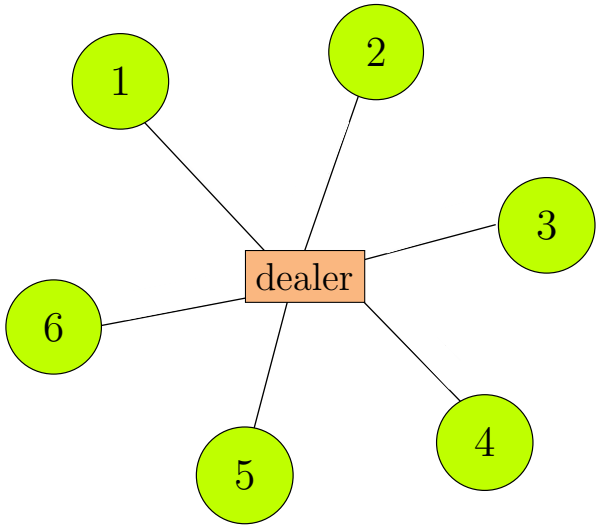
# Secret Sharing Across a Network with Low Communication Cost: Distributed Algorithm and Bounds

Nihar B Shah, K V Rashmi, Kannan Ramchandran

University of California, Berkeley

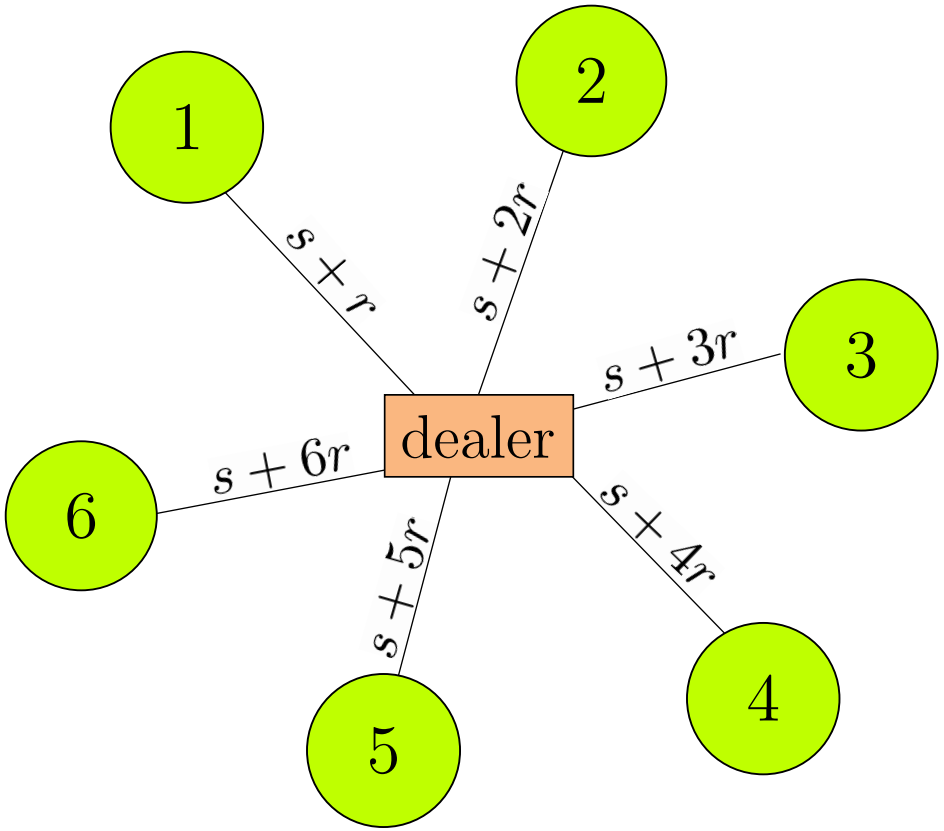
# Secret Sharing

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




n = 6

# Example: n = 6, k = 2




- alphabet is $\mathbf{F}_7$
- r is chosen uniformly at random from the field

# Applications

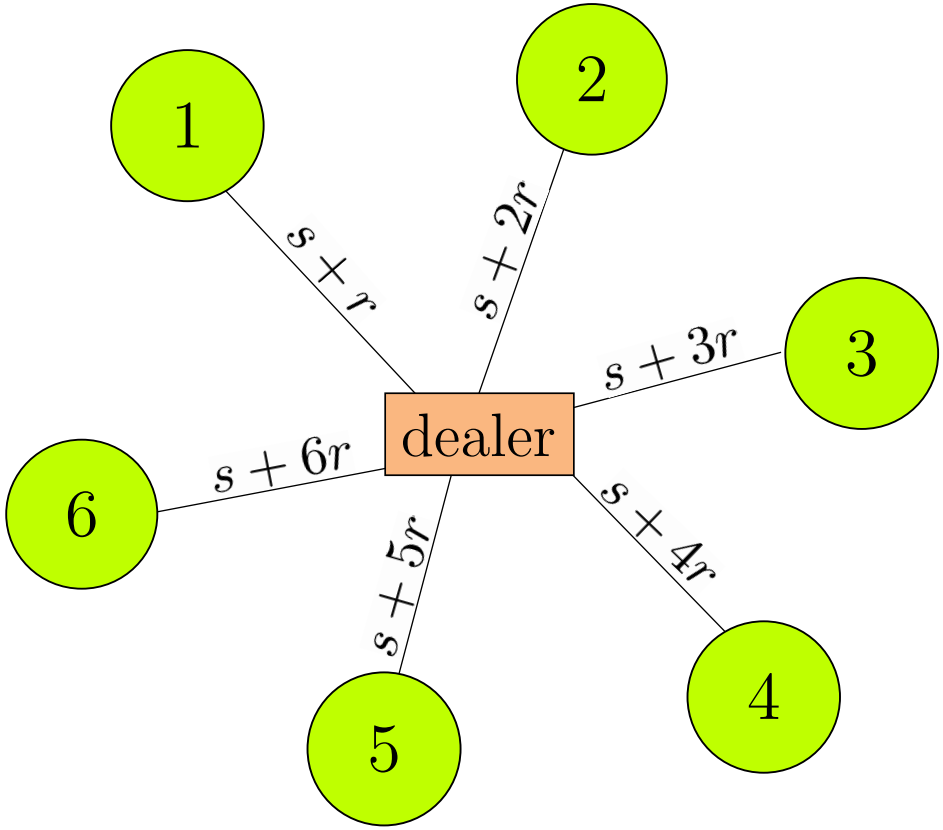
Several cryptographic protocols use Shamir's secret sharing:

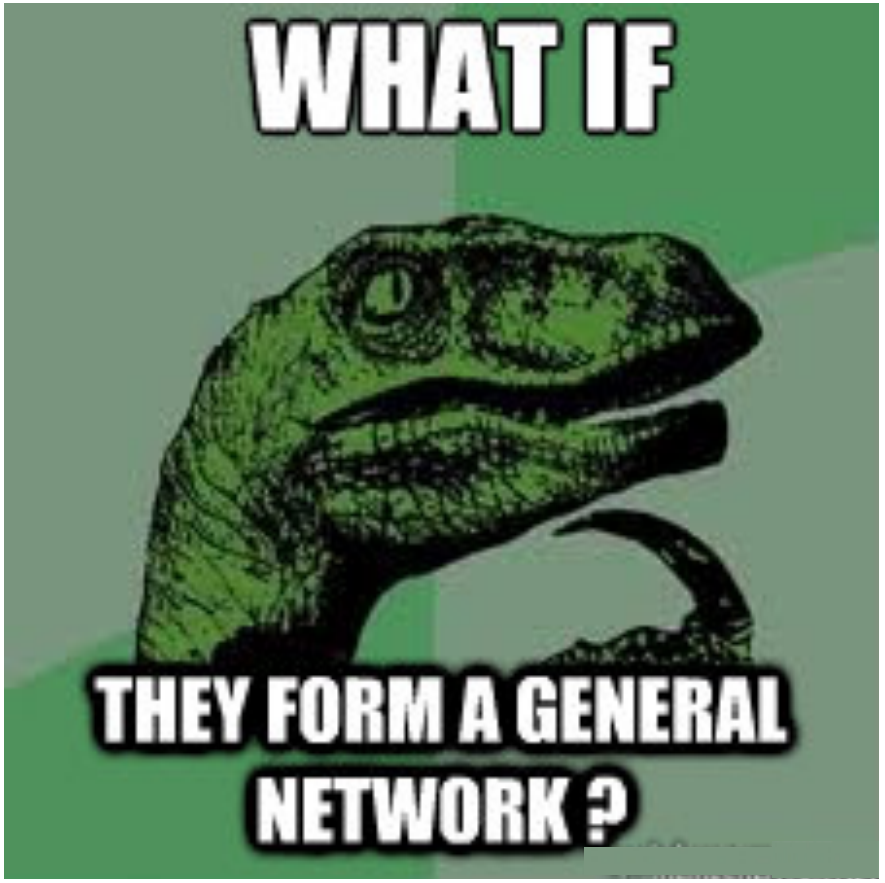
- Secure multiparty function computation
- Key distribution
- Archival storage

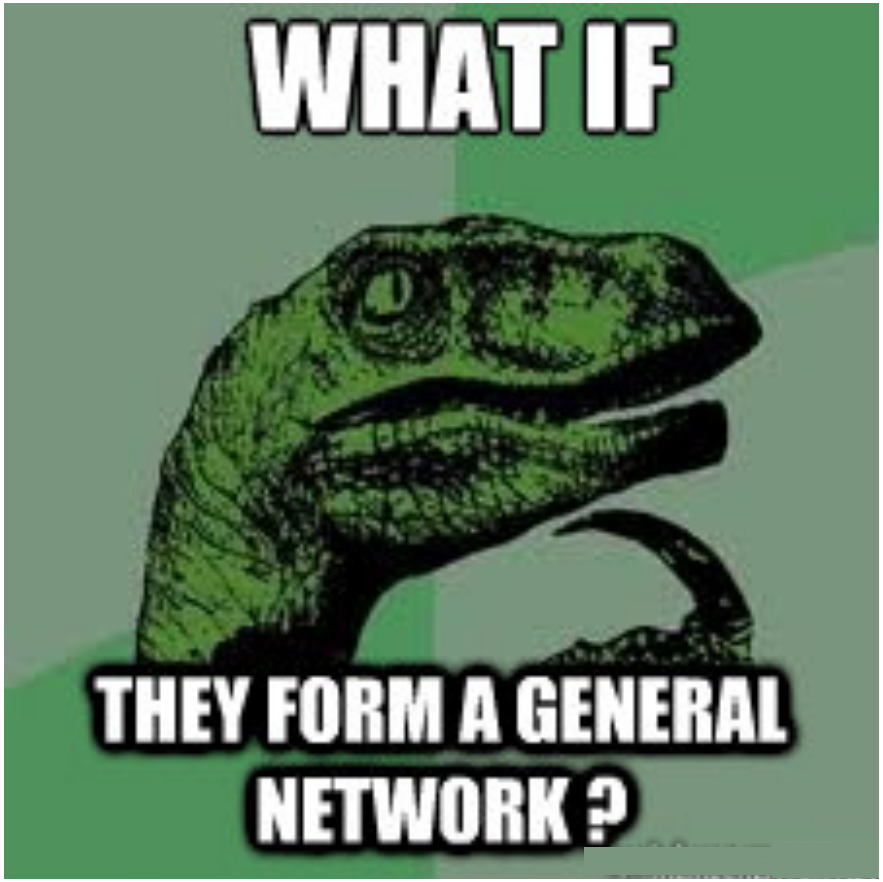


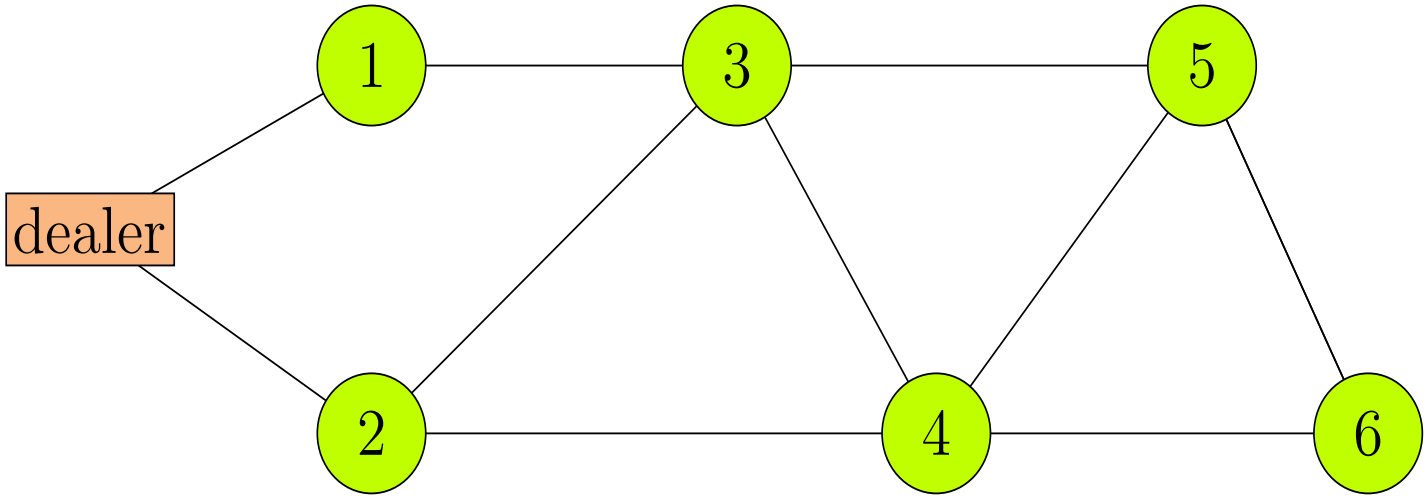
e.g., Ben-Or–Goldwasser–Wigderson (BGW) protocol for secure n-party function computation: 2n secret sharings initially, n more for each multiplication

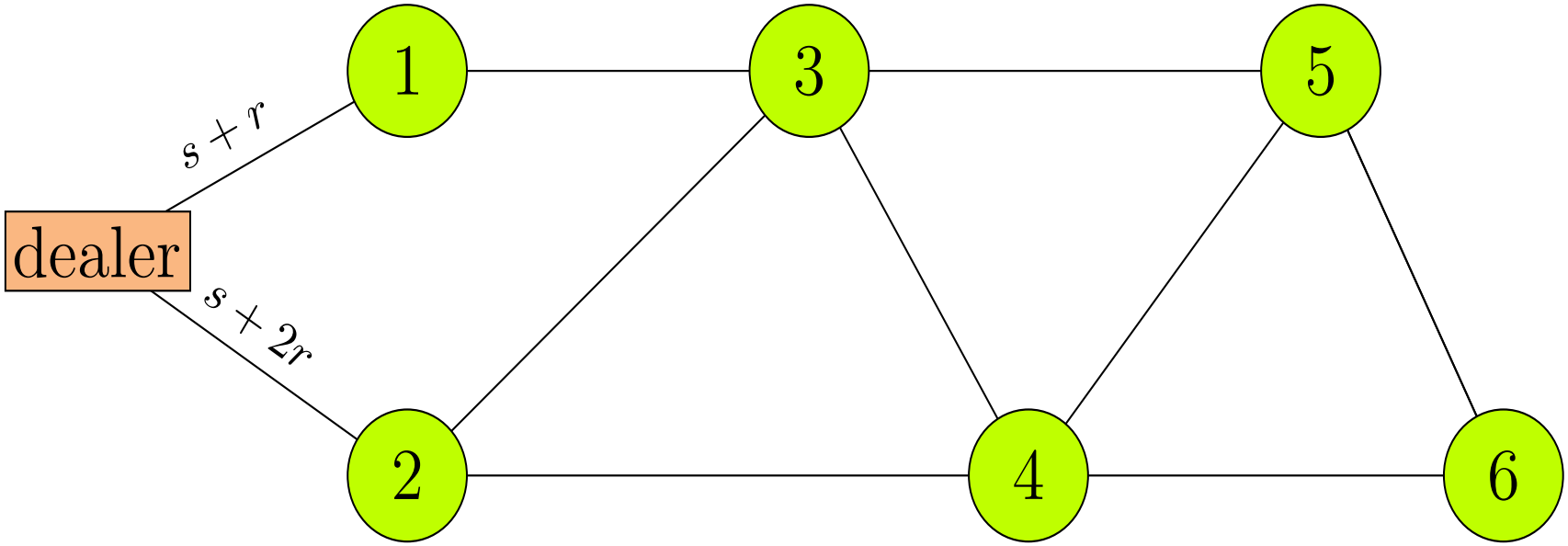
# Most protocols assume dealer can communicate directly with all participants

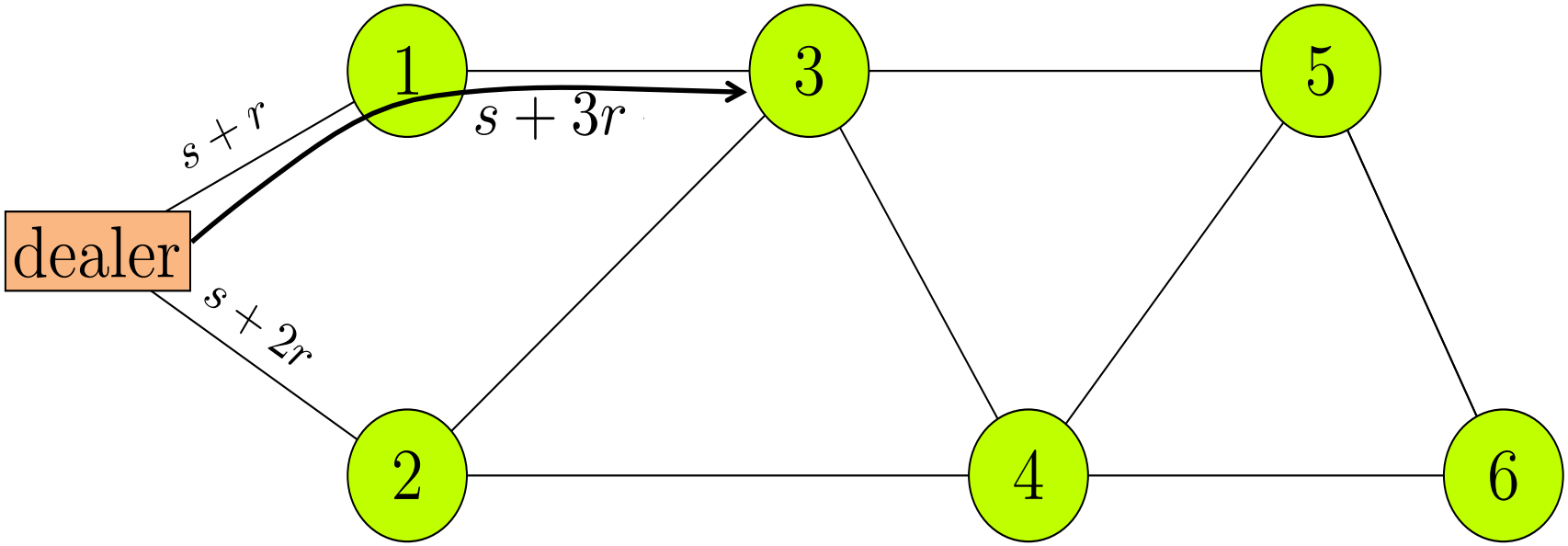



WHAT IF
THEY FORM A GENERAL NETWORK ?

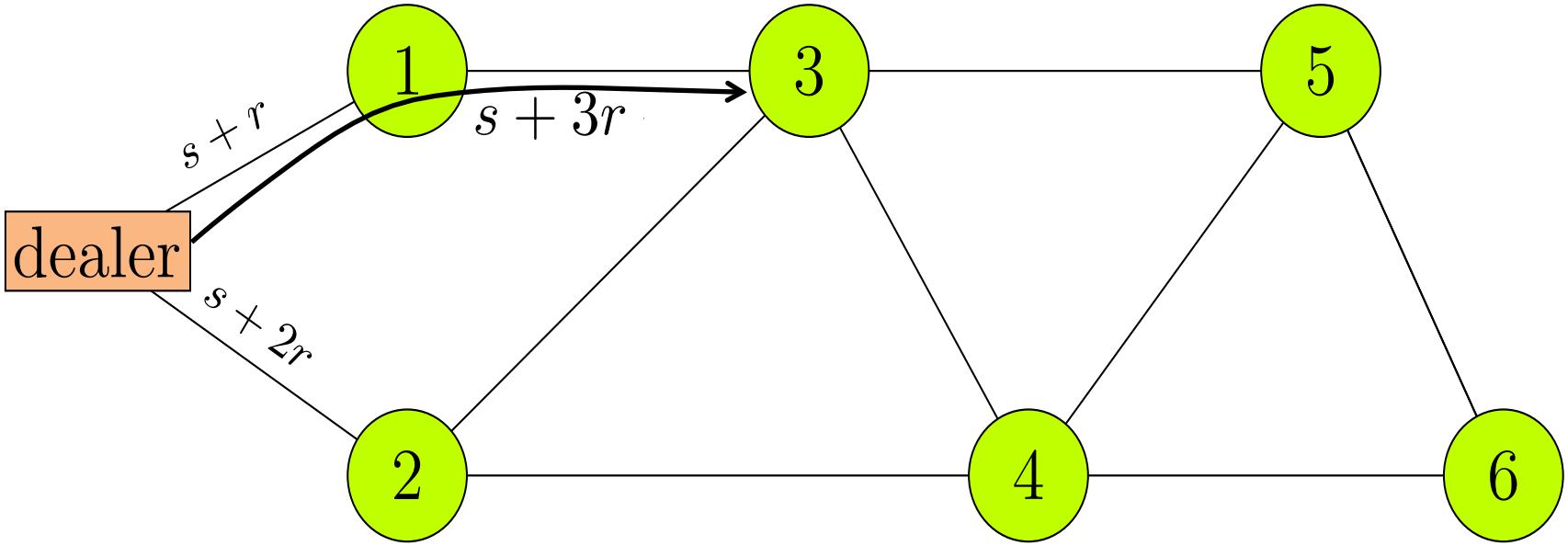

WHAT IF
THEY FORM A GENERAL NETWORK ?


dealer
1
2
3
4
5
6

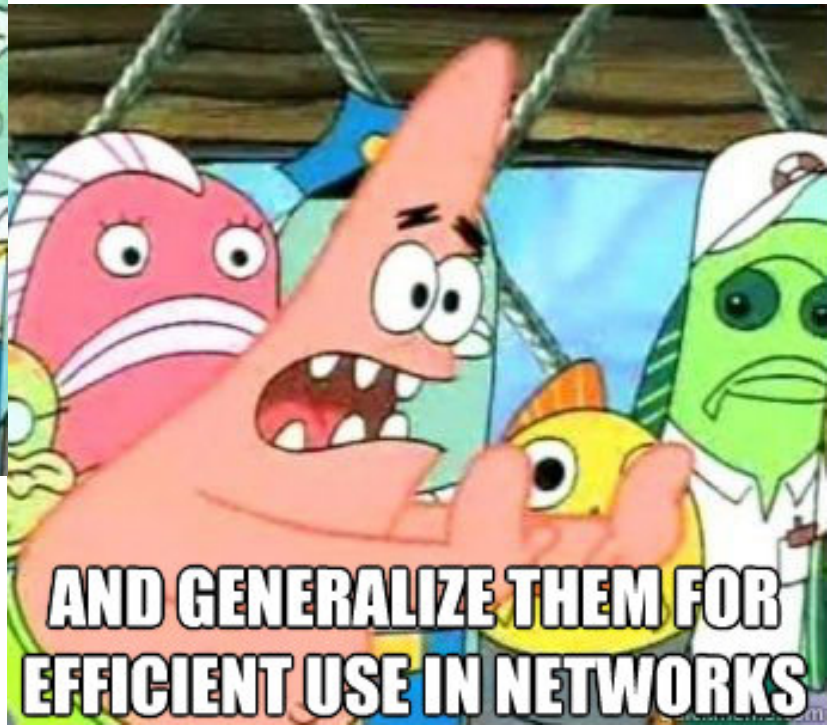

dealer
$s + r$
$s + 2r$
1
2
3
4
5
6


dealer
1
2
3
4
5
6
$s+r$
$s+2r$
$s+3r$

**not allowed:**
**participant 1 can obtain secret**



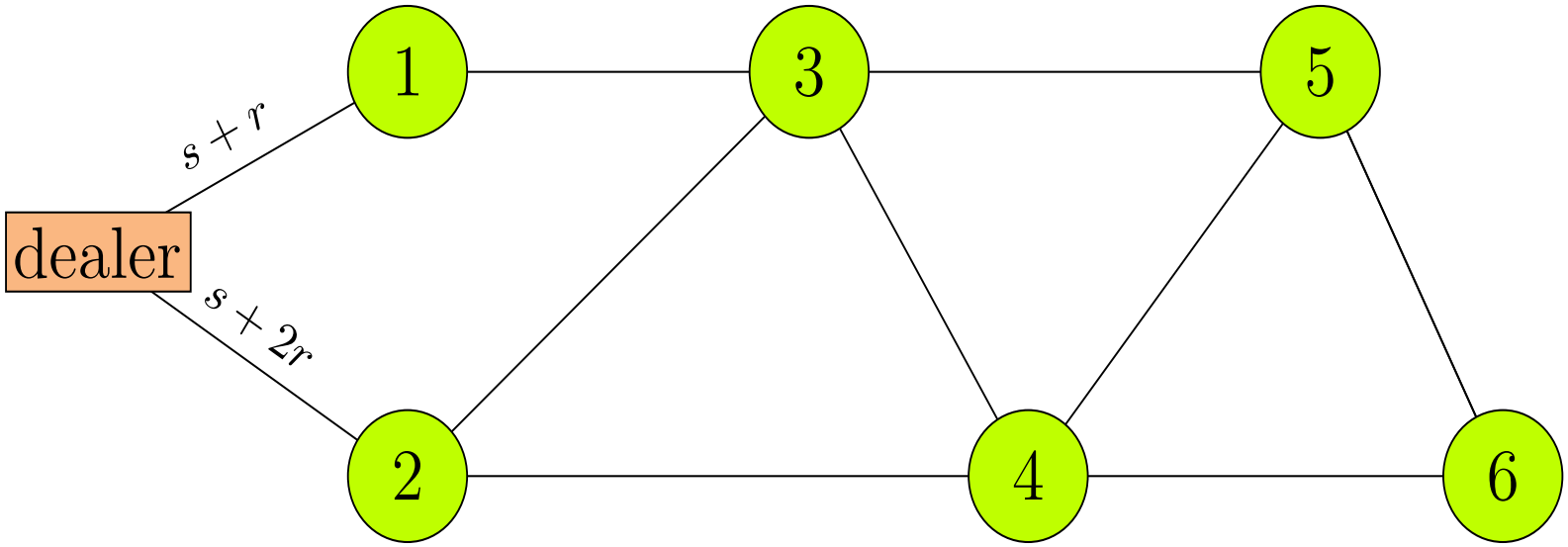
# Secret sharing across networks

# Outline

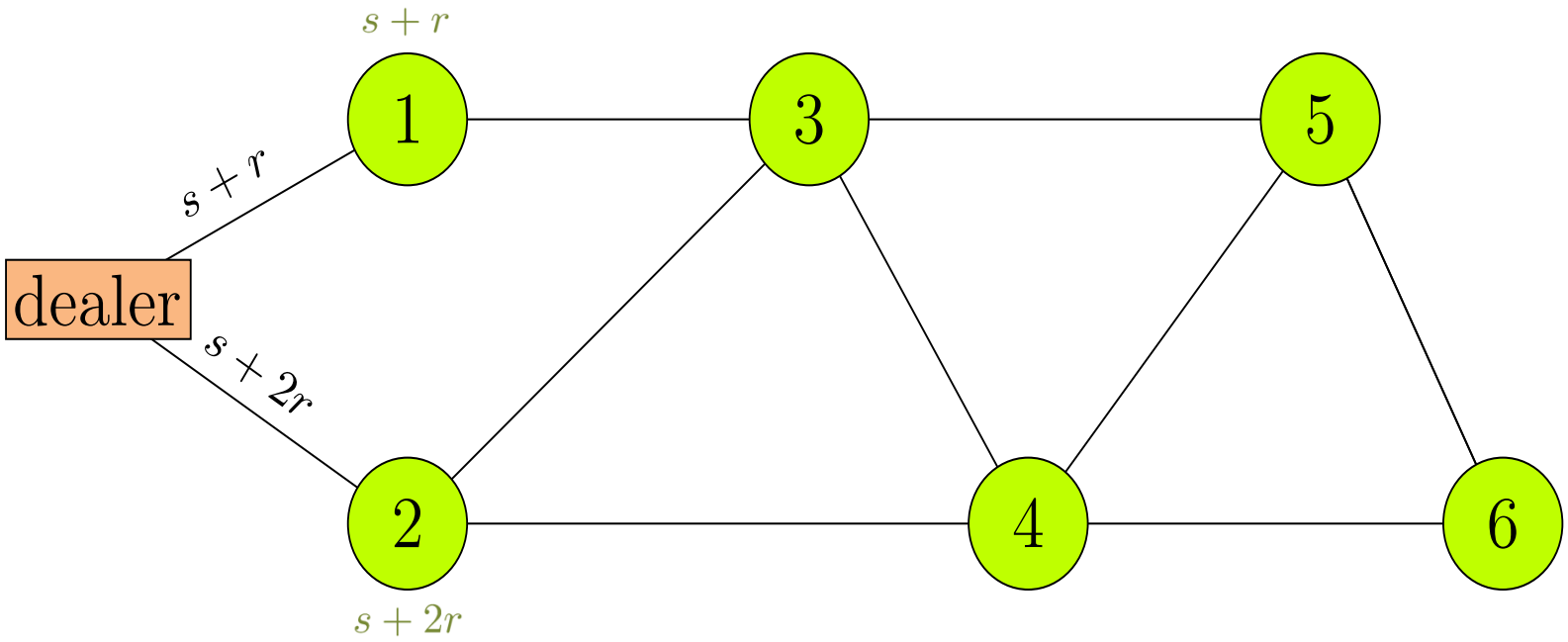
- Literature
- New “SNEAK” algorithm
- Information-theoretic lower bounds
- Summary & open problems

# Literature: Pairwise agreement protocols

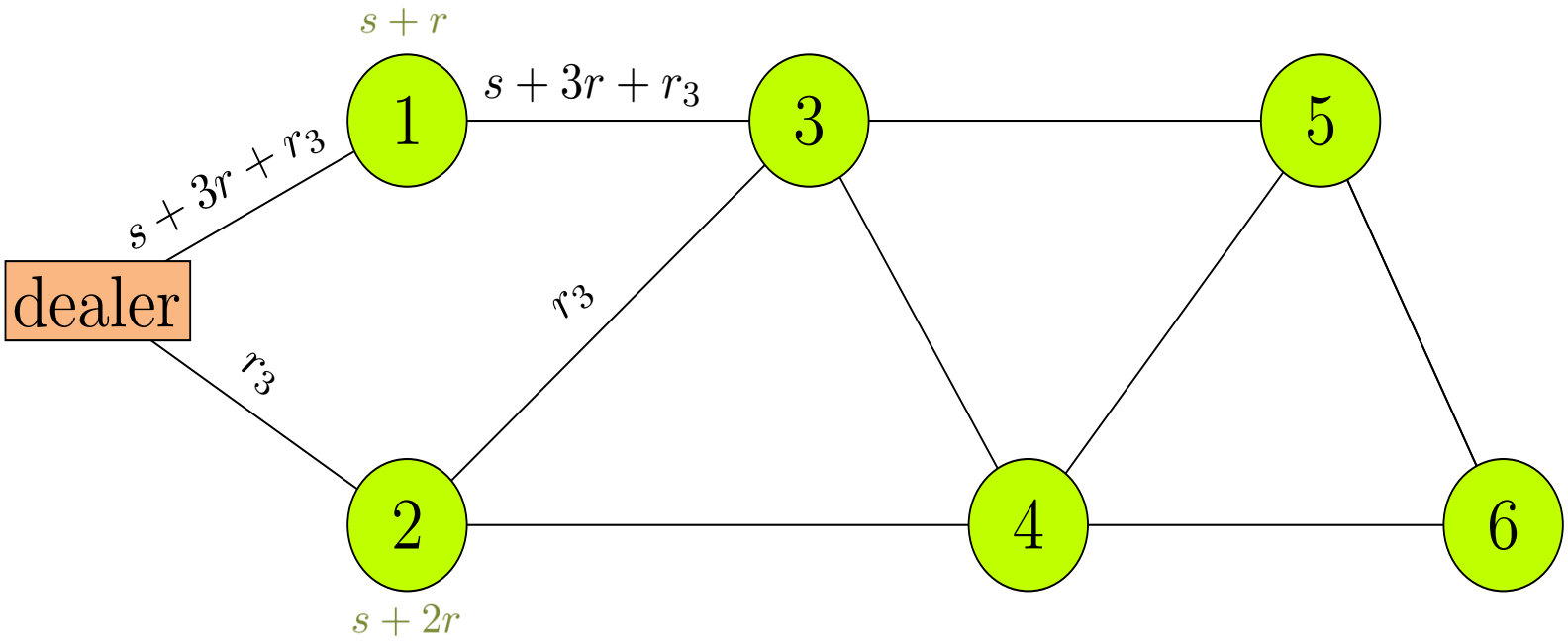



D. Dolev, C. Dwork, O. Waarts, and M. Yung, "Perfectly secure message transmission," *Journal of the ACM*, vol. 40, no. 1, pp. 17–47, 1993.

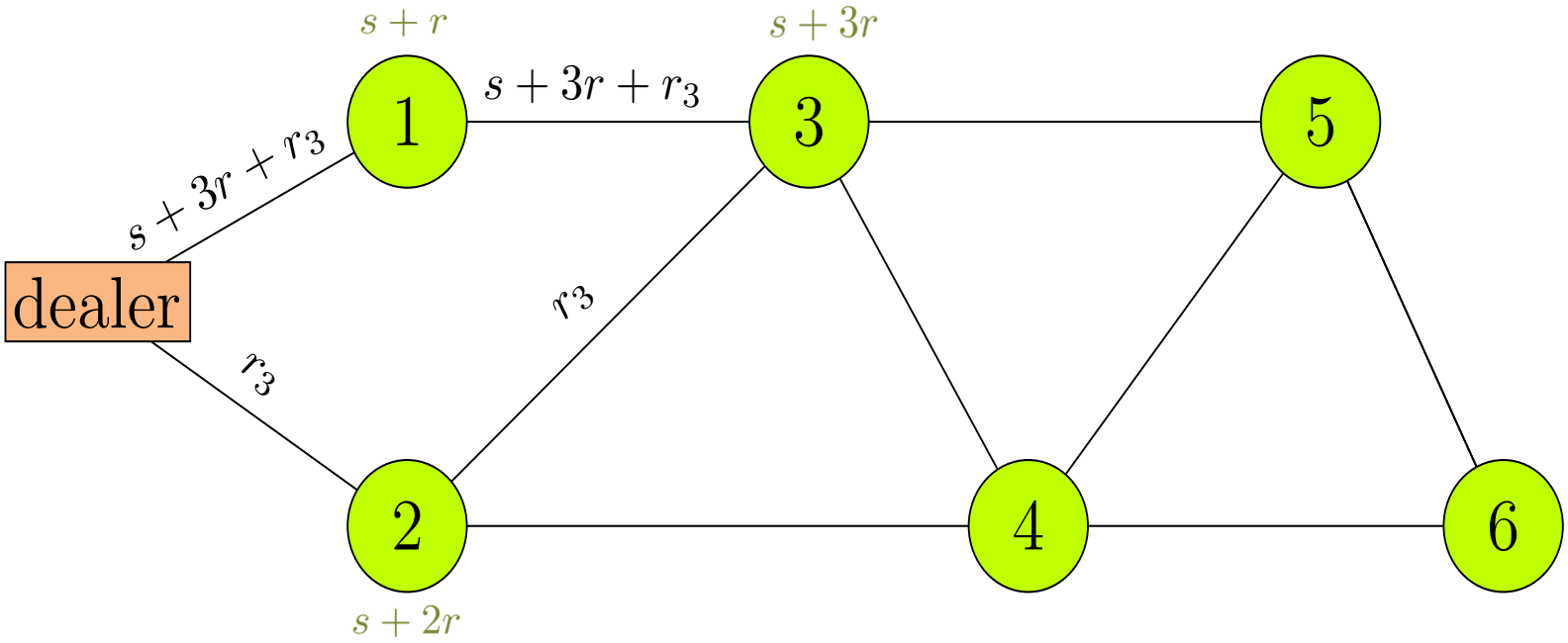
# Literature: Pairwise agreement protocols



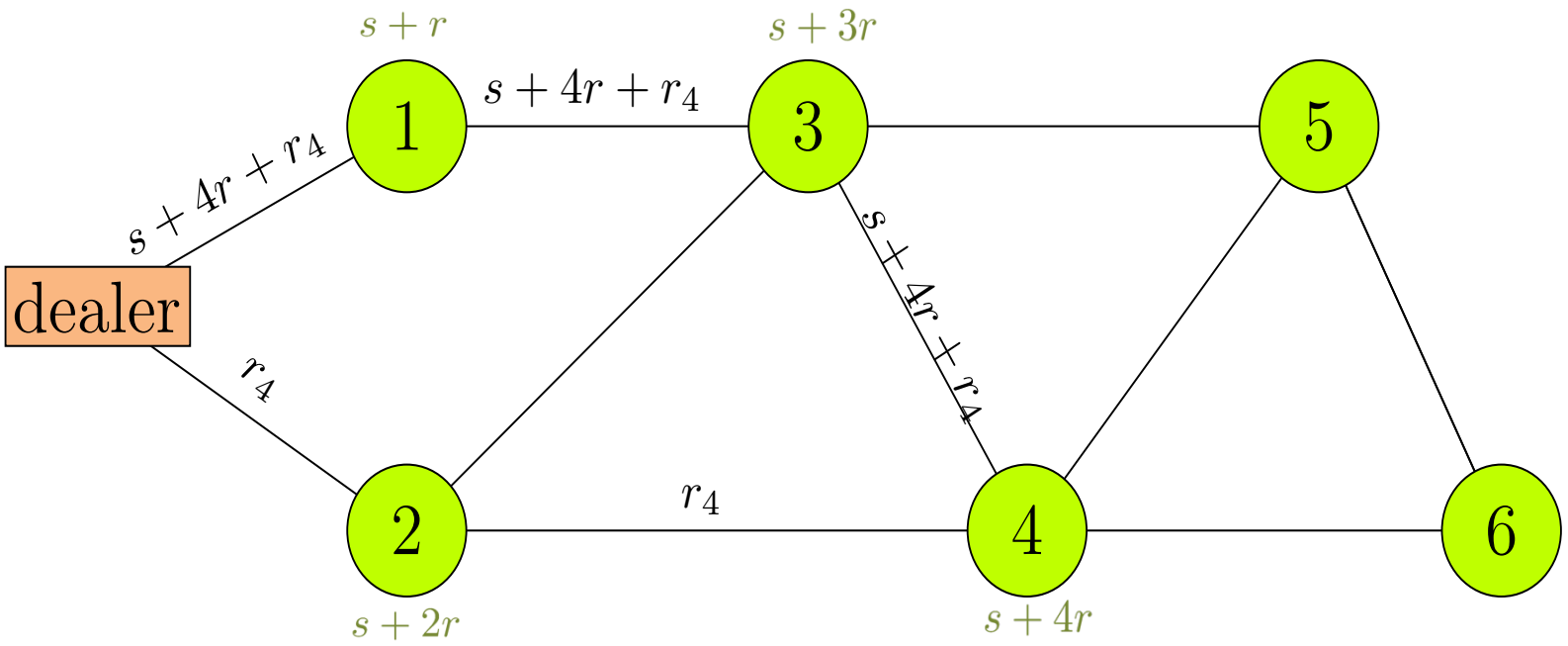
# Literature: Pairwise agreement protocols



# Literature: Pairwise agreement protocols



# Literature: Pairwise agreement protocols



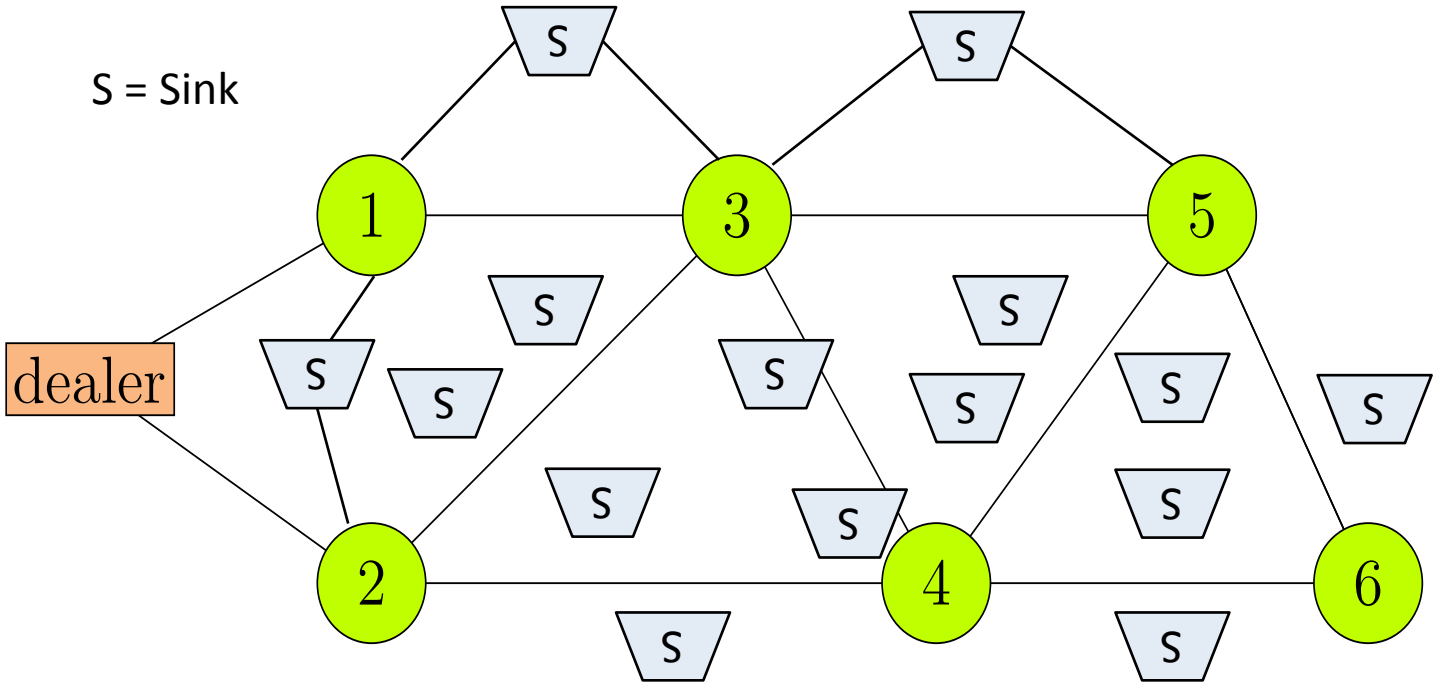

For every participant i :

1. Dealer finds k node disjoint paths to i
2. Computes secret shares of this i's share
3. Transmits these new shares on these k paths

# Literature: Pairwise agreement protocols

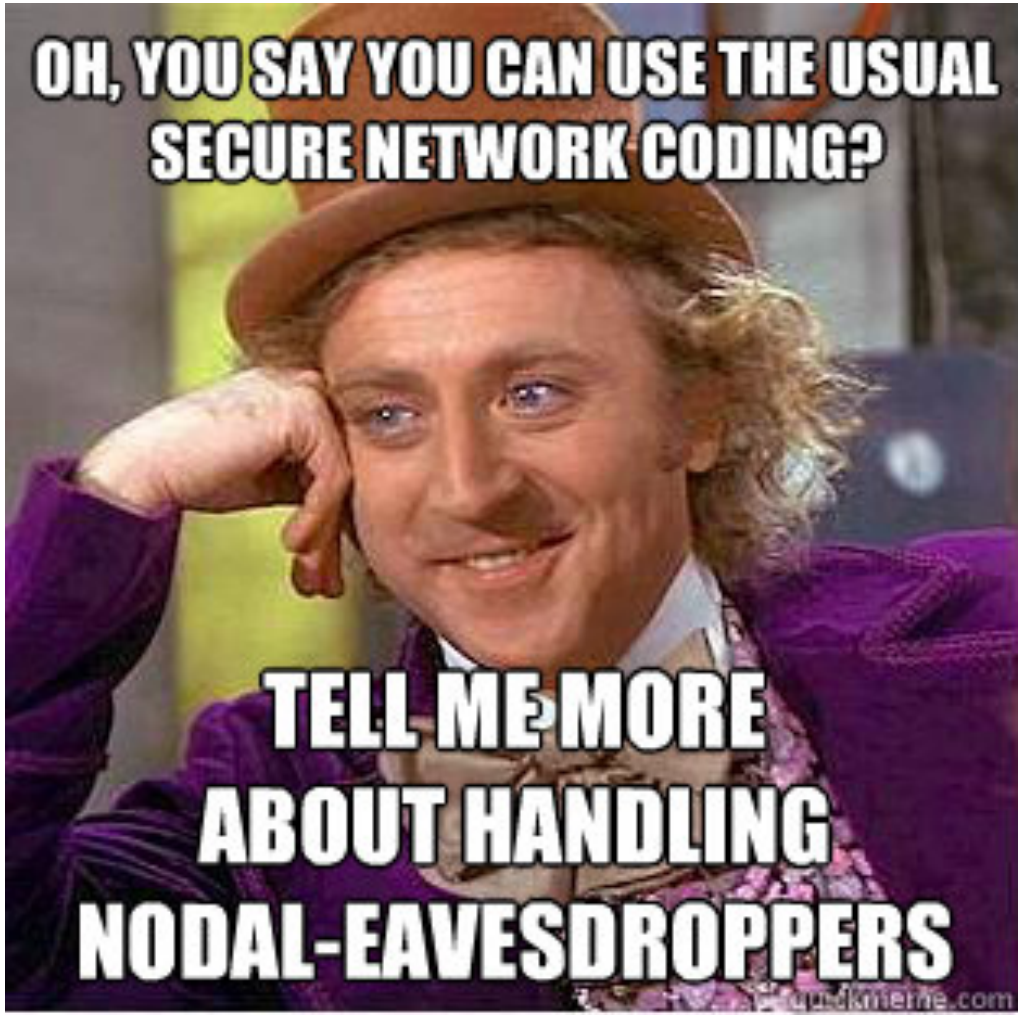
- Communication inefficient
- High amount of randomness
- Significant coordination in the network

# Literature: Secure Network Coding



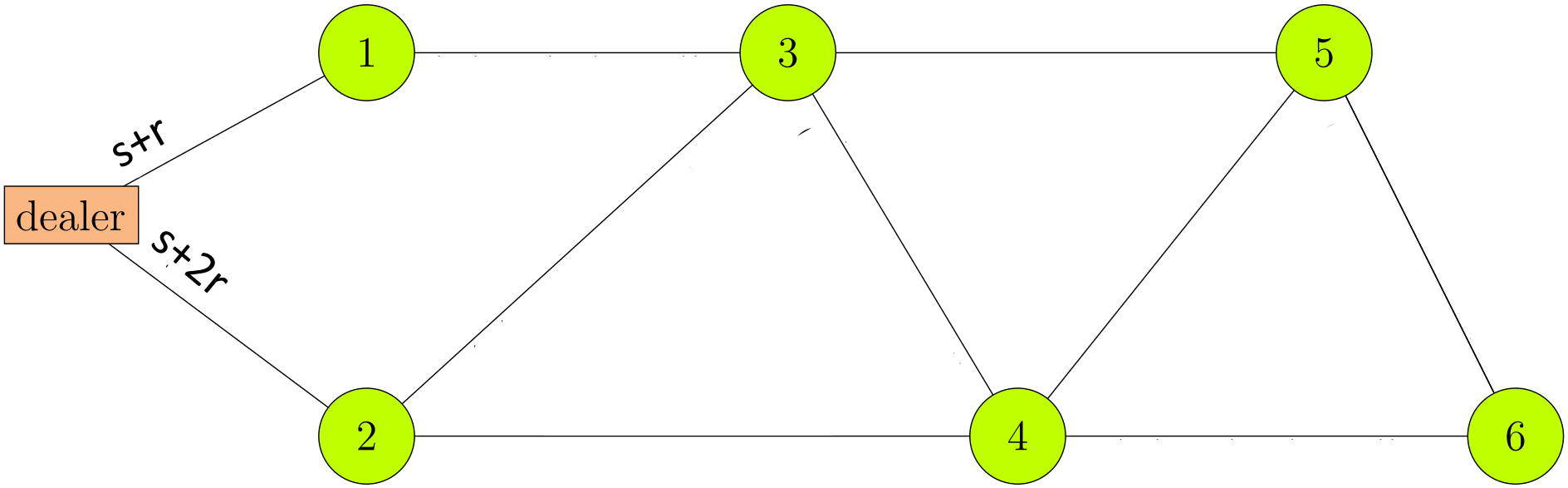

- Every set of k participants has a sink
- Eavesdropping of any (k-1) **nodes** should leak no information

# Nodal-eavesdropping: Very little known

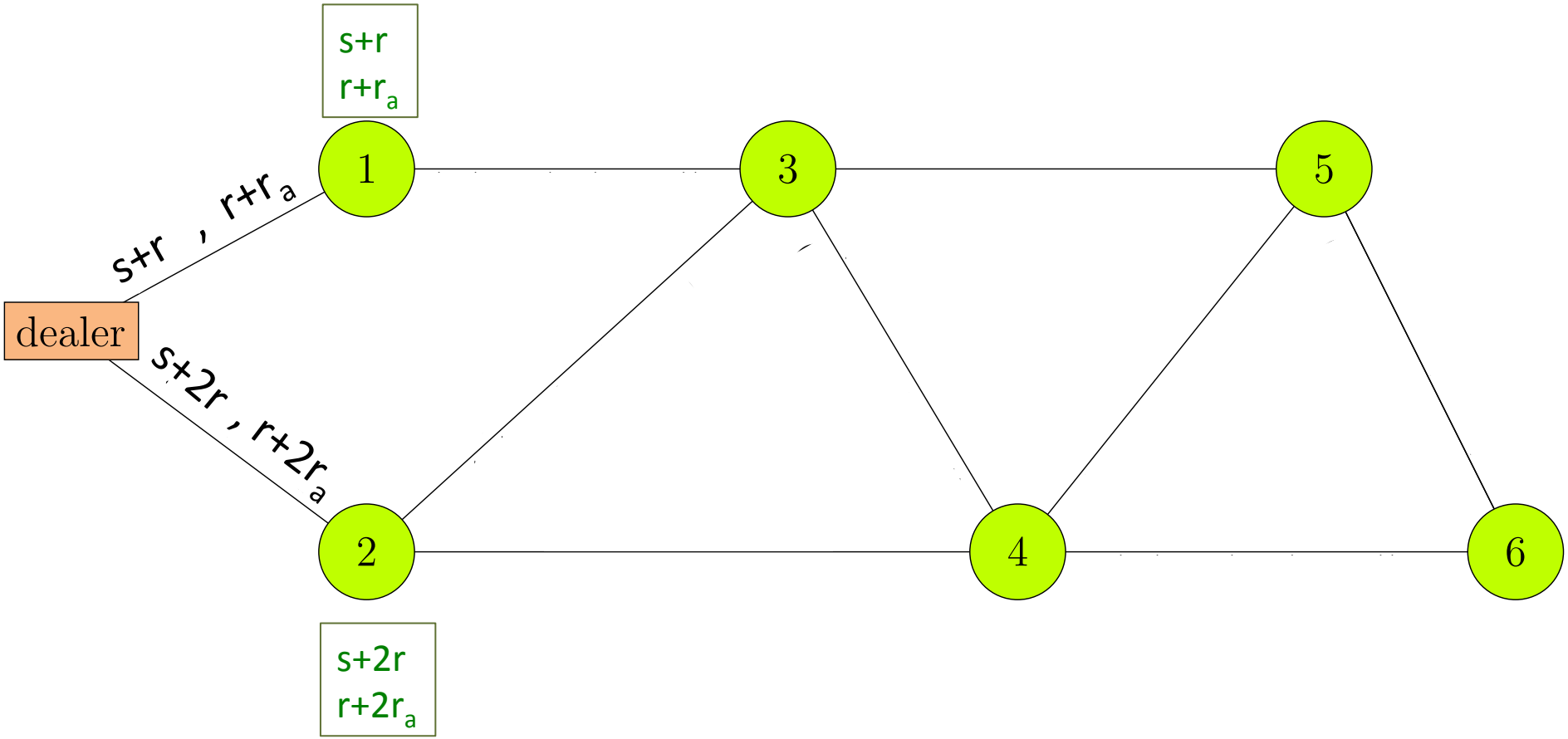


# Our “SNEAK” algorithm

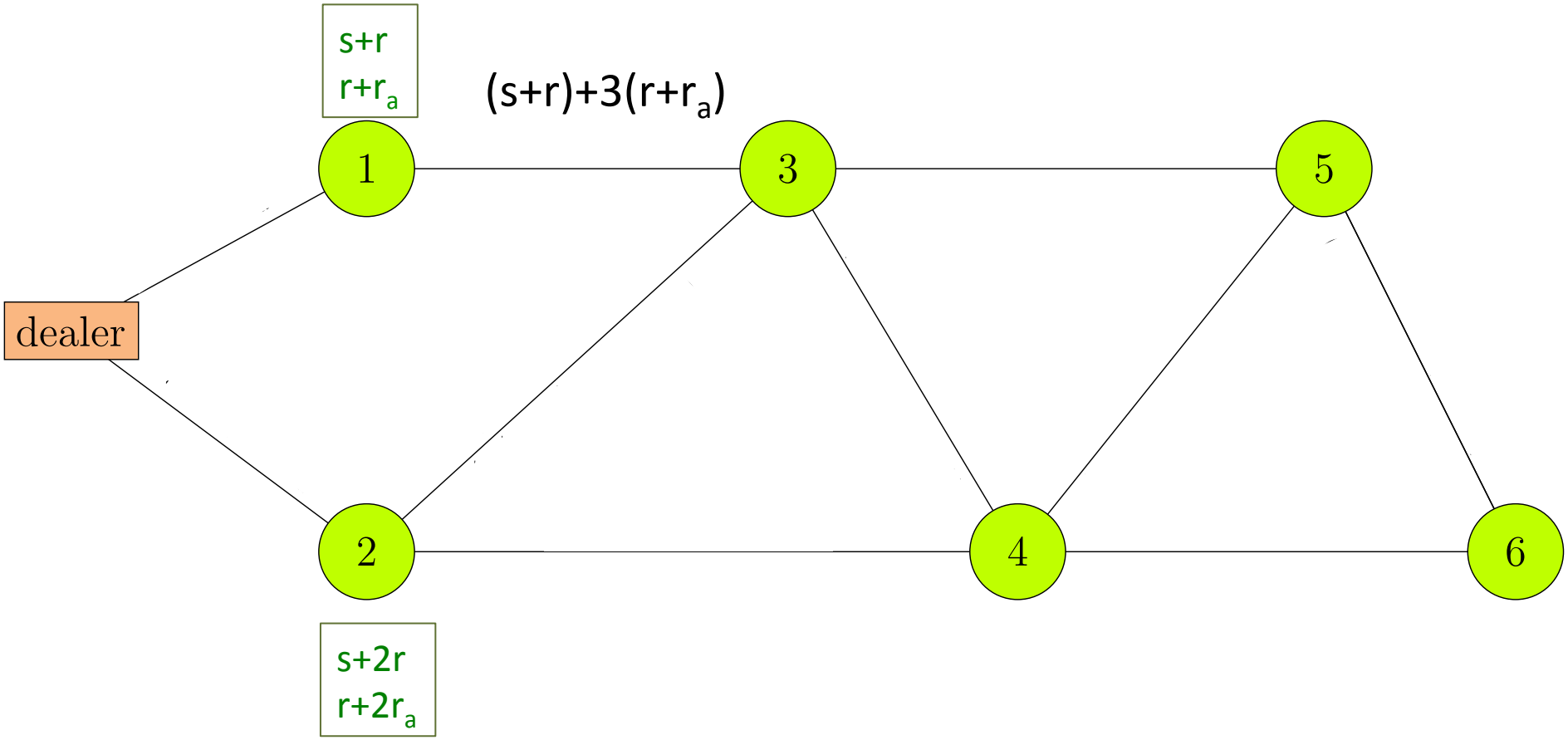

SNEAK = Secret-sharing over a Network with Efficient communication
And distributed Knowledge-of-topology



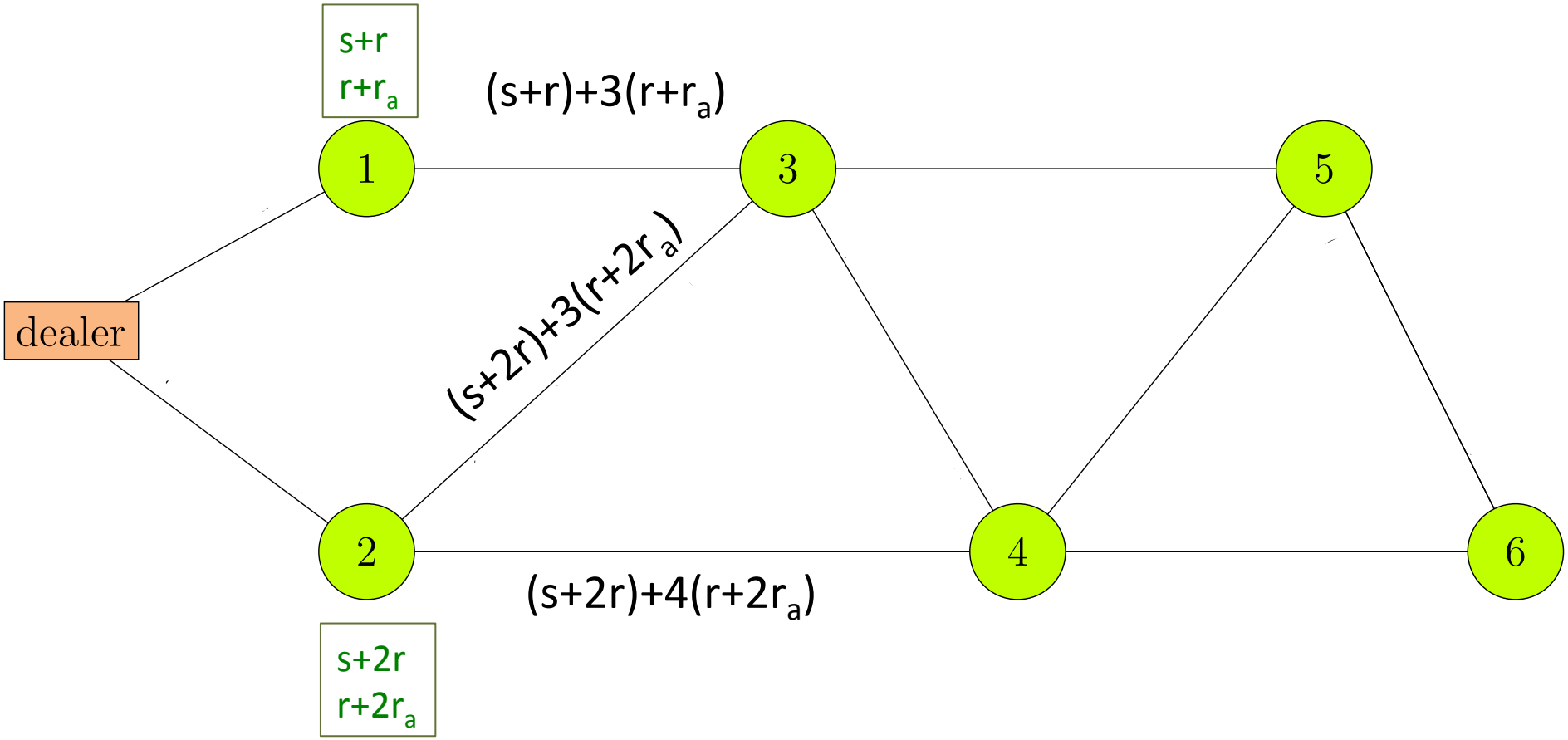

SNEAK algorithm



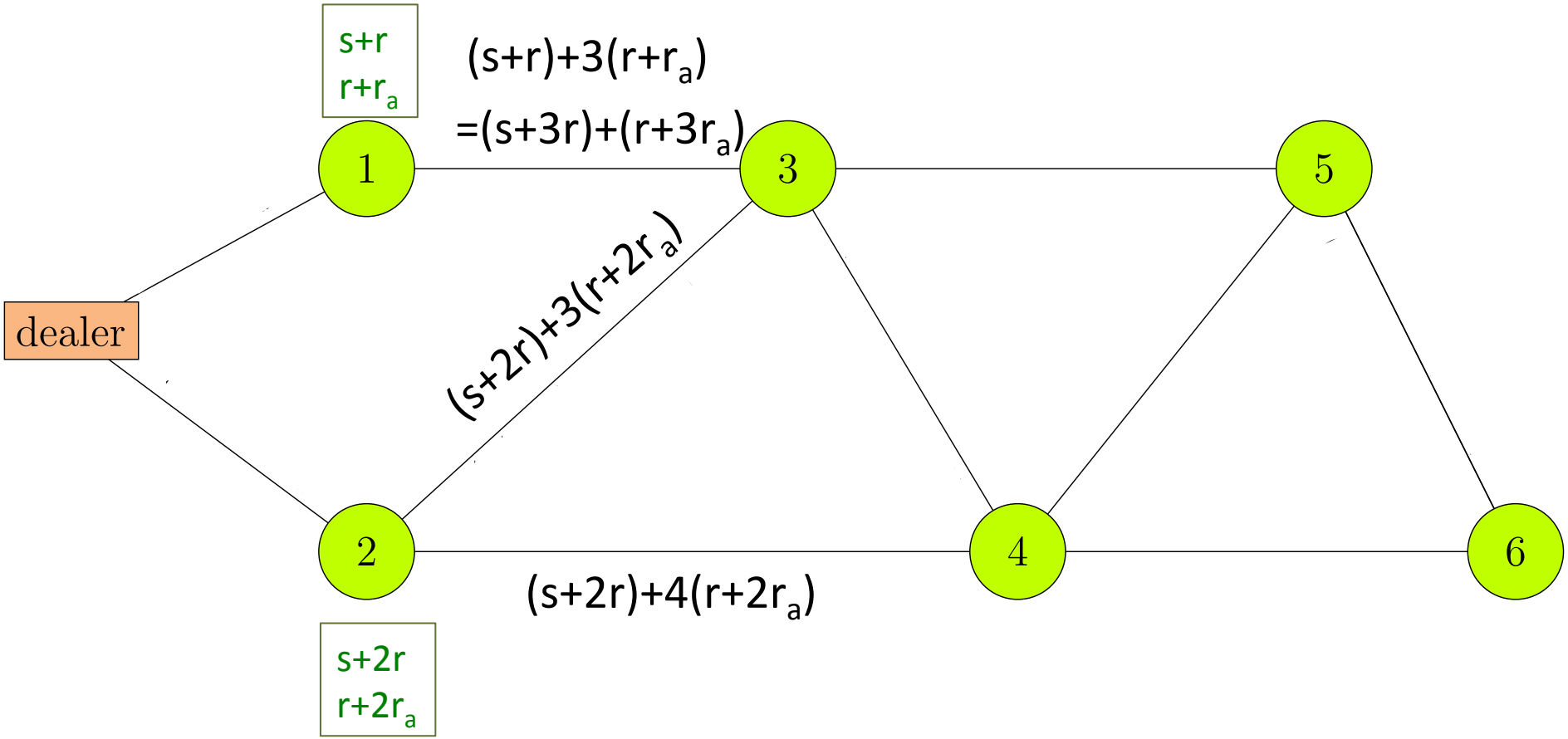

SNEAK algorithm



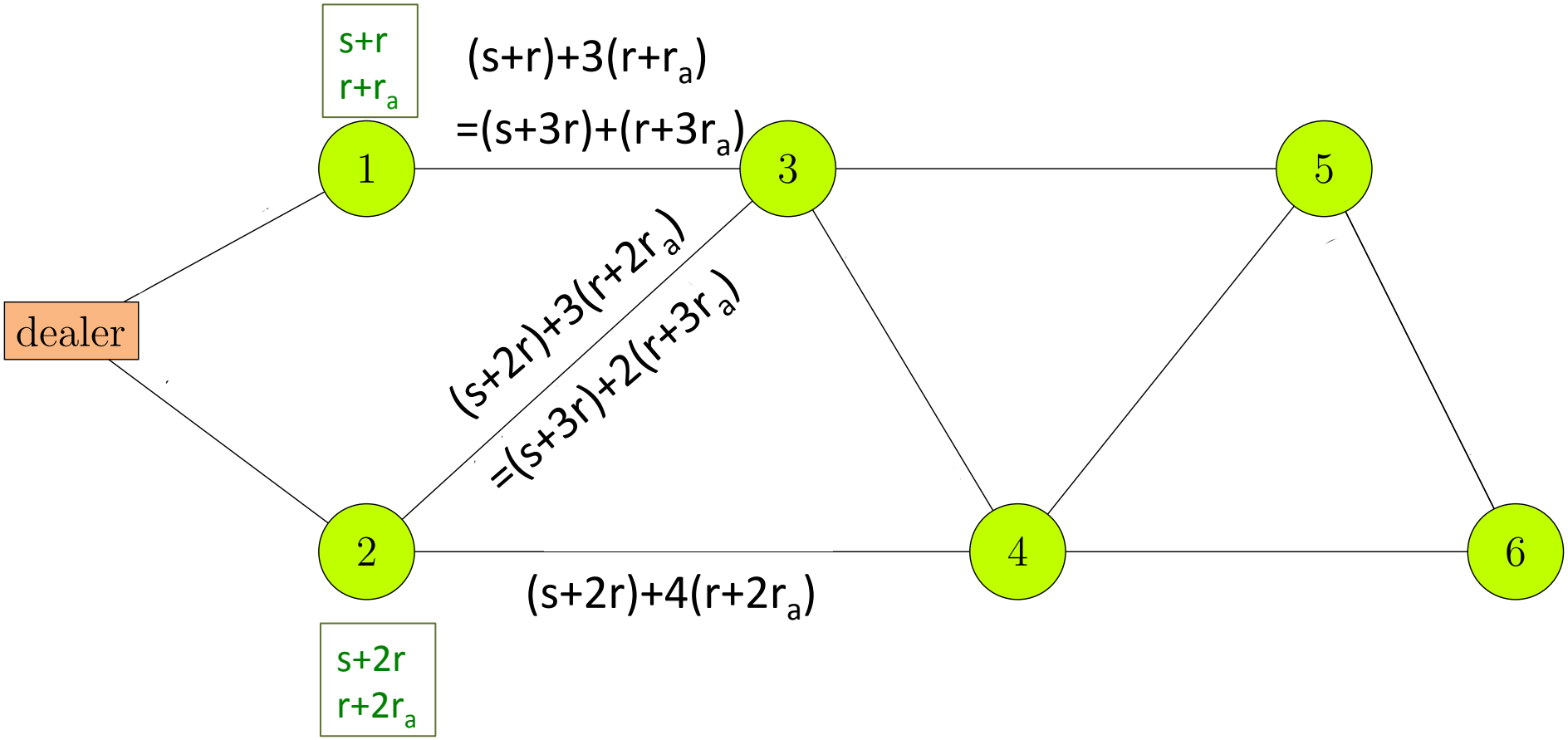

SNEAK algorithm



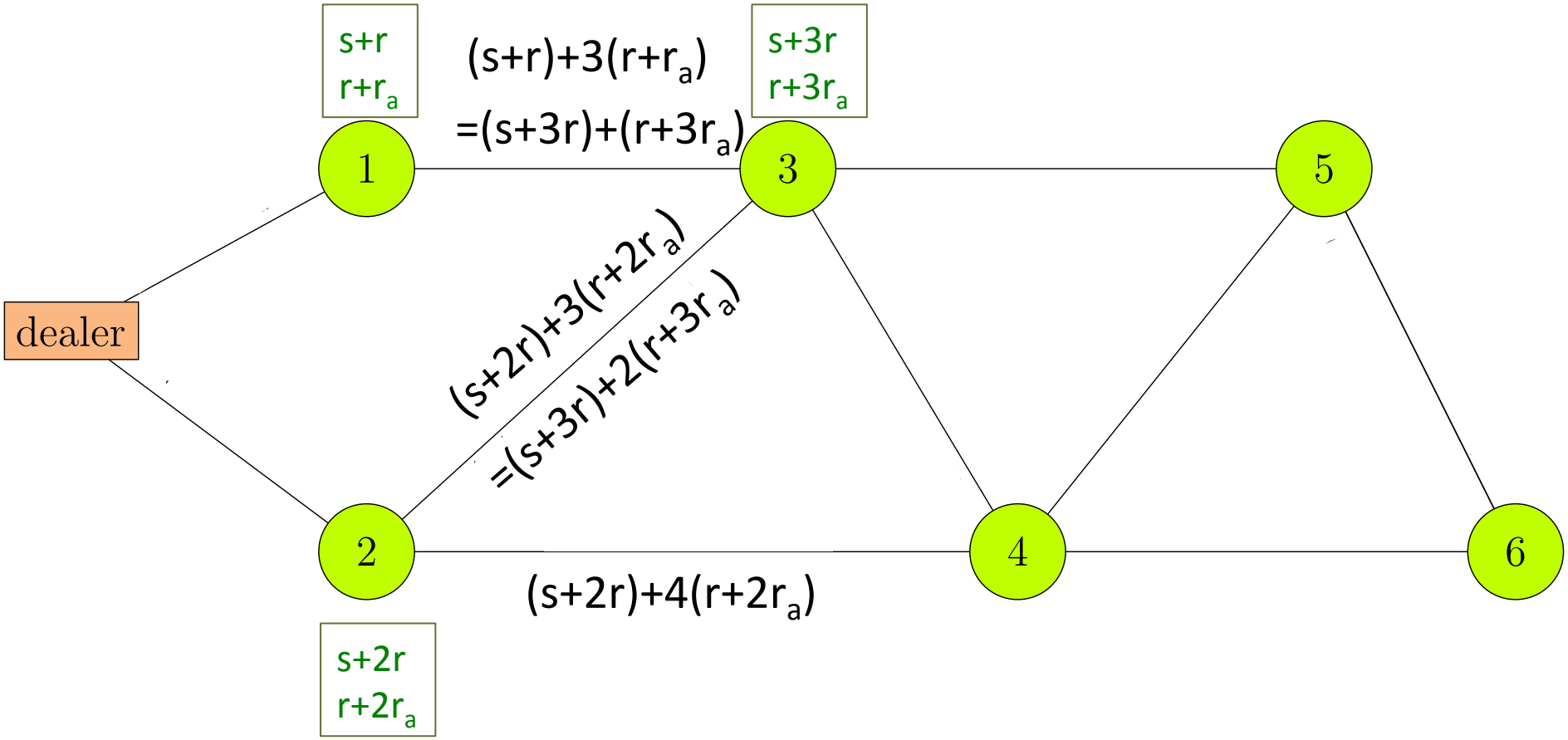

SNEAK algorithm



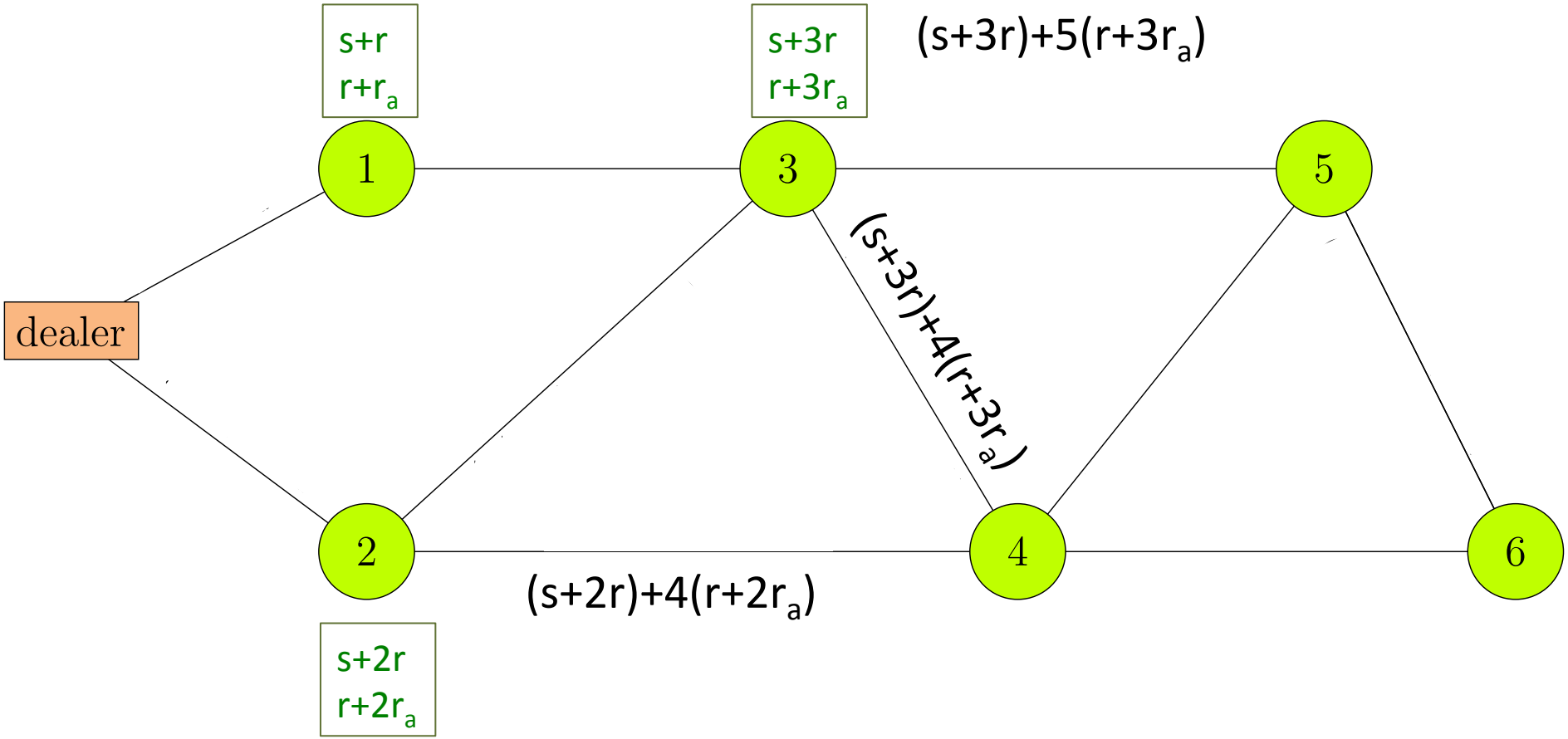

SNEAK algorithm



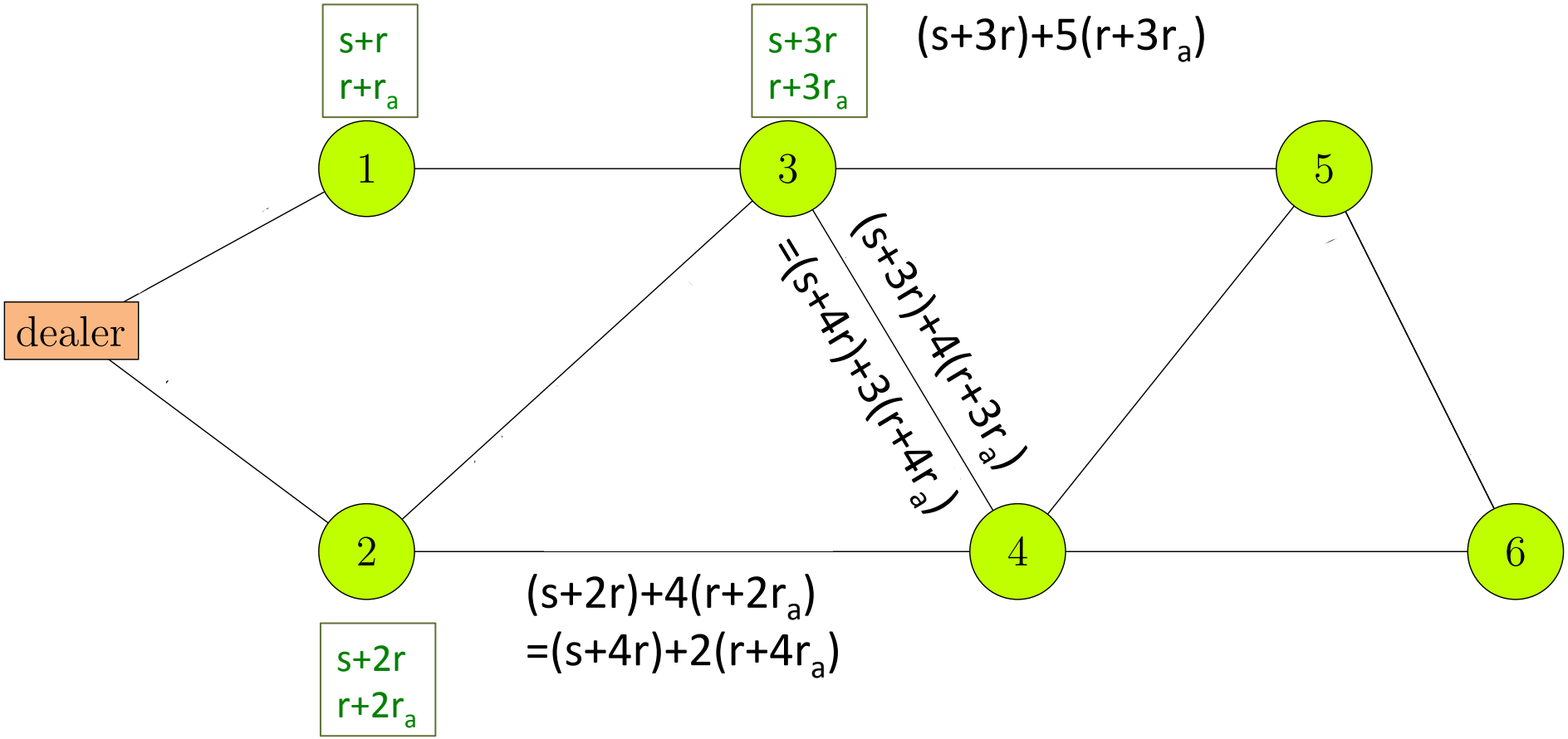

SNEAK algorithm



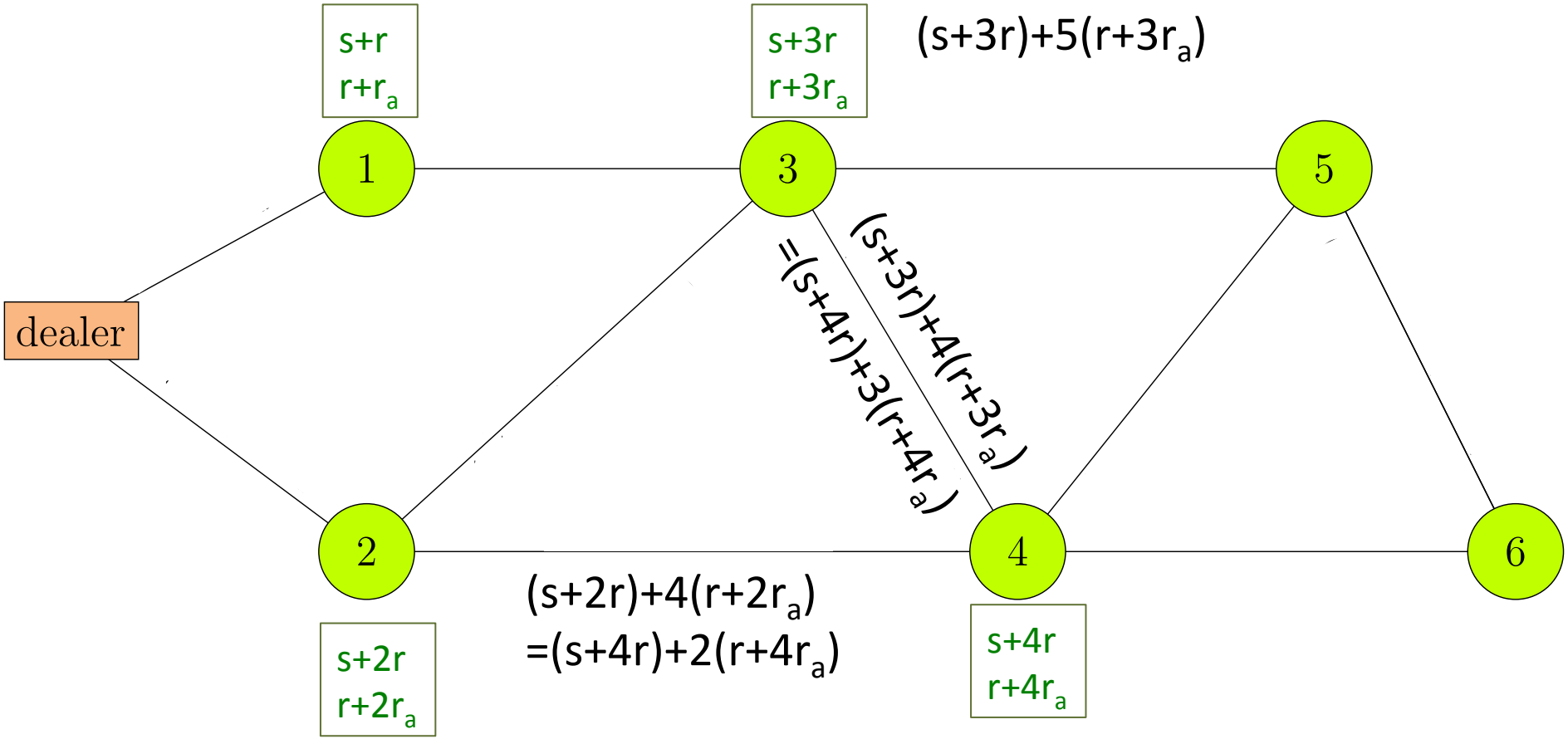

SNEAK algorithm



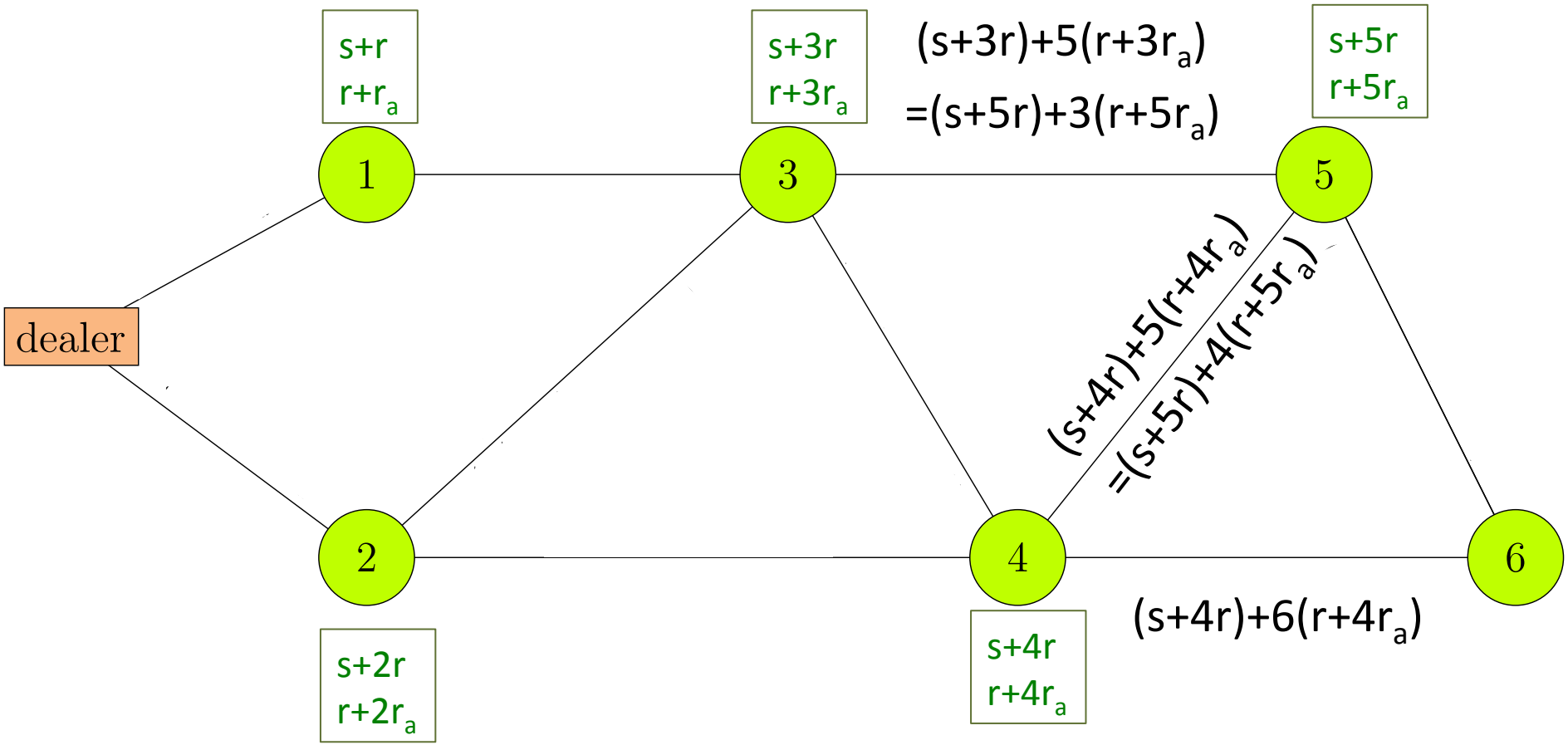

SNEAK algorithm



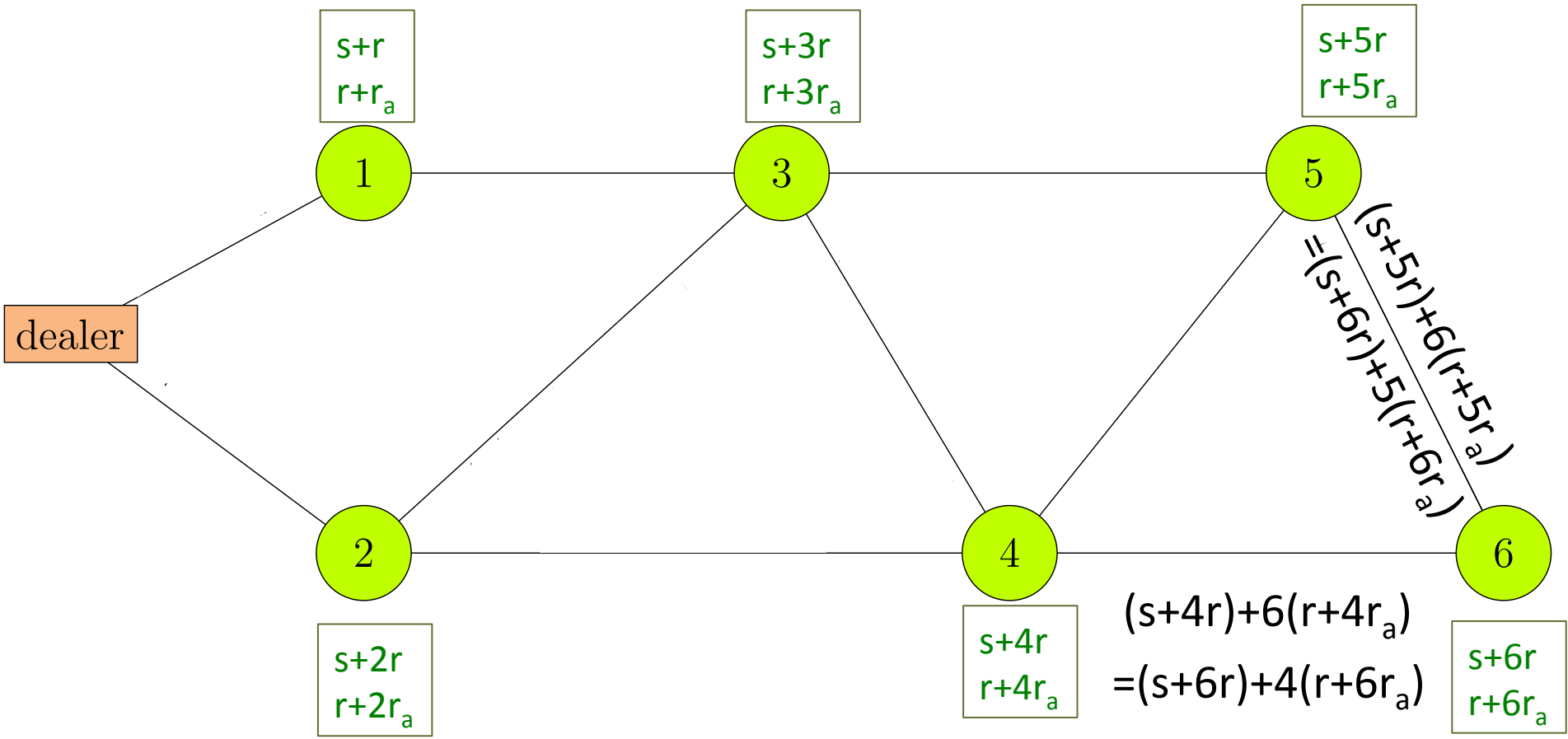

SNEAK algorithm



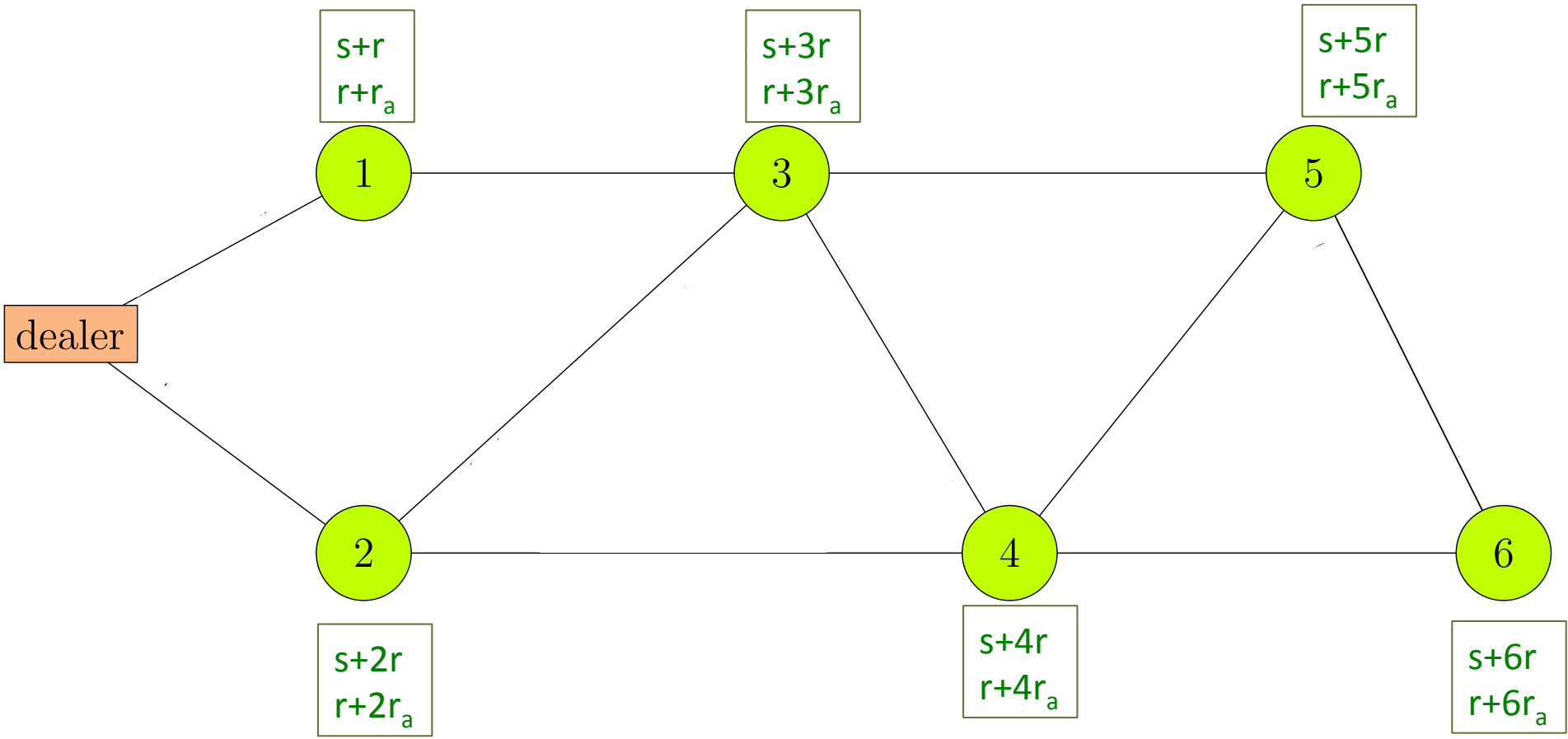

SNEAK algorithm



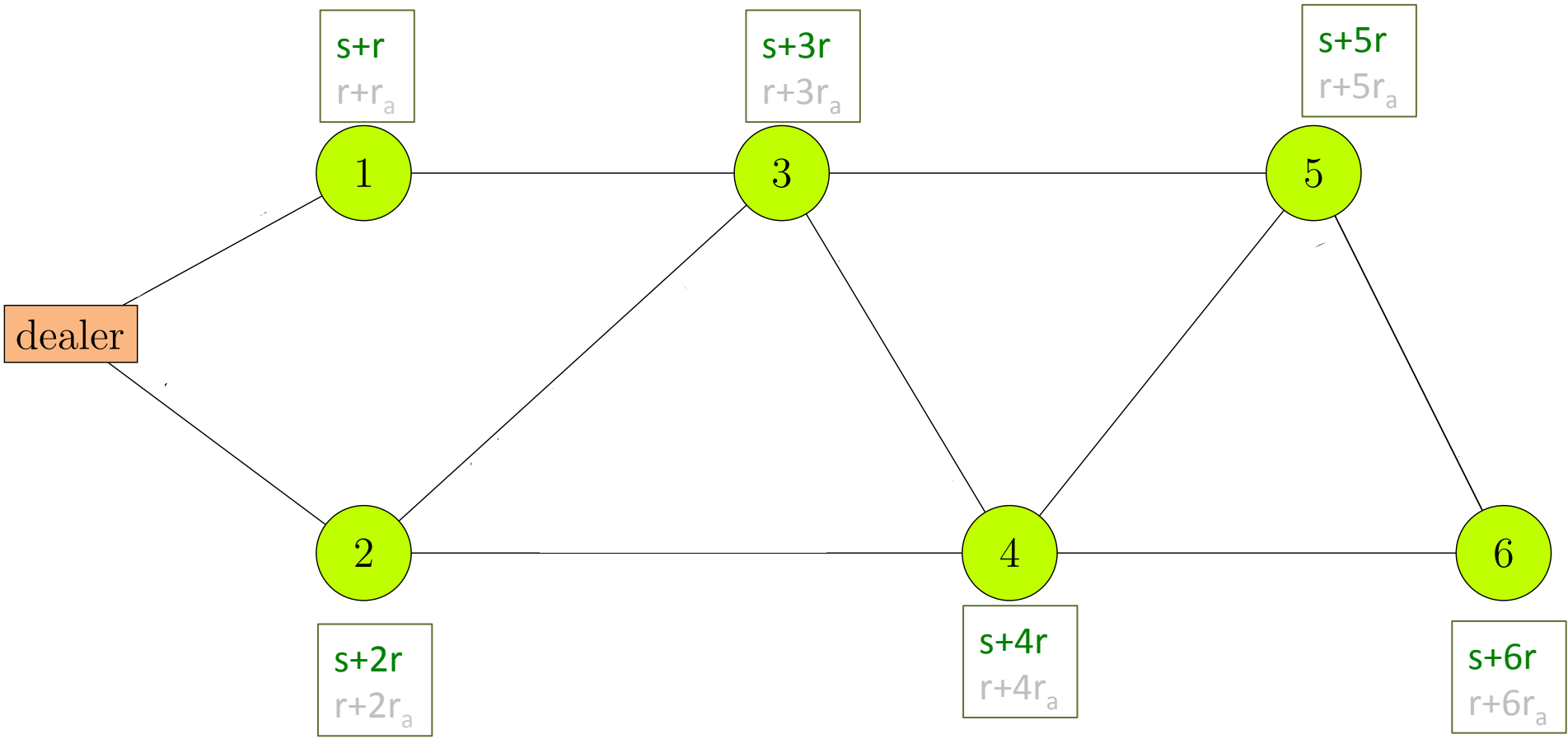

SNEAK algorithm



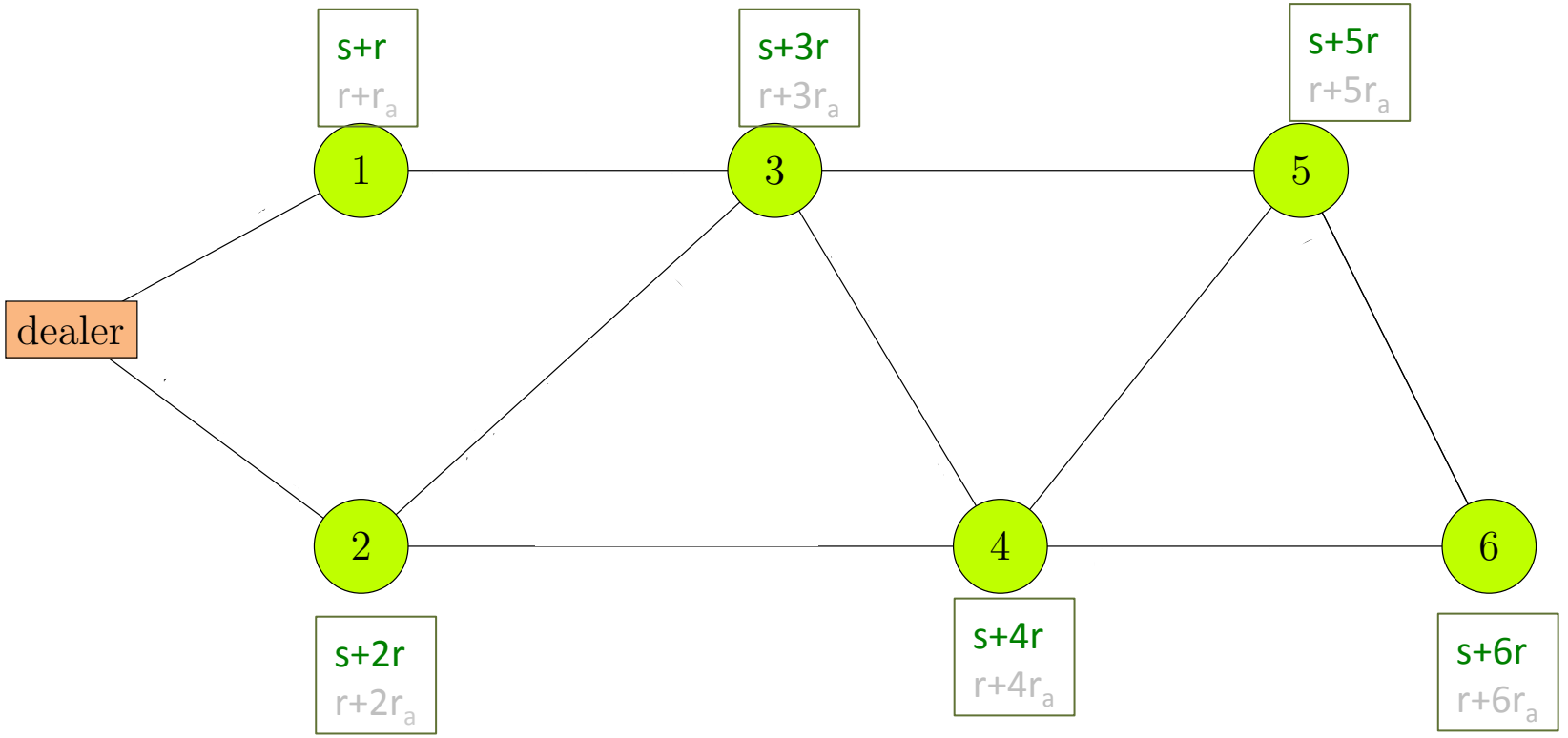

SNEAK algorithm



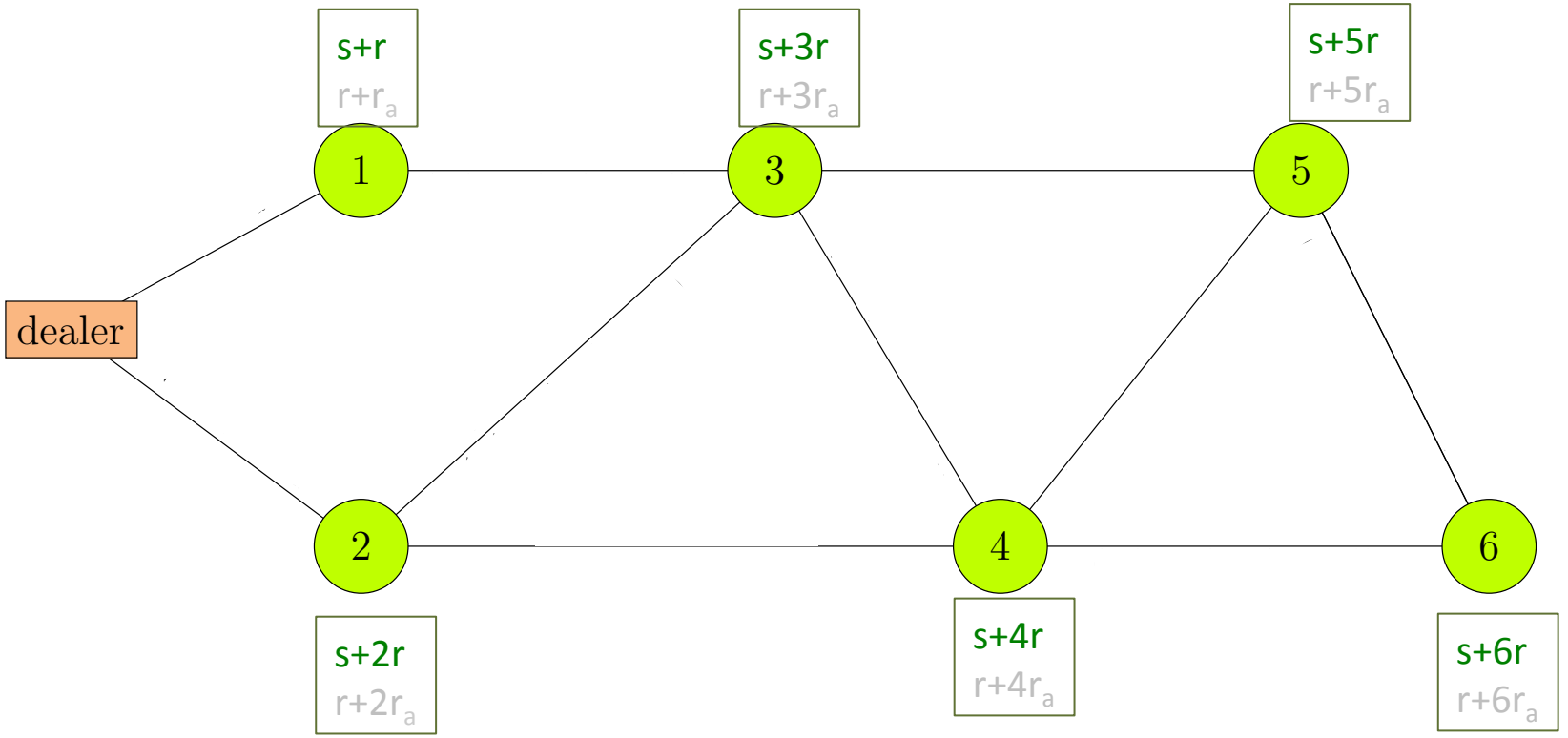

SNEAK algorithm



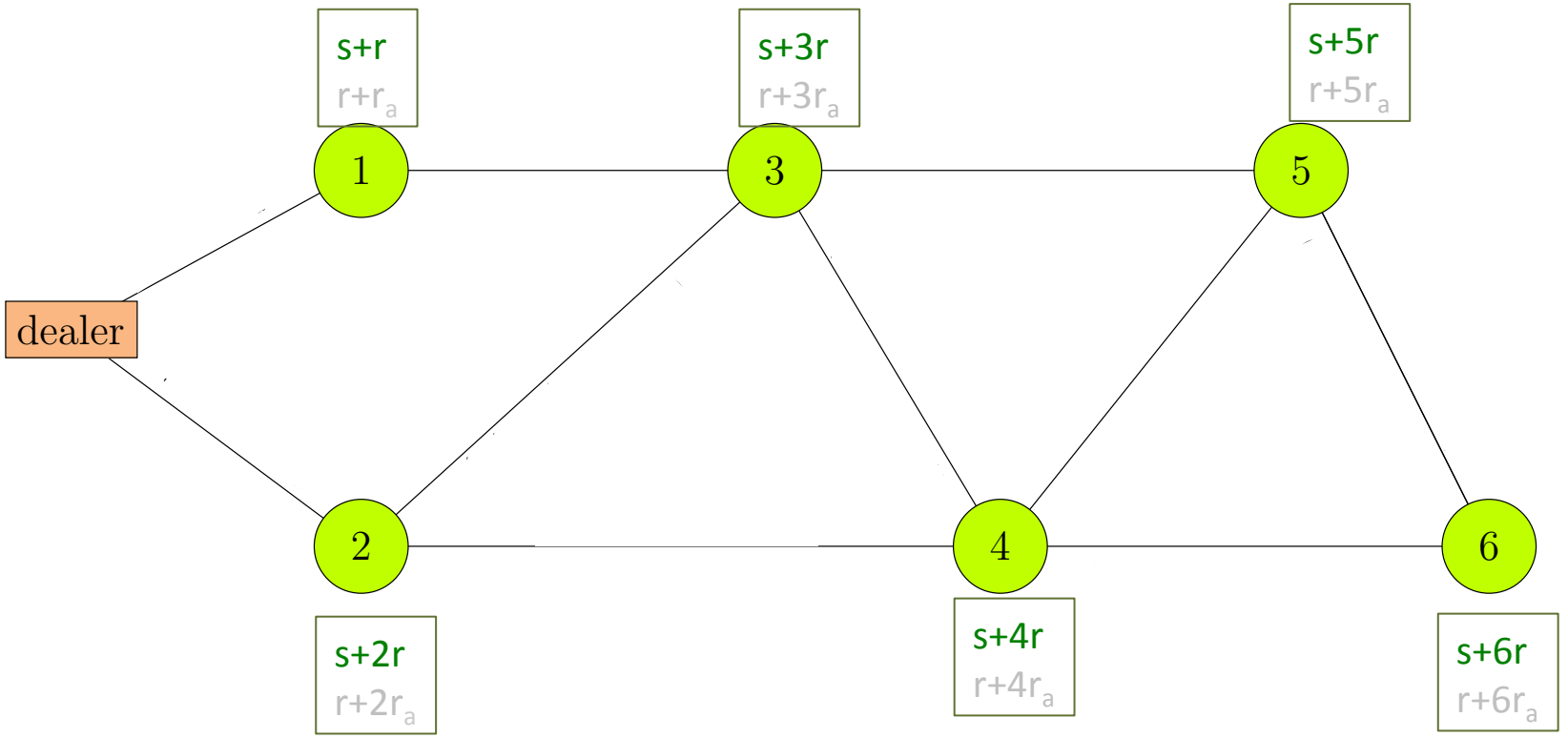

SNEAK algorithm




| | SNEAK | Pairwise-agreement |
|---|---|---|
| **Communication** | 12 | 24 |




| | SNEAK | Pairwise-agreement |
|---|---|---|
| **Communication** | 12 | 24 |
| **Knowledge of topology** | know only one-hop neighbours | node disjoint paths on entire graph |




| | SNEAK | Pairwise-agreement |
|---|---|---|
| **Communication** | 12 | 24 |
| **Knowledge of topology** | know only one-hop neighbours | node disjoint paths on entire graph |
| **Randomness** | 2 | 5 |

# General SNEAK algorithm

Details in ISIT paper/arXiv

- ✓ communication-efficient
- ✓ randomness-efficient
- ✓ distributed
- ✓ deterministic

SNEAK = Secret-sharing over a Network with Efficient communication And distributed Knowledge-of-topology

# General SNEAK algorithm

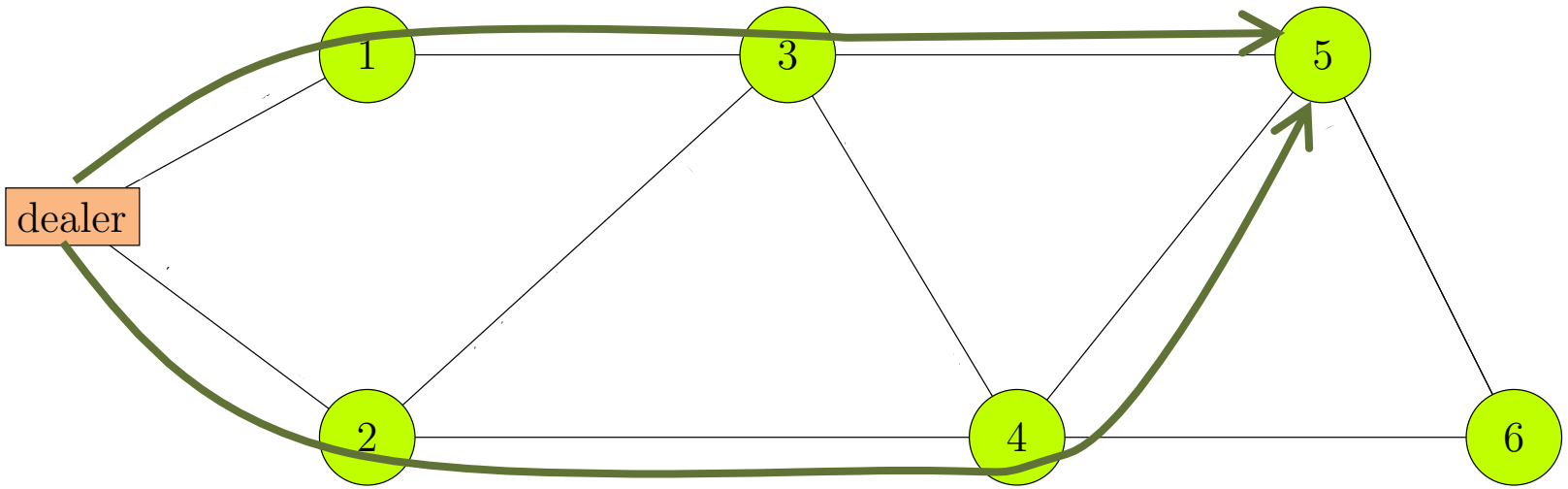
Details in ISIT paper/arXiv

- ✓ communication-efficient
- ✓ randomness-efficient
- ✓ distributed
- ✓ deterministic

Needs graph to satisfy
a certain condition

# Conditions on the graph

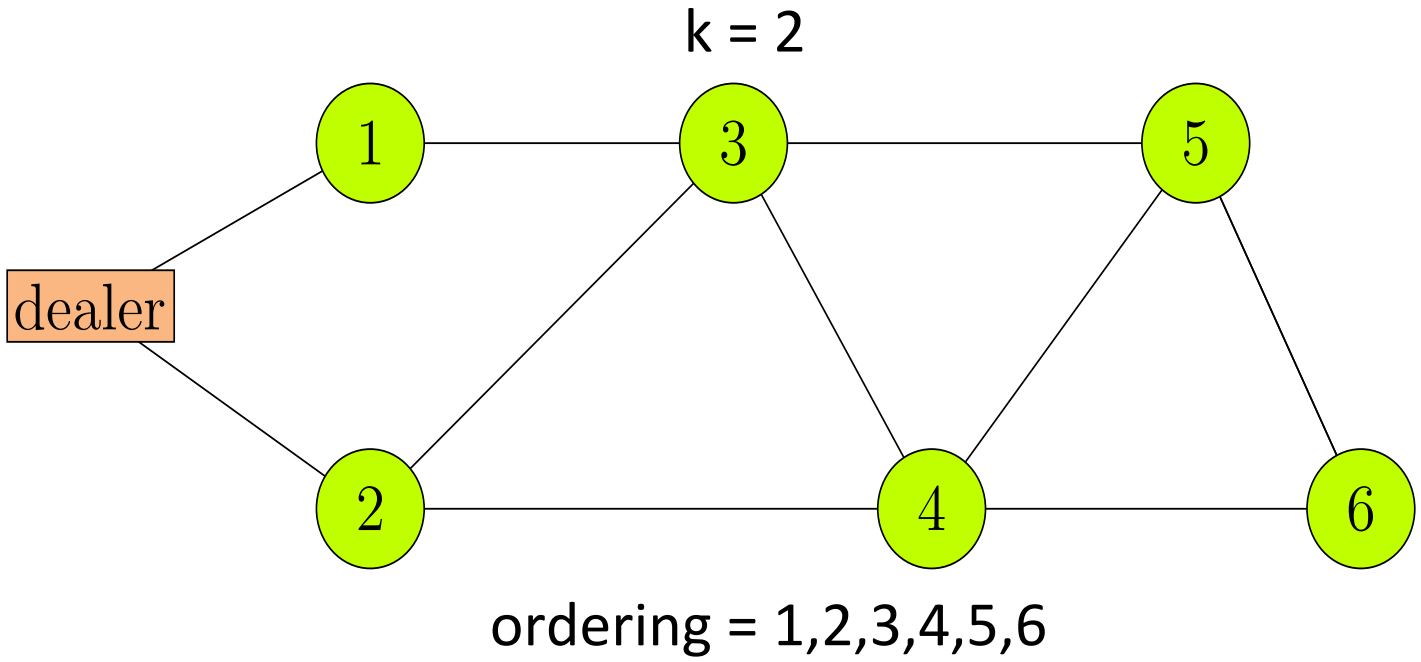
- Necessary for *any* algorithm: *"k-connected-dealer"*
  - Exist k node-disjoint paths from dealer to every participant




k=2

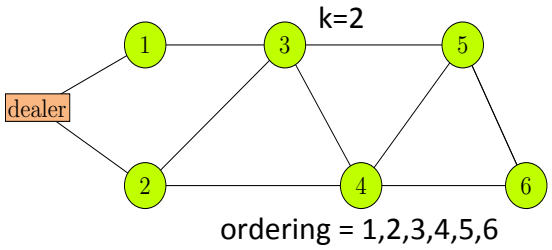
# Conditions on the graph

- Required for our algorithm: "*k-propagating-dealer*"
  - ∃ ordering of participants such that each participant has edges coming in from either (a) the dealer or (b) from k participants preceding it in the ordering

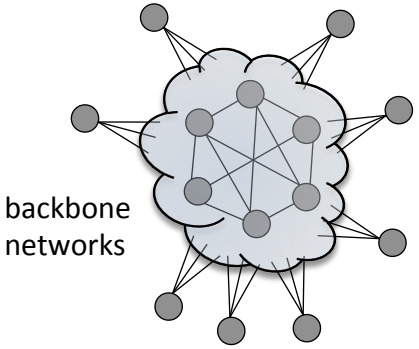


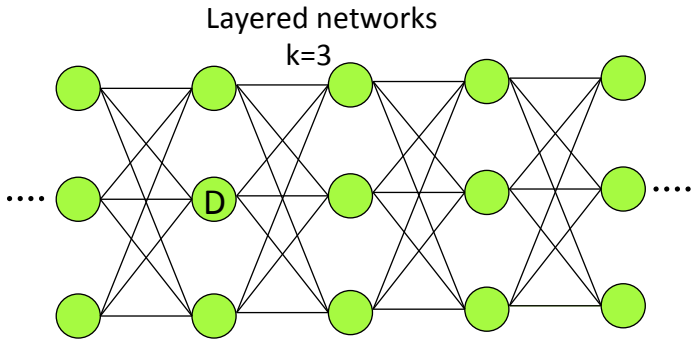
# Conditions on the graph

- Many graphs satisfying *k-propagating-dealer*

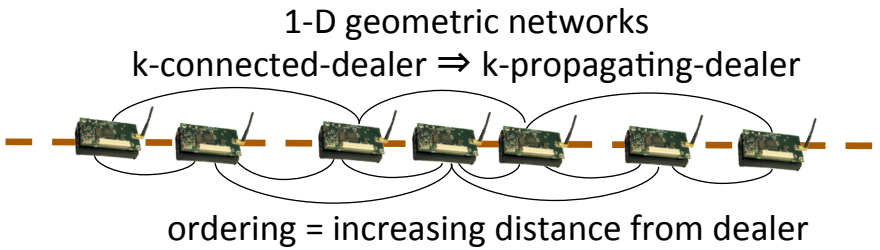



Any DAG:
k-connected-dealer
⇒ k-propagating-dealer




ordering = layers next to dealer, rest increasing distance from dealer



# SNEAK algorithm is oblivious to ordering

- Need not know anything about the network
- Nodes only know one hop neighbours

# What if ‘k-propagating-dealer’ not satisfied ?

- No leak of information
  - No (k-1) nodes get any information about s
- Extensions of SNEAK (heuristic) in paper

# Information-theoretic Lower Bounds

# Information-theoretic Lower Bounds

## Theorem: Lower Bound

Any node $\ell \in [n]$ with incoming degree $\deg(\ell)$ must download at least

$$\begin{cases} 1 & \text{if } \ell \in \mathcal{N}(D) \\ \infty & \text{if } \ell \notin \mathcal{N}(D) \text{ and } \deg(\ell) < k \\ \frac{\deg(\ell)}{\deg(\ell)-k+1} & \text{if } \ell \notin \mathcal{N}(D) \text{ and } \deg(\ell) \geq k \ . \end{cases}$$

Furthermore, this bound is the best possible, given only the identities of the neighbours of node $\ell$.

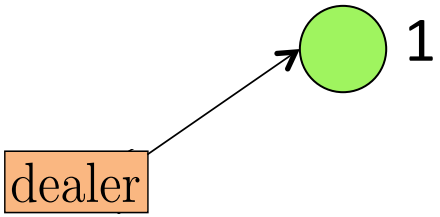
# Information-theoretic Lower Bounds

## Theorem: Lower Bound

Any node $\ell \in [n]$ with incoming degree $\deg(\ell)$ must download at least

$$\begin{cases} 1 & \text{if } \ell \in \mathcal{N}(D) \\ \infty & \text{if } \ell \notin \mathcal{N}(D) \text{ and } \deg(\ell) < k \\ \frac{\deg(\ell)}{\deg(\ell)-k+1} & \text{if } \ell \notin \mathcal{N}(D) \text{ and } \deg(\ell) \geq k \ . \end{cases}$$

Furthermore, this bound is the best possible, given only the identities of the neighbours of node $\ell$.



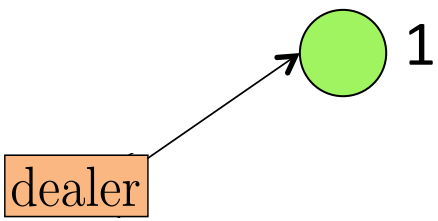
# Information-theoretic Lower Bounds

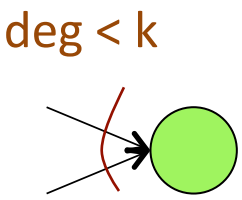
## Theorem: Lower Bound

Any node $\ell \in [n]$ with incoming degree $\deg(\ell)$ must download at least

$$\begin{cases} 1 & \text{if } \ell \in \mathcal{N}(D) \\ \infty & \text{if } \ell \notin \mathcal{N}(D) \text{ and } \deg(\ell) < k \\ \frac{\deg(\ell)}{\deg(\ell)-k+1} & \text{if } \ell \notin \mathcal{N}(D) \text{ and } \deg(\ell) \geq k \ . \end{cases}$$

Furthermore, this bound is the best possible, given only the identities of the neighbours of node $\ell$.




not possible

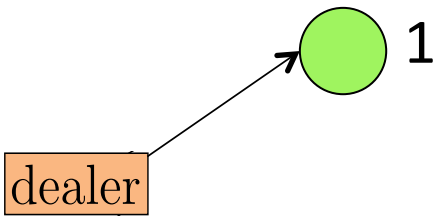
# Information-theoretic Lower Bounds

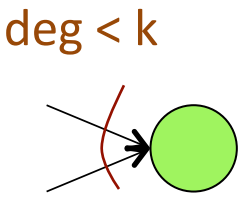
## Theorem: Lower Bound

Any node $\ell \in [n]$ with incoming degree $\deg(\ell)$ must download at least

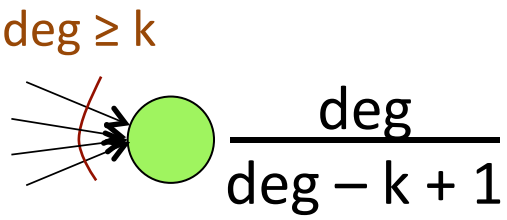
$$\begin{cases} 1 & \text{if } \ell \in \mathcal{N}(D) \\ \infty & \text{if } \ell \notin \mathcal{N}(D) \text{ and } \deg(\ell) < k \\ \frac{\deg(\ell)}{\deg(\ell)-k+1} & \text{if } \ell \notin \mathcal{N}(D) \text{ and } \deg(\ell) \geq k \ . \end{cases}$$

Furthermore, this bound is the best possible, given only the identities of the neighbours of node $\ell$.




not possible



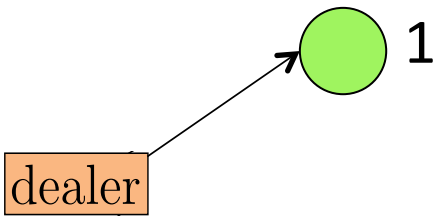
# Information-theoretic Lower Bounds

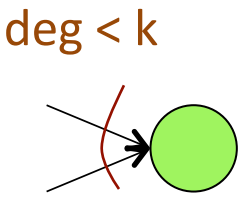
## Theorem: Lower Bound

Any node $\ell \in [n]$ with incoming degree $\deg(\ell)$ must download at least

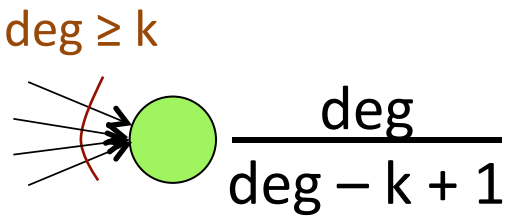
$$\begin{cases} 1 & \text{if } \ell \in \mathcal{N}(D) \\ \infty & \text{if } \ell \notin \mathcal{N}(D) \text{ and } \deg(\ell) < k \\ \frac{\deg(\ell)}{\deg(\ell)-k+1} & \text{if } \ell \notin \mathcal{N}(D) \text{ and } \deg(\ell) \geq k \ . \end{cases}$$

Furthermore, this bound is the best possible, given only the identities of the neighbours of node $\ell$.




not possible




Corollary: communication ≥ n

# Communication Complexity

Suppose graph satisfies “d-propagating-dealer” for some $d \geq k$

# Communication Complexity

Suppose graph satisfies “d-propagating-dealer” for some $d \geq k$

- any algorithm $\geq n$

# Communication Complexity

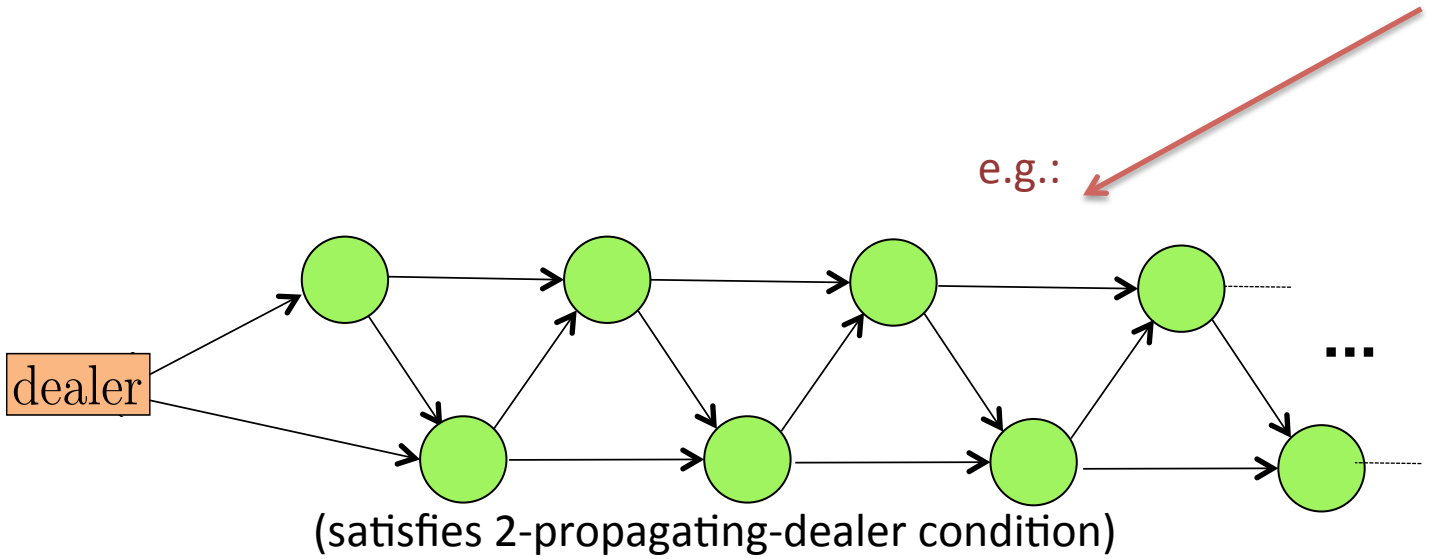
Suppose graph satisfies “d-propagating-dealer” for some d ≥ k

- any algorithm ≥ n
- SNEAK = $n\frac{d}{d-k+1}$ (linear in n)

# Communication Complexity

Suppose graph satisfies "d-propagating-dealer" for some d ≥ k

- any algorithm ≥ n
- SNEAK = $n\frac{d}{d-k+1}$ (linear in n)
- pairwise-agreement: 'typically' super-linear, worst case $\approx n^2$




(satisfies 2-propagating-dealer condition)

# Further, in the paper

- Analysis of randomness requirements
- Additional analysis of communication complexity

# Summary & Future Work

- SNEAK algorithm
  - efficient, distributed
- Information-theoretic lower bounds
  - download for any node
  - tight for the case when knowledge of only one-hop neighbours is available

# Summary & Future Work

- SNEAK algorithm
  - efficient, distributed

Heuristic extension when k-propagating-dealer condition is not met. Guarantees ?

- Information-theoretic lower bounds
  - download for any node
  - tight for the case when knowledge of only one-hop neighbours is available

# Summary & Future Work

- SNEAK algorithm
  - efficient, distributed

Heuristic extension when k-propagating-dealer condition is not met. Guarantees ?

Other classes of graphs satisfying k-propagating-dealer condition?

- Information-theoretic lower bounds
  - download for any node
  - tight for the case when knowledge of only one-hop neighbours is available

# Summary & Future Work

- SNEAK algorithm
  - efficient, distributed

Heuristic extension when k-propagating-dealer condition is not met. Guarantees ?

Other classes of graphs satisfying k-propagating-dealer condition?

- Information-theoretic lower bounds
  - download for any node
  - tight for the case when knowledge of only one-hop neighbours is available

Tighter bounds for secret sharing in a network

# Summary & Future Work

- SNEAK algorithm
  - efficient, distributed

Heuristic extension when k-propagating-dealer condition is not met. Guarantees ?

Other classes of graphs satisfying k-propagating-dealer condition?

- Information-theoretic lower bounds
  - download for any node
  - tight for the case when knowledge of only one-hop neighbours is available

Tighter bounds for secret sharing in a network

What carries over to general secure network coding ?


Thanks! Questions?