

SECURE KEY EXCHANGE IN WIRELESS NETWORKS



ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

László Czap, Christina Fragouli

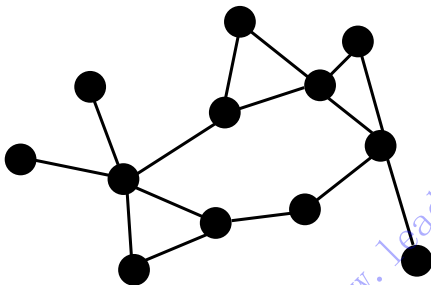
NetCod 2011

July 25, 2011

<http://www.leaderstudio.net/>

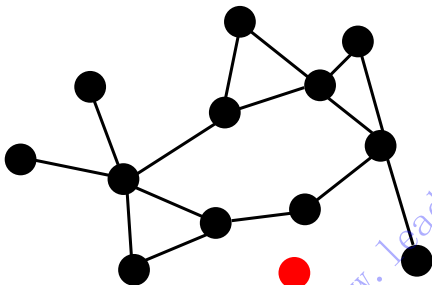
PROBLEM STATEMENT

Group key in wireless network



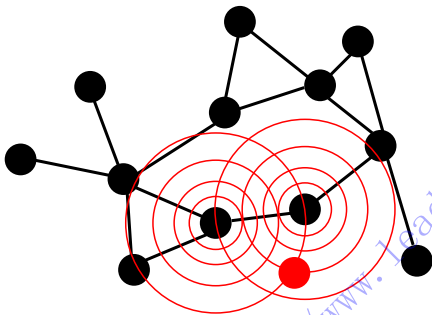
PROBLEM STATEMENT

Group key in wireless network



PROBLEM STATEMENT

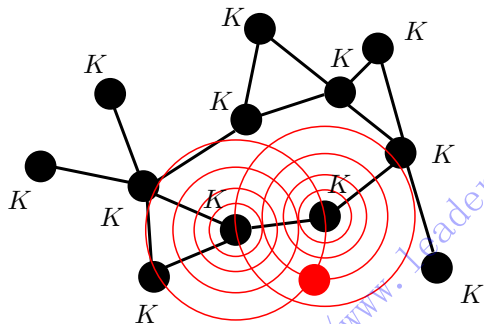
Group key in wireless network



PROBLEM STATEMENT

Group key in wireless network

$$K = [1011100110001]$$



RELATED WORK

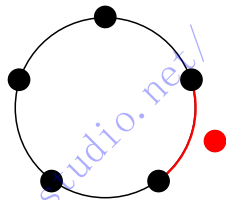
- Key exchange over a noisy point-to-point channel
 - Wyner's wiretap channel [1]
 - With feedback [2]
- Key exchange in groups
 - With free public channel available [3, 4]

- [1] A. D. Wyner, "The wire-tap channel," *The Bell system Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [2] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [3] I. Csiszár and P. Narayan, "Secrecy capacities for multiterminal channels," *IEEE Transactions on Information Theory*, vol. 54, no. 8, pp. 2437–2452, 2008.
- [4] S. Diggavi, C. Fragouli, M. Jafari Siavoshani, U. K. Pulleti, and K. Argyraki, "Group secret key generation over broadcast erasure channels," in *Asilomar Conference on Signals, Systems, and Computers*, 2010.

SIMPLIFIED MODEL

Network setting:

- Circle topology, broadcast transmissions
- Two channel modes: independent erasures/reliable transmissions
- Eve eavesdrops on any one link of her choice



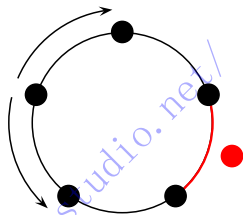
Requirement and performance metric:

- K is computable for every node,
 $H(K|Z) \approx H(K)$
- Efficiency: $\frac{\text{\#of wireless transmissions}}{\text{size of } K}$

SIMPLIFIED MODEL

Network setting:

- Circle topology, broadcast transmissions
- Two channel modes: independent erasures/reliable transmissions
- Eve eavesdrops on any one link of her choice



Requirement and performance metric:

- K is computable for every node,
 $H(K|Z) \approx H(K)$
- Efficiency: $\frac{\text{\#of wireless transmissions}}{\text{size of } K}$

DESIGN OF ACHIEVABILITY SCHEMES

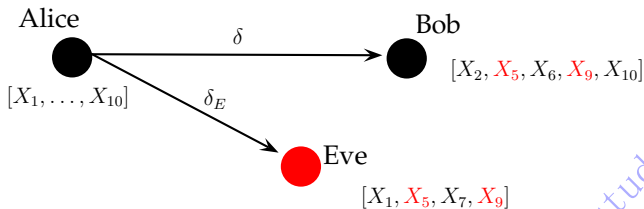
What we can benefit from?

- Erasures towards Eve
- Topology of the network

<http://www.leaderstudio.net/>

SECRECY OVER THE ERASURE CHANNEL

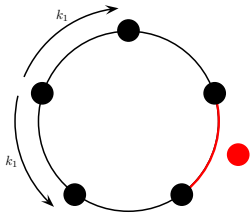
Two party case (e.g. $\delta = 0.5, \delta_E = 0.6$):



- Bob can form 3 linear combinations independent from Eve's knowledge
- The same principle works in a group with an additional public reconciliation phase

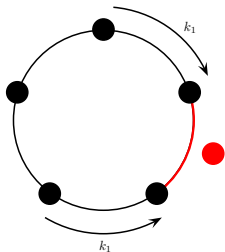
SECRECY FROM TOPOLOGY

E.g. $\delta_E = 0$



SECURITY FROM TOPOLOGY

E.g. $\delta_E = 0$



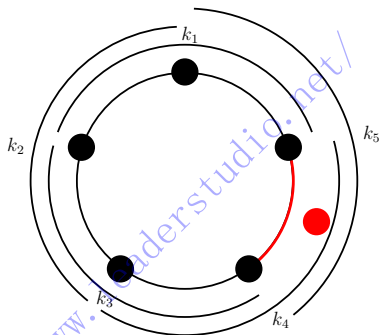
- k_1 would be secret from Eve, but we don't know where Eve is
- \Rightarrow run the same in parallel at every node

$$K = k_1 \oplus k_2 \oplus k_3 \oplus k_4 \oplus k_5$$

- Advantage: efficient broadcast

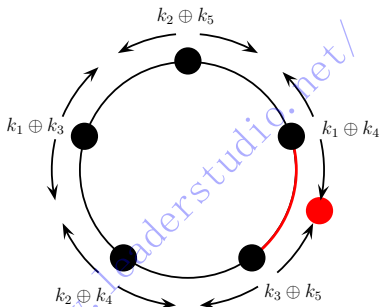
ACHIEVABILITY SCHEME

1. Local key exchange over the erasure channel



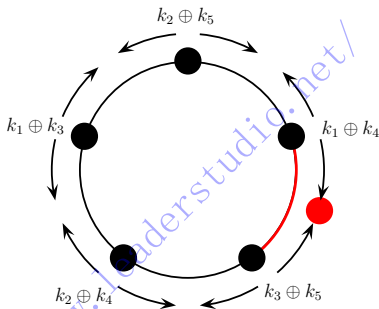
ACHIEVABILITY SCHEME

1. Local key exchange over the erasure channel
2. Dissemination of local keys



ACHIEVABILITY SCHEME

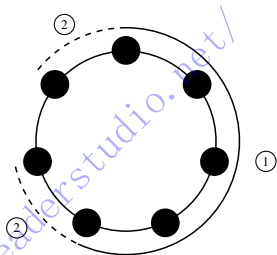
1. Local key exchange over the erasure channel
2. Dissemination of local keys
 - Eve learns 2 combinations
 \Rightarrow we can create 3 combinations securely



GENERAL SCHEME

Major steps (run in parallel at every node):

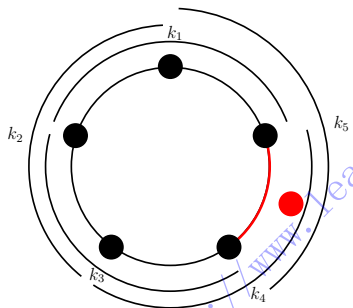
1. Local key exchange in the k -hop neighborhood
2. Disseminate local keys to the rest of the network



PARAMETERS

Two parameters to set:

- k : Number of hops for the local key exchange
 - More hops are more expensive, but more secure
- β : Size of the exchanged key
 - It may not worth to conservatively create keys



PERFORMANCE EVALUATION

$$A = 2 \sum_{i=1}^k N \delta_E (\beta(1 - \delta^2) - (1 - \delta)^i)^+$$

$$\mathcal{K} = (2d + 1)N \delta_E \beta(1 - \delta^2) - A - 2(d - k)N \delta_E \beta(1 - \delta^2)$$

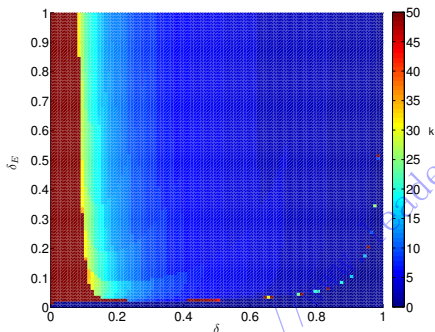
$$\mathcal{C} = N \left(\delta_E(1 - \delta^2)(d\beta + k(1 - \beta)) + \frac{1 - (1 - \delta)^k}{\delta} (1 - \delta_E(1 - \delta)) \right)$$

$$\frac{(2d + 1)\mathcal{C}}{\mathcal{K}}$$

PARAMETER VALUES

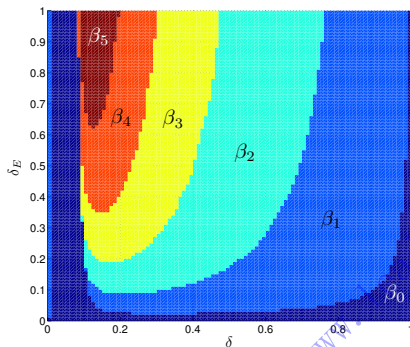
If Eve's channel is too good, we set $k = 0$

$$\delta_E \leq \frac{1}{n(1 - \delta)}$$



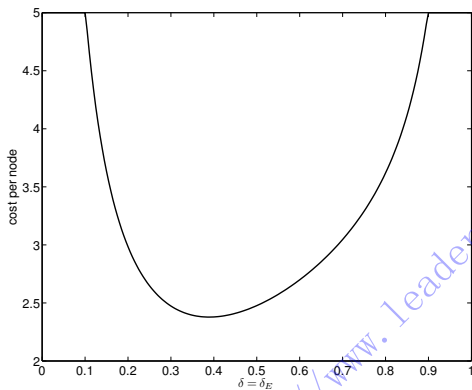
PARAMETER VALUES

β_i means that local keys are perfectly secure up to the i th hop



COST OF KEY SETUP

of wireless transmissions per node to set up a unit size key



SUMMARY

- Group keys for multi-hop wireless networks
- Achievability scheme in a simplified model
- Parameters that influence the performance
- Generalizations? Theoretical bounds?