On the Wire-tap Channel of Type II with Side Information

Chaichana Mitrpant, Yuan Luo, A.J. Han Vinck
University of Essen, Germany

January 30, 2003

I Introduction

The Wire-tap channel of type II, as introduced by Ozarow and Wyner in [1], is a noiseless channel from which an adversary can wiretap μ coded bits. The transmitter and the receiver may not know when the channel is being wiretapped by the adversary and, therefore, would like to encode the information in such a way that the minimum uncertainty of the information can be guaranteed when μ bits are wiretapped from the channel.

Ozarow and Wyner showed the existence of linear codes to be used in conjunction with the coset coding method to achieve the optimal trade-off between the rate of transmission, the equivocation (the minimum uncertainty) and the number of bits being wiretapped.

We review the original system proposed in [1], and investigate how well it performs if the wiretapper is given some of the uncoded bits as side information.

II Model Description

Let S^K represent a K-bit data sequence to be protected from a wiretapper by encoding it into an N-bit sequence X^N, where S_k are independent and identically distributed binary random variables with uniform distribution. Let $\hat{S}^K$ be the output of the decoder whose input is X^N. Let Z^μ be the wiretapped bits consisting of μ bits of X^N indexed by the set τ^c where $\tau^c \subseteq \{1, 2, \ldots, N\}$ and $|\tau^c| = \mu$. Let $S_2^{a_2} = S_\rho^K$ be the side information consisting a_2 bits of S^K indexed by the set ρ where $\rho \subseteq \{1, 2, \ldots, K\}$ and $|\rho| = a_2$. Let $S_1^{a_1} = S_{\rho^c}^K$, where $a_1 = K - a_2$.

We are interested in the trade-offs between K, N, P_e and $\Delta_{S_1|S_2,Z}$, where

$$P_e = \frac{1}{K}\sum_{k=1}^{K} \Pr\{S_k \neq \hat{S}_k\},$$

and

$$\Delta_{S_1|S_2,Z} = \min_{\substack{\tau^c:|\tau^c|=\mu \\ \rho:|\rho|=a_2}} H(S_1^{a_1}|S_2^{a_2}, Z^\mu).$$

We say that (R, R_1, α, δ) is achievable if for all $\epsilon > 0$, there exists an encoder/decoder pair with parameters $N \geq N_0$, $K \geq (R-\epsilon)N$, $a_1 \geq (R_1-\epsilon)N$, $\mu \geq (\alpha-\epsilon)N$, $\Delta_{S_1|S_2,Z} \geq (\delta-\epsilon)a_1$, and $P_e \geq \epsilon$.

Coding Method

1. Given a message $\mathbf{s}^K$ and a parity-check matrix $\mathbf{A}_{K\times N}$, solve for the set of solutions $\{\mathbf{x}^N : \mathbf{A}\mathbf{x}^T = \mathbf{s}^T\}$, and randomly select a vector from the set of solutions to be transmitted as a code word.
2. To decode, solve the equation $\mathbf{s}^T = \mathbf{A}\mathbf{x}^T$ for $\mathbf{s}^K$, where $\mathbf{x}^N$ is the received vector.

III Main Results

Theorem 1 *If the coset coding method is used with linear block codes, (R, R_1, α, δ) is achievable if and only if $R \geq 0, 0 \leq R_1 \leq R, \alpha \leq 1$ and*

$$0 \leq \delta \leq \begin{cases} 1, & 0 \leq \alpha \leq 1-R, \\ 1-\alpha-(R-R_1), & 1-R \leq \alpha \leq 1-(R-R_1), \\ 0, & 1-(R-R_1) \leq \alpha \leq 1. \end{cases}$$

The theorem implies that there exists a linear code that allows the information $S_1^{a_1}$ to be fully protected if $S_2^{a_2}$ and μ bits of X^N are given to the wiretapper, where $\mu \leq N-K$. However, the equivocation of $S_1^{a_1}$ decreases linearly as a function of μ as μ increases. If μ is greater than $N-a_2$, the coding cannot guarantee the equivocation of $S_1^{a_1}$ anymore. Furthermore, if $\mathbf{A}$ is the generator matrix of an MDS code, the upper bound on the equivocation can be achieved. Nevertheless, using MDS generator matrix is not necessary as we have found non-MDS generator matrices that allows the equivocation to meet the upper bound.

References

[1] L. H. Ozarow and A. D. Wyner, "Wire-Tap Channel II," *AT&T Bell Laboratories Technical Journal*, vol. 63, pp. 2135-2157, December 1984.

[2] G. David Forney, Jr., "Dimension/Length Profiles and Trellis Complexity of Linear Block Codes," *IEEE Trans. Inform. Theory*, vol. 40, pp.1741-1752, November 1994.

[3] Yuan Luo, Chaichana Mitrpant and A.J. Han Vinck, "The Multi-user Wire-tap Channel of Type II Using Coset Coding Method," submitted to *IEEE Trans. Inform. Theory*, July 2002.