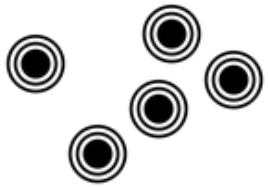
Reconsidering Attacker Models in Ad-hoc Networks

An attacker is neither random, nor jumping

Radim Ostadal, Petr Švenda, Vashek Matyas
ostadal@mail.muni.cz {svenda, matyas}@fi.muni.cz
Faculty of Informatics, Masaryk University

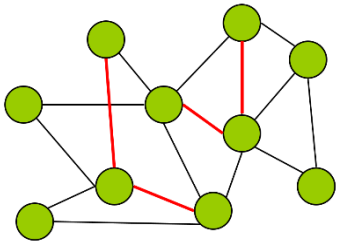
CROCS
Centre for Research on Cryptography and Security

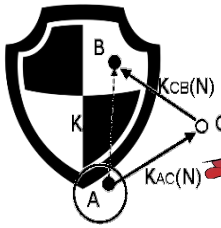
What we are trying to achieve



Nodes deployment

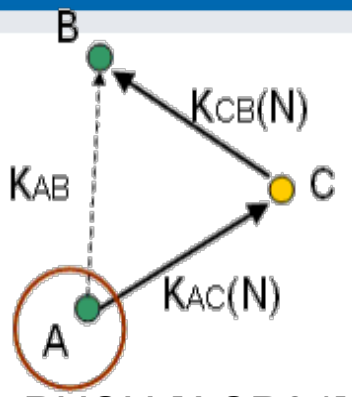
Basic link keys establishment



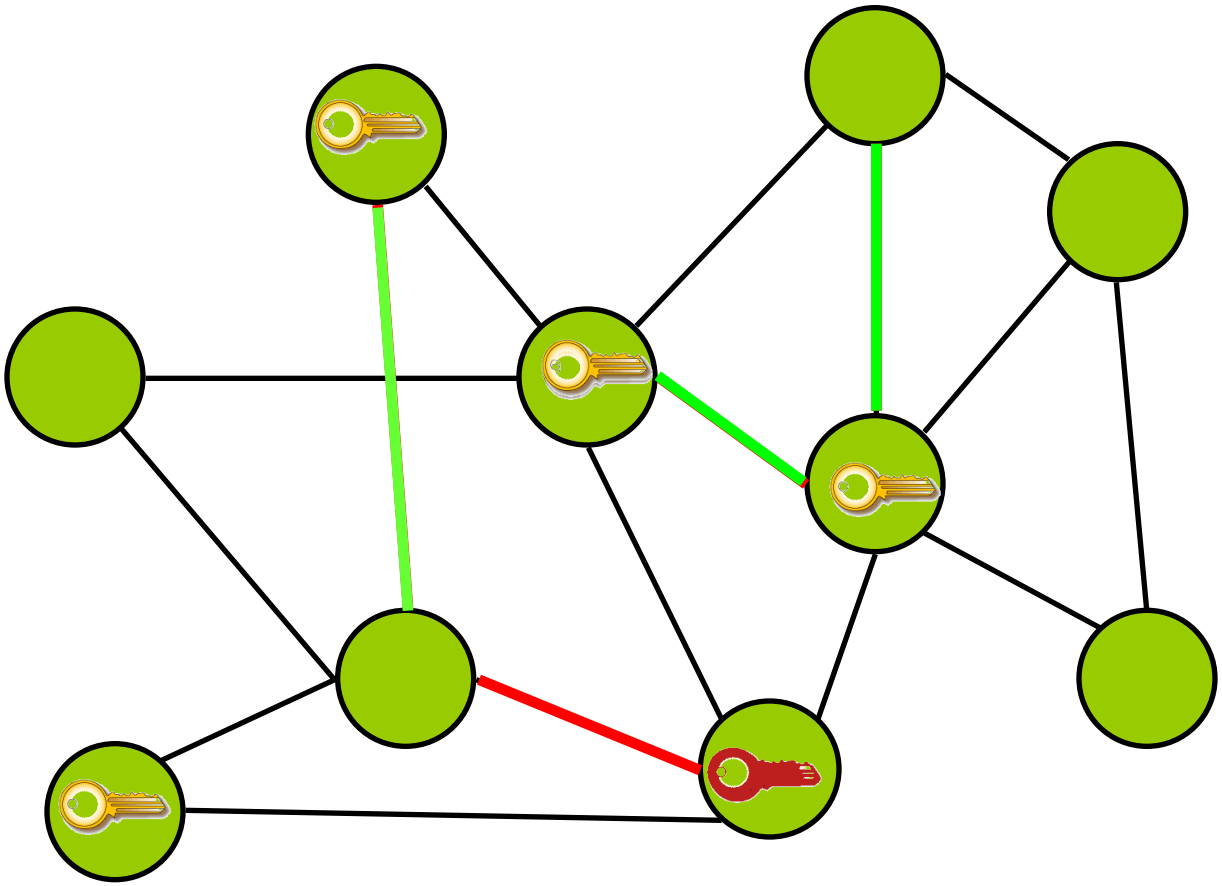


Secrecy amplification (SA)

Secrecy amplification protocol

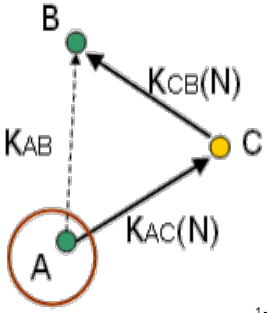


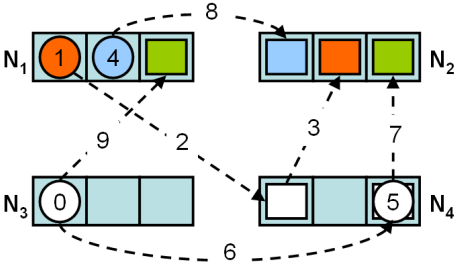
PUSH [ACP04]

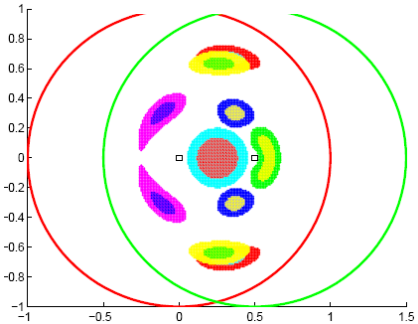


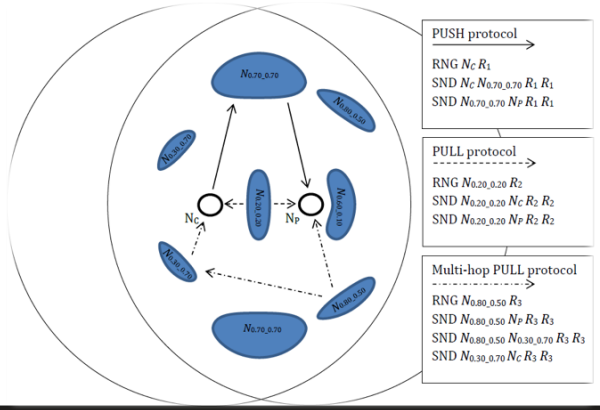
Published secrecy amplification protocols

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}, HP_{FINAL} semi-automatic [OSM14]
   - HP_{OPT} semi-automatic [OSM15]

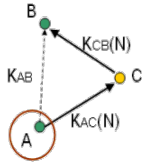
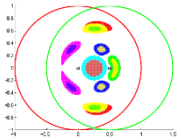
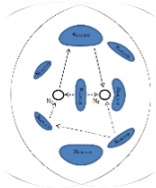






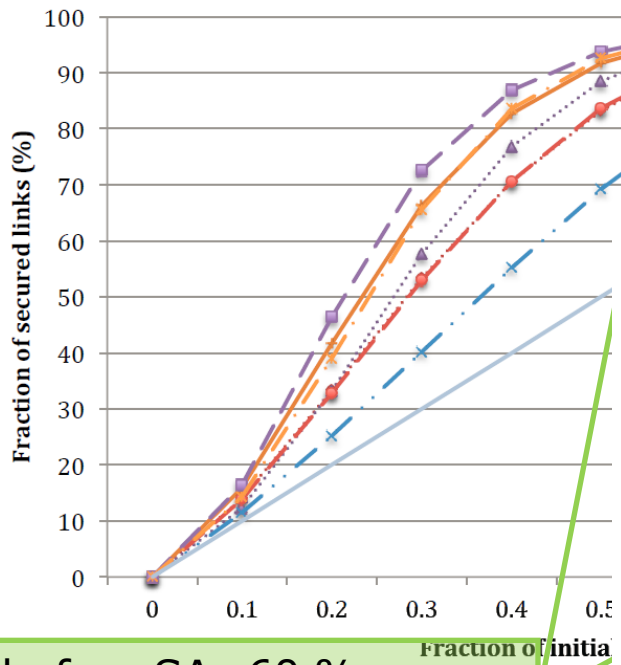


Very brief comparison

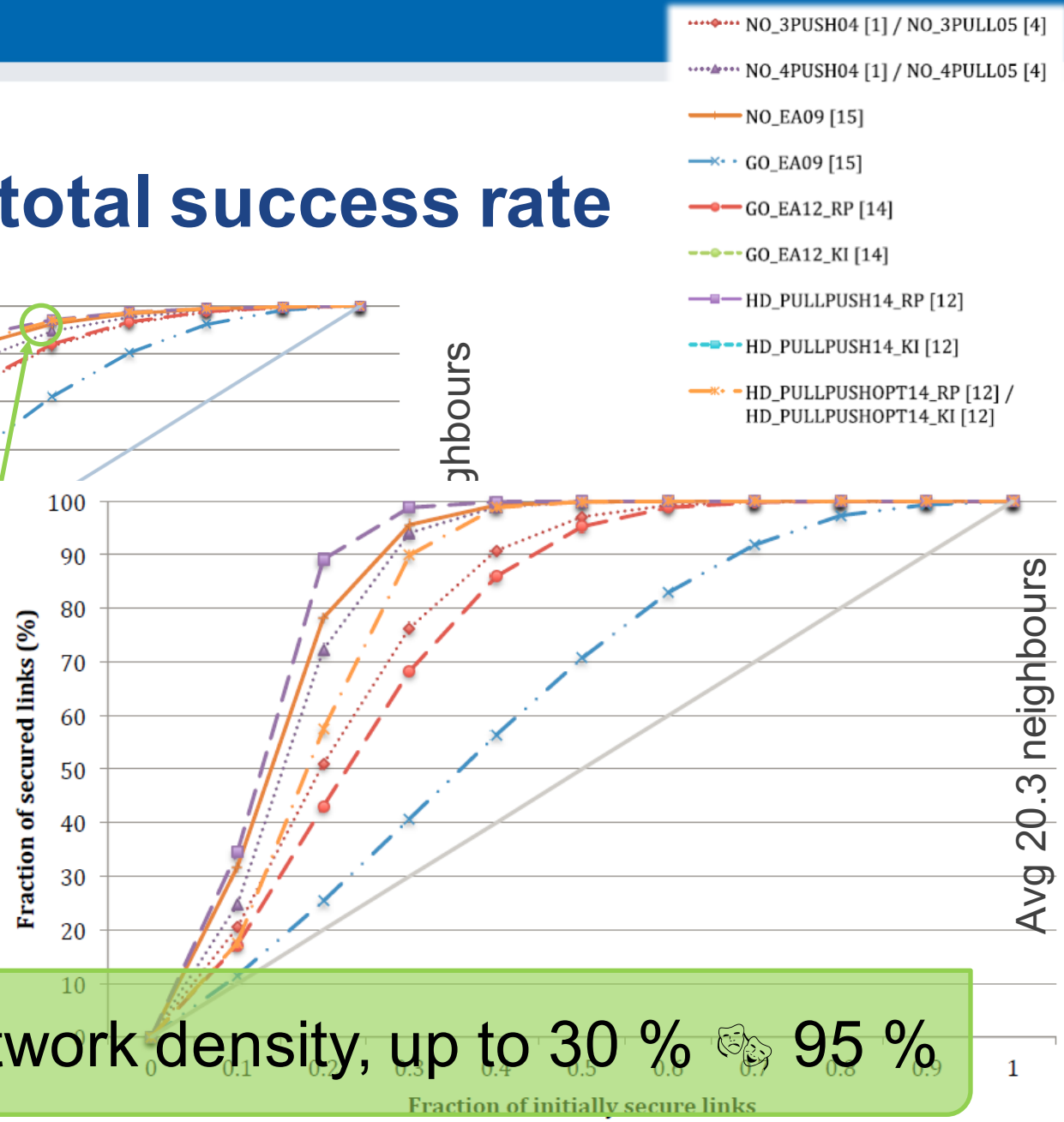
	Success rate (secure links)	# messages (for SA)
 Node-oriented	High ☺	High ☹
 Group-oriented	Medium 😐	Low ☺
 Hybrid	High ☺	Low ☺

See http://www.crcs.cz/papers/wistp2015 for details

Comparison: total success rate



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



Depending on network density, up to 30 % 🎭 95 %

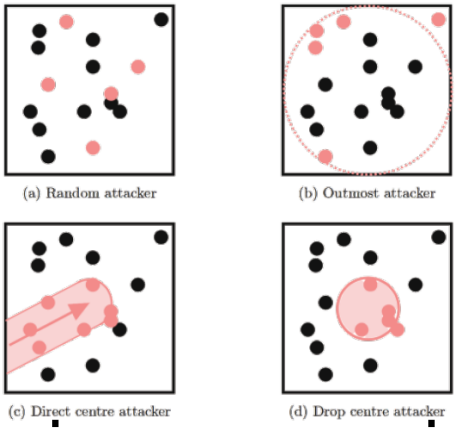
How realistic are the results?

1. Initial work done on fast, but simplified simulators
   - Possibility to explore large number of configuration
2. Replicated on fully-fledged simulator (OMNet++)
   - Significantly more realistic packet transmissions
   - Possibility to simulate advanced attacker
3. Implemented also on real platform (TinyOS)
   - < 500B RAM (peak usage), ~3KB code
   - ~1 KB total payload overhead, ~1 sec local computation
   - 1-10 seconds to transmit amplification messages

All results for random compromise => is it representative ?

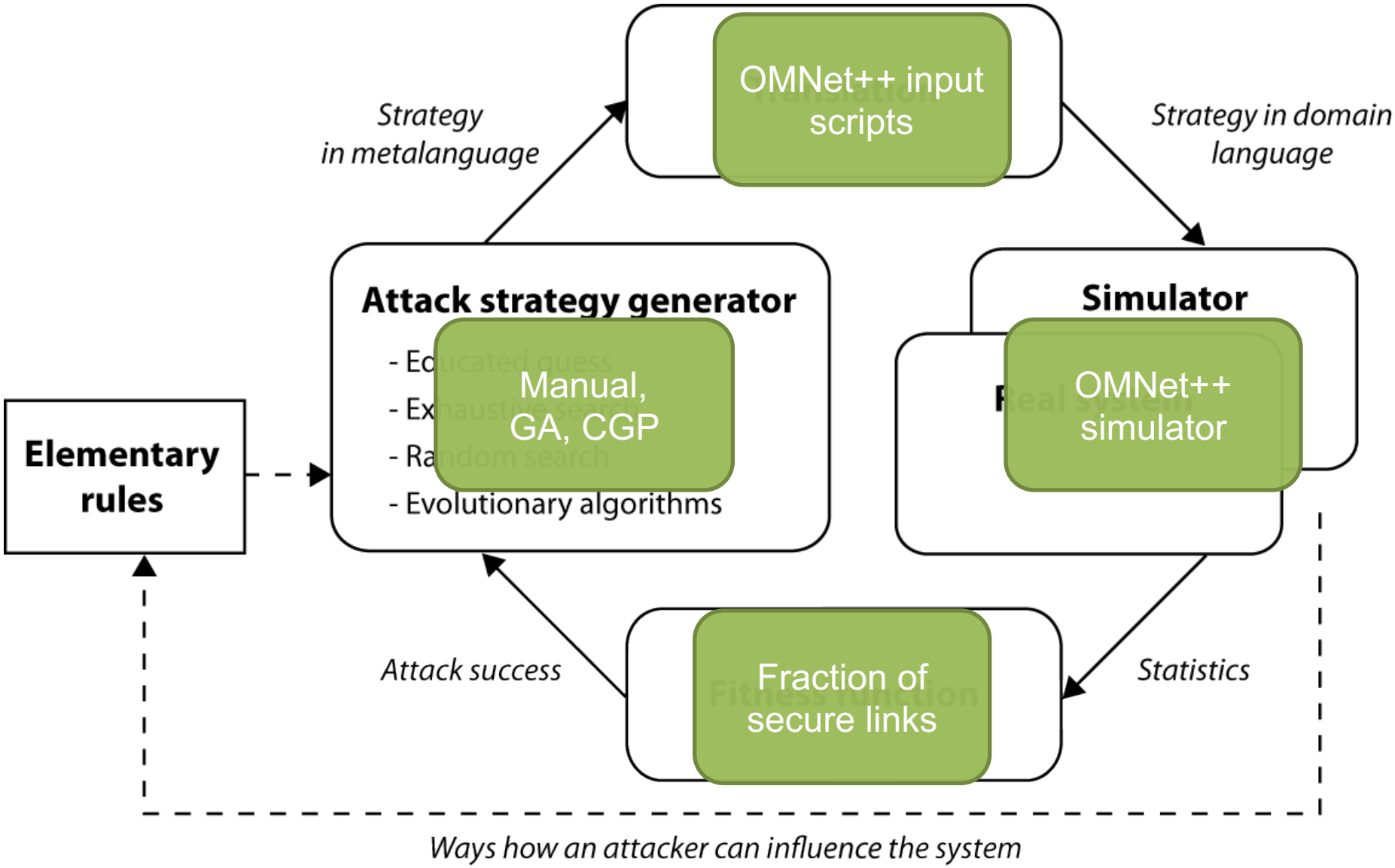
Attacker strategies in phases

I. Attacker's strategy during initial compromise
- Accurate simulator needed (Omnet++ & MiXiM)
- Jurnecka, Matyas, SPW 2014
- Initial compromise pattern


(a) Random attacker
(b) Outmost attacker
(c) Direct centre attacker
(d) Drop centre attacker

II. Attacker's strategy to maintain compromise
- If not maintained, compromise is lost
- Aim of this work
- Basic exploration of parameters vs. full optimization

J. Kůr, V. Matyáš, P. Švenda: Evolutionary design of attack strategies, SPW'2009 [KMS09]

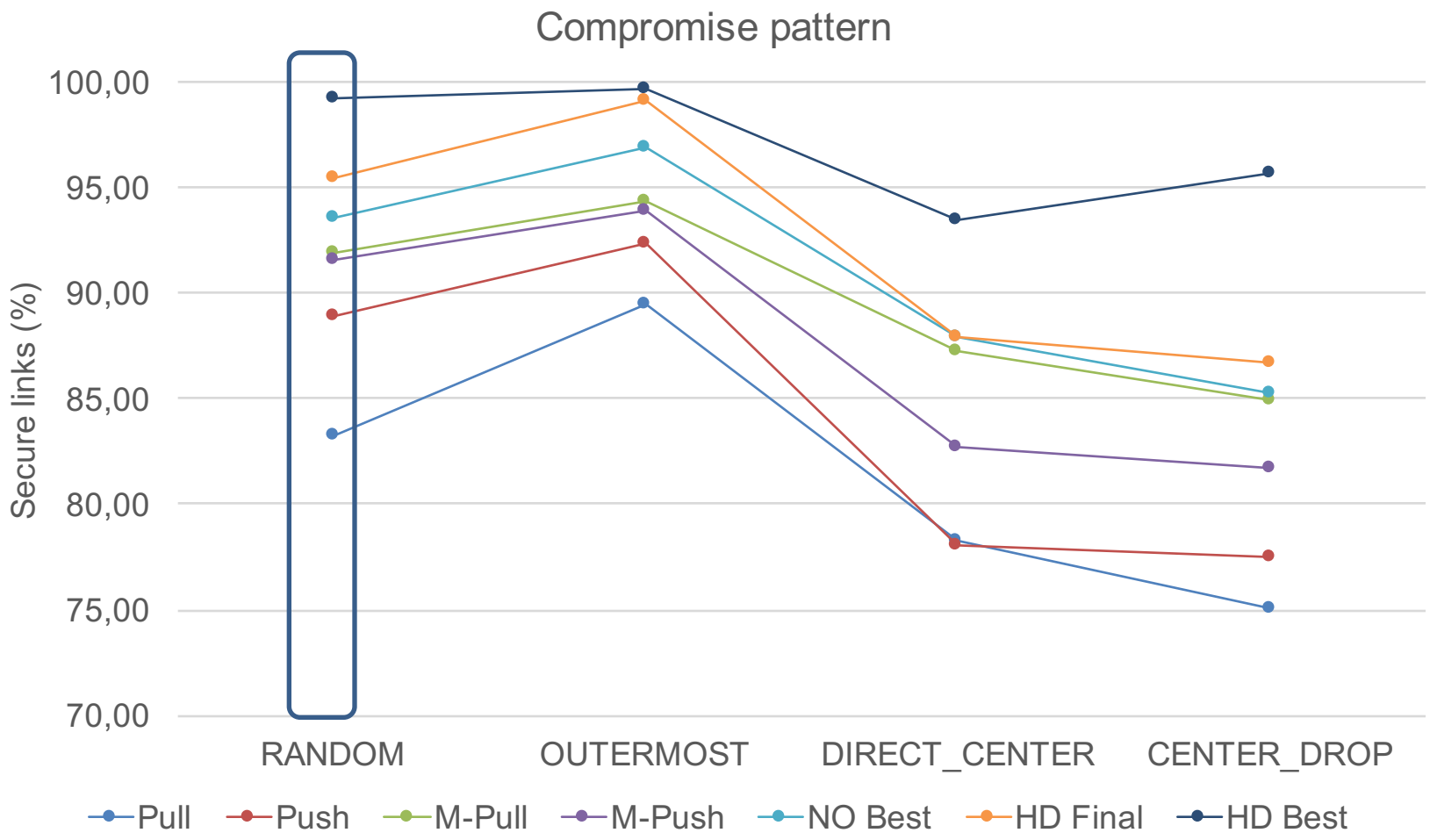


Simulated parameters of an attacker

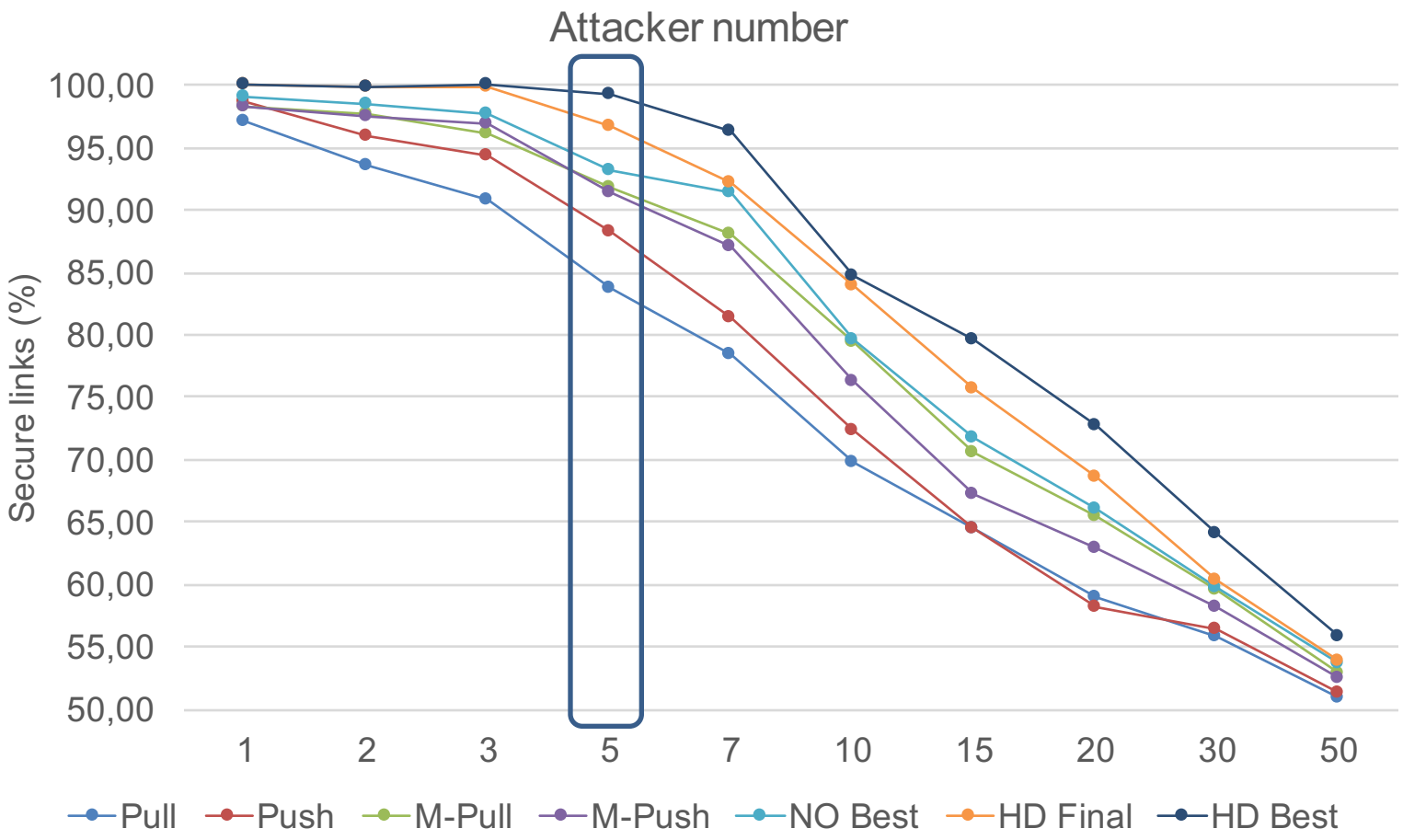
- Initial compromise: 50% links compromised
- Parameters tested
  I. Initial compromise strategy (key distribution phase)
  II. Number of attackers
  III. Start place for attackers
  IV. Eavesdropping strategy during secrecy amplification
  V. Speed of movement
  VI. Receiving range (attacker's antenna sensitivity)

1. Baseline values selected ("average" attacker)
2. One variable manipulated at the time (10 repeats, avg)
3. Success metric: fraction of compromised links

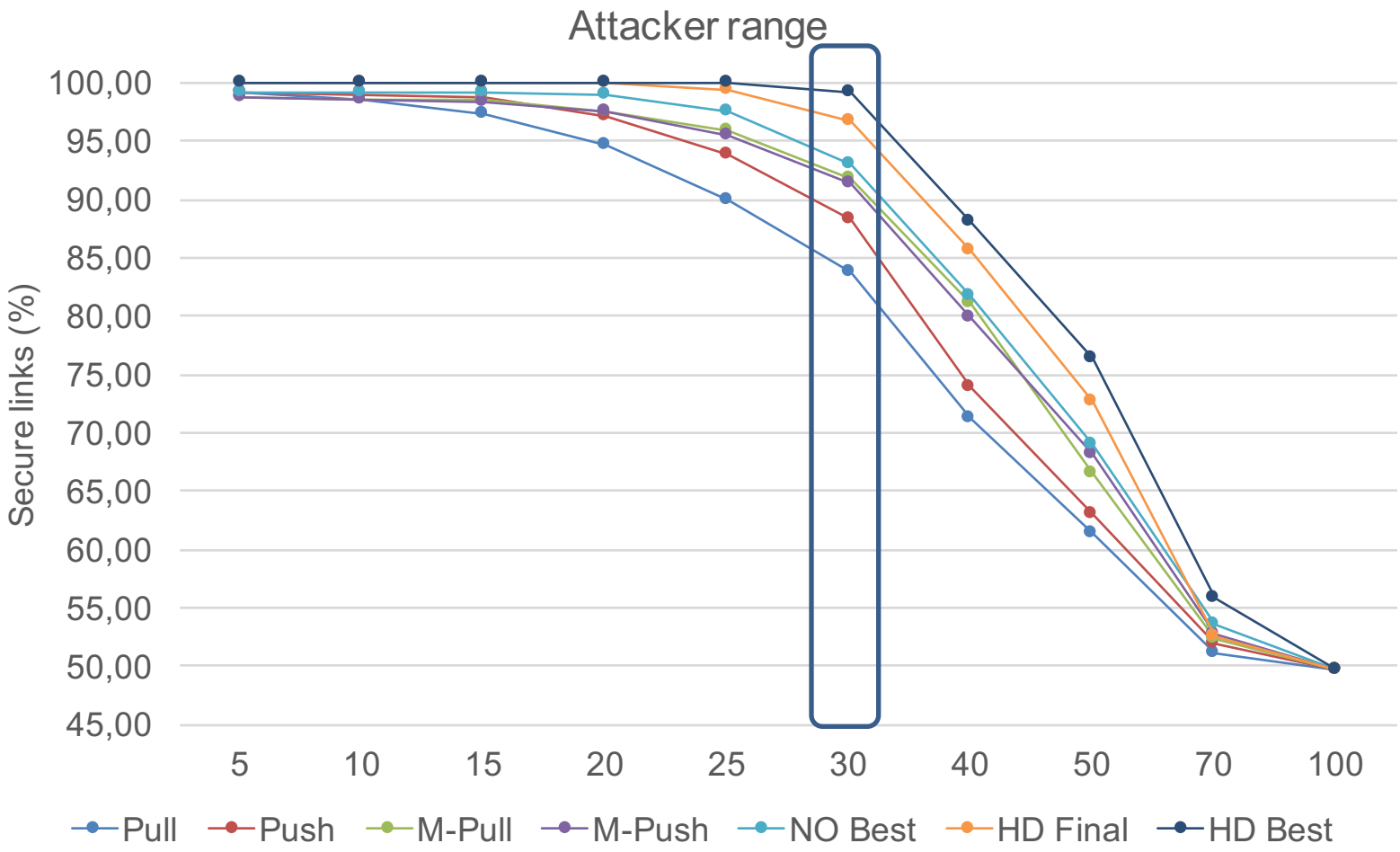
Initial compromise strategy (phase I.)



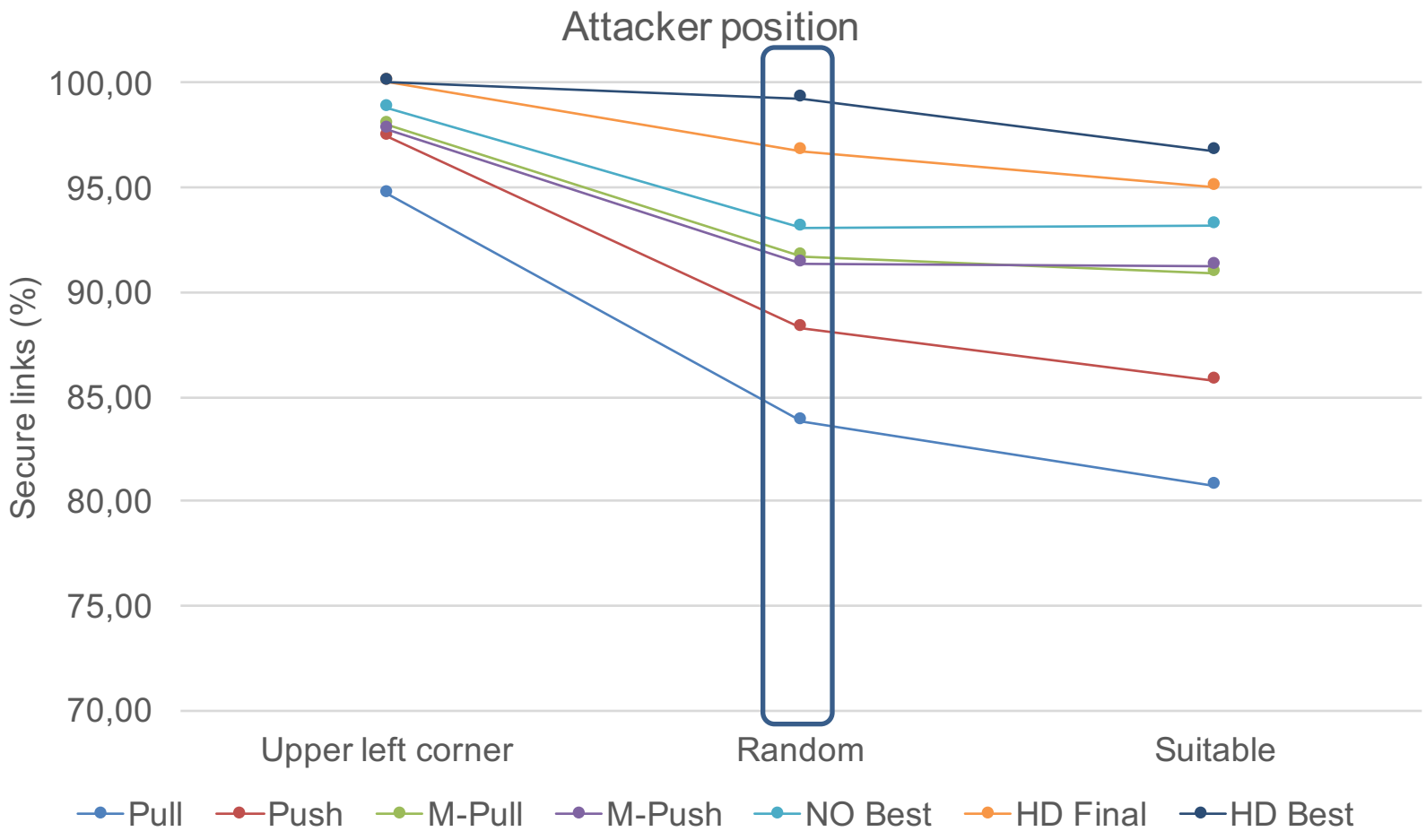
Number of attackers (phase II.)



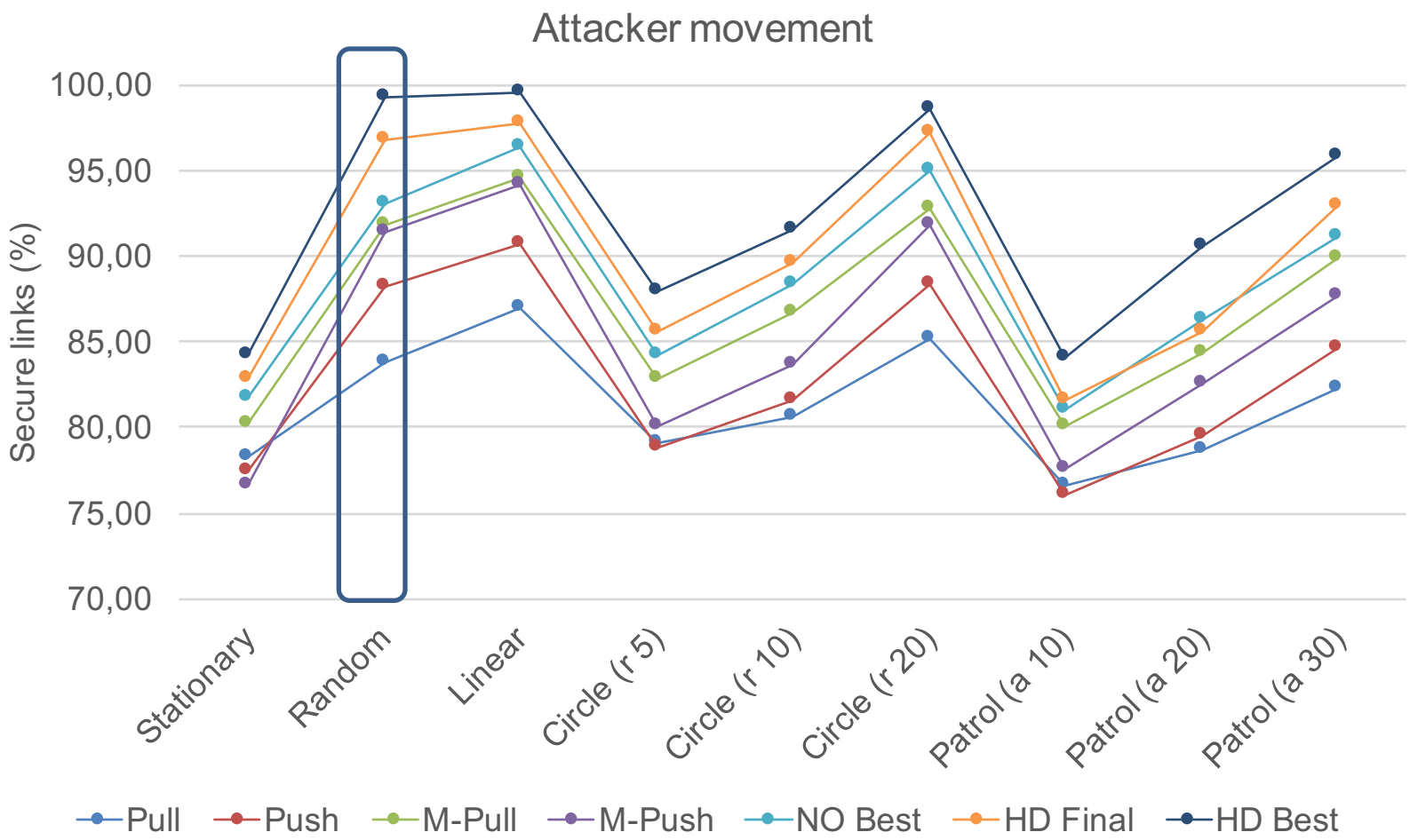
Receiving range (phase II.)



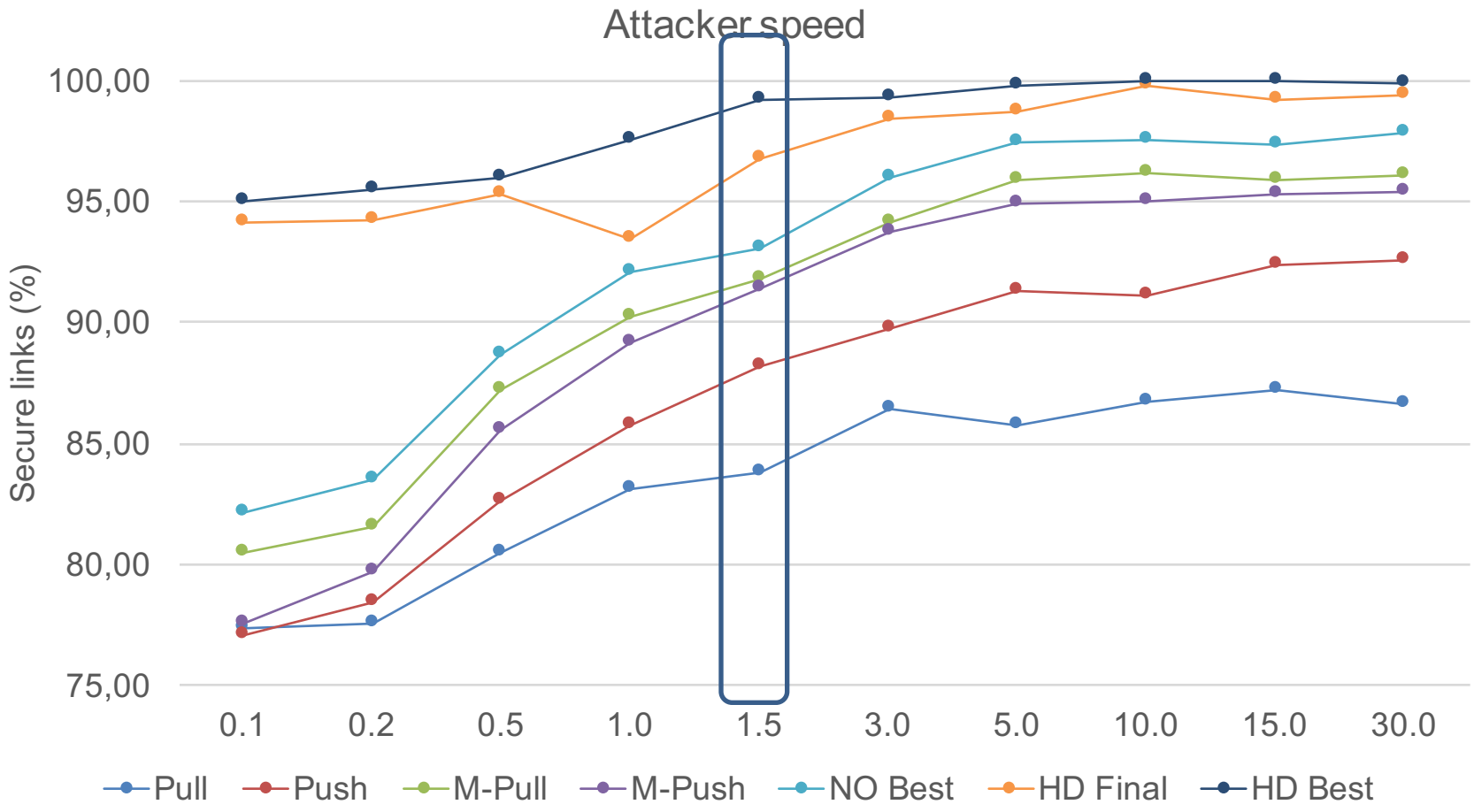
Initial attacker position (phase II.)



Attacker(s) movement (phase II.)



Speed of attacker movement (phase II.)



Stationary attack performs best?

- Surprising result on the first look
  - Best maintain compromise strategy: don't move
- Reason: success metric as # compromised links
- Other suitable metrics?
  - Fraction of compromised/delivered messages?
  - Network latency?
  - Realistic network simulator allows to simulate this

What else can be explored?

- Simulation of attacker is CPU intensive task
  - 6params x 10values x 100repeats x 60min => >2 CPU years
- Further (automatic) optimization with more than one variable requires suitable heuristics
  - Random search, GA, CGP…
- Other parameters of an attacker model?

Thank you for your attention!

Questions 

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.

[KMS09] J. Kůr, V. Matyas, P. Švenda, Evolutionary design of attack strategies, SPW'2009

[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.

[OSM15] Radim OŠŤÁDAL, Petr ŠVENDA a Václav MATYÁŠ. On Secrecy Amplification Protocols. In Raja Naeem Akram, Sushil Jajodia. LNCS 9311. Berlin: Springer International Publishing, 2015. s. 3-19, 18 s. ISBN 978-3-319-24017-6.

http://www.crcs.cz/papers/wistp2015

The ultimate goal

- Provide parameters of network and attacker
- We will provide you realistic compromise expectations (maximal success for optimized attacker)
- Spread the word about secrecy amplification
  - Works great even under stronger compromise model