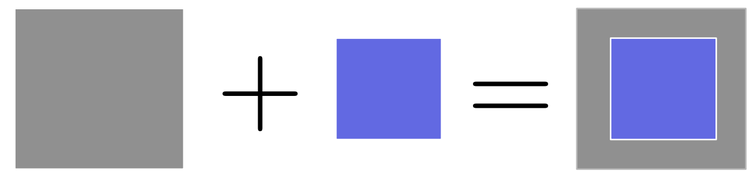
# Communication under Adversarial Attacks in Complex Networks

Joerg Kliewer
New Jersey Institute of Technology

**The objective of this project is to study coding schemes against adversaries in emerging complex network communication scenarios.**

- Investigate analytical tools to characterize the fundamental tradeoff between security and performance in adversarial networks
- Adversarial actions include jamming, Byzantine attacks, distributed Denial-of-Service attacks
- Use reductions to assess the information-theoretic security-performance trade-off
- Develop low-complexity coding schemes for features which have not been properly addressed in the literature:
  - multiple sources, independent demands
  - non-uniform links or non-uniform adversarial error sets, delay requirements

Reduction principle:



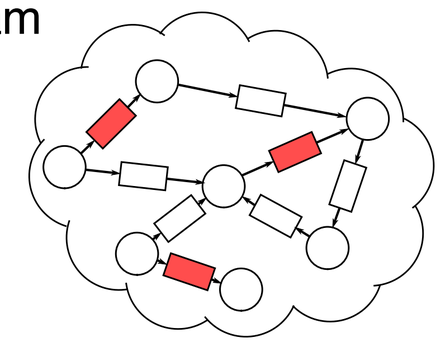

- Solution for problem A may be hard
- Solution for problem B may be easier and can be used to solve A

**Initial approach:**

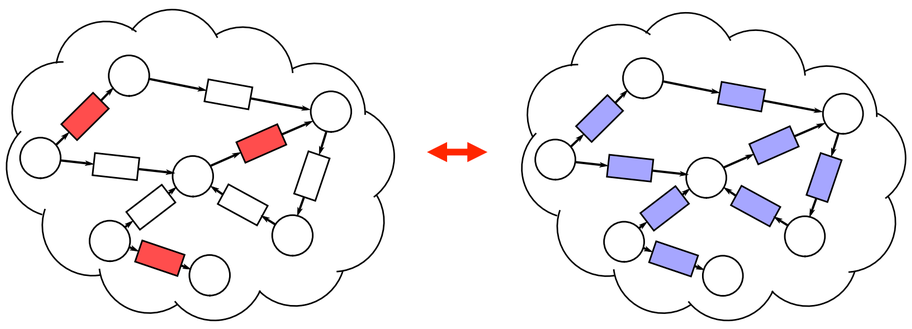
- Derive bounds on the network capacity in an omniscent adversarial settings (worst case performance)
- Idea: Transform adversarial into a non-adversarial problem by using reductions
- Classical bounding techniques from information theory can be applied to the non-adversarial case
- Bounds will be used as guidelines for code design

## Network equivalence for adversarial channels [Kosut & Kliewer, ITW 2016; arXiv.org 2016]

- Adversary selects a set of channels he decides to jam



- Under a fully connected assumption network can be transformed into an equivalent network with noiseless (stateless) bitpipes → capacity bounds well known from standard network IT

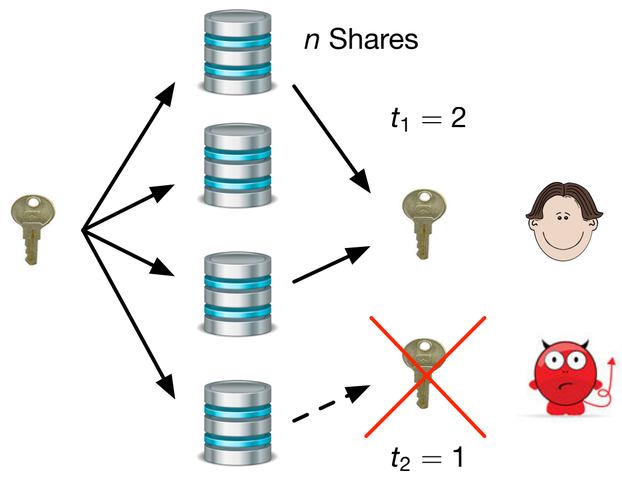


## Communication efficient secret sharing

[Huang, Langberg, Kliewer, Bruck, IEEE Trans IT, Dec. 2016]

*Threshold secret sharing scheme*:

- Secret is encoded into $n$ shares, such that any set of at least $t_1$ shares suffice to decode the secret, and any set of at most $t_2 < t_1$ shares reveal no information about the secret
- Designed a scheme that achieves optimal decoding bandwidth when $d$ parties participate, universally for all $t_2 \leq d \leq n$




Interested in meeting the PI? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

NJIT New Jersey's Science & Technology University