Cryptology ePrint Archive: Report 2011/288

On the Communication Complexity of Reliable and Secure Message Transmission in Asynchronous Networks

Ashish Choudhury and Arpita Patra

Abstract: In this paper, we study the communication complexity of Reliable Message Transmission (RMT) and Secure Message Transmission (SMT) protocols in asynchronous settings. We consider two variants of the problem, namely perfect} (where no error is allowed in the protocol outcome) and statistical (where the protocol may output a wrong outcome with negligible probability). RMT and SMT protocols have been investigated rigorously in synchronous settings. But not too much attention has been paid to the asynchronous version of the problem. In a significant work, Choudhury et al. (ICDCN 2009 and JPDC 2011) have studied the network connectivity requirement for perfect and statistical SMT protocols in asynchronous settings. Their investigation reveals the following two important facts:

1. Perfect SMT protocols require more network connectivity in asynchronous network than synchronous network.

2. Connectivity requirement of statistical SMT protocols is same for both synchronous and asynchronous network.

Unfortunately, nothing is known about the communication complexity of RMT and SMT protocols in asynchronous settings. In this paper, we derive tight bounds on the communication complexity of the above problems and compare our results with the existing bounds for synchronous protocols. The interesting conclusions derived from our results are:

1. Asynchrony increases the communication complexity of perfect RMT protocols. However, asynchrony has no impact on the communication complexity of statistical RMT protocols.

2. SMT: Communication complexity of SMT protocols is more in asynchronous network, for both perfect as well as statistical case.

Category / Keywords: cryptographic protocols /

Publication Info: To appear in ICISC 2011

Date: received 1 Jun 2011, last revised 31 Oct 2011

Contact author: partho31 at gmail com, arpitapatra10@gmail com