On combining information-theoretic and cryptographic approaches to network coding security against the pollution attack

Title	On combining information-theoretic and cryptographic approaches to network coding security against the pollution attack
Publication Type	Conference Paper
Year of Publication	2009
Authors	Vyetrenko, S., Khosla, A., Ho, T.
Conference Name	2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers
Date Published	nov
Keywords	computer networks, cryptographic approach, cryptographic protocols, cryptographic signature, cryptography, error correction, error correction codes, Human Behavior, Information rates, Information security, information theoretic security, Information theory, information-theoretic approach, Metrics, multicast communication, network coding, network coding security, network error correction, policy-based governance, Pollution, pollution attack, pubcrawl, Resiliency, Scalability, telecommunication security, Upper bound, Wireless sensor networks
Abstract	In this paper we consider the pollution attack in network coded systems where network nodes are computationally limited. We consider the combined use of cryptographic signature based security and information theoretic network error correction and propose a fountain-like network error correction code construction suitable for this purpose.
DOI	10.1109/ACSSC.2009.5469966
Citation Key	vyetrenko_combining_2009

Scalability telecommunication security Cryptographic Protocols Resiliency Human behavior pubcrawl policy-based governance wireless sensor networks Cryptography Metrics information theory information security computer networks error correction codes network coding error correction Upper bound multicast communication information theoretic security cryptographic approach cryptographic signature Information rates information-theoretic approach network coding security network error correction Pollution pollution attack