On Secrecy Amplification Protocols

Improving security of partially compromised network

Radim Ošťádal (ostadal@mail.muni.cz)
Petr Švenda (svenda@fi.muni.cz)
Vashek Matyáš (matyas@fi.muni.cz),
CRoCS, Masaryk University, Czech Republic

CRoCS
Centre for Research on Cryptography and Security

Focus and Outline

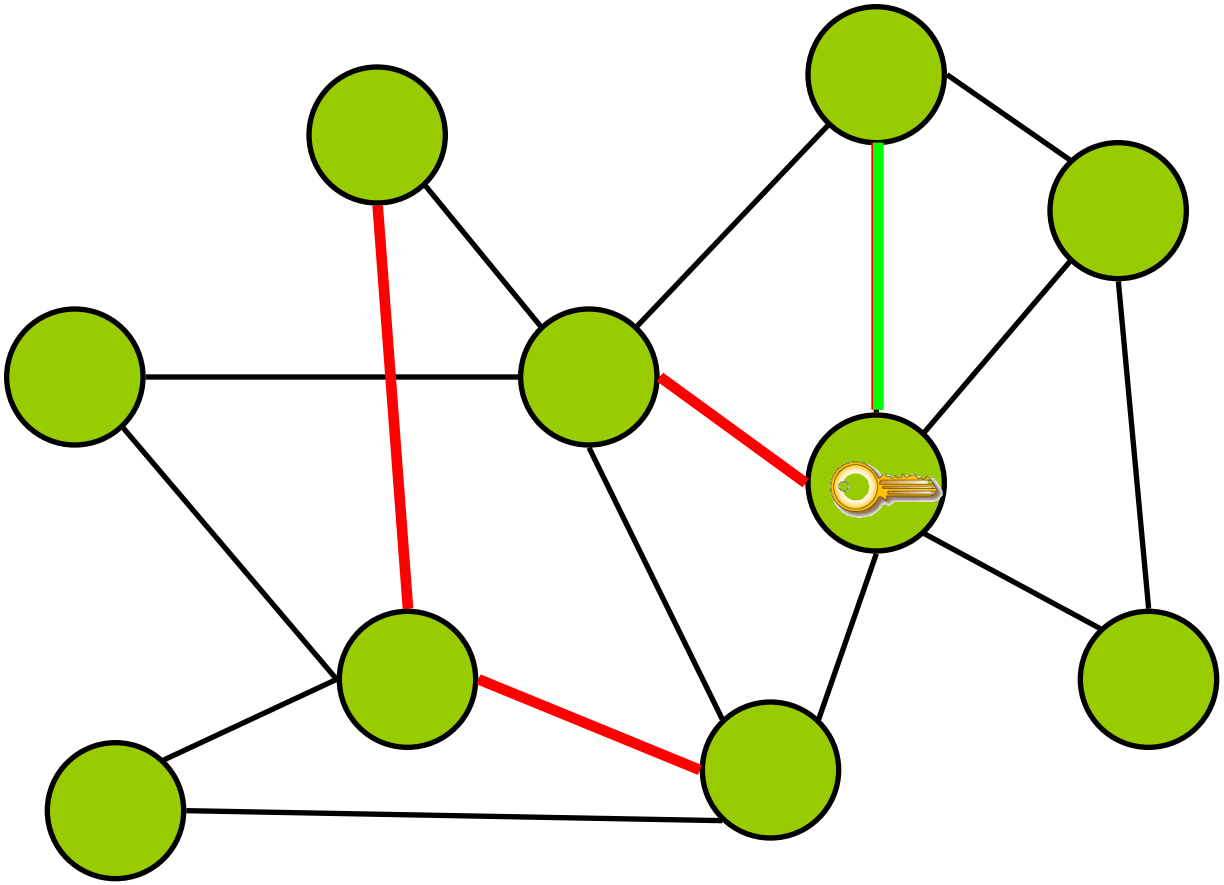
Focus on link security between lightweight wireless nodes

Outline:

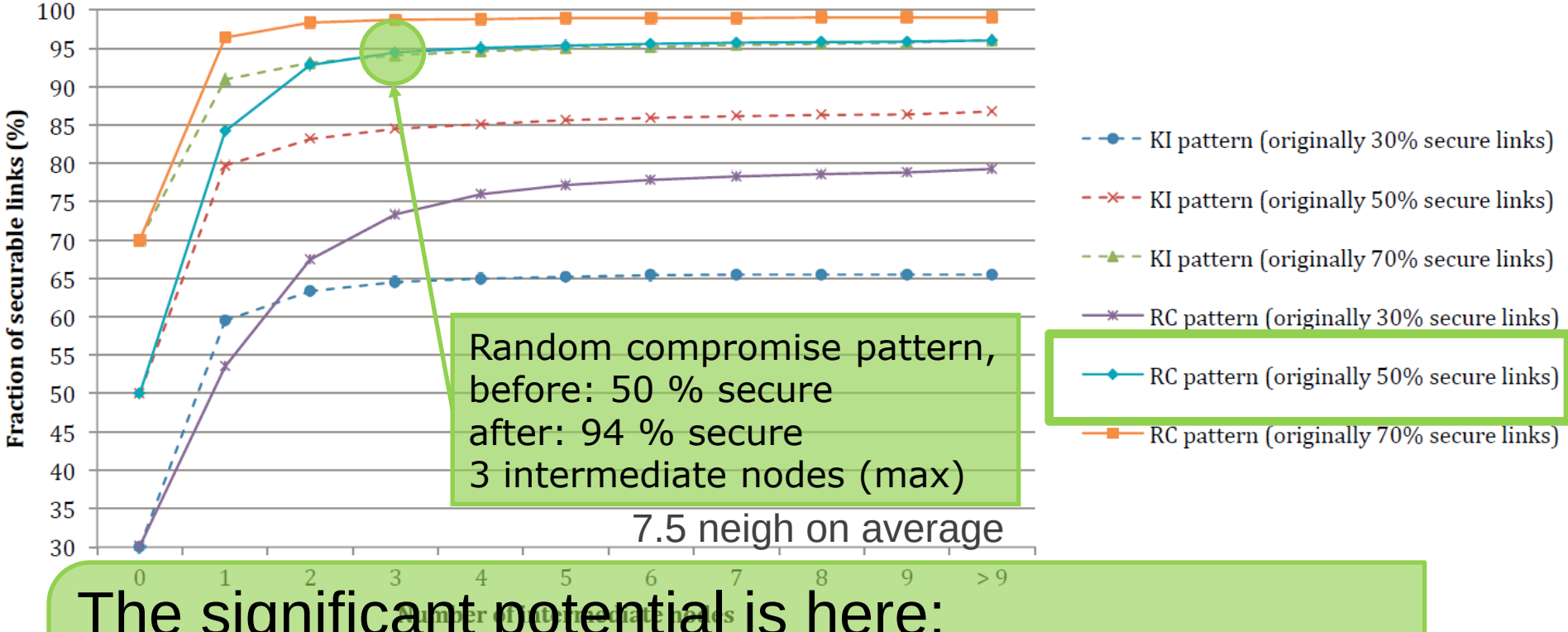
- Motivation: partially compromised network
- Secrecy amplification protocols – principle
- Node/group/hybrid-type secrecy amplification
- Performance comparison
- Summary

MOTIVATION

Partially compromised network



Floyd-Warshall on network connectivity



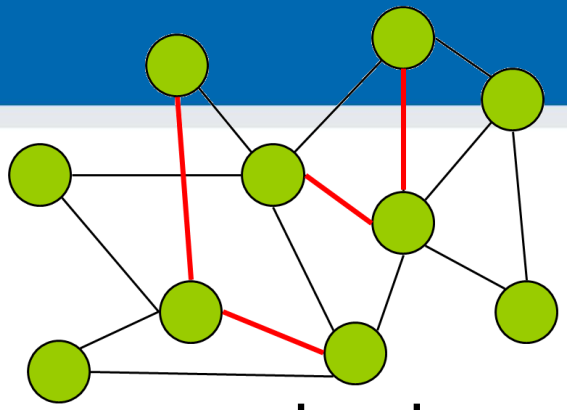
Random compromise pattern,
before: 50 % secure
after: 94 % secure
3 intermediate nodes (max)

7.5 neigh on average

The significant potential is here:

If 7.5 neighbors: 50 → 94 % (3 inter. nodes)

If 20 neighbors: 30 % → 95 %



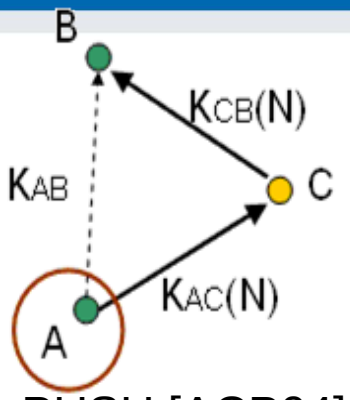
But…

- We don’t know which links are compromised
  - Neither global nor local knowledge (!Floyd-Warshall)
- We can’t try all possible paths (message, energy)
- Overall success depends on compromise pattern
  - Suboptimal performance of tailored protocol in another
- Do we have use for that?
  - Ad-hoc/sensor networks with local communication
  - WSN → hype around 2000 → reasonable hardware now
    - Cost less then $10
    - Weightless-N ($2 module, 10 years battery lifetime)

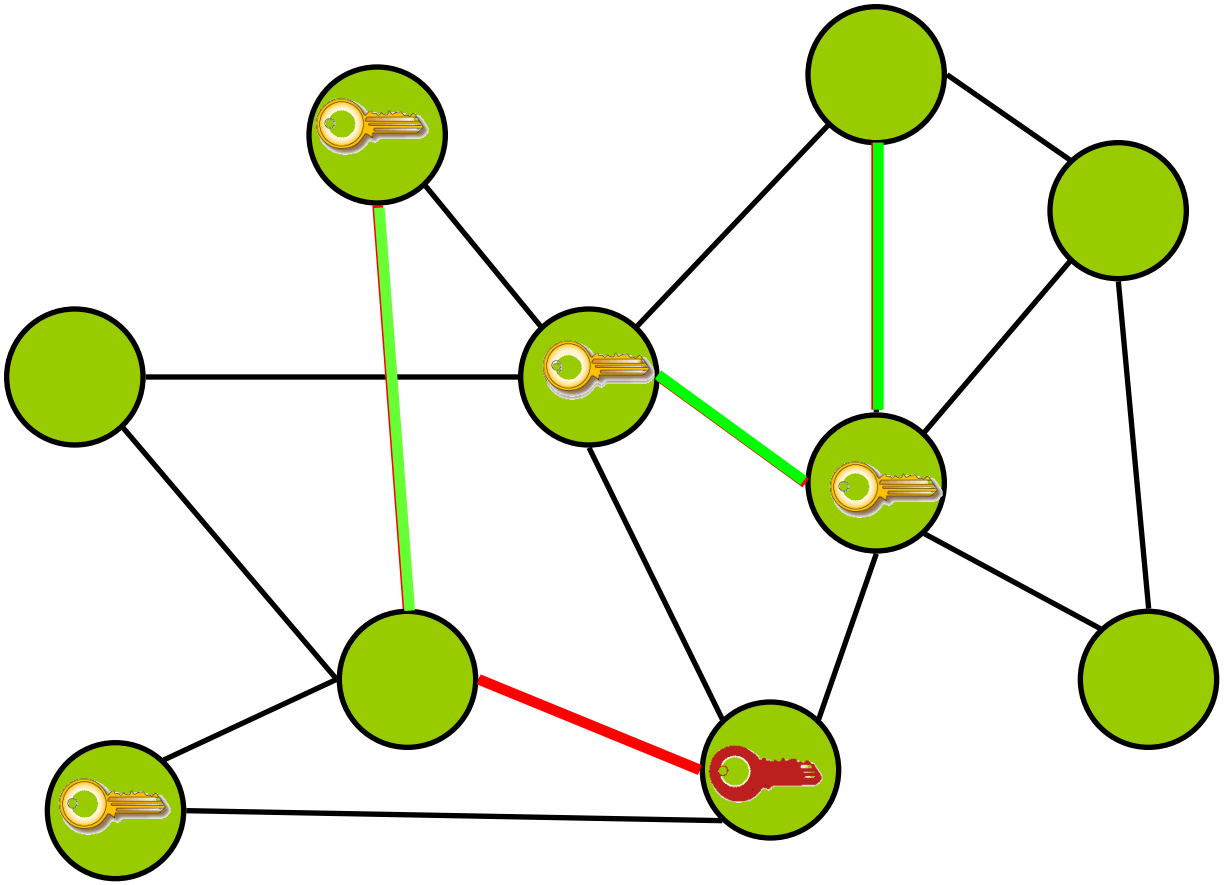
What secrecy amplification protocols types are known?

SECRECY AMPLIFICATION

Secrecy amplification protocol

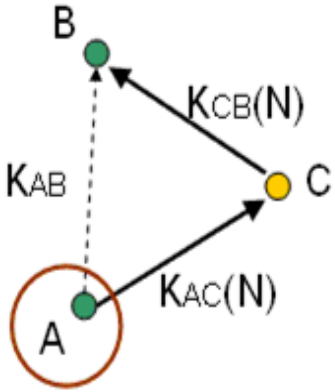


PUSH [ACP04]



What is secrecy amplification protocol?

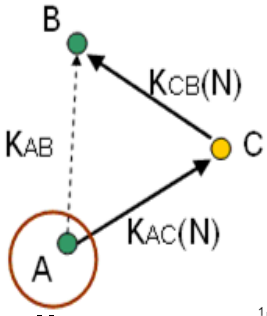
- Series of operations executed by nodes
  1. RNG: Generate new key share N
  2. SND: Transmit key share to selected node
  3. Repeat from 1 or 2
  4. Combine shares: hash(N | K_{AB})

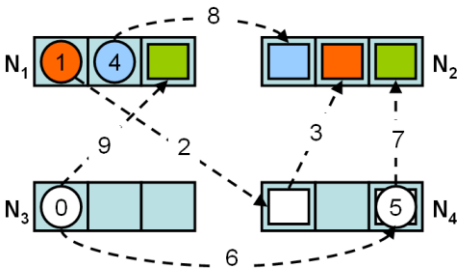


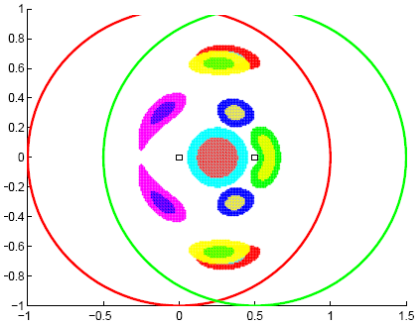
- Transmission uses already established link keys
- New shares are combined with existing keys
  – Existing key might be already secure, but N compromised

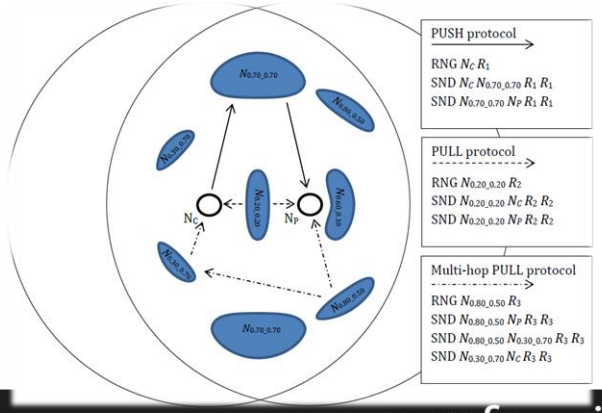
Published secrecy amplification protocols

1. Node-oriented protocols
   - PUSH [ACP04], 2004, manually
   - PULL [CS05], 2005, manually
   - COMODITY [KKLK05], 2005, manually
   - NO_{BEST} [SSM09], 2009, automatically
2. Group-oriented protocols
   - GO-SA [SSM09], GO_{BEST} [SSSM12]
3. Hybrid protocols
   - HP_{BEST}, semi-automatic [OSM14]
   - HP_{FINAL}, semi-automatic [OSM14]
   - this work, semi-automatic



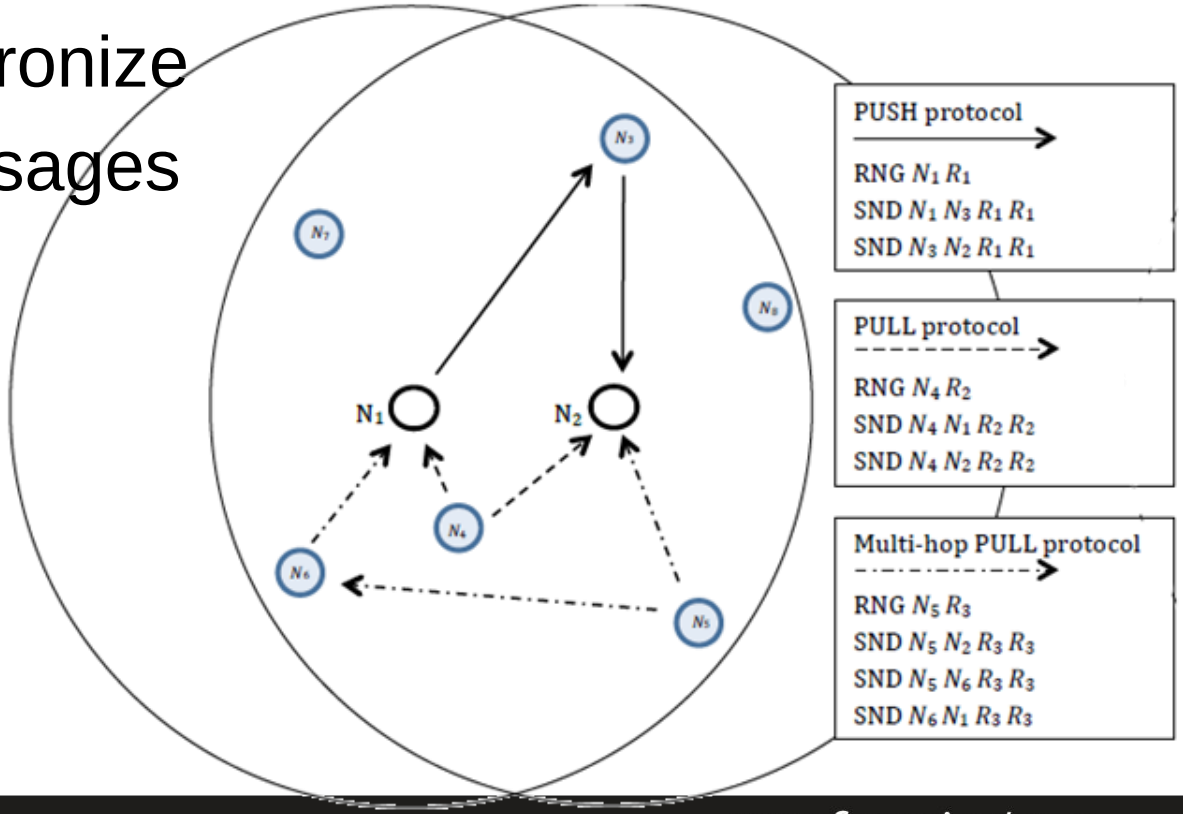






Node-oriented secrecy amplification

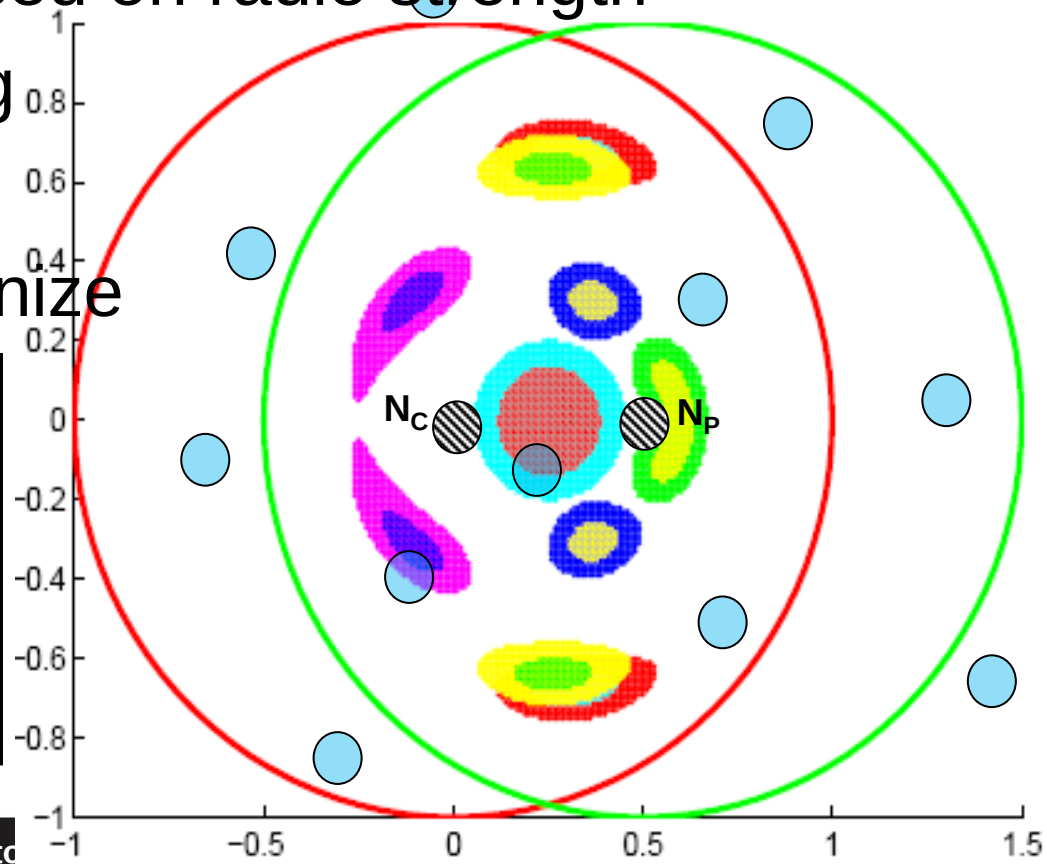
- Execute with all k-tuples of neighbors
- Combine all resulting shares
- ☺ Easy to synchronize
- ☹ High # of messages



Group-oriented secrecy amplification

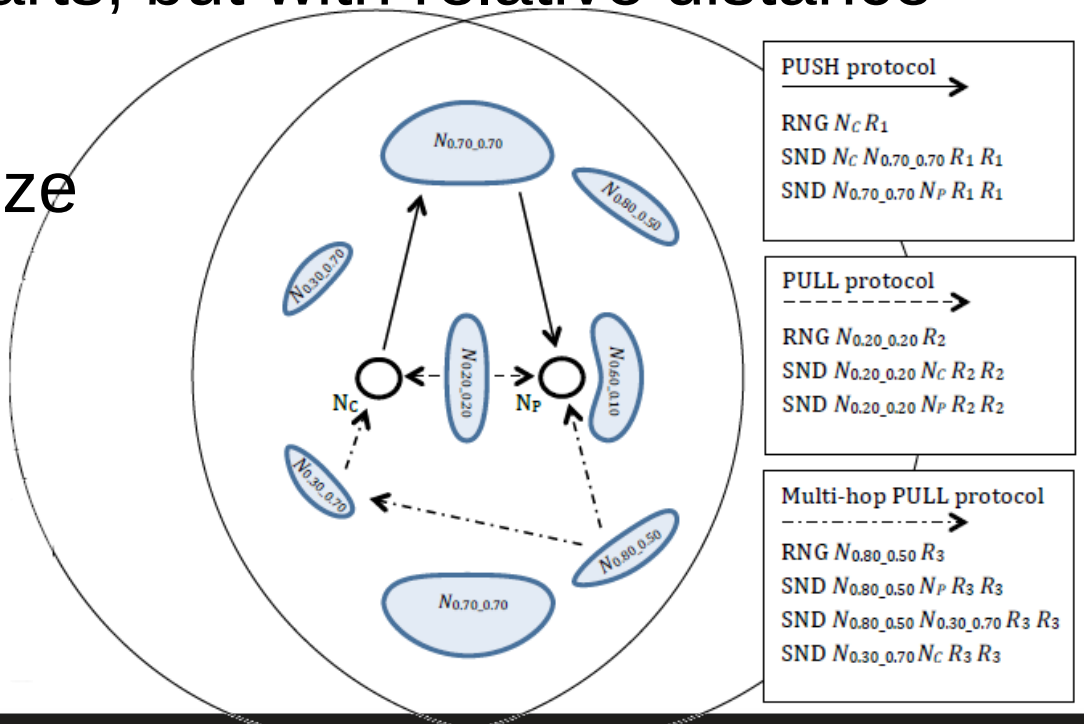
- Group of neighbors at once
- Relative distance based on radio strength
- Genetic programming
- ☺ Low # messages
- ☹ Difficult to synchronize

…
RNG N_P Rt11
SND N0.59 0.11 N_P Rv7 Rt3
SND N_P N0.75 0.70 Rv6 Rt1
SND N_P N0.01 0.00 Rv11 Rt12
…



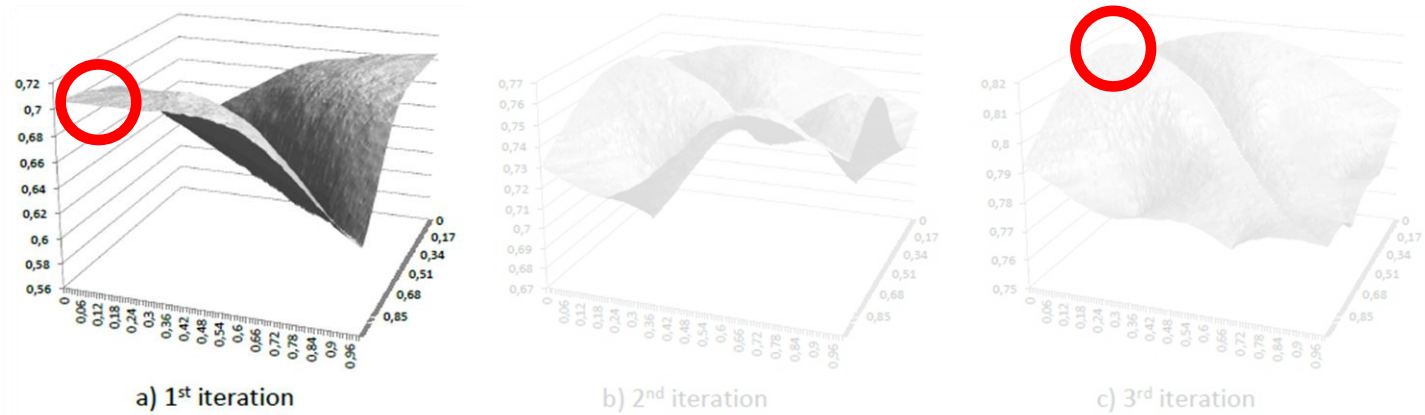
Hybrid-type secrecy amplification

- Combined advantages of node and group-oriented
- Group of nodes at once
- Node-oriented subparts, but with relative distance
- ☺ Low # messages
- ☺ Easy to synchronize
- Optimal placement



Hybrid-type: optimal placement

- Because of simple (node-oriented) protocol
  - We can model optimal placement via simulator



PUSH protocol

RNG N_1 R_1

SND N_1 N_3 R_1 R_3

SND N_3 N_2 R_1 R_1

PUSH protocol (hybrid)

RNG N_C R_1

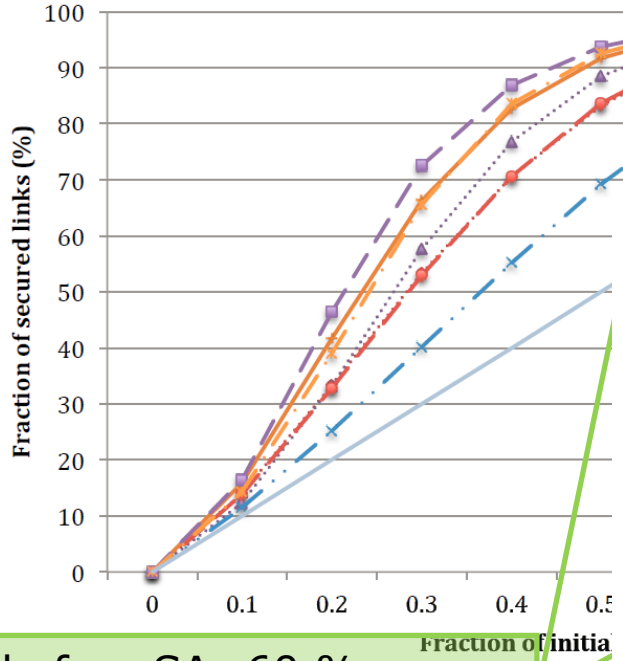
SND N_C $N_{0.7\_0.7}$ R_1 R_1

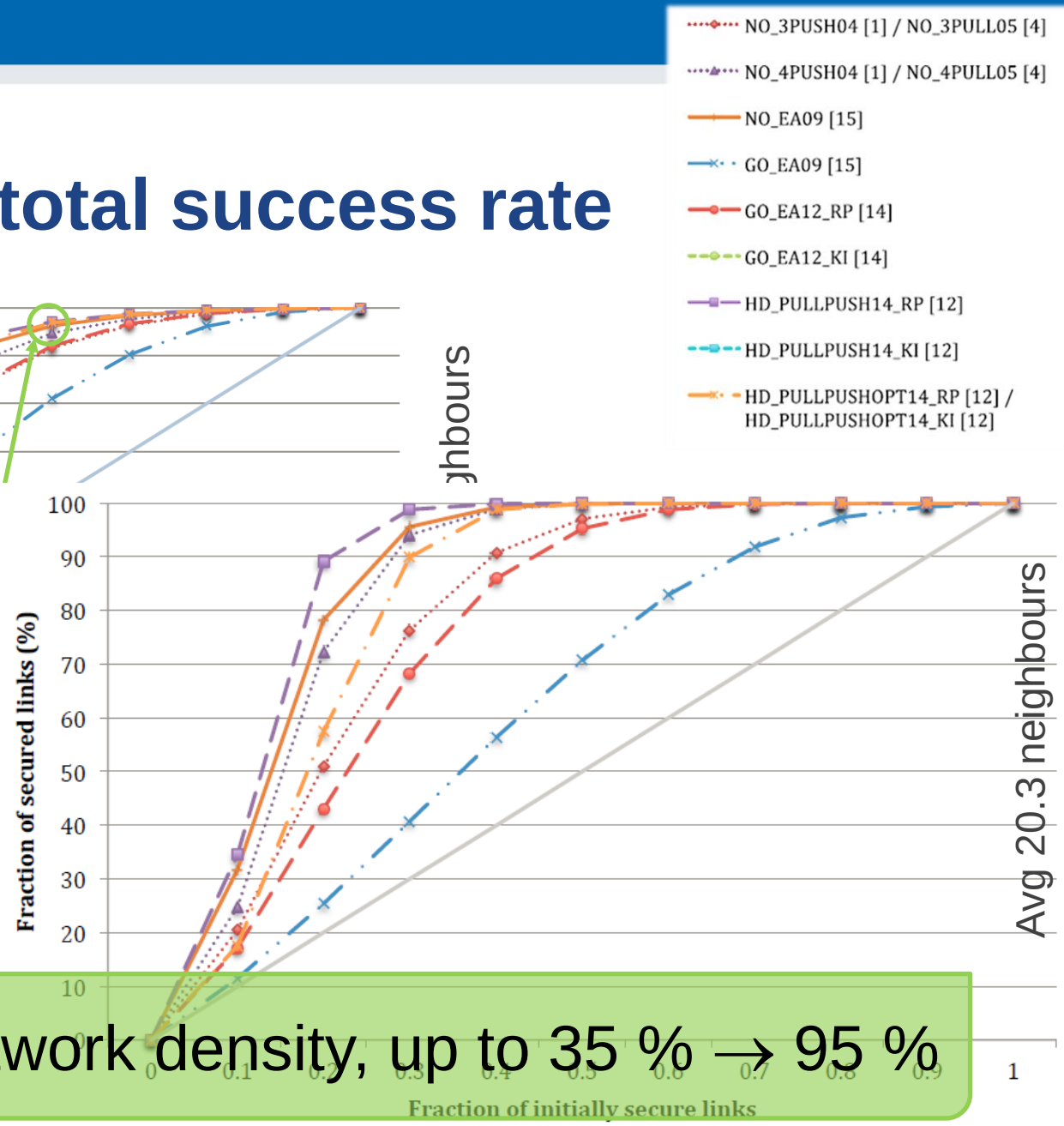
SND $N_{0.7\_0.7}$ N_P R_1 R_1

How well secrecy amplification performs?

COMPARISON

Comparison: total success rate

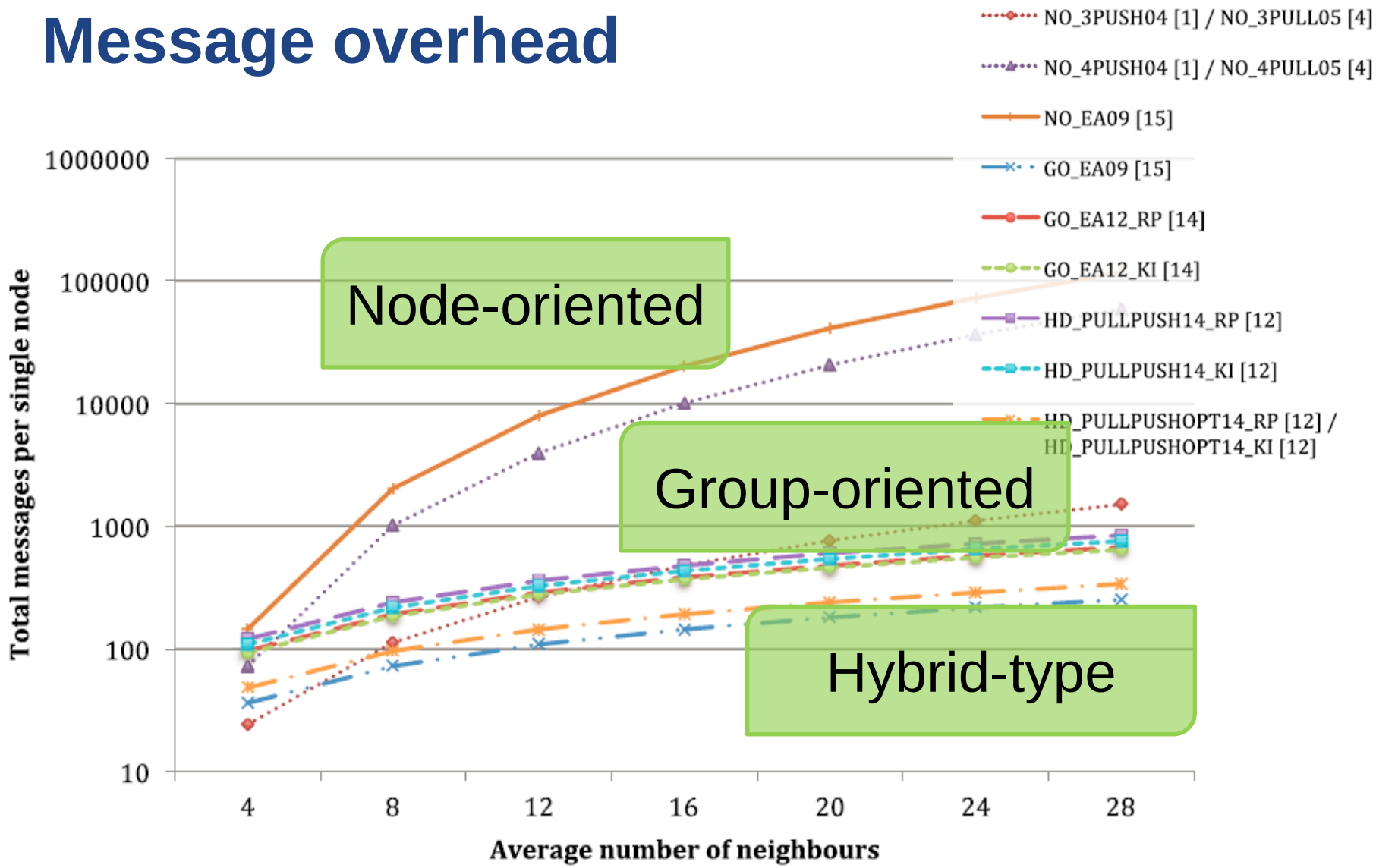




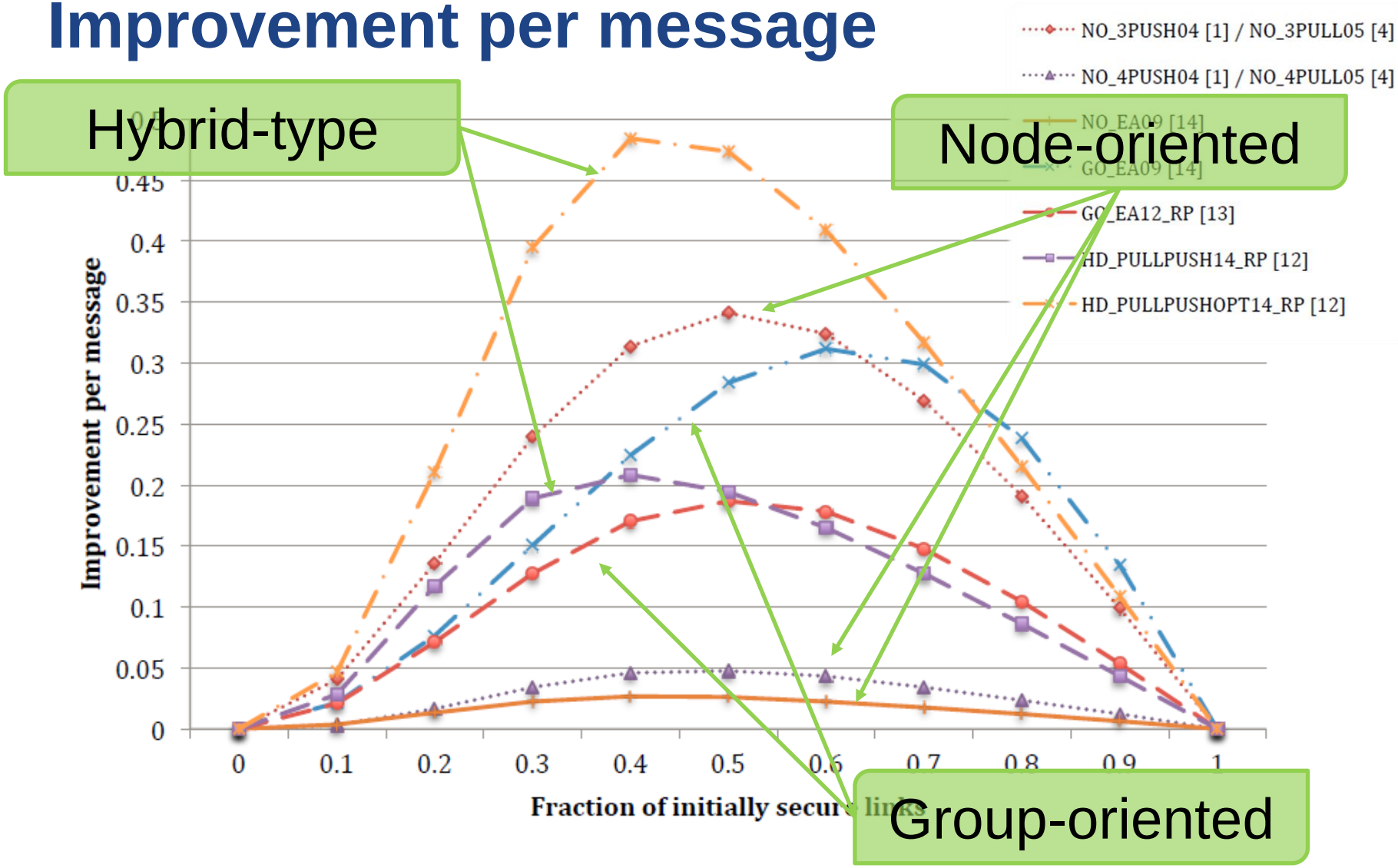
before SA: 60 % secure
after SA: 97 % secure

Depending on network density, up to 35 % → 95 %

Message overhead



Improvement per message



Practical implementation

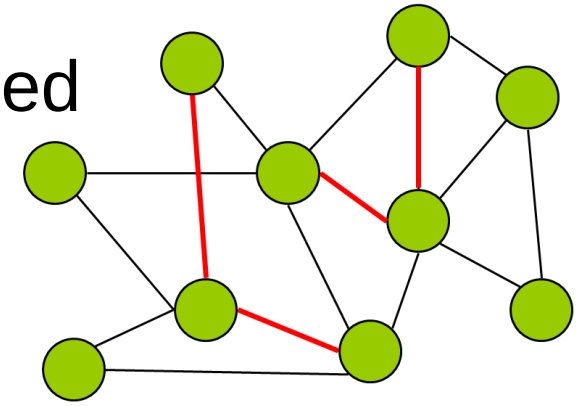
- TinyOS 2.1.2 implementation on TelosB node
- Size of state: #neighbors * 41 bytes (RAM)
- Size of code: less then 3 kB (EEPROM)
- E.g. if 10 neighbors on average:
  - 1kB data transmitted, seconds to execute
- Longest part is to establish relative radio distances
  - Minutes, but can be obtained from normal traffic

More in paper (and technical report)

- Unified notation of all compared protocols
- Comparison of important characteristics
- Comparison for different compromise patterns
  - Success rate
  - Message efficiency
- Practical implementation (TinyOS@TelosB)
- Open research questions
- Supplementary data
- http://crcs.cz/papers/wistp2015

Secrecy amplification usable when:

1. Networks with missing secure links
   – Compromised or not possible to establish
2. No knowledge which links are compromised
3. No knowledge about positioning of nodes
   – Only radio strength
4. Lightweight operation is required
   – Low number of messages
   – Small state size
   – Symmetric cryptography-based
5. Combined with key distribution scheme



Thank you for your attention!

Questions 

Supplementary info available here: http://crcs.cz/papers/wistp2015

References

- **[ACP04]** Anderson, R., Chan, H., Perrig, A.: Key infection: Smart trust for smart dust. 2004
- **[CS05]** D. Cvrček, P. Švenda. Smart dust security - Key Infection revisited. 2005
- **[KKLK05]** Yong Ho Kim, Mu Hyun Kim, Dong Hoon Lee, and Changwook Kim. A key management scheme for commodity sensor networks, 2005.
- **[SSM09]** P. Švenda, L. Sekanina, V. Matyáš, Evolutionary Design of Secrecy Amplification Protocols for Wireless Sensor Networks, 2009
- **[SSSM12]** T. Smolka, P. Švenda, L. Sekanina, V. Matyáš, Evolutionary design of message efficient secrecy amplification protocols, 2012
- **[OSM14]** Radim OŠŤÁDAL, Petr ŠVENDA a Václav MATYÁŠ. A New Approach to Secrecy Amplification in Partially Compromised Networks. In Rajat Subhra Chakraborty. *Security, Privacy, and Applied Cryptography Engineering - 4th International Conference*. Heidelberg: Springer, 2014. s. 92-109, 18 s. ISBN 978-3-319-12059-1.