Wiretap Channel with Side Information

Yanling Chen

Abstract

In this thesis, we consider a communication problem over the wiretap channel, where one wants to send a message to the legitimate receiver and at the same time keep it from the wiretapper as secret as possible. Due to known results, the theory on the model of the wiretap channel where side information is not present, is fairly complete. Introducing side information noncausally known at the transmitter into the model, we wonder whether side information could help the secret communication over the wiretap channel.

We investigate the wiretap channel with side information and explore its security capacity and capacity region. For the discrete memoryless case, we establish a coding theorem, which implies an achievable rate equivocation region and a bound for the secrecy capacity. In particular, the secrecy capacity is determined for some special cases.

Extending our result for the discrete memoryless case to the Gaussian case, our contribution to the Gaussian wiretap channel with side information is twofold. First, we derive an achievable rate equivocation region by applying Costa's strategy, which improves an earlier result given by Mitrpant. Compare it with the capacity region for the corresponding Gaussian wiretap channel given by Leung-Yan-Cheong and Hellman. We show that for the Gaussian wiretap channel, side information helps to achieve a larger secrecy capacity and a larger capacity region. Thus we can draw a conclusion that side information plays a positive role in the secret communication over the Gaussian wiretap channel. Furthermore, we generalize Costa's strategy by taking the correlation coefficient of the codeword and side information as another parameter into our consideration. We show that the achievable region derived by applying Costa's strategy can be enlarged by applying the generalized Costa's strategy. In other words, for the Gaussian wiretap channel, it can be a better choice to send a codeword dependent on the side information, in order to yield a higher rate at a certain security level. In addition, we give the optimum choice of the parameters for the generalized Costa's strategy to achieve the maximal rate at perfect secrecy.

In this thesis, we also investigate the problem of developing forward coding schemes for secure communication over the wiretap channel. A code construction is considered for the specific case when both the main channel and the wiretap channel are binary symmetric. Theoretically, we show that its secrecy capacity can be achieved by using random linear codes. For practical purpose, we evaluate the performance of the coding schemes when specific linear codes are used in the construction.

As an application, we reformulate the security problem in biometrics as a communication problem over the wiretap channel. We review two fuzzy commitment schemes, one by Juels and Wattenberg and the other by Cohen and Zémor. We characterize the performances of both schemes with the terminologies for the wiretap channel. For the Juels-Wattenberg scheme, we give a security proof in the information theoretic sense. For the Cohen-Zémor scheme, we consider its practicality and give some insight into the choice of the parameters that yields good performance.