Int. J. Electron. Commun. (AEÜ) 69 (2015) 1047–1057

Contents lists available at ScienceDirect

International Journal of Electronics and Communications (AEÜ)

journal homepage: www.elsevier.com/locate/aeue

Feedback enhances the security of wiretap channel with states

B. Dai [a,b,*], A.J. Han Vinck [c], Y. Wang [d]

[a] School of Information Science and Technology, Southwest JiaoTong University, Chengdu, China
[b] The National Mobile Communications Research Laboratory, Southeast University, Nanjing, China
[c] Institute for Experimental Mathematics, Duisburg-Essen University, Ellernstr. 29, Essen, Germany
[d] China Information Technology Security Evaluation Center, Beijing, China

ARTICLE INFO

Article history:
Received 20 April 2013
Accepted 8 April 2015

Keywords:
Wiretap channel
Channel state information
Capacity-equivocation region
Noiseless feedback
Secrecy capacity

ABSTRACT

Wyner, in his well-known paper on the wiretap channel, studied the problem on how to transmit the confidential messages to the legitimate receiver via a degraded broadcast channel, while keeping the wiretapper as ignorant of the messages as possible. In this paper, the model of wiretap channel has been reconsidered for the case that the main channel is controlled by channel state information (CSI), and it is available at the transmitter in a noncausal manner (termed here noncausal channel state information) or causal manner (termed here causal channel state information). Moreover, there is a noiseless feedback from the legitimate receiver to the transmitter. Measuring the uncertainty of the wiretapper by equivocation, the capacity-equivocation regions for both manners (causal and noncausal) are determined. Furthermore, the secrecy capacities are formulated, which provide the best transmission rate with perfect secrecy. The results of this paper are further explained via binary and Gaussian examples, and we find that the noiseless feedback helps to enhance the security of wiretap channel with noncausal or causal CSI at the transmitter.

1. Introduction

The most important issues in communication are reliability and security. The reliability quantifies the maximum rate achievable with small probability of error. Security is an important issue when the transmitted information is confidential and needs to be kept as secret as possible from wiretapper. Communication of confidential messages has been studied in the literature for some classes of channel models, and the wiretap channel is the most important model of them.

The concept of the wiretap channel was first introduced by Wyner [1]. It is a kind of degraded broadcast channels. The wiretapper knows the encoding scheme used at the transmitter and the decoding scheme used at the legitimate receiver, see Fig. 1. The object is to describe the rate of reliable communication from the transmitter to the legitimate receiver, subject to a constraint of the equivocation to the wiretapper. After the publication of Wyner's work, Csiszár and Körner [2] investigated a more general situation: the broadcast channels with confidential messages. It is clear that Wyner's wiretap channel is a special case of the model of Csiszár and Körner, in a manner that the main channel is less noisy than the wiretap channel. Furthermore, Leung-Yan-Cheong and Hellman studied the Gaussian wiretap channel (GWC) [3], and showed that its secrecy capacity was the difference between the main channel capacity and the overall wiretap channel capacity (the cascade of main channel and wiretap channel). In addition, Merhav [4] studied a variation of the wiretap channel, and obtained the capacity region, where both the legitimate receiver and the wiretapper have access to some leaked symbols from the source, but the channels for the wiretapper are more noisy than the legitimate receiver, which shares a secret key with the encoder.

In communication systems there is often a feedback link from the receiver to the transmitter. For example, the two-way channels for telephone connections. It is well known that feedback does not increase the capacity of discrete memoryless channel (DMC) [18, pp. 216–218]. However, does the feedback increase the capacity region of the wiretap channel? In order to solve this problem, Ahlswede and Cai studied the general wiretap channel (the wiretap channel does not need to be degraded) with noiseless feedback from the legitimate receiver to the transmitter [5] (see Fig. 2), and both the upper and lower bounds of the secrecy capacity were provided. Specifically, for the degraded case, they showed that the secrecy capacity is larger than that of Wyner's wiretap channel (without feedback). In the achievability proof, Ahlswede and Cai [5] used the noiseless feedback as a secret key shared by the

* Corresponding author at: School of Information Science and Technology, Southwest JiaoTong University, Chengdu, China.
E-mail address: daibin@home.swjtu.edu.cn (B. Dai).

http://dx.doi.org/10.1016/j.aeue.2015.04.005
1434-8411/

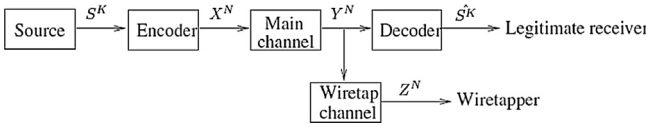

Fig. 1. Wiretap channel.

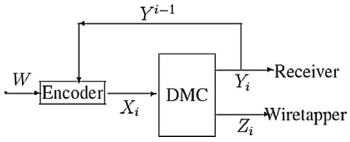

Fig. 2. The general wiretap channel with noiseless feedback.

transmitter and the legitimate receiver, while the wiretapper had no knowledge about the key except his own received symbols. Based on the work of [5], Dai et al. [6] studied a special case of the general wiretap channel with noiseless feedback, and found that the noiseless feedback enhances the secrecy capacity of the non-degraded wiretap channel. Besides Ahlswede and Cai's work, the wiretap channel with noisy feedback was studied in [7], and the wiretap channel with secure rate-limited feedback was studied in [8], and both of them focused on bounds of the secrecy capacity.

The coding for channels with causal (past and current) channel state information at the encoder was first investigated by Shannon [9] in 1958. After that, in order to solve the problem of coding for a computer memory with defective cells, Kuznetsov and Tsybakov [10] considered a channel in the presence of noncausal channel state information at the transmitter. They provided some coding techniques without determination of the capacity. The capacity was found in 1980 by Gel'fand and Pinsker [11]. Furthermore, Max H.M. Costa [12] investigated a power constrained additive noise channel, where part of the noise is known at the transmitter as side information. This channel is also called dirty paper channel. In order to introduce channel state information to the broadcast channels, Steinberg investigated the degraded broadcast channel with channel state information [13], where both causal and noncausal channel state information were considered in his paper. Specifically, inner and outer bounds on capacity region were provided for the degraded broadcast channel with noncausal channel state information [13], meanwhile, the capacity region of the degraded broadcast channel with causal channel state information was totally determined [13].

Inspired by the works of [12] and [1], Mitrpant et al. [14] studied transmission of confidential messages in the channels with channel state information (CSI). In [14], an inner bound on the capacity-equivocation region was provided for the Gaussian wiretap channel with CSI. Furthermore, Chen et al. [15] investigated the discrete memoryless wiretap channel with noncausal CSI (see Fig. 3), and also provided an inner bound on the capacity-equivocation region. Note that the coding scheme of [15] is a combination of those in [11,1]. Based on the work of [15], Dai [16] provided an outer bound on the wiretap channel with noncausal CSI, and determined the capacity-equivocation region for the model of wiretap channel with memoryless CSI, where the memoryless means that at the i-th time,

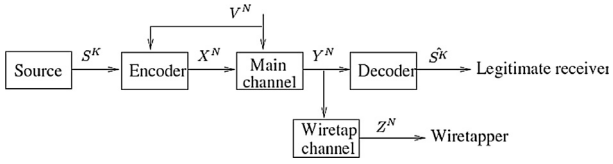

Fig. 3. Wiretap channel with noncausal channel state information.

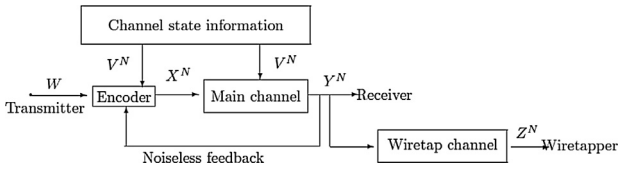

Fig. 4. Wiretap channel with channel state information and noiseless feedback.

the output of the channel encoder depends only on the i-th time CSI.

In this paper, we study the model of wiretap channel with channel state information and noiseless feedback, see Fig. 4. It is derived from the model of Fig. 2 and the model of Fig. 3. *The motivation of this work is to investigate how the feedback works in the mode of the wiretap channel with channel state information, and whether the achievable region of [15] can be enhanced by using the noiseless feedback.*

In the new model of Fig. 4, the conditional transition probability distribution of the main channel depends on a channel state information sequence V^N, which is available at the encoder in a noncausal or causal manner. In addition, there is a noiseless feedback from the output of the main channel to the transmitter. The wiretapper can get a degraded version of the symbols Y^N via a wiretap channel.

The capacity-equivocation region is determined for this new model in both causal and noncausal manners. Furthermore, the secrecy capacity is formulated, which provides the best transmission rate with perfect secrecy.

The organization of this paper is as follows. In Section 2, we present the basic definitions and the main results on the capacity-equivocation regions. Section 3 is for examples about the model of Fig. 4. Final conclusions are presented in Section 4.

2. Notations, definitions and the main results

In this paper, random variables, sample values and alphabets are denoted by capital letters, lower case letters and calligraphic letters, respectively. A similar convention is applied to the random vectors and their sample values. For example, U^N denotes a random N-vector $(U_1, \ldots, U_N)$, and $u^N = (u_1, \ldots, u_N)$ is a specific vector value in $\mathcal{U}^N$ that is the Nth Cartesian product of $\mathcal{U}$. U_i^N denotes a random $N-i+1$-vector $(U_i, \ldots, U_N)$, and $u_i^N = (u_i, \ldots, u_N)$ is a specific vector value in $\mathcal{U}_i^N$. Let $p_V(v)$ denote the probability mass function $Pr\{V = v\}$. Throughout the paper, the logarithmic function is to the base 2.

In this section, the model of Fig. 4 is considered into two parts. The model of Fig. 4 with noncausal CSI is described in Section 2.1, and the model of Fig. 4 with causal CSI is described in Section 2.2, see the followings.

2.1. The model of Fig. 4 with noncausal channel state information

In this subsection, a description of the model of Fig. 4 with noncausal CSI is given by Definition 1 to Definition 4. The capacity-equivocation region $\mathcal{R}^{(n)}$, which is composed of all achievable (R, R_e) pairs in the model of Fig. 4 with noncausal CSI, are characterized in Theorem 1. The achievable (R, R_e) pair is defined in Definition 5.

Definition 1. (**Channel encoder for the noncausal manner**) The message W is uniformly distributed over $\mathcal{W}$. The channel state information V^N is the output of a discrete memoryless source $P_V(\cdot)$, and it is available at the channel encoder in a noncausal manner. V^N is independent of W. The feedback Y^{i-1} (where $2 \le i \le N$ and Y^{i-1} takes values in $\mathcal{Y}^{i-1}$) is the previous $i-1$ time output of the main channel. At the i-th time, the inputs of the channel encoder