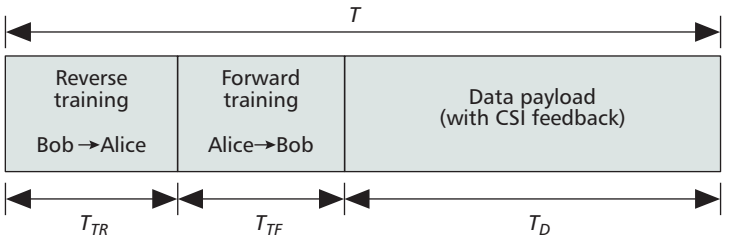

Figure 4. The transmission scheme with both reverse and forward training.

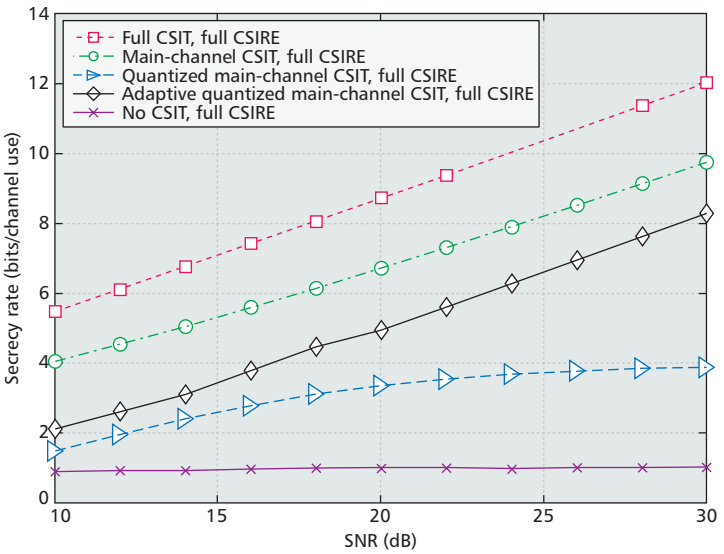

Figure 5. The achievable secrecy rates vs. transmit power for schemes with various channel feedback.

Alice to pre-compensate for the amplitude and phase variations of the fading channel to enable coherent detection at Bob while leaving Eve confused by the uncertainty of its own channel. It was shown in [14] that under certain conditions, the achievable secrecy rate can actually be significantly higher than that with perfect CSI at all terminals. This implies that under the secrecy scenario, CSI at the transmitter plays a more important role than CSI at the receiver.

Besides the aforementioned schemes, [15] further considered the case where neither training nor feedback is applied, and thus, no instantaneous CSI is available at any node. A constant norm channel input was proposed to exploit the noncoherent nature of the channel and was shown to achieve the optimal performance at high SNR (in terms of the secure degrees of freedom).

Performance Assessments and Discussions

In this section, we compare the achievable secrecy rates of the aforementioned schemes in wireless fading scenarios. We assume that Alice has four antennas, while both Bob and Eve have only a single antenna each. The 1×4 channel vectors $\mathbf{h}_r(t)$ and $\mathbf{h}_e(t)$ have i.i.d. entries with variances 2 and 1, respectively. The variances of the AWGN at both receivers are given by 1.

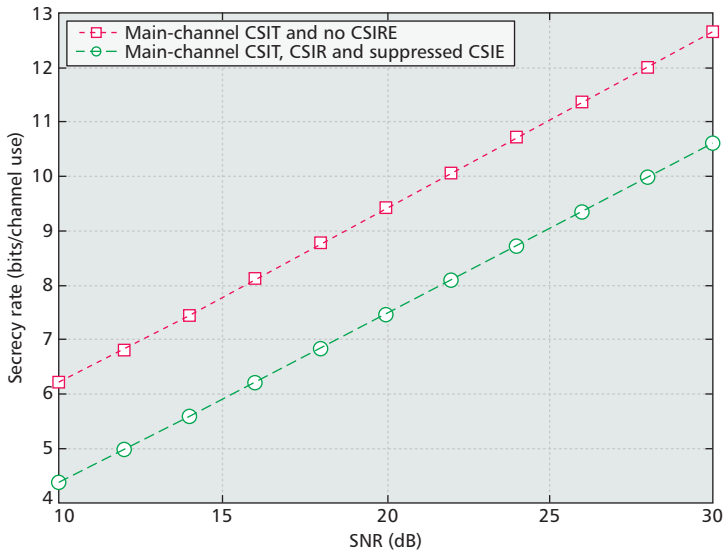

Figure 6. The achievable secrecy rates vs. transmit power for the cases with suppressed CSIE and no CSIRE, respectively.

In Fig. 5, we compare the secrecy rates achievable under four different CSI assumptions introduced earlier. These CSI assumptions result from traditional forward training and channel feedback procedures. In this figure, we can see that the case with full CSIT and full CSI at the receiver and the eavesdropper (CSIRE) achieves the highest secrecy rate. However, the case with only main-channel CSIT and full CSIRE, where AN-assisted secrecy beamforming is adopted, scales at approximately the same rate with respect to the transmit SNR as the full CSIT case. In the case with quantized main-channel CSI, we consider the scenario in [9] where only the channel direction (i.e., the normalized main channel vector) is quantized. The curve is plotted for the case of 10 quantization bits. Due to AN leakage, the achievable secrecy rate eventually saturates as the transmit SNR increases. This can be improved by scaling the number of quantization bits logarithmically with respect to the transmit SNR. When no CSIT is available, the achievable secrecy rate saturates rapidly at low SNR, and thus performs significantly worse than the other schemes, which shows the importance of CSIT.

In Fig. 6, we show the secrecy rates that are achievable with protection against CSI leakage, that is, the case with suppressed CSI at the eavesdropper (CSIE) and the case with only main-channel CSIT, described earlier. For the scheme with suppressed CSI at Eve (i.e., the scheme that utilizes DCE in the training phase), the coherence time is set to be $T = 100$ (channel uses), and the training length is given as $T_{TF} = N_A = 4$ and $T_{TR} = N_B = 1$, which correspond to the number of antennas at Alice and Bob, respectively. Notice that, as opposed to all other curves, the cost of training and the effect of imperfect channel estimation are both considered in the computation of the secrecy rate. We can see that, even considering the above practical issues, the achievable secrecy rate of the DCE-enabled scheme is still higher than that of the case with main-channel CSIT and full CSIRE (Fig. 5). This shows the advantage of discriminating the quality of the two channels before the secret data is actually transmitted. Moreover, for the case with only main-channel CSIT and no CSIRE, the achievable secrecy rate can actually be higher than that under full CSIT and full CSIRE. This implies that the prevention of CSI leakage is more important than providing Bob with the CSI.

Even though, in the scenarios considered in Figs. 5 and 6, the schemes that avoid CSI leakage are shown to outperform schemes that do not, this is not always the case. In fact, the conventional schemes are still useful due to the following reasons:

- The schemes that avoid CSI leakage do not always lead to better performance. For example, at high SNR, the DCE scheme may not necessarily achieve higher secrecy rates than the conventional AN-assisted secrecy beamforming scheme. This is due to the fact that the reverse training in DCE occupies extra temporal resources without carrying any information, and thus produces a loss in secrecy rate that can be significant at high SNR. Due to similar reasons, the DCE scheme also may not perform well when the coherence time is short.
- Even though the schemes that avoid CSI leakage may be suitable for basic wiretap channels with only a single receiver and eavesdropper, they may not be suitable for other, more general, settings such as the broadcast or interference channels with confidential messages. For example, the reverse training required in several of these schemes may not be efficient in broadcast channels since the time required for all receivers to emit their reverse training signals may occupy too many channel uses. In this case, it may be more efficient to have the transmitter send a single forward training signal to all receivers and utilize the schemes that do not avoid CSI leakage. Moreover, for schemes that utilize AN, such as the DCE scheme, the transmission of AN may cause additional interference to other users, and thus may not be suitable for interference channels.
- The schemes that do not avoid CSI leakage were devised by assuming that perfect CSI of the main and eavesdropper channels are available at Eve. These schemes can be viewed as worst-case schemes that can be used when the level of CSI at Eve is uncertain.

Conclusion

In this article, we discuss how different CSI assumptions resulting from conventional and unconventional ways of doing training and channel feedback may affect the achievable secrecy rate. In the conventional case, training is performed in the forward direction, and channel feedback is provided in an insecure manner, which both benefit Eve in terms of obtaining the CSI and strengthening its eavesdropping capability. In this case, secrecy beamforming can be used to direct the message-bearing signal toward dimensions that are more favorable to Bob, and AN can be used to further suppress the reception quality at Eve. These schemes are devised

by assuming perfect CSI at Eve and hence are suitable for the worst-case scenario. On the other hand, if the system setting allows for the prevention of CSI leakage, significant gains may be obtained by adopting new training and channel feedback schemes. In fact, by capitalizing on reverse training, CSI can be provided to Alice without revealing too much (if any) CSI to Eve, causing Eve to be confused by its own channel during reception. Notice that in most schemes, some level of the eavesdropper-channel CSI, such as the statistics of the channel, is required in order to achieve good secrecy performance. However, this is difficult to obtain in practice. Therefore, it is interesting to see how physical layer secrecy can be performed in the absence of any eavesdropper-channel CSI (not even the statistics), which is still an open problem. Moreover, it is also important to construct practical wiretap codes that are suitable for practical systems and determine ways to incorporate physical layer secrecy transmission into current standards.

References

[1] A. D. Wyner, "The Wire-Tap Channel," *Bell Sys. Tech. J.*, vol. 54, Oct. 1975, pp. 1355–87.

[2] I. Csiszár and J. Körner, "Broadcast Channels with Confidential Messages," *IEEE Trans. Info. Theory*, vol. 24, no. 3, Oct. 1978, pp. 339–48.

[3] S. Shafiee, N. Liu, and S. Ulukus, "Towards the Secrecy Capacity of the Gaussian Mimo Wire-Tap Channel: The 2-2-1 Channel," *IEEE Trans. Info. Theory*, vol. 55, no. 9, Sept. 2009, pp. 4033–39.

[4] A. Khisti and G. Wornell, "Secure Transmission with Multiple Antennas I: The Misome Wiretap Channel," *IEEE Trans. Info. Theory*, vol. 56, no. 7, July 2010, pp. 3088–3104.

[5] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, June 2008, pp. 2180–89.

[6] P.-H. Lin *et al.*, "On Secrecy Rate ot the Generalized Artificial-Noise Assisted Secure Beamforming for Wiretap Channels," *IEEE JSAC*, vol. 31, no. 9, Sept. 2013, pp. 1728–40.

[7] S. Gerbracht, C. Scheunert, and E. A. Jorswieck, "Secrecy Outage in MISO Systems with Partial Channel Information," *IEEE Trans. Info. Forensics Security*, vol. 7, no. 2, Apr. 2012, pp. 704–16.

[8] S. Yang *et al.*, "Secrecy Degrees of Freedom of MIMO Broadcast Channels with Delayed CSIT," *IEEE Trans. Info. Theory*, vol. 59, no. 9, Sept. 2013, pp. 5244–56.

[9] S. C. Lin *et al.*, "On the Impact of Quantized Channel Feedback in Guaranteeing Secrecy with Artificial Noise: The Noise Leakage Problem," *IEEE Trans. Wireless Commun.*, vol. 10, no. 3, Mar. 2011, pp. 901–15.

[10] Z. Rezki, A. Khisti, and M.-S. Alouini, "Ergodic Secret Message Capacity of the Wiretap Channel with Finite-Rate Feedback," *IEEE Trans. Wireless Commun.*, vol. 13, no. 6, June 2014, pp. 3364–79.

[11] P.-H. Lin and E. A. Jorswieck, "On the Fading Gaussian Wiretap Channel with Statistical Channel State Information at Transmitter," *IEEE Trans. Info. Forensics Security*, vol. 11, no. 1, Jan. 2015, pp. 46–58.

[12] T.-Y. Liu *et al.*, "How Much Training Is Enough for Secrecy Beamforming with Artificial Noise," *Proc. IEEE ICC*, June 2012.

[13] C.-W. Huang *et al.*, "Two-Way Training for Discriminatory Channel Estimation in Wireless MIMO Systems," *IEEE Trans. Signal Process.*, vol. 61, no. 10, May 2013, pp. 2724–38.

[14] P.-C. Lan, Y.-W. P. Hong, and C.-C. J. Kuo, "Enhancing Secrecy in Fading Wiretap Channels with Only Transmitter-Side Channel State Information," IEEE GLOBECOM Wksp. Trusted Commun. with Physical Layer Security, Dec. 2014.

[15] T.-Y. Liu *et al.*, "Secure Degrees of Freedom of MIMO Rayleigh Block Fading Wiretap Channels with No CSI Anywhere," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, May 2015, pp. 2655–69.

Biographies

TA-YUAN LIU received his B.S. degree in electrical engineering from National Tsing Hua University, Hsinchu, Taiwan, in 2009, and is currently pursuing his Ph.D. degree in the Institute of Communications Engineering at National Tsing Hua University. His research interests include physical layer security, information theory, and wireless communications.

PIN-HSUN LIN received his Ph.D. degree in electrical engineering from National Taiwan University, Taipei, Taiwan, in 2010. Since 2014 he has been a research fellow and packet leader for the DIWINE project with Technische Universität Dresden, Germany, for physical layer security. His research interests include wireless communications and information theory.

SHIH-CHUN LIN received his Ph.D. degree in electrical engineering from National Taiwan University in 2007. He is currently an assistant professor at National Taiwan University of Science and Technology, Taipei. His research interests include coding/information theory, communications, and signal processing. He has also served as a Technical Program Committee member for the IEEE ICC Workshop on Wireless Physical Layer Security, CNS Workshop on Physical-Layer Method for Wireless Security, and ICC.

Y.-W. PETER HONG received his B.S. from National Taiwan University in 1999 and his Ph.D. from Cornell University in 2005. He joined the Institute of Communications Engineering at National Tsing Hua University in fall 2005 and is now a full professor. His research interests include physical layer secrecy, cooperative communications, and signal processing for sensor networks. He is an Associate Editor for *IEEE Transactions on Signal Processing* and *IEEE Transactions on Information Forensics and Security*.

EDUARD AXEL JORSWIECK (Eduard.Jorswieck@tu-dresden.de) received his Dipl.-Ing. and Dr.-Ing. degree from Technische Universität Berlin in 2000 and 2004. From 2006 until 2008, he was a postdoctoral fellow and later an assistant professor at the Royal Institute of Technology, Sweden. Since 2008, he has been head of the Chair of Communications Theory and a full professor at Technische Universität Dresden, Germany. His research interests include applied information theory, signal processing for communication networks, and communications theory. He serves on the Editorial Boards of *IEEE Transactions on Signal Processing* and *IEEE Transactions on Wireless Communications*.

Even though the schemes that avoid CSI leakage may be suitable for basic wiretap channels with only a single receiver and eavesdropper, it may not be suitable for other, more general, settings such as the broadcast or the interference channels with confidential messages.