

Cryptology ePrint Archive: Report 2011/320

Minimal Connectivity for Unconditionally Secure Message Transmission in Synchronous Directed Networks

Manan Nayak and Shashank Agrawal and Kannan Srinathan

Abstract: In this paper we give the minimal connectivity required in a synchronous directed network, which is under the influence of a computationally unbounded *\emph{Byzantine}* adversary that can corrupt a subset of nodes, so that Secure Message Transmission is possible between sender S and receiver R . We also show that secure communication between a pair of nodes in a given synchronous directed network is possible in both directions if and only if reliable communication is possible between them. We assume that in a network, every node is capable of computation and we model the network along the lines of *\cite{SR06}*.

Category / Keywords: Directed networks, Connectivity, Information-theoretic security

Publication Info: A shorter version of this paper appeared in International Conference on Information Theoretic Security (ICITS), 2011

Date: received 16 Jun 2011

Contact author: manan.nayak@research.iiit.ac.in

Available formats: [PDF](#) | [BibTeX Citation](#)

Version: 20110617:071202 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]