Analysing Probabilistic Network Flooding

KeY Symposium 2007

Frank Werner

University Karlsruhe

15.06.2007

Overview

Introduction

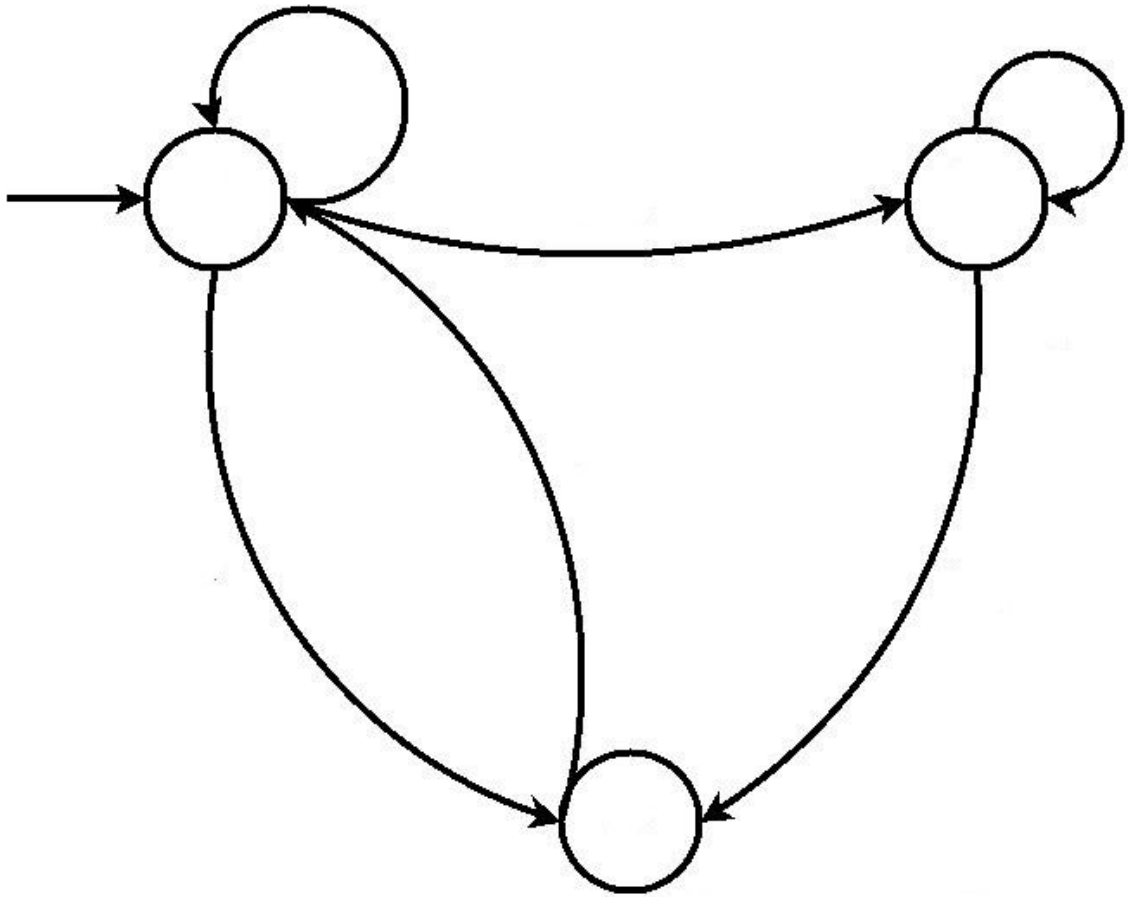
Application Areas of PMC:

- unreliable or unpredictable behaviour
- analyse system performance
- distributed algorithms

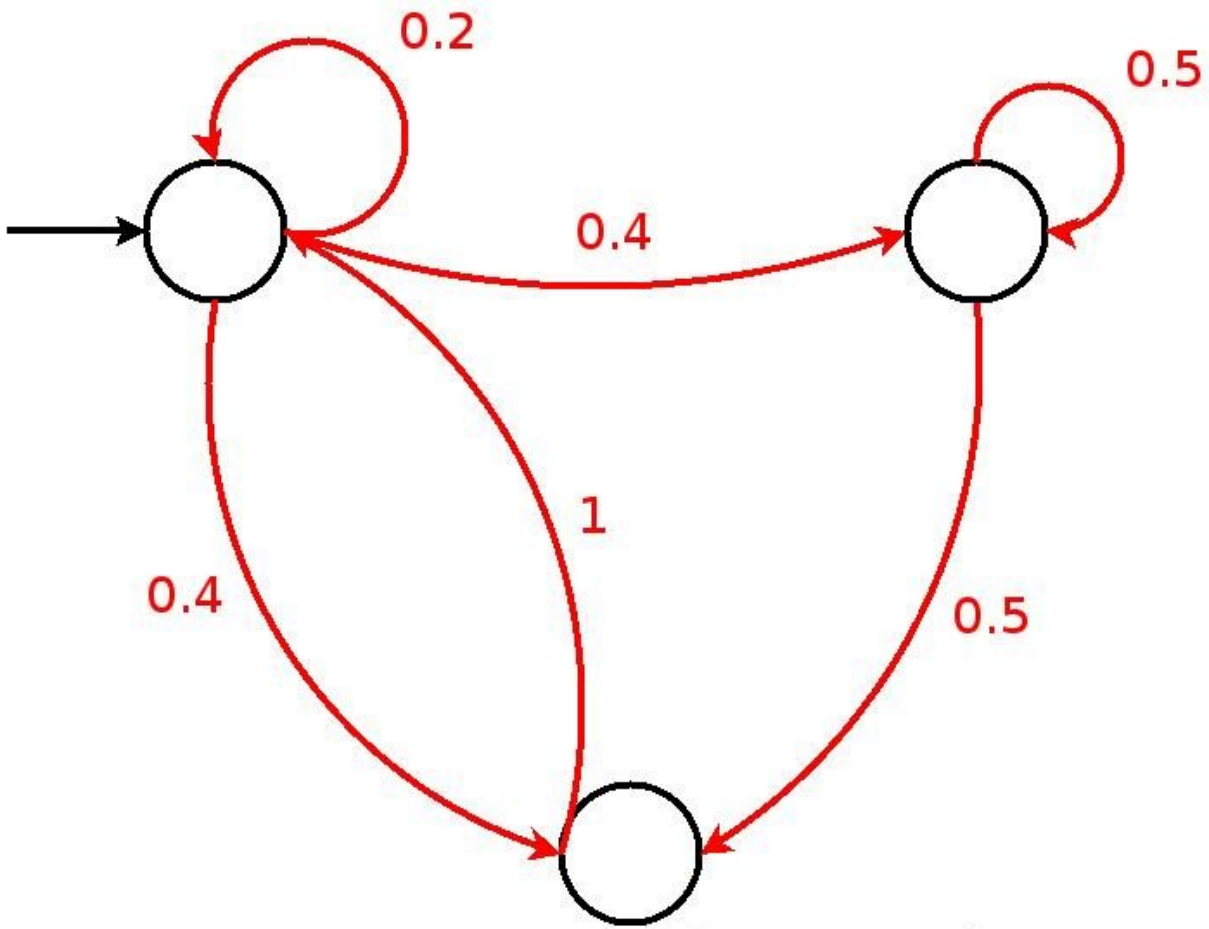
Application Examples

- randomised leader election algorithm
- any system that can suffer failures
- communication with unreliable links (wireless networks)
- security systems

Introduction: DTMC

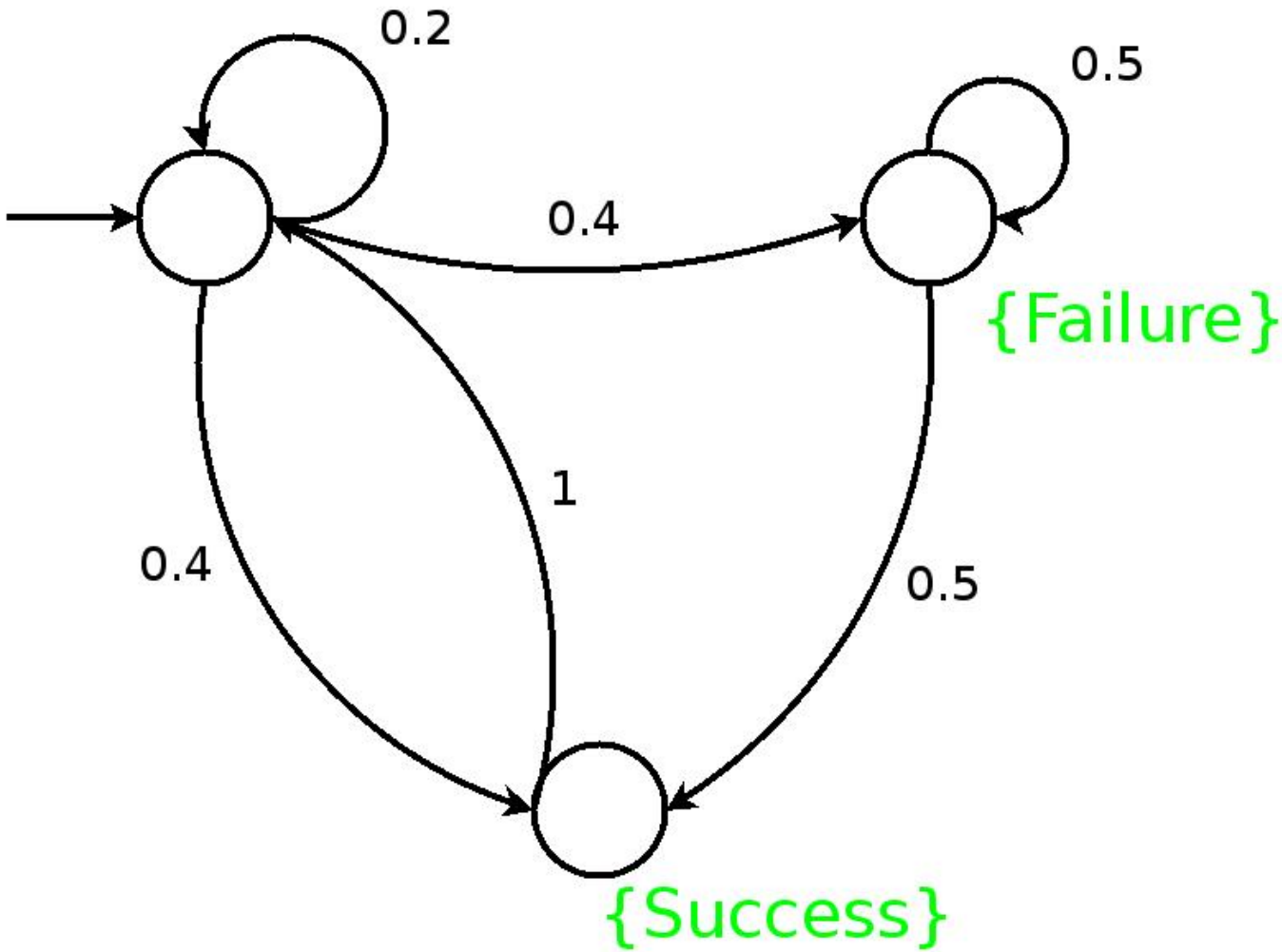


Discrete Time Markov Chains: Transitions



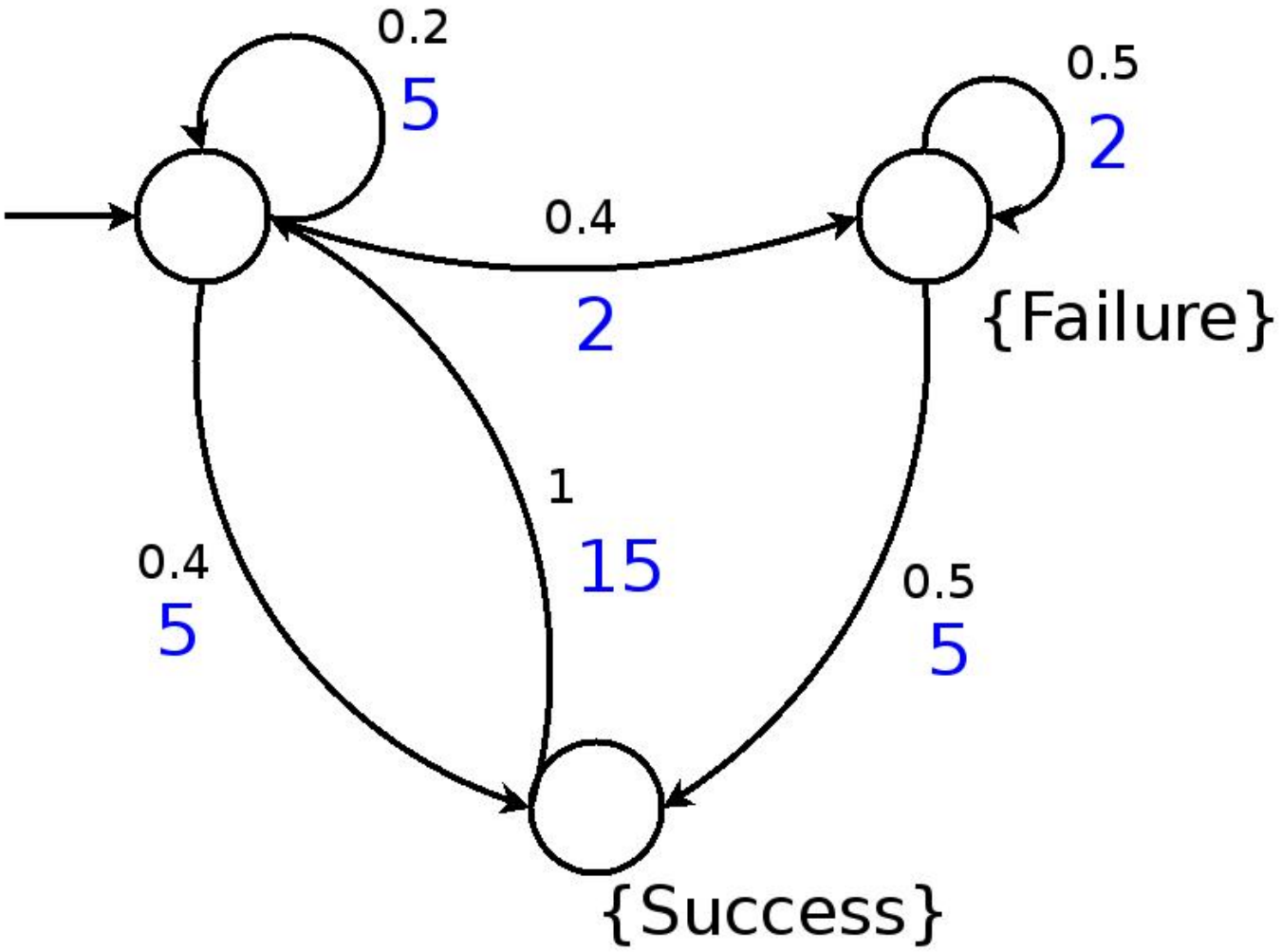
Transition Probabilities

Discrete Time Markov Chains: Labels



State Labels

Introduction: Reward Rates



Reward Variables

Probabilistic Computation Tree Logic (PCTL)

State Formulas ϕ:

- *true*
- a
- $\neg\phi$
- $\phi_1 \wedge \phi_2$
- $\mathcal{P}_{\triangleleft p}[\psi]$
- $\mathcal{C}_{\triangleleft c}[\phi]$

Path Formulas ψ:

- ϕ
- $\phi_1 \mathcal{U} \phi_2$
- $\phi_1 \mathcal{U}^{\leq k} \phi_2$

with $\triangleleft \in \{\leq, <, \geq, >\}$, $p \in [0,1]$, $c \in \mathbb{R}^{\geq 0}$, $k \in \mathbb{N}$

Network Flooding

Why doing Authenticated Query Flooding...

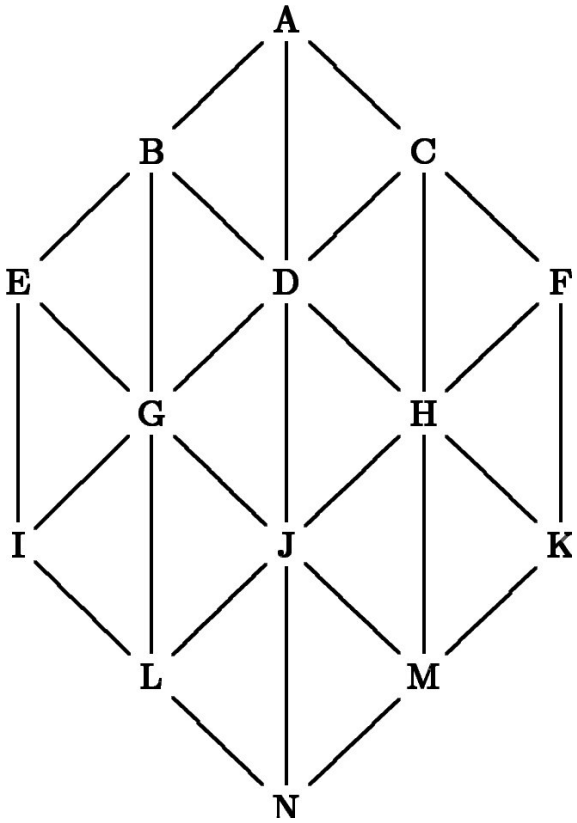
Secure technique for obtaining information about the network and recognize fake queries which possibly stem from an “intruder“

Assumptions underlying the model:

- queries are injected by a base station at sensor A
- propagation along the bidirectional links

What a sensor does

- upon packet reception
  $\Longrightarrow$ apply the AQF algorithm
- after processing
  $\Longrightarrow$ go to sleep



Introduction to AQF

- security mechanism for multicast communication (ID-based key distribution)
- a tradeoff between MACs and digital signatures
- each sensor loaded with a defined number of keys
- on reception of a packet q:
  - packet is authenticated and distributed to the sensor's neighbours
  - packet is not authenticated and dropped
  - packet q can not be authenticated due to a missing key $\rightarrow$ q is distributed to the neighbours (`AQF-pass`)

proability that a sensor accepts query with fake authenticator

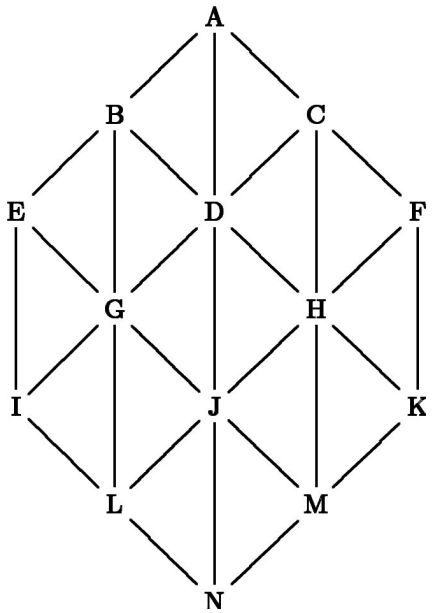
$$p_f = \left(\frac{l-k}{l} + \frac{k}{l} \frac{B}{m} \right)^m$$

Analysis of the AQF algorithm

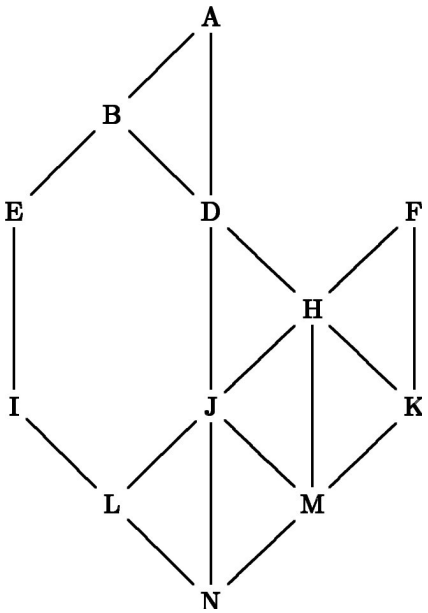
- Modelling using probabilistic automata (Prism tool)
- finding proper parameters for the AQF algorithm
  $\Rightarrow$ energy/security trade-off
- estimation of energy consumption (reward variables) with real-world sensor data from the TMote Sky sensor board
- comparison of different topologies with regard to energy efficiency, security, and AQF parameter

Selected Network Topologies

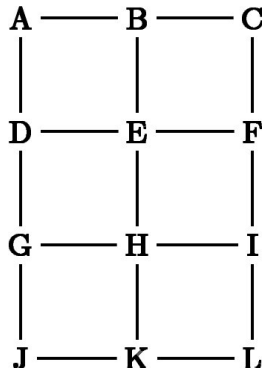
topology 7



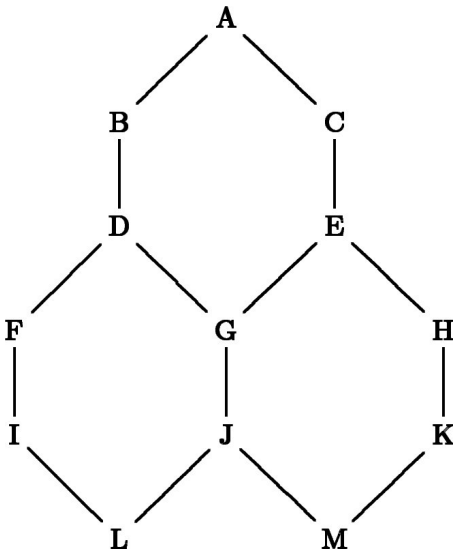
topology 8



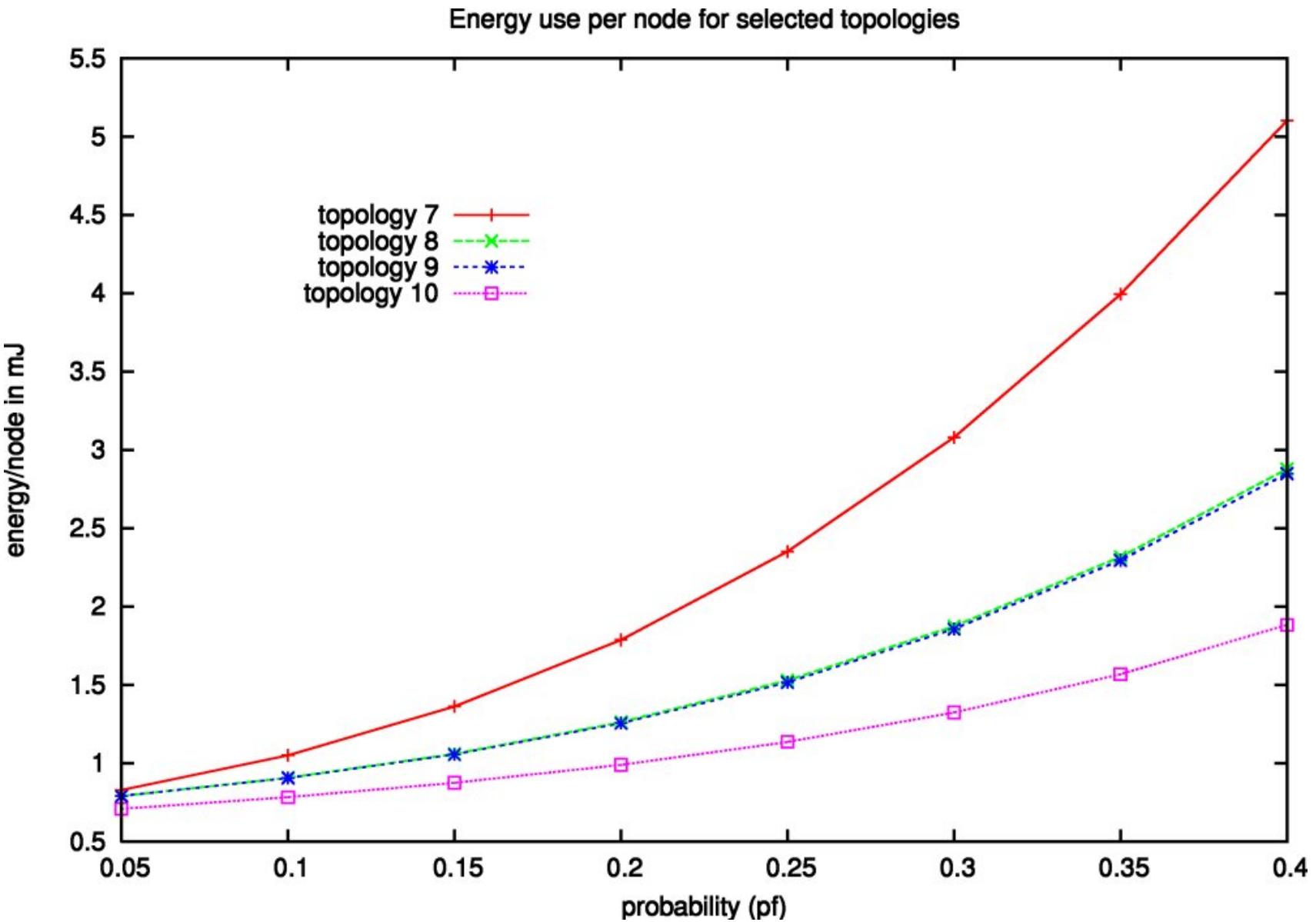
topology 9



topology 10



Results: Energy Rewards for Sensor Network



Summary and Concluding Words

- Analysis of arbitrary complex topologies by PA
- proper solutions for the energy/security tradeoff
- fast and exact solutions (no confidence levels as opposed in simulation)
- maximal network size somehow restricted to about 20 nodes (sufficient for many real life scenarios)

THANK YOU...