In Favour of Posting

香港中文大學
The Chinese University of Hong Kong

Institute of Theoretical Computer Science and Communications

Theory Seminar Series

Codes against Online Adversaries

By
Prof. Sidharth Jaggi
Department of Information Engineering, CUHK

July 14, 2009 (Tuesday)
3:00p.m. – 5:00p.m.
Rm. 121, Ho Sin Hang Engineering Building, CUHK

Abstract: In this work we consider the communication of information in the presence of an online adversarial jammer. In the setting under study, a sender wishes to communicate a message to a receiver by transmitting a codeword x = (x1 , . . . , xn) symbol-by-symbol over a communication channel. The adversarial jammer can view the transmitted symbols xi one at a time, and can change up to a p-fraction of them. However, the decisions of the jammer must be made in an online or causal manner. Namely, for each symbol xi the jammer's decision on whether to corrupt it or not (and on how to change it) must depend only on xj for $j \leq i$. This is in contrast to the "classical" adversarial jammer which may base its decisions on its complete knowledge of x.

More generally, for a delay parameter $d \in (0, 1)$, we study the scenario in which the jammer's decision on the corruption of xi must depend solely on xj for $j \leq i - dn$. In this work, we study codes for online adversaries when the transmitted symbols are assumed to be over a sufficiently large field F. We present a tight characterization of the amount of information one can transmit in both the 0-delay and, more generally, the d-delay online setting. We show that for 0-delay adversaries, the achievable rate asymptotically equals that of the classical adversarial model. For positive values of d we show that the achievable rate can be significantly greater than that of the classical model. We prove tight results for both additive and overwrite jammers. In the additive case the jammer may corrupt information $xi \in F$ by adding onto it a corresponding error $ei \in F$. In this case the receiver gets the symbol yi = xi + ei . In the overwrite case, the jammer may corrupt information $xi \in F$ by replacing it with a corresponding corrupted symbol $yi \in F$. For positive delay d, symbol xi may not be known to the adversarial jammer at the time it is being corrupted, hence these two error models, and the corresponding achievable rates, are shown to differ substantially. Finally, we extend our results to a jam-or-listen online model, where the online adversary can either jam a symbol or eavesdrop on it. This corresponds to several scenarios that arise in practice. We again provide a tight characterization of the achievable rate for several variants of this model. The rate-regions we prove for each model are informational-theoretic in nature and hold for computationally unbounded adversaries. The rate regions are characterized by "simple" piecewise linear functions of p and d. The codes we construct to attain the optimal rate for each scenario are computationally efficient.

This is joint work with B.K.Dey and M. Langberg.

***** ALL ARE WELCOME *****

Host & Enquiries : Institute of Theoretical Computer Science and Communications Tel: 2696 1257