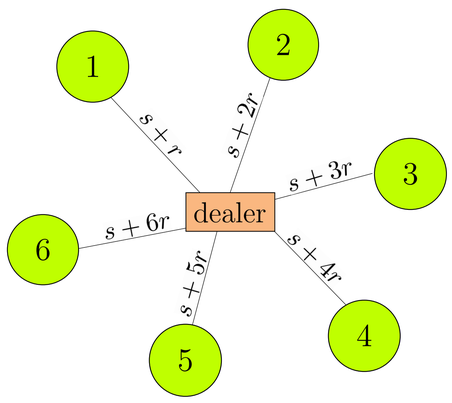
Secret Share Dissemination across a Network

Nihar B. Shah K. V. Rashmi Kannan Ramchandran

Shamir's Secret Sharing Scheme

- A dealer has a secret **s**
- Distribute shares (functions of s) to n participants such that
  - any k can recover s
  - any (k-1) get no information about s

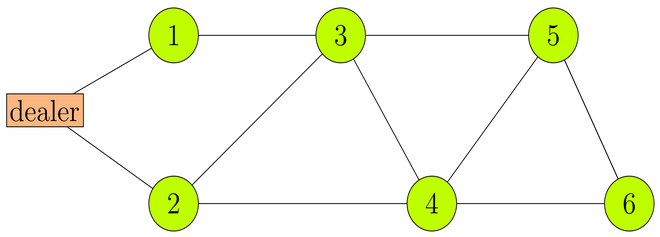
Example: k = 2



- Most protocols assume dealer has direct links to all participants

Problem

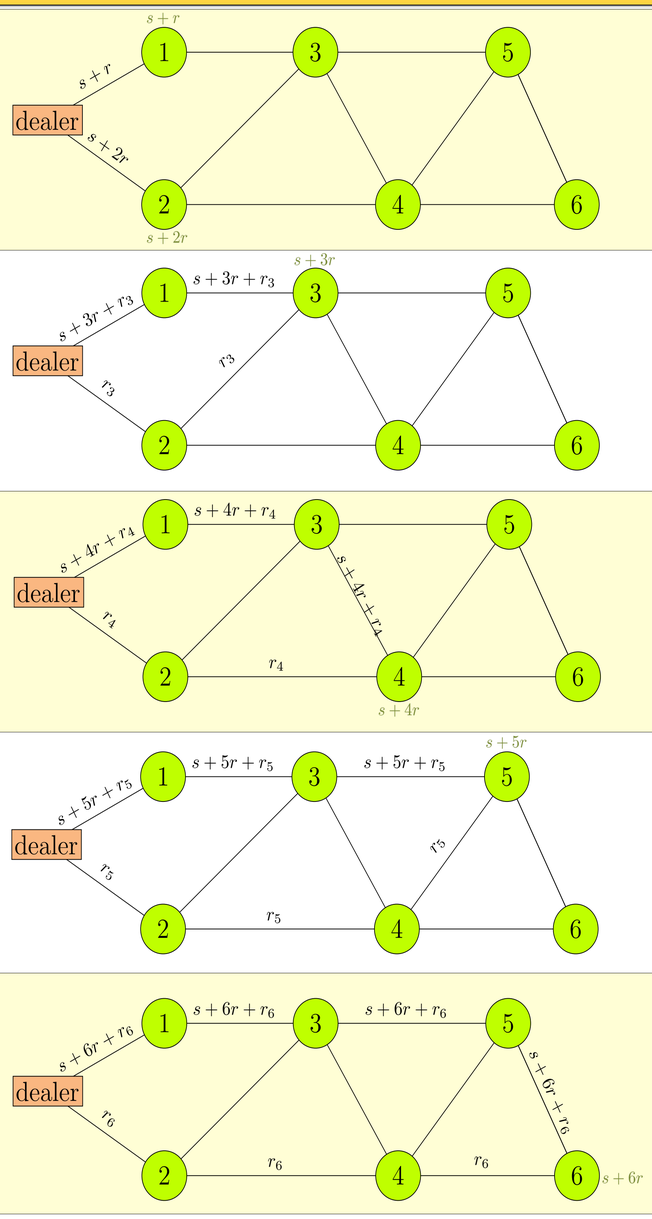
What if they are part of a general communication network ?



Applications

- Secure multiparty function computation
- Secure key distribution
- General Byzantine agreement between all nodes
- Archival storage
- Generating common random number across a network
- Proactive secret sharing

Literature

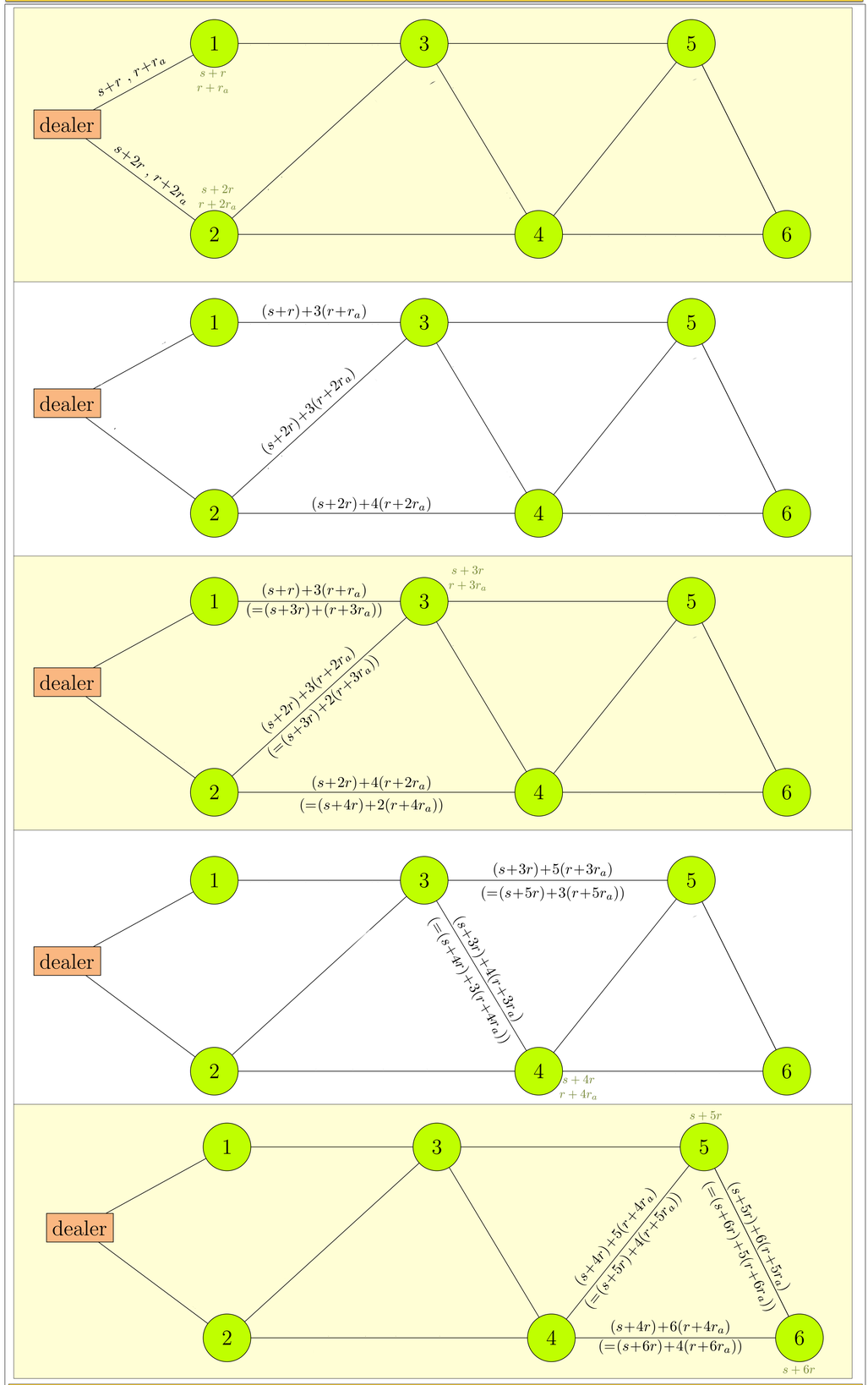


- Using pairwise agreement protocols (above)
- Another option: network coding
  - Eavesdropping nodes: hard

New Algorithm

- Distributed
- Deterministic (guaranteed)
- Communication optimal
- Computation efficient
- Distinctive instance of a network-coding algorithm that is both distributed and deterministic
  - Solution to nodal eavesdropping
- Works for a wide subclass of networks

Toy Example of the Algorithm



References

- "Optimal Exact-Regenerating Codes for Distributed Storage at the MSR and MBR Points via a Product-Matrix Construction", K. V. Rashmi, N. B. Shah and P. V. Kumar, IEEE Transactions on Information Theory, August 2011.
- "Information-theoretically Secure Regenerating Codes for Distributed Storage", N. B. Shah, K. V. Rashmi, and P. V. Kumar, Globecom 2011.
- "How to share a secret," A. Shamir, Communications of the ACM, Nov. 1979.
- "Completeness theorems for non-cryptographic fault-tolerant distributed computation," M. Ben-Or, S. Goldwasser, and A. Wigderson, STOC 1988.
- "Secret share dissemination across a network," N. B. Shah, K. V. Rashmi, K. Ramchandran, available on arXiv.