Cryptology ePrint Archive: Report 2011/013

Secure Message Transmission In Asynchronous Directed Networks

Shashank Agrawal and Abhinav Mehta and Kannan Srinathan

Abstract: We study the problem of information-theoretically secure message transmission (SMT) in asynchronous directed networks. In line with the literature, the distrust and failures of the network is captured via a computationally unbounded Byzantine adversary that may corrupt some subset of nodes. We give a characterization of networks over which SMT from sender S to receiver R is possible in both the well-known settings, namely perfect SMT (PSMT) and unconditional SMT (USMT). We distinguish between two variants of USMT: one in which R can output an incorrect message (with small probability) and another in which R never outputs a wrong message, but may choose to abort (with small probability). We also provide efficient protocols for an important class of networks.

Category / Keywords: foundations / information-theoretic security, asynchronous network, directed network, Byzantine adversary

Date: received 6 Jan 2011

Contact author: shashank agrawal at research iiit ac in

Available formats: PDF | BibTeX Citation

Version: 20110108:015141 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]