BUSLab

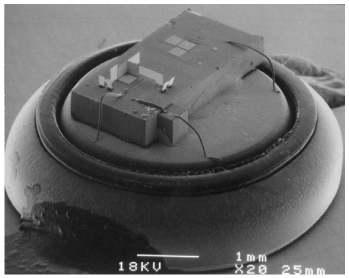
Brno University Security Laboratory

Evolutionary Design of Message Efficient Secrecy Amplification Protocols

Tobiáš Smolka*, Petr Švenda*, Lukáš Sekanina’, Vashek Matyáš*

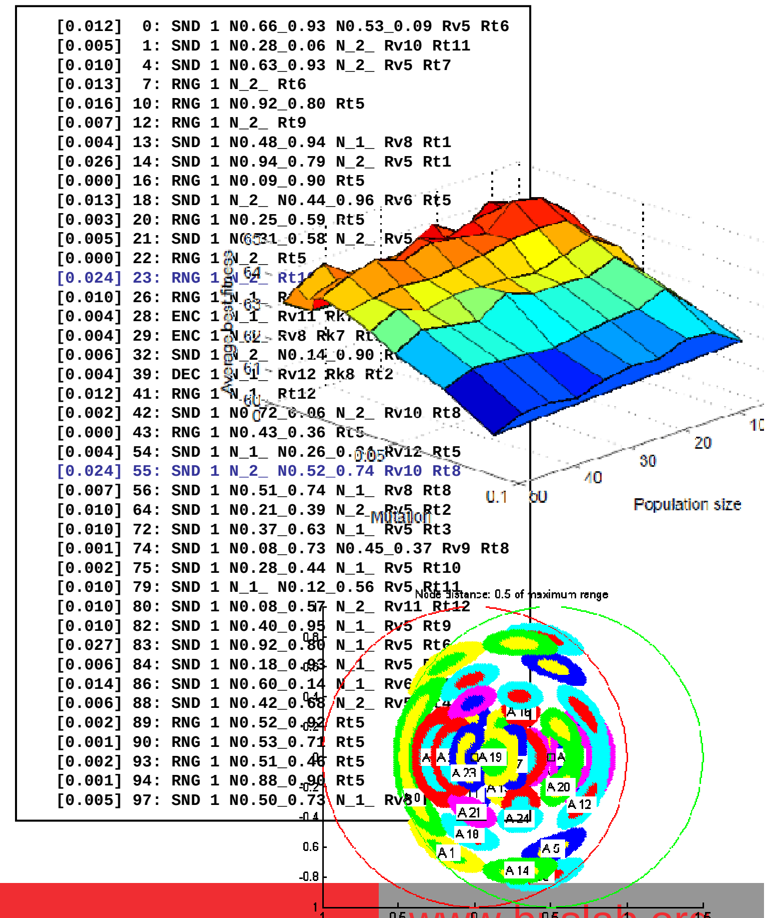
*Masaryk University, Czech Republic

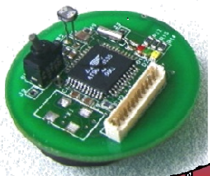
‘Brno University of Technology, Czech Republic



Wireless Sensor Networks (WSN)

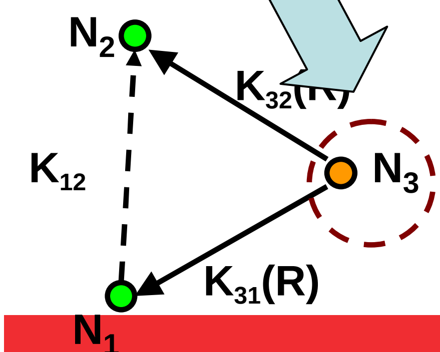
New results and EA behavior

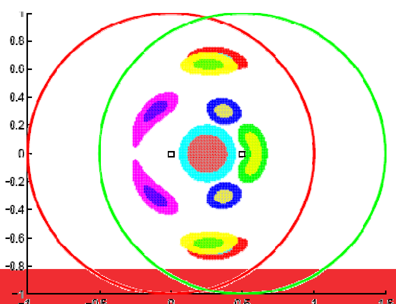


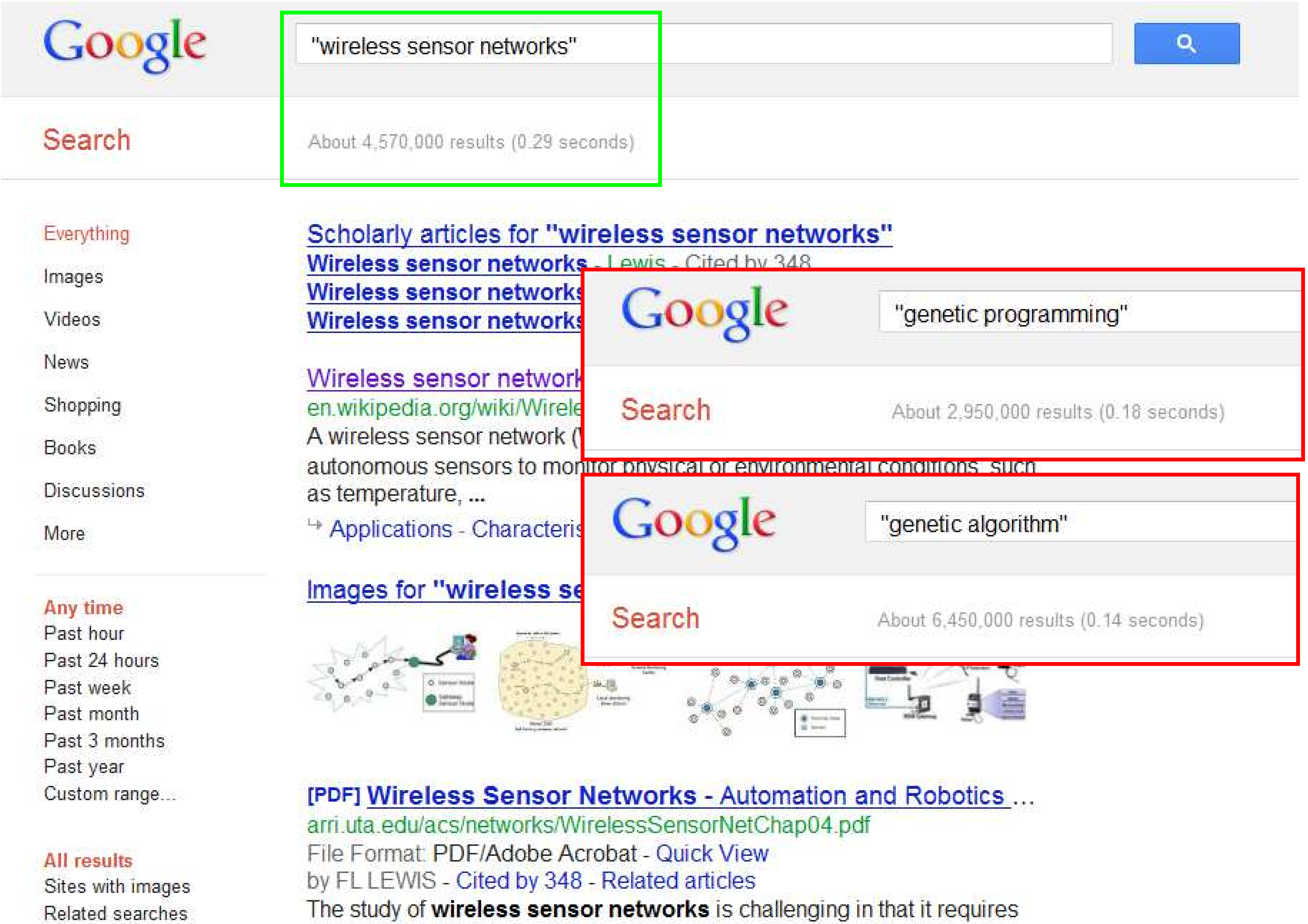


Security in WSN

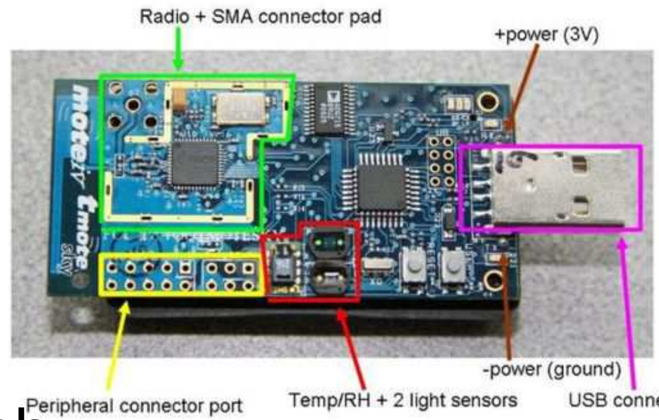
Secrecy Amplification Protocols



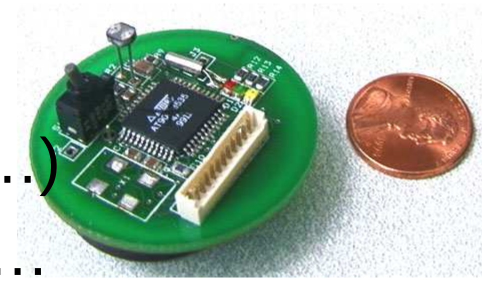



Google
"wireless sensor networks"
Search
About 4,570,000 results (0.29 seconds)
Everything
Images
Videos
News
Shopping
Books
Discussions
More
Any time
Past hour
Past 24 hours
Past week
Past month
Past 3 months
Past year
Custom range...
All results
Sites with images
Related searches
Scholarly articles for "wireless sensor networks"
Wireless sensor networks - Lewis - Cited by 348
Wireless sensor network
en.wikipedia.org/wiki/Wirele
A wireless sensor network (
autonomous sensors to monitor physical or environmental conditions, such
as temperature, ...
Applications - Characteris
Images for "wireless se
[PDF] Wireless Sensor Networks - Automation and Robotics ...
arri.uta.edu/acs/networks/WirelessSensorNetChap04.pdf
File Format: PDF/Adobe Acrobat - Quick View
by FL LEWIS - Cited by 348 - Related articles
The study of wireless sensor networks is challenging in that it requires
Google
"genetic programming"
Search
About 2,950,000 results (0.18 seconds)
Google
"genetic algorithm"
Search
About 6,450,000 results (0.14 seconds)

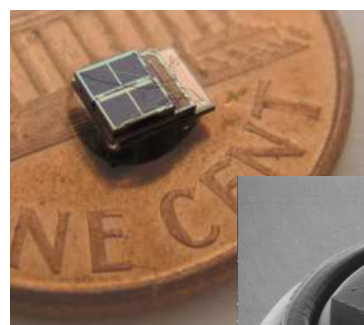
Wireless Sensor Node

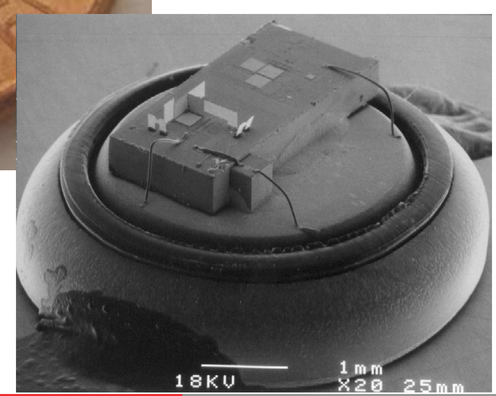


- Basic technology
  - 8 bit CPU, ~1 kB RAM, ~10^2 kB flash
  - short range radio, battery powered
  - condition sensor (temperature, pressure…)
  - xBow MicaZ, TelosB, Philips smart node…



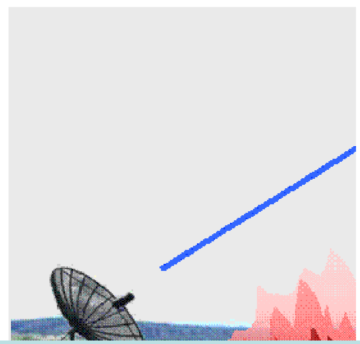
- Putting pieces together…
  - battery-powered small MCU
  - + efficient radio module
  - + environmental sensor
  - => Wireless Sensor Network (WSN)

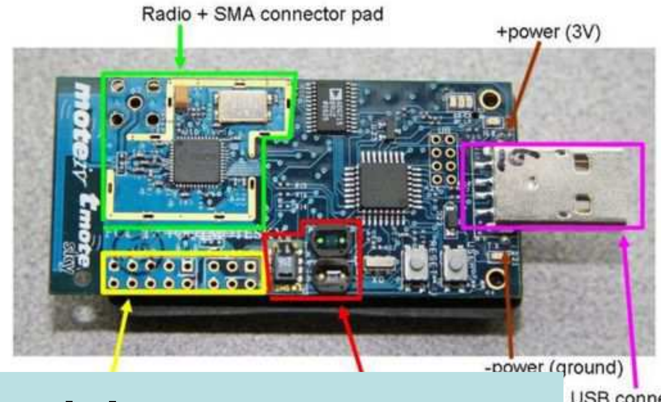




Ideal in 2000:

WSN is highly distributed network with high number of low-cost sensor nodes powered by battery connected via multi-hop communication with base station



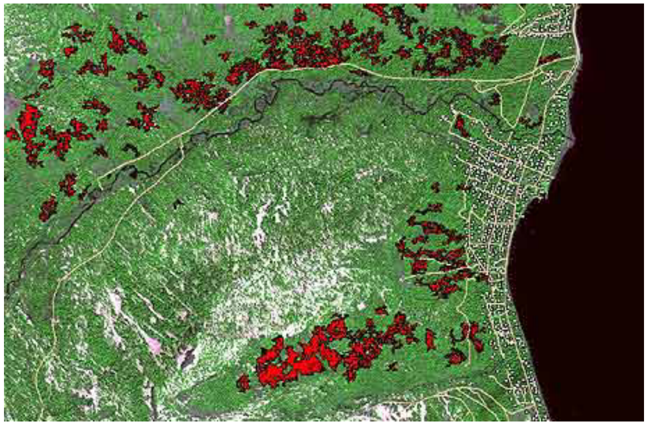


- The price of node is a current problem
  - currently ~100$ or more (complete node)
  - (but 3.35 $ for CC1110F32)

Do we have useful application for WSN?

Traffic control

Medical information



Remote fire detection

Combat field control

We (will) have exciting technology.

Why/What security measures should be used?

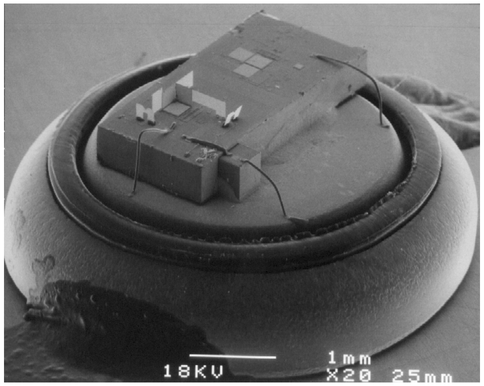
Where do we need security in WSN?

- Sensitive data are often sensed/processed
  - military application
  - medical information, location data (privacy)
- Commercially viable information
  - information for sale – cost for owner of the network
  - know-how - agriculture monitoring
- Protection against vandalism
- Early stage of WSN allows to build security in rather than as late patch
  - as is the case with Internet today

We will limit ourselves to key establishment protocols

Why not to use existing cryptographic solutions?

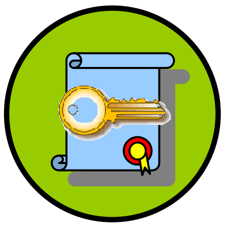
Some differences from standard networks



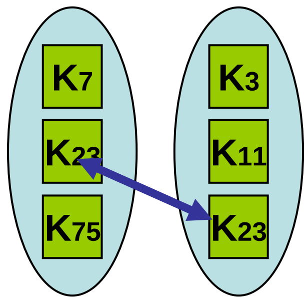
- Running on battery (limited resource)
  - days for personal network
  - years for large scale monitoring network
  - especially communication is energy-expensive
- Relatively limited computation power
  - powerful CPU possible, but energy demanding
- Nodes can be captured by an attacker
  - all secrets can be extracted from unprotected nodes
  - and returned back as malicious node

Many ways how to establish keys

Asymmetric cryptography

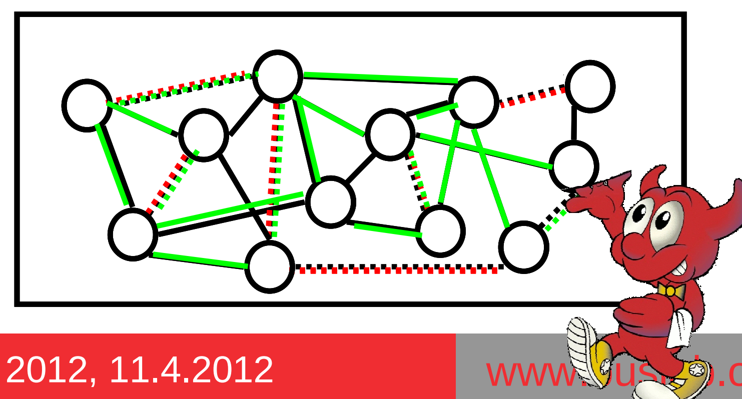


Probabilistic pre-distribution

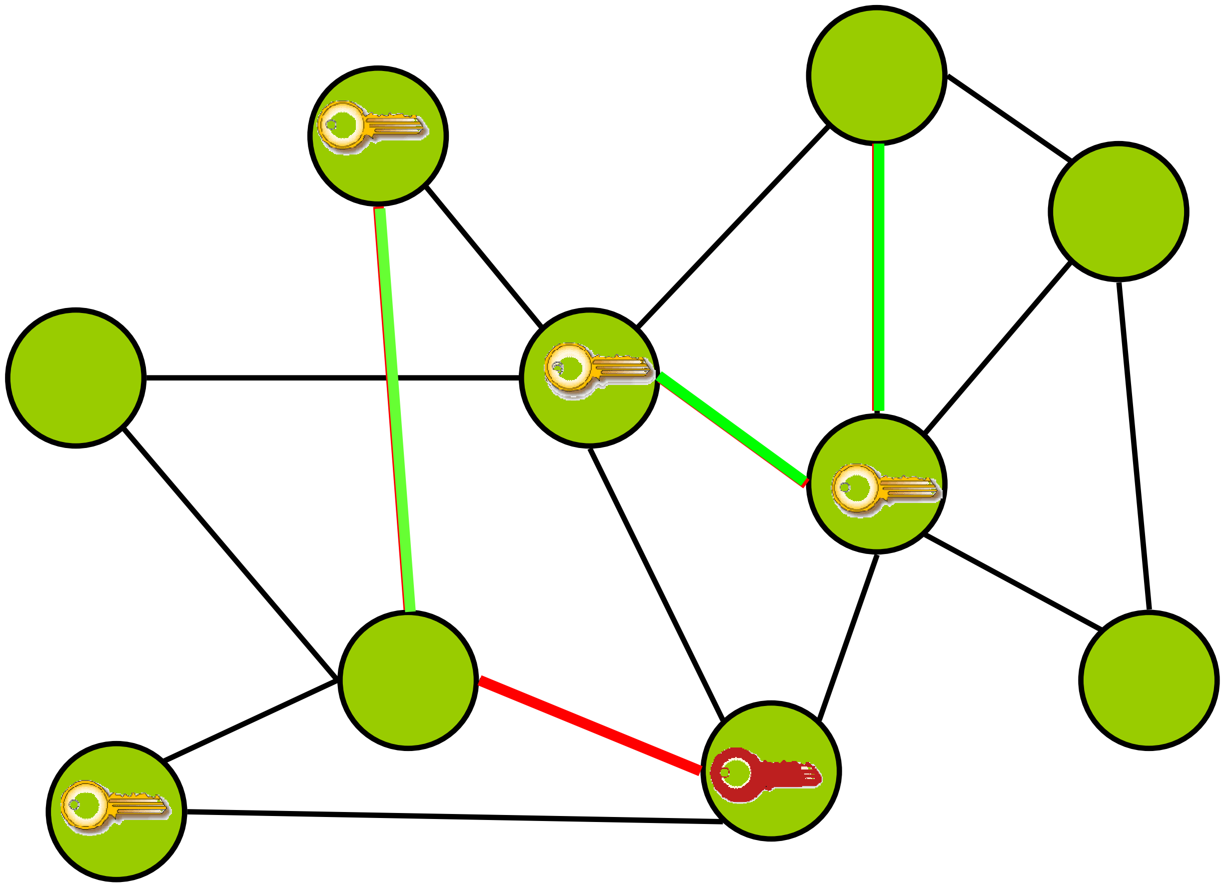


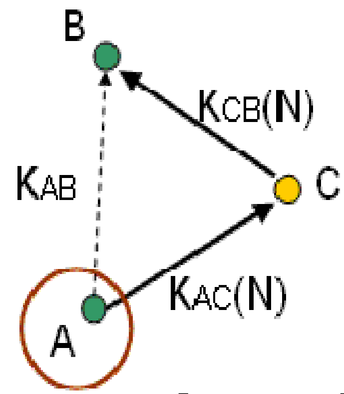
Trusted party

Master key, pairwise keys



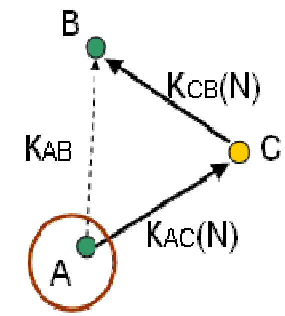
Secrecy amplification protocols



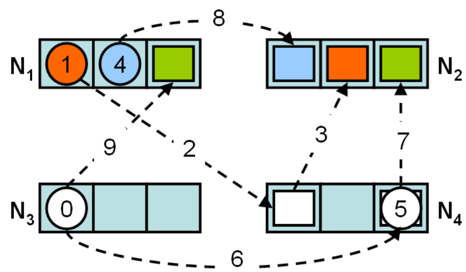


PUSH [ACP04]

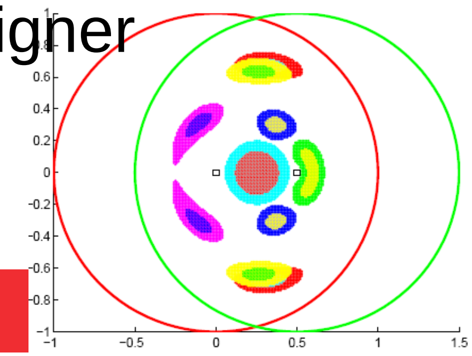
Published secrecy amplification protocols



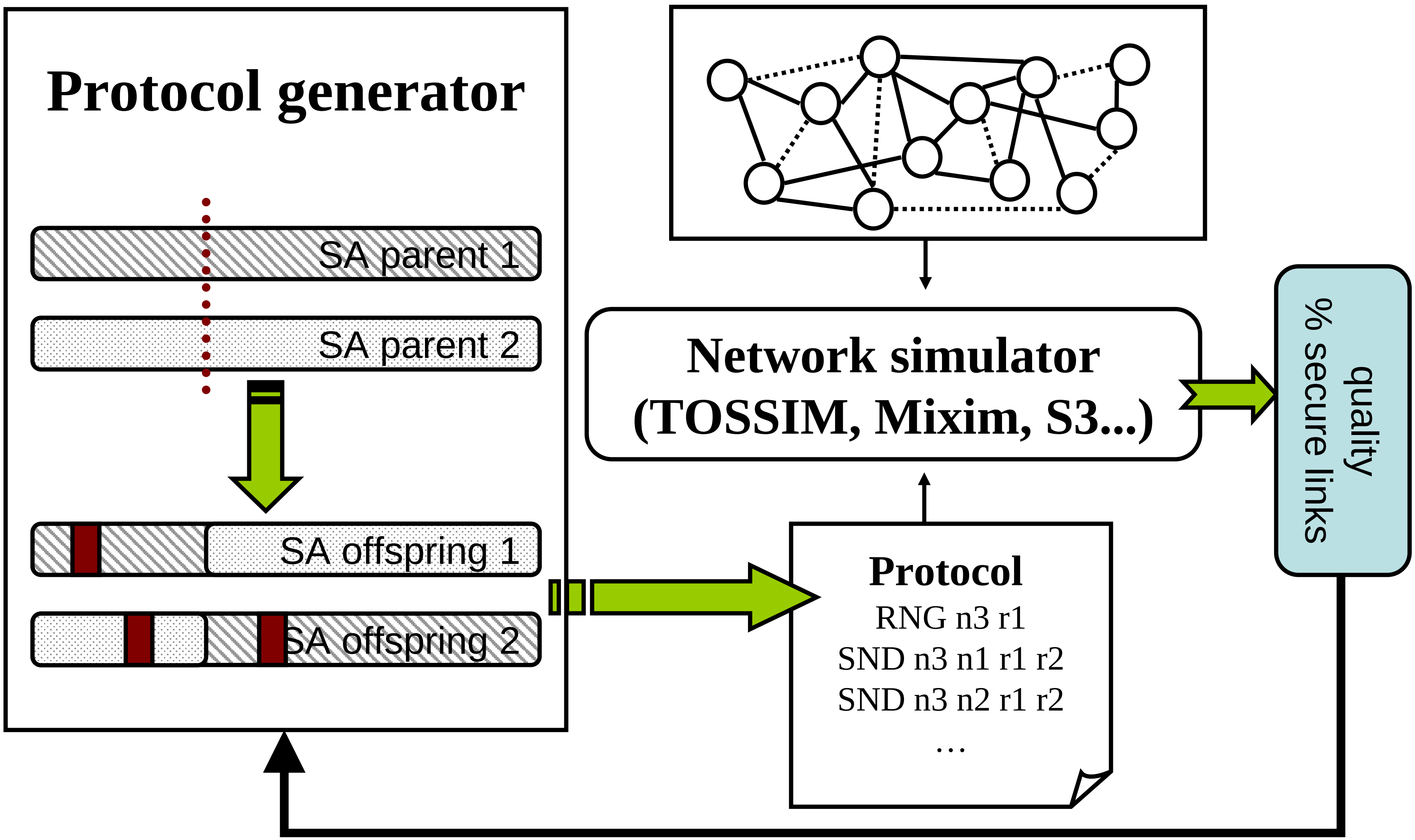
- Node-oriented protocols
  - PUSH [ACP04], 2004, manually
  - PULL [CS05], 2005, manually
  - COMODITY [KKLK05], 2005, manually
  - NOEA [SSM09], 2009, automatically
    - all published reinvented + better found
  - Problem: very message expensive



- Group-oriented protocols
  - less messages achieved by different protocol design
  - but far more complicated for protocol designer
  - GOEA [SSM09], 2009, automatically

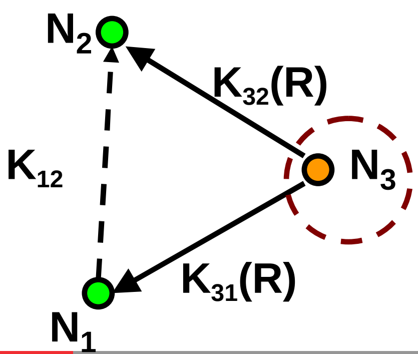


Automatic protocol generation (APG)



Elementary instructions

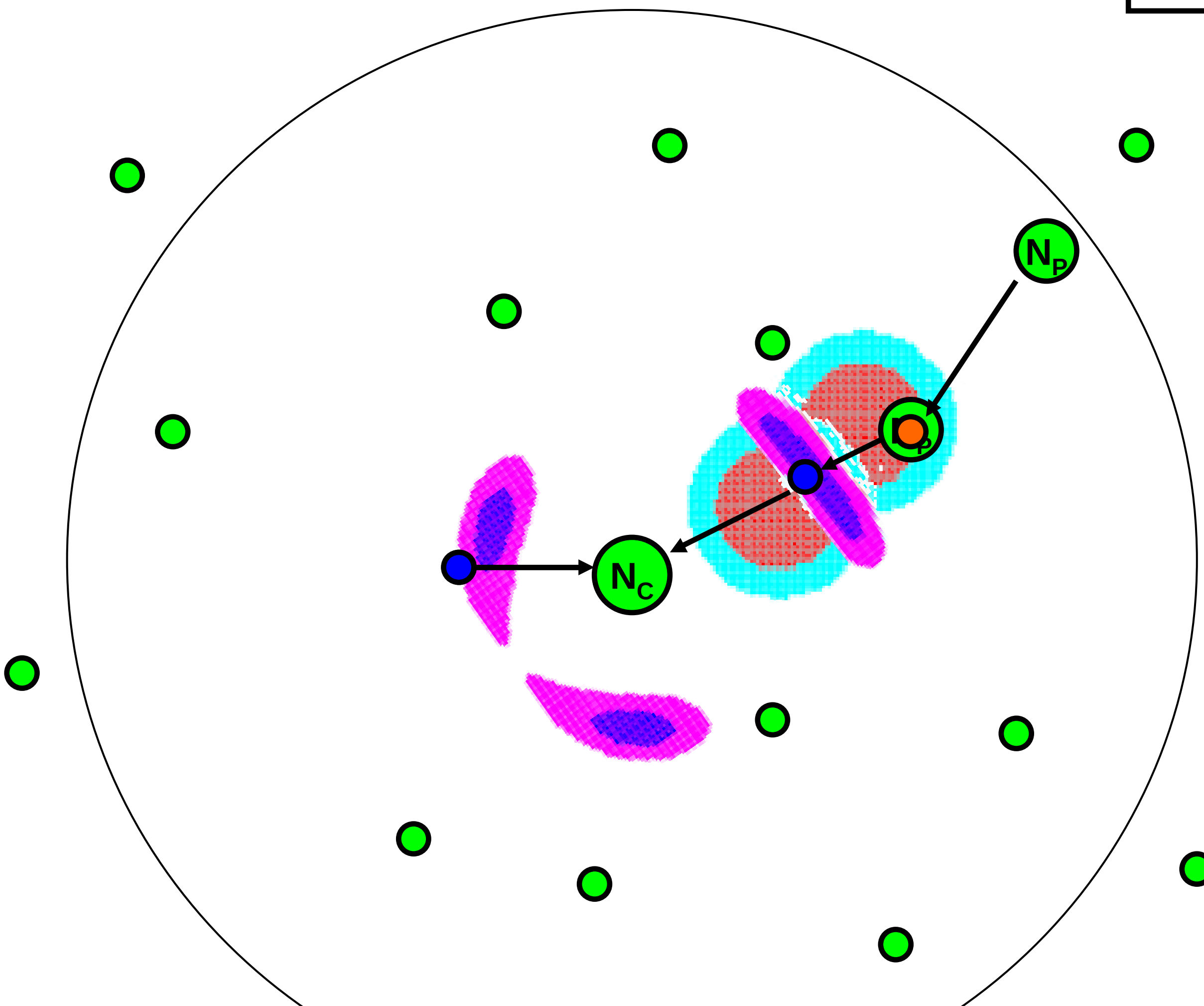
- Node (N) modeled as a simple machine with limited number of memory registers (R)
  - usually around 10-20
- Protocol with fixed number of elementary instruction
  - RNG N_a R_i — *generate new key*
  - ENCRYPT N_a R_i R_j R_k — *encrypt value with key*
  - DECRYPT N_a R_i R_j R_k — *decrypt value with key*
  - SEND N_a N_b R_i R_j — *send value between nodes*
  - COMBINE N_a R_i R_j R_k — *combination of two values*
  - NOP, on/off switch — *no operation*
- Example PULL [CS05]:
  - RNG N_3 R_1; SND N_3 N_1 R_1 R_1; SND N_3 N_2 R_1 R_1;

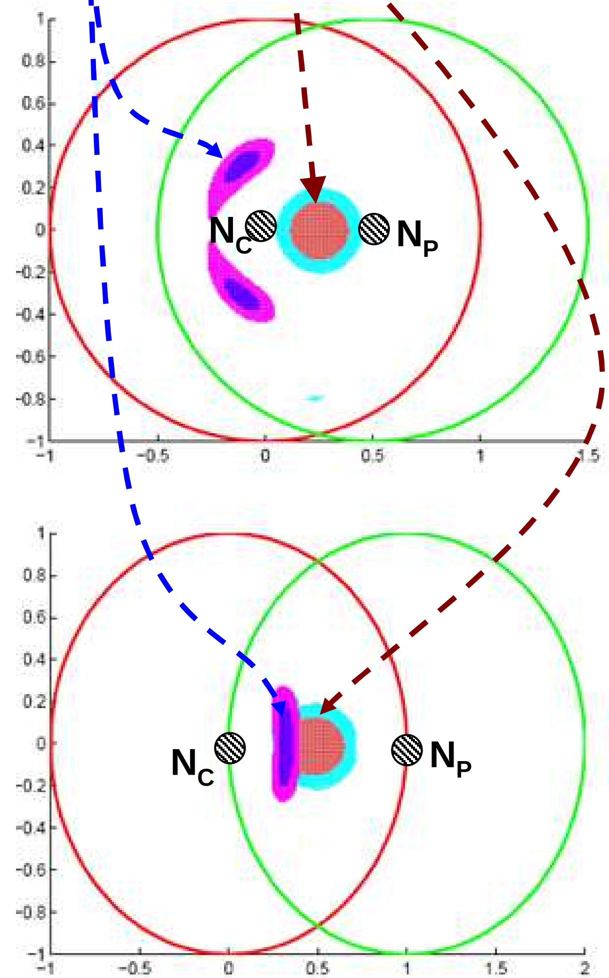


$$\min[(Np_1 - |N_C - Nx|)^2 + (Np_2 - |N_P - Nx|)^2]$$

Group-oriented protocol

RNG N_P Rt11
SND N_P N0.00 0.00 Rv11 Rt12
SND N0.35 0.67 N_C Rv12 Rt2

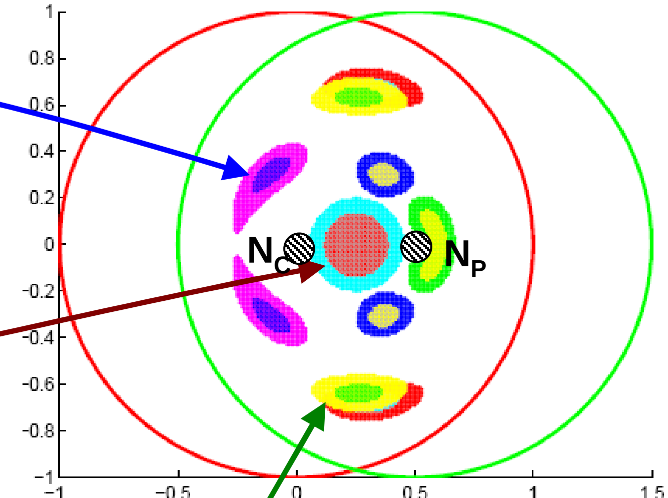


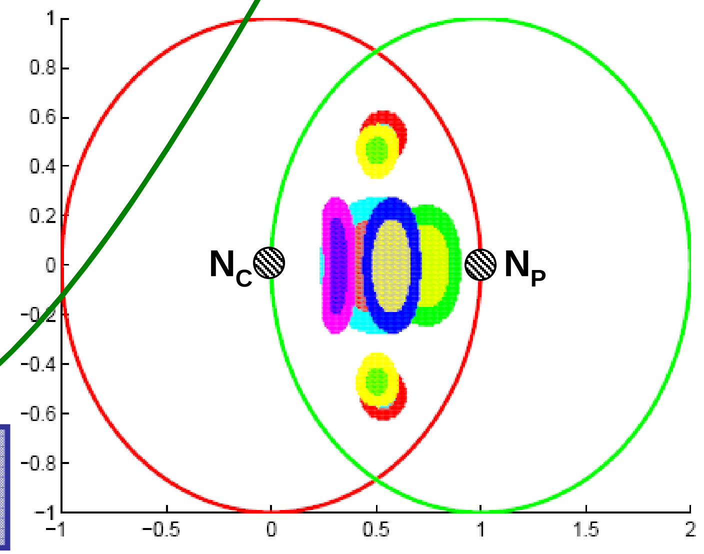


Total protocols runs: 11, ~100 messages

Results found – group-oriented [SSM09]

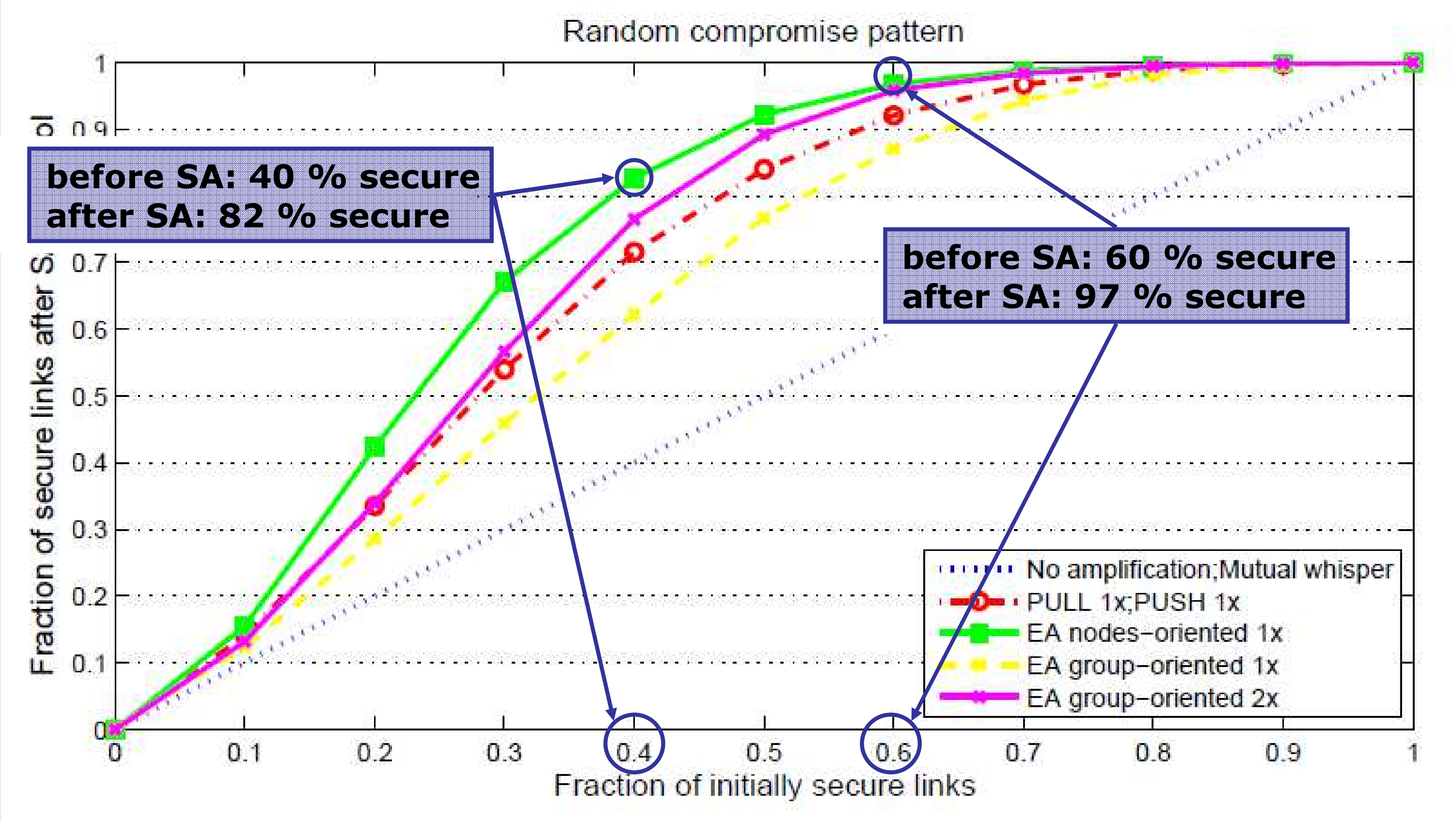
(0.070) 00: SND N0.33 0.68 N_P Rv6 Rt8
(0.070) 01: SND N0.35 0.67 N_C Rv6 Rt2
(0.334) 02: RNG N_P Rt11
(0.010) 03: SND N0.59 0.11 N_P Rv7 Rt3
(0.007) 04: SND N_P N0.75 0.70 Rv6 Rt1
(0.334) 05: SND N_P N0.01 0.00 Rv11 Rt12
(0.003) 06: SND N0.01 0.00 N_C Rv1 Rt5
(0.334) 07: SND N0.01 0.00 N_C Rv12 Rt6
(0.014) 08: RNG N0.03 0.00 Rt1
(0.014) 09: SND N0.48 0.33 N_P Rv1 Rt7
(0.077) 10: RNG N0.01 0.00 Rt6
(0.017) 11: SND N0.69 0.68 N_C Rv1 Rt7





12 instructions, 6 different areas for nodes

How well is secrecy amplification working?



How evolutionary algorithms behave on such a problem?

What can we search/optimize for?

- Instructions and protocol length
- Number of nodes involved
- Geographic identification of parties
- Number of memory slots used
- Repetitions of subparts or whole protocol

Used framework

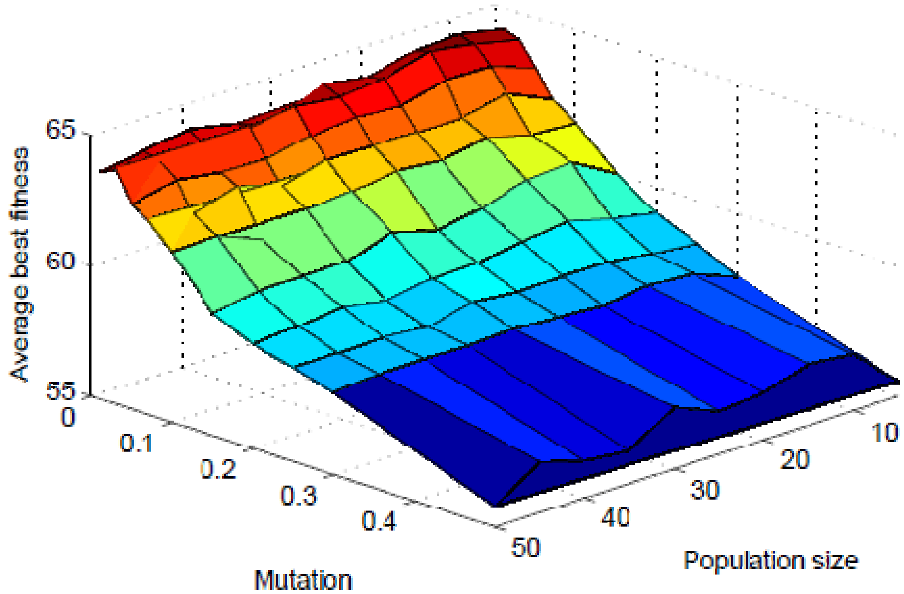
280 CPUs @ 3GHz

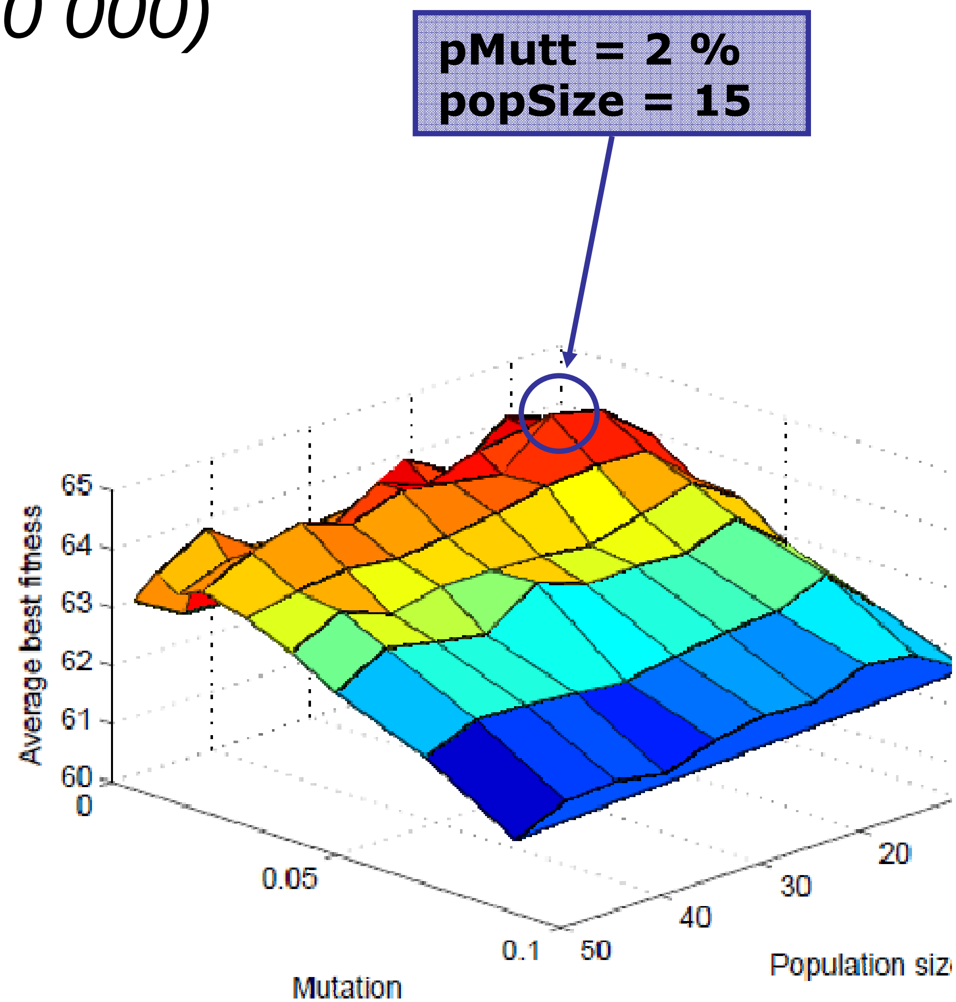
GALib library

Sensor Security Simulator – task optimized simulator
http://www.fi.muni.cz/~xsvenda/s3.html

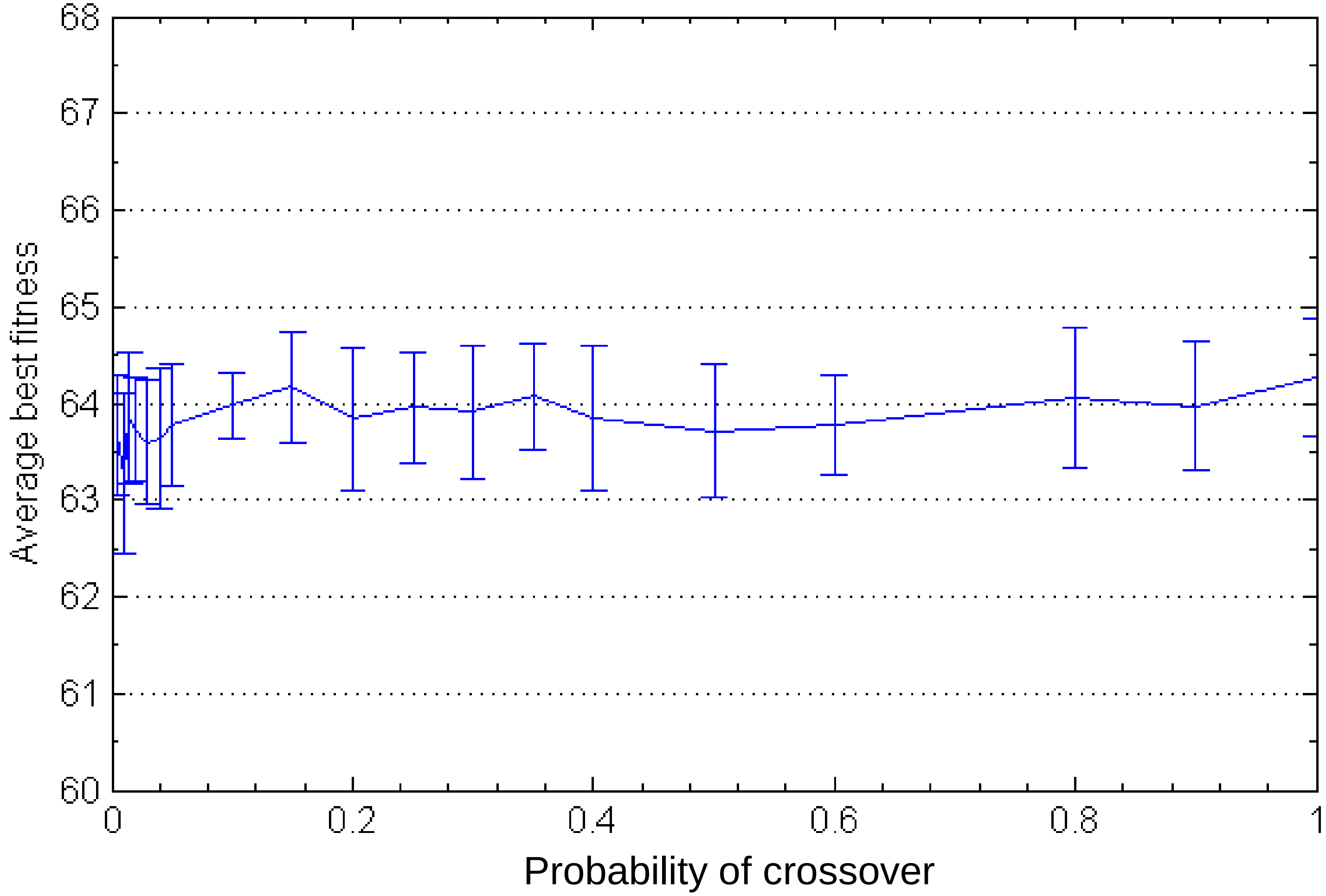
Optimal pop size, mutation probability

- *(popSize * numGen = 40 000)*

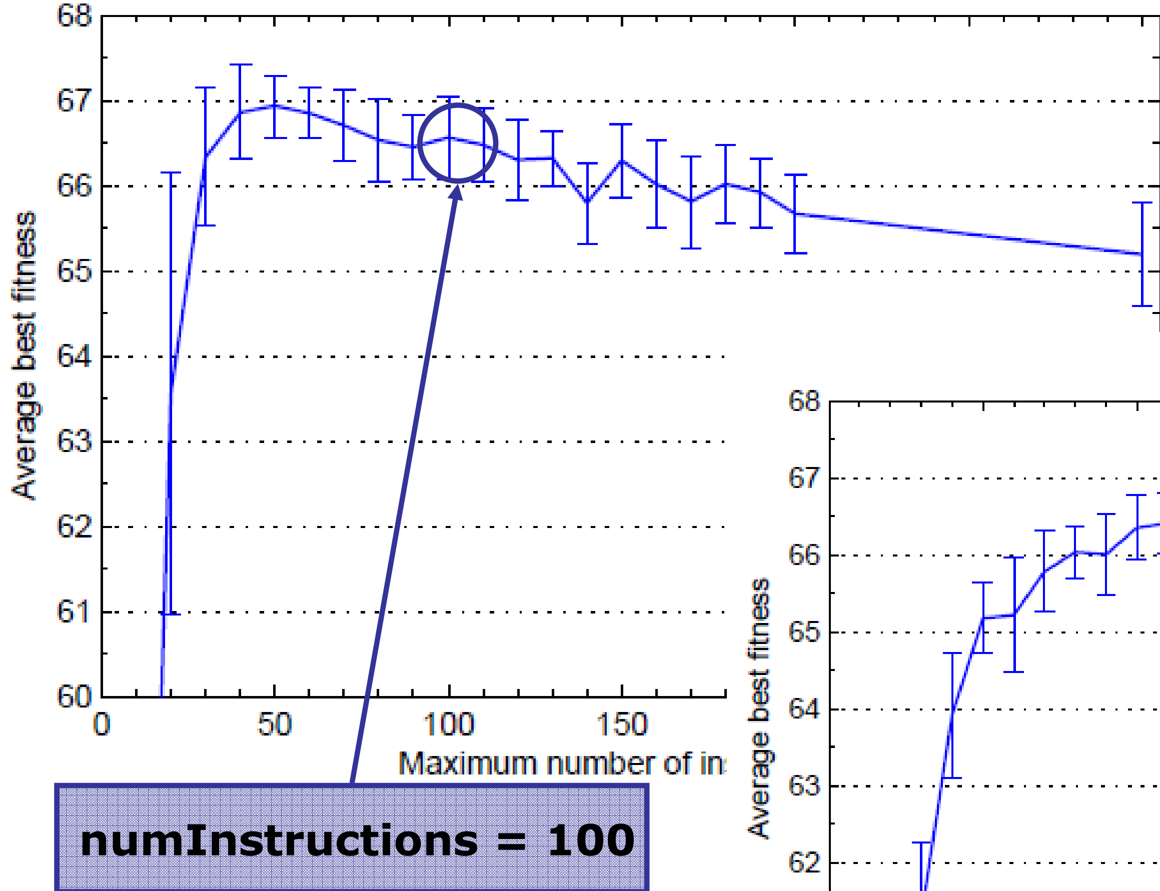


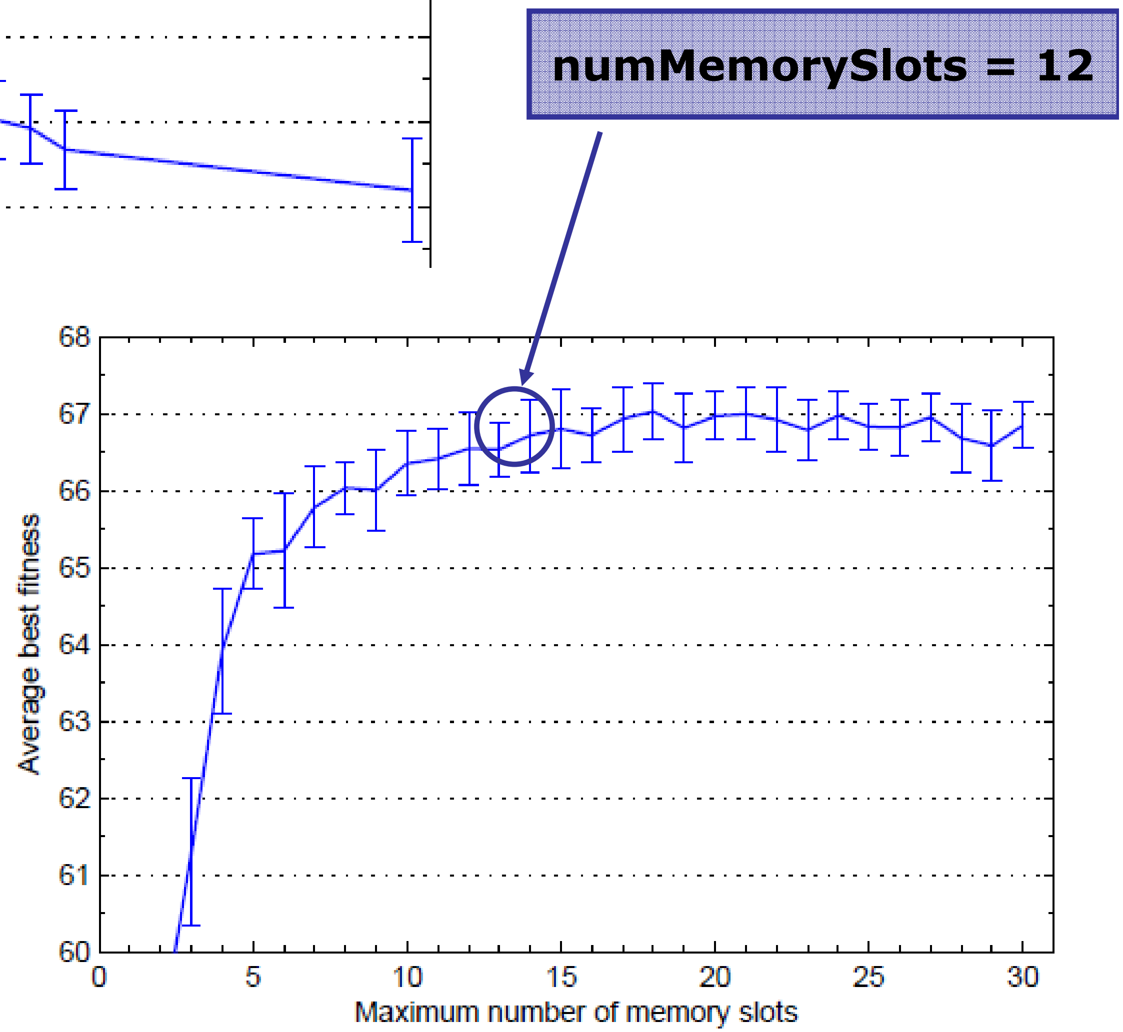


Crossover (no significant impact)



Number of instructions/memory slots



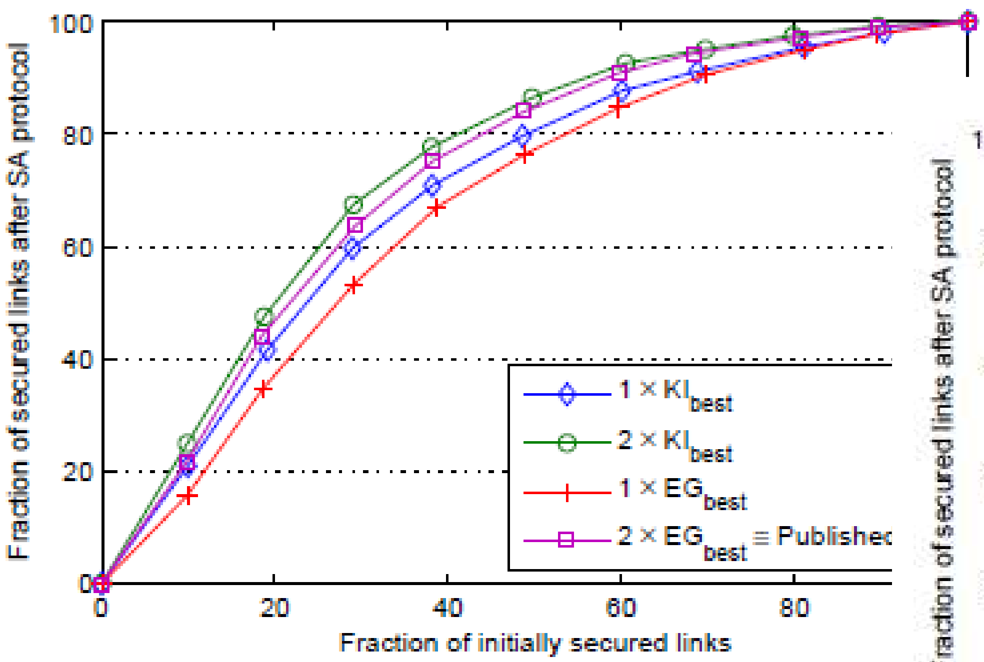


- *(numIns * numGer*

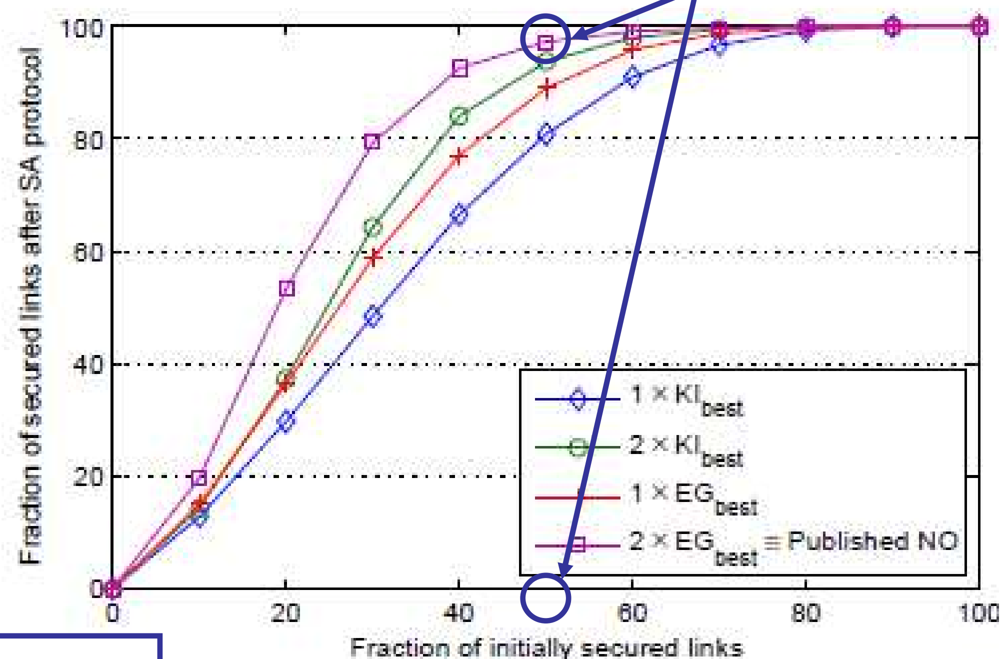
Long running experiments

- For two different compromise patterns KI & EG
- Best after 330641 (KI) & 165365 (EG) generations

before SA: 50 % secure
after SA: 98 % secure



(a) KI compromise pattern

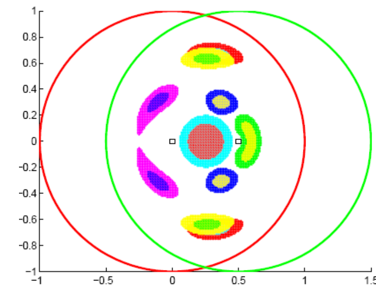


(b) EG compromise pattern

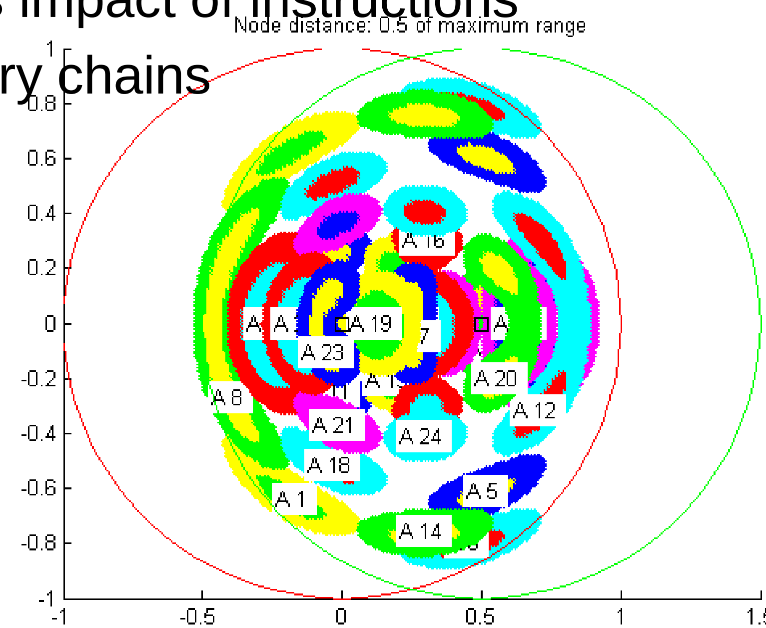
group oriented == node oriented
but only 1/20 messages used

New protocol(s) found (EG_{best})

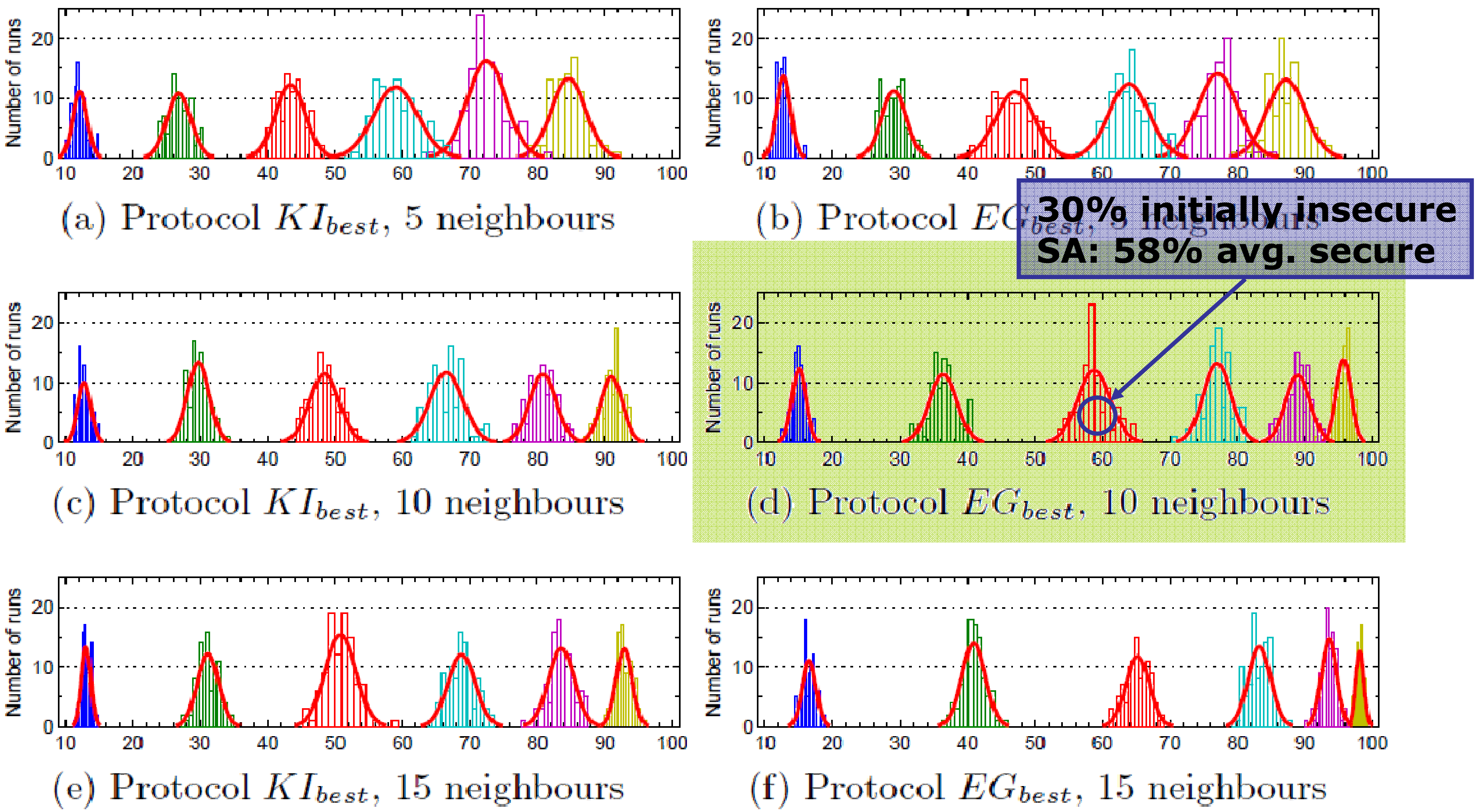
```
[0.012]  0: SND 1 N0.66_0.93 N0.53_0.09 Rv5 Rt6
[0.005]  1: SND 1 N0.28_0.06 N_2_ Rv10 Rt11
[0.010]  4: SND 1 N0.63_0.93 N_2_ Rv5 Rt7
[0.013]  7: RNG 1 N_2_ Rt6
[0.016] 10: RNG 1 N0.92_0.80 Rt5
[0.007] 12: RNG 1 N_2_ Rt9
[0.004] 13: SND 1 N0.48_0.94 N_1_ Rv8 Rt1
[0.026] 14: SND 1 N0.94_0.79 N_2_ Rv5 Rt1
[0.000] 16: RNG 1 N0.09_0.90 Rt5
[0.013] 18: SND 1 N_2_ N0.44_0.96 Rv6 Rt5
[0.003] 20: RNG 1 N0.25_0.59 Rt5
[0.005] 21: SND 1 N0.31_0.58 N_2_ Rv5 Rt3
[0.000] 22: RNG 1 N_2_ Rt5
[0.024] 23: RNG 1 N_2_ Rt10
[0.010] 26: RNG 1 N_1_ Rt5
[0.004] 28: ENC 1 N_1_ Rv11 Rk7 Rt8
[0.004] 29: ENC 1 N_1_ Rv8 Rk7 Rt12
[0.006] 32: SND 1 N_2_ N0.14_0.90 Rv9 Rt5
[0.004] 39: DEC 1 N_1_ Rv12 Rk8 Rt2
[0.012] 41: RNG 1 N_1_ Rt12
[0.002] 42: SND 1 N0.72_0.06 N_2_ Rv10 Rt8
[0.000] 43: RNG 1 N0.43_0.36 Rt5
[0.004] 54: SND 1 N_1_ N0.26_0.34 Rv12 Rt5
[0.024] 55: SND 1 N_2_ N0.52_0.74 Rv10 Rt8
[0.007] 56: SND 1 N0.51_0.74 N_1_ Rv8 Rt8
[0.010] 64: SND 1 N0.21_0.39 N_2_ Rv5 Rt2
[0.010] 72: SND 1 N0.37_0.63 N_1_ Rv5 Rt3
[0.001] 74: SND 1 N0.08_0.73 N0.45_0.37 Rv9 Rt8
[0.002] 75: SND 1 N0.28_0.44 N_1_ Rv5 Rt10
[0.010] 79: SND 1 N_1_ N0.12_0.56 Rv5 Rt11
[0.010] 80: SND 1 N0.08_0.57 N_2_ Rv11 Rt12
[0.010] 82: SND 1 N0.40_0.95 N_1_ Rv5 Rt9
[0.027] 83: SND 1 N0.92_0.80 N_1_ Rv5 Rt6
[0.006] 84: SND 1 N0.18_0.93 N_1_ Rv5 Rt4
[0.014] 86: SND 1 N0.60_0.14 N_1_ Rv6 Rt11
[0.006] 88: SND 1 N0.42_0.68 N_2_ Rv5 Rt4
[0.002] 89: RNG 1 N0.52_0.92 Rt5
[0.001] 90: RNG 1 N0.53_0.71 Rt5
[0.002] 93: RNG 1 N0.51_0.46 Rt5
[0.001] 94: RNG 1 N0.88_0.90 Rt5
[0.005] 97: SND 1 N0.50_0.73 N_1_ Rv8 Rt7
```



- Found after 165 365 generations
- Pruned version from 100 INS
  - 41=24 SND+14 RNG+3ENC/DEC
- Functional analysis is an issue
  - visualization of probable positions
  - fitness impact of instructions
  - memory chains



Robustness of discovered protocols



(a) Protocol KI_{best}, 5 neighbours

(b) Protocol EG_{best}, 5 neighbours

(c) Protocol KI_{best}, 10 neighbours

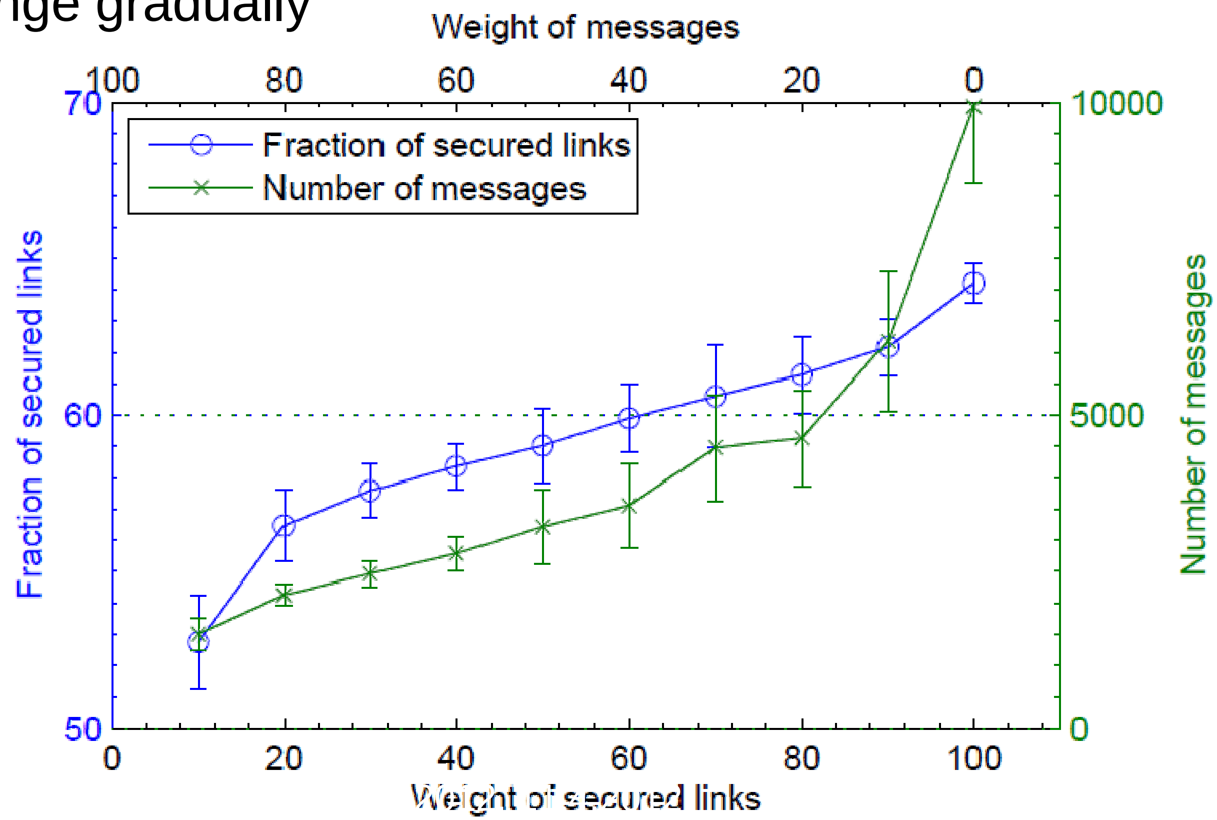
(d) Protocol EG_{best}, 10 neighbours

(e) Protocol KI_{best}, 15 neighbours

(f) Protocol EG_{best}, 15 neighbours

Multi-criteria optimization

- Fitness = **#secure_links** & **#messages_transmitted**
- Weighted fitness construction
  - 90:10 weights "optimal"
  - 20-80 range change gradually



Summary

- Secrecy amplification protocols significantly increase security of partially compromised networks
  - new protocols constructed from simple instructions
  - automated search based on LGP used
- Detailed examination of LGP settings
- New and better group-oriented protocols found
  - outperforms node-oriented with only about 1/20 messages
  - turning 50% compromised network into 98% secured

Thank you for your attention!

Questions

http://www.fi.muni.cz/~xsvenda/papers/EuroGP2012

References

- [EG02] L. Eschenauer, V. D. Gligor. A key-management scheme for distributed sensor networks. 2002
- [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.
- [SM07] P. Švenda, V. Matyáš. Authenticated key exchange with group support for wireless sensor networks. 2007
- [SSM09] P. Švenda, L. Sekanina, V. Matyáš, Evolutionary Design of Secrecy Amplification Protocols for Wireless Sensor Networks, 2009