Steganographic Communication in Ordered Channels

R.C. Chakinala[1,⋆], A. Kumarasubramanian[1,⋆], R. Manokaran[1,⋆], G. Noubir[1,⋆⋆], C. Pandu Rangan[2,⋆⋆⋆], and R. Sundaram[1,⋆,†]

[1] Northeastern University, Boston, MA
ravich,abishe,rajsekar,noubir,koods@ccs.neu.edu
[2] Indian Institute of Technology - Madras, Chennai
rangan@iitm.ernet.in

Abstract. In this paper we focus on estimating the amount of information that can be embedded in the sequencing of packets in ordered channels. Ordered channels, e.g. TCP, rely on sequence numbers to recover from packet loss and packet reordering. We propose a formal model for transmitting information by packet-reordering. We present natural and well-motivated channel models and jamming models including the k-distance permuter, the k-buffer permuter and the k-stack permuter. We define the natural information-theoretic (continuous) game between the channel processes (max-min) and the jamming process (min-max) and prove the existence of a Nash equilibrium for the mutual information rate. We study the zero-error (discrete) equivalent and provide error-correcting codes with optimal performance for the distance-bounded model, along with efficient encoding and decoding algorithms. One outcome of our work is that we extend and complete D. H. Lehmer's attempt to characterize the number of distance bounded permutations by providing the asymptotically optimal bound - this also tightly bounds the first eigenvalue of a related state transition matrix [1].

1 Introduction

In this paper we model and prove the existence of a novel covert channel in any ordered channel. We define a *ordered* channel as one in which the basic units of communication (eg. packets in network channels) are linearly ordered. A common

⋆ Greatly appreciate financial and moral support from Mr. Madhav Anand, benefactor of Northeastern University, and founder and president of International Integrated Inc. (NASDAQ:ICUB).

⋆⋆ The research of this author was in part supported by NSF Career Award CNS-0448330.

⋆⋆⋆ The author would like to thank Microsoft Research, India for their generous support.

† The research of this author was in part supported by a grant from the DARPA NMS program.

J. Camenisch et al. (Eds.): IH 2006, LNCS 4437, pp. 42–57, 2007.

example of an ordered channel is the TCP communication channel which uses the *sequence number* field to order the packets. The crux of our hiding scheme is to re-order the packets, and thus sending information. Thus, the scheme involved coding by permuting the packets in the channel.

Communication in covert channels is usually modeled using five players namely, Alice, stego-Alice, Jammer, stego-Bob, Bob, in the order of access to a basic unit of communication (eg. packet). Alice and Bob are the legitimate senders using the ordered channel. stego-Alice and stego-Bob are the players involved in extracting a covert channel. stego-Alice works by permuting the packets sent by Alice and thus trying to communicate with stego-Bob. We use the notion of a Jammer to encapsulate the effects of attempts to intercept such covert channels. The Jammer works by permuting the packets, after they are sent by stego-Alice and before received by stego-Bob[1].

The capacity of the channel is measured by the information rate [2] of the channel. Since the channel is covert, stego-Alice should not inordinately permute the packets. Similarly, giving the Jammer, complete permuting power would render any stego-Alice useless[2]. Hence, we assign permuting power to the stego-Alice and the Jammer. Also, stego-Alice and Jammer are usually implemented in hardware and the permuting powers come up due to restricting the hardware complexity.

We formalize a variety of natural models of permuting power for the stego-Alice and the Jammer. We consider two distinct ways of analyzing the capacity of the channel. In the *continuous* case, we formulate the channel as a zero-sum game played by the stego-Alice and the Jammer where the stego-Alice tries to maximize the capacity of the channel. We prove the existence of a nash equilibrium for any given power (strategy space) of the stego-Alice and the Jammer. On the other hand, we have the *discrete* case, where we provide concrete encoding and decoding algorithms, parametrized on the stego-Alice and Jammer power, to communicate. We obtain tight bounds on the capacity of the covert channel were possible.

The rest of the paper is organized as follows. The following section talks about the related works. In section III, we formalize the channel model and introduce the various models to restrict the stego players and the jammers. In Section IV we analyze the general channel capacity as a two player game and prove that a Nash equilibrium exists. We set the stage for the following sections by characterizing the zero-error capacity of the channel. Section V is an analysis of restricted permutations, and in particular distance restricted permutations. In section VI, VII we prove bounds on zero-error the channel capacity in the models that we introduce and provide polynomial time encoding and decoding schemes.

[1] The concept of Jammer also encapsulates the inherent errors (eg. re-ordering of packets due to routing) that exist in the ordered channel.

[2] As we prove, for many natural models, the stego-Alice needs more power than the Jammer to effectively communicate.