Network coding and information security

István Vajda

CrySys Lab
TU of Budapest
vajda@hit.bme.hu

Laboratory of Cryptography and System Security (CrySys)
Budapest University of Technology and Economics

The mission of the laboratory:

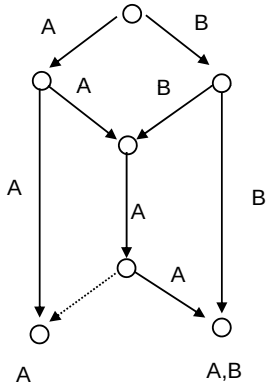
•to carry out fundamental and applied *research* in cryptography and systems security;

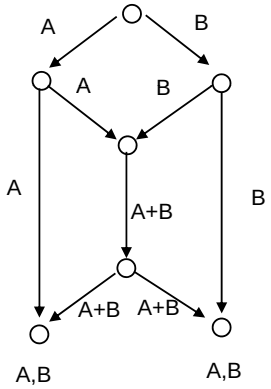
•to teach cryptography and systems security in the context of undergraduate and graduate university *courses*, as well as in the context of industrial training programs;

•to participate in R&D *projects* and to provide consulting services without compromising the general academic objectives

CrySyS
To be on the safe side

The idea of network coding

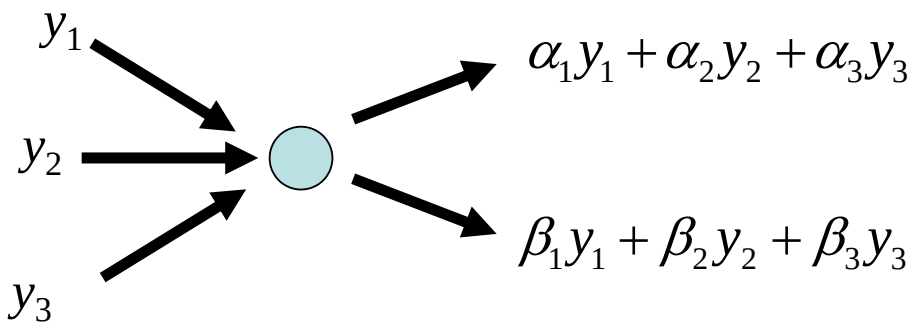




Throughput maximization
Multicast capacity

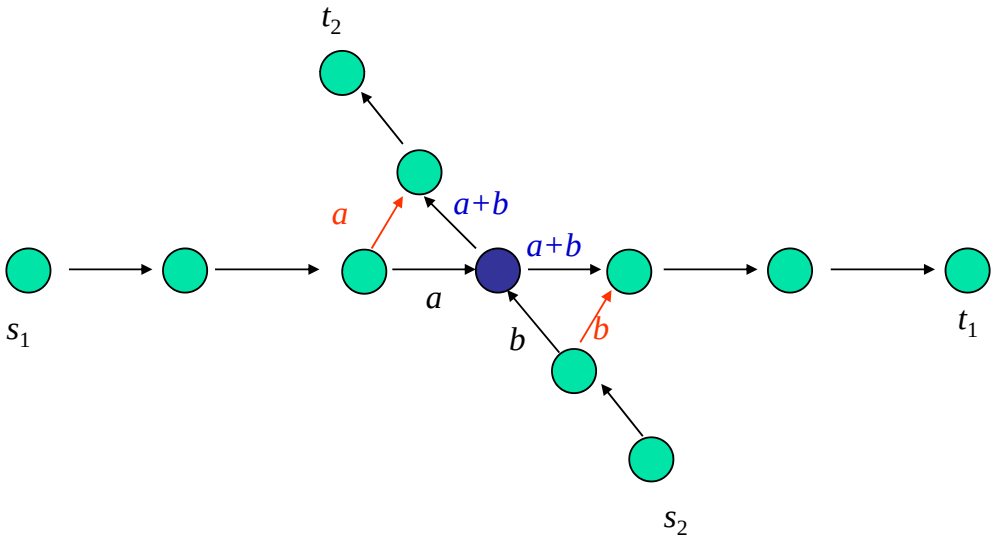
Pioneering work: [1] R. Ahlswede, N. Cai, S.-Y. R. Li, and R.W. Yeung, "Network information flow," *IEEE Trans. on Information Theory*, vol. 46, no. 4, July 2000.

Random linear coding



$$\alpha_i, \beta_i \in GF(q) \text{ random coefficients}$$

Wireless networks: XOR in-the-air

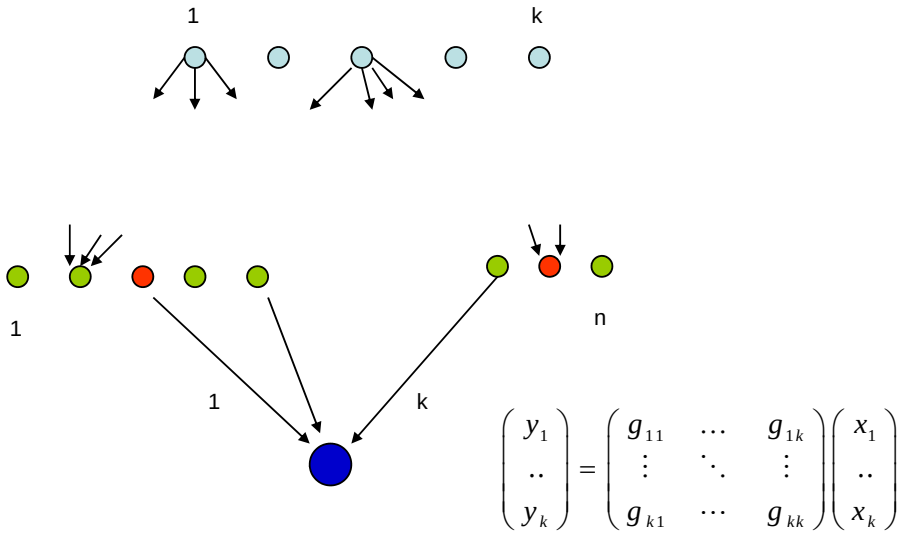


Benefits and main applications

Main benefits:
Maximizing throughput
Robustness

Main applications:
File download
Distributed storage
Wireless mesh networks
Sensor networks
...

Network coding security: distributed storage



Pollution attack: attack detection and recovery

Network coding in wireless mesh networks

- *Mobility support*: network access control novel *re-authentication mechanisms* (secure and fast handover between access points possibly belonging to different operators)
- *Routing security:* multi-destination, multi-constrained, QoS-aware *routing protocols* (preventing the creation of incorrect or suboptimal routing state in the mesh nodes)

Coding-aware routing can improve efficiency

Protocol overview: link state approach

(1) Source builds a communication graph

(2) Find a set of path satisfying QoS requirements for the new flow

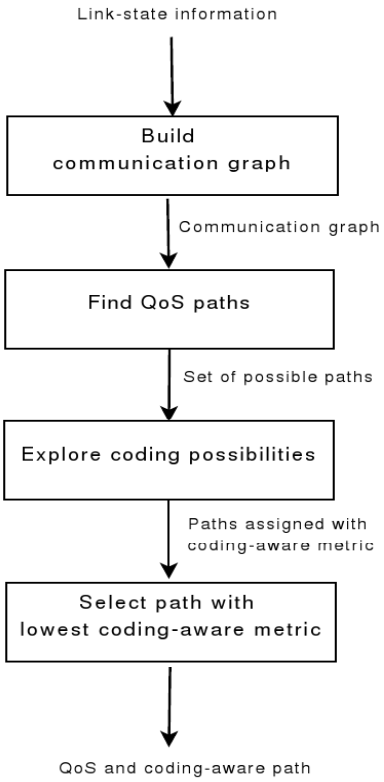
(3) Explore and evaluate coding possibilities along each potential path

(4) Nodes broadcast link-state messages periodically

(5) Select the path that loads the system least

(6) Reserve resources along the path

(7) Release resources



Summary

Network coding:
new algorithmic technology to improve throughput and robustness in many networking problems in Internet, sensor networks, wireless mesh networks.

Hot research topic:
coding aware routing
security (crypto-, non crypto approaches)