A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge

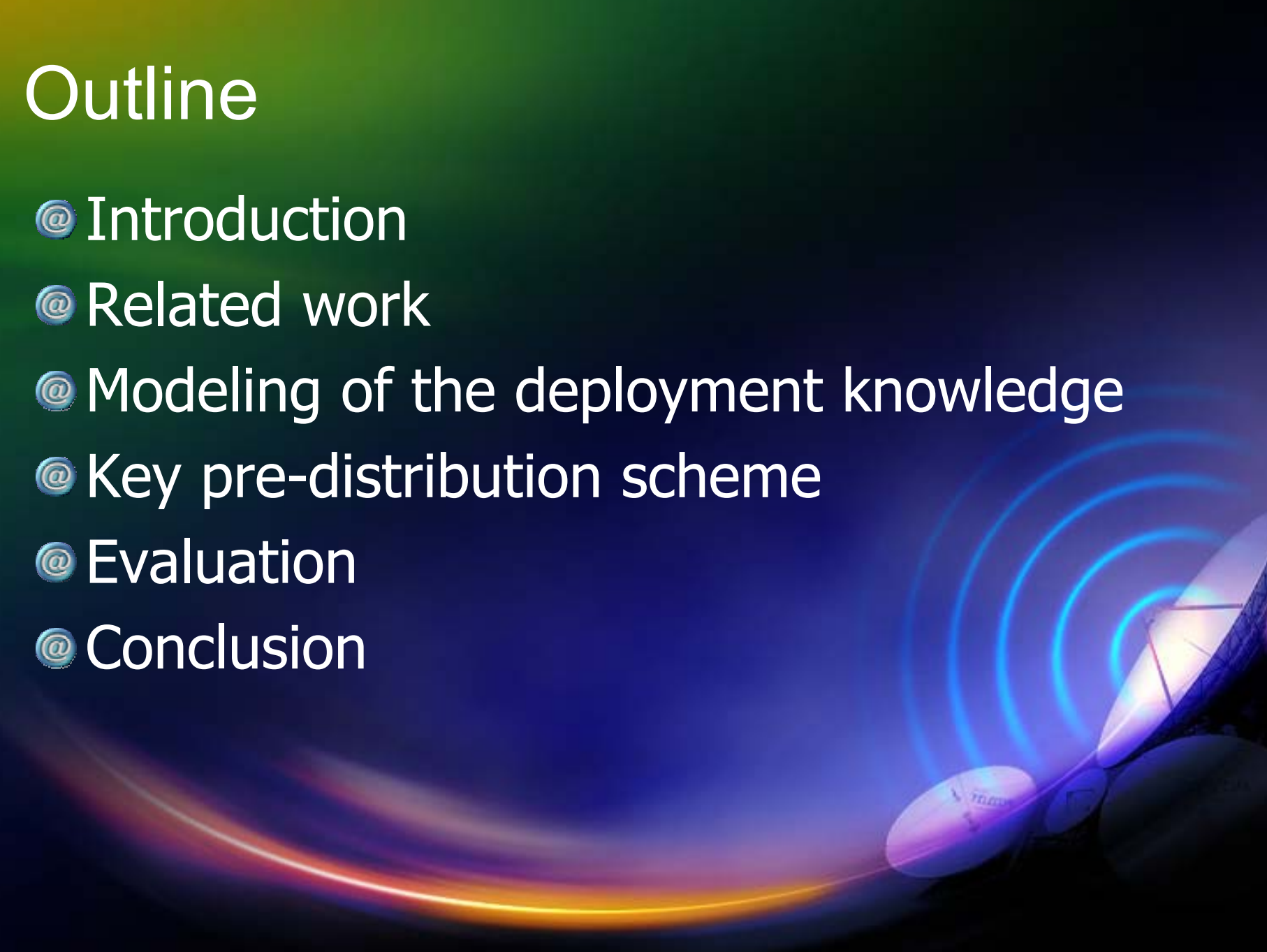
INFOCOM 2004

2004.06.10

Yu-Ching Lin

Outline

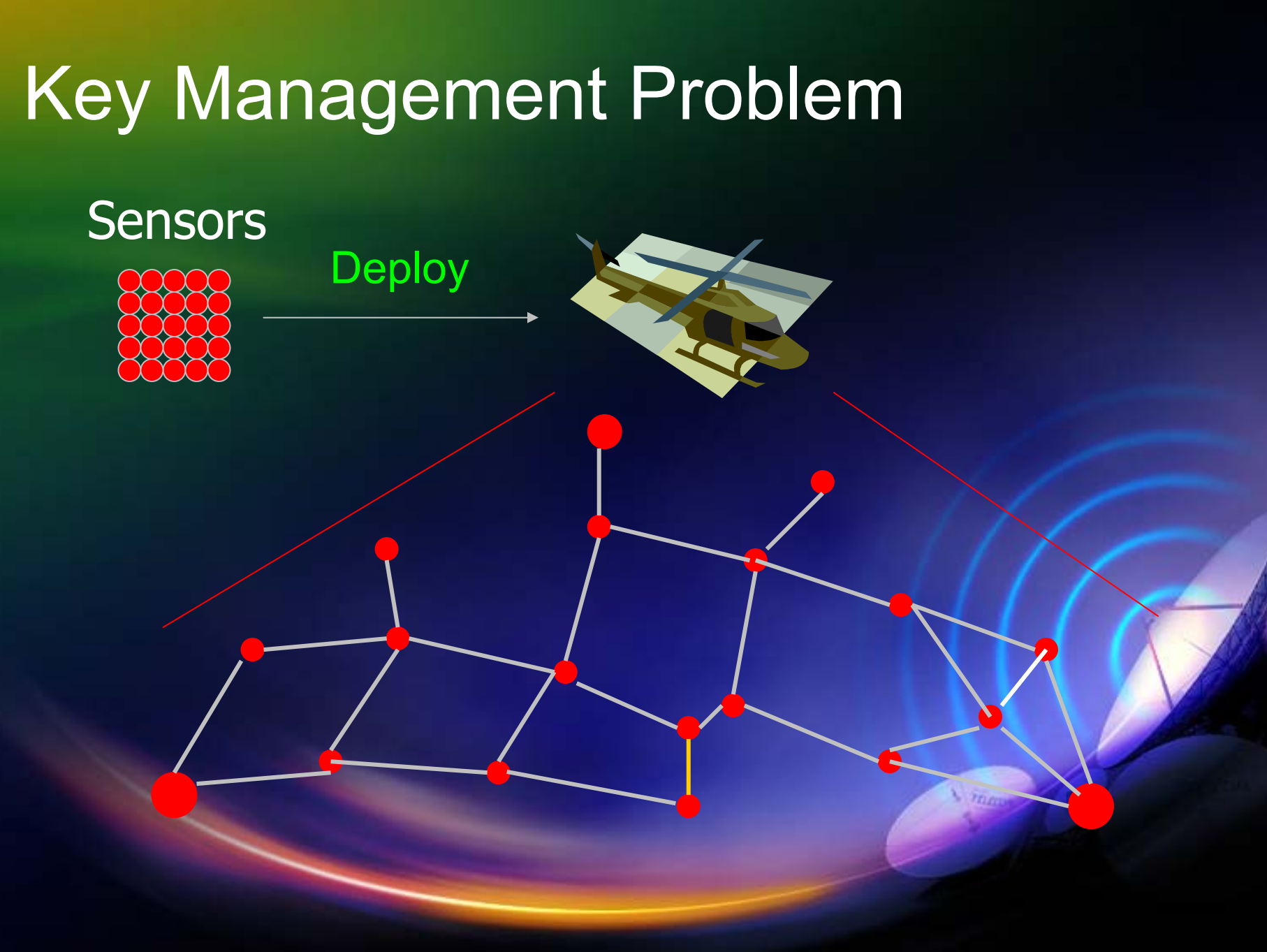
- Introduction
- Related work
- Modeling of the deployment knowledge
- Key pre-distribution scheme
- Evaluation
- Conclusion



Introduction

- Applications of sensor networks
  - Military sensing and tracking
  - Environmental monitoring
  - Hospital tracking systems
- Sensor node constraints
  - Battery power
  - Computing ability
  - Memory
- Sensor networks' constraints affect the design of security mechanisms.

Key Management Problem



Key Management Approaches

- Trusted server schemes
  - Finding trusted servers is difficult
- Public key schemes
  - Expensive and infeasible for sensors
- Key pre-distribution schemes
  - Key information is distributed among all sensor nodes prior to deployment

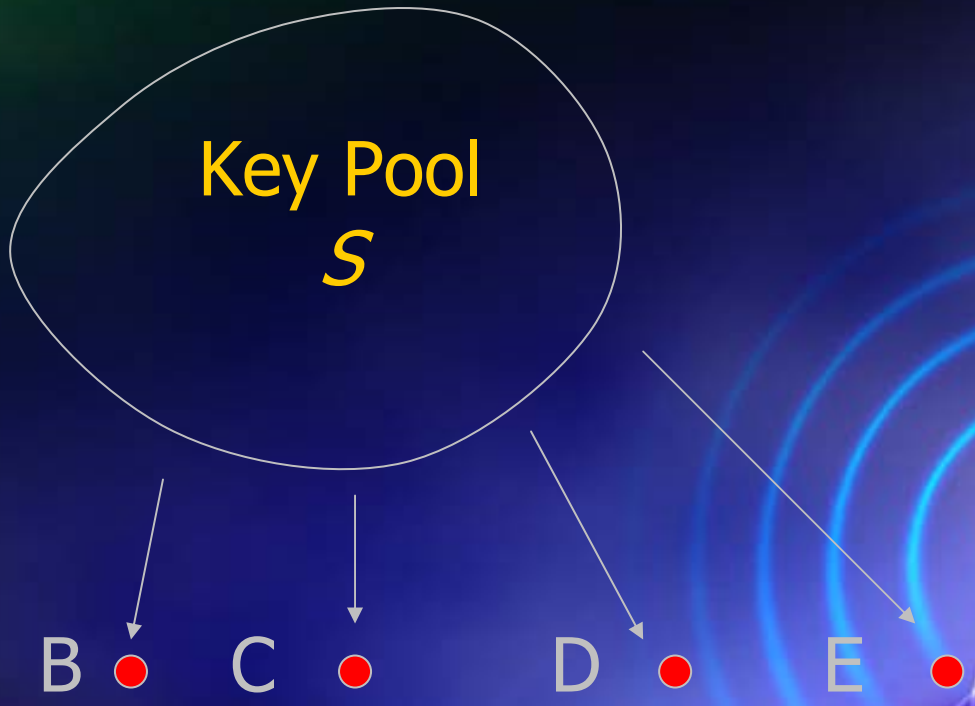
Naïve Solutions

- Master-key approach
  - Memory efficient
  - One node is compromised, the whole sensor networks will be compromised
  - Needs Tamper-resistant hardware
- Pair-wise key approach
  - Each sensor carry N-1 keys
  - Security is perfect
  - Need a lot of memory

Eschenauer-Gligor Scheme

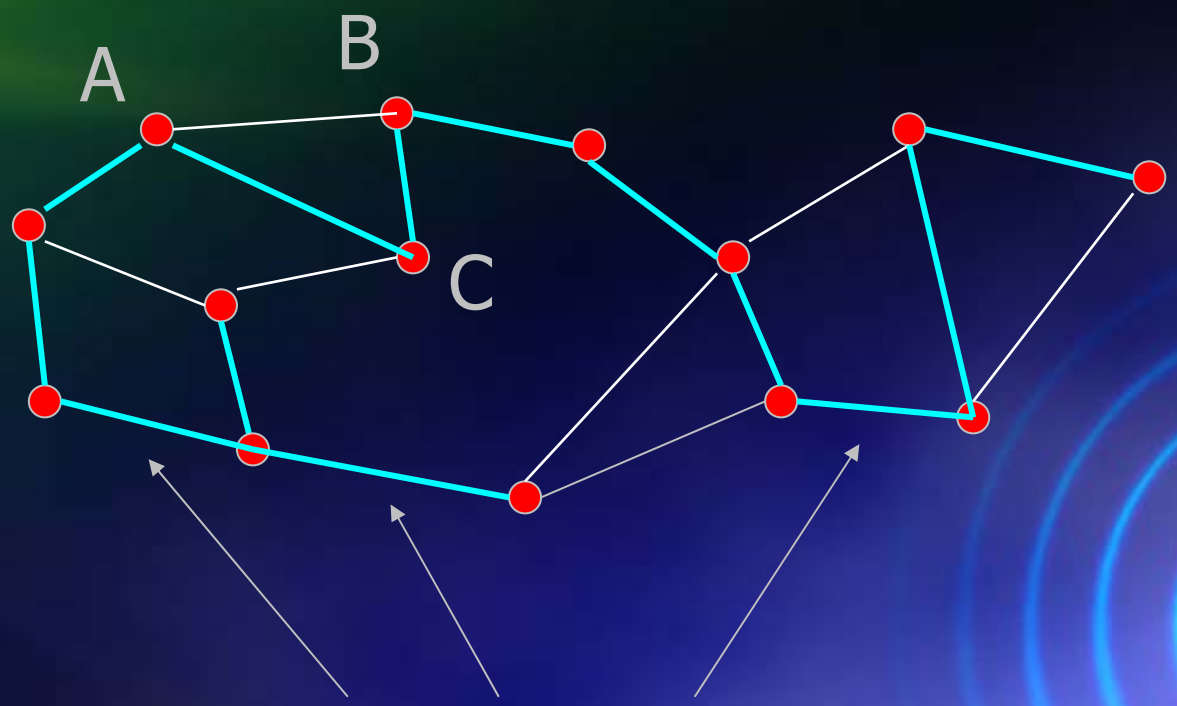
- Key pre-distribution

Each node randomly selects m keys from key pool



- When |S| = 10,000, m=75
  Pr (two nodes have a common key) = 0.50

Key Sharing Graph



Secure Channels

Modeling the Deployment Knowledge

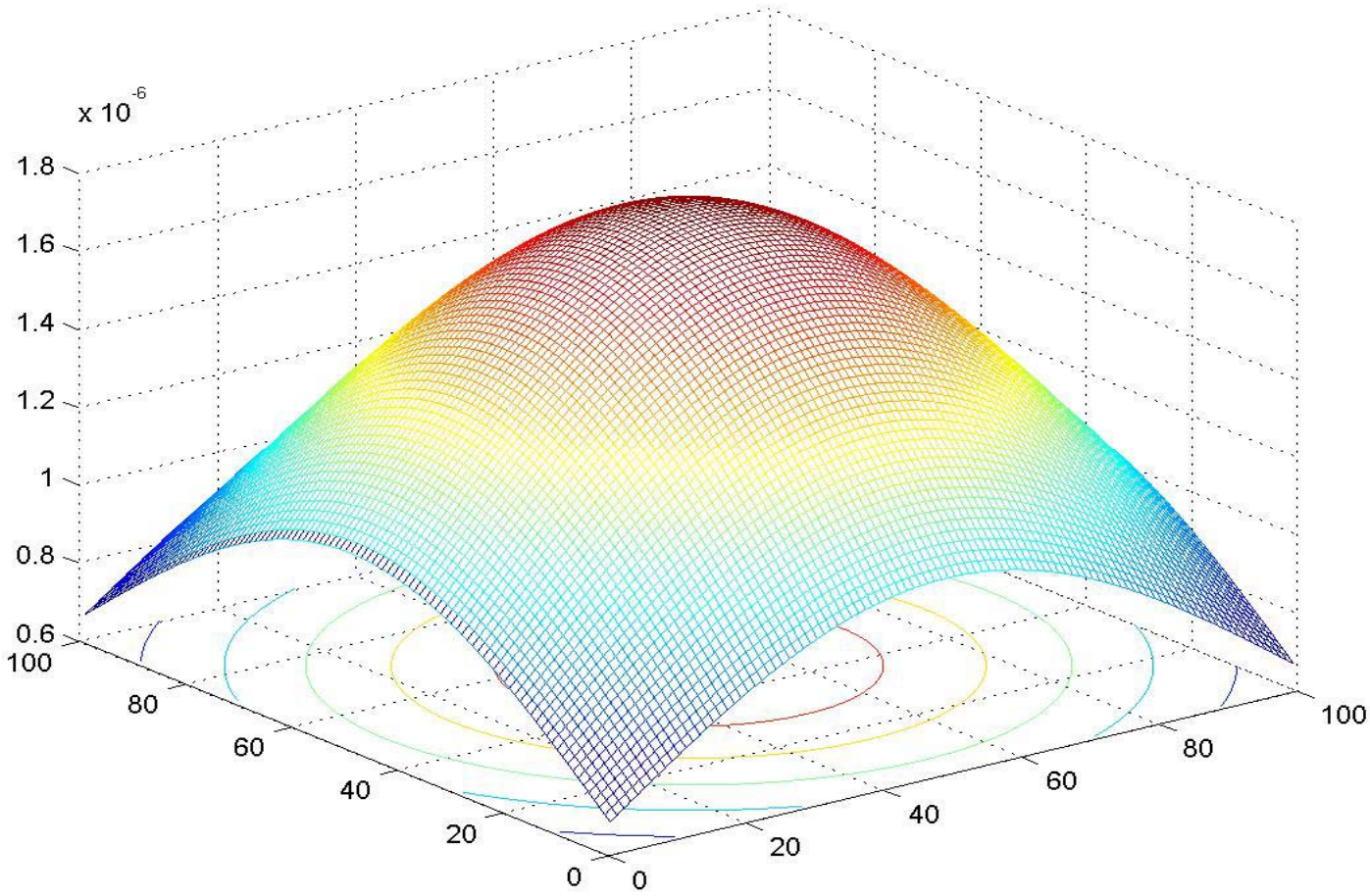
- Group-based deployment model
- Normal distribution

$$f_k^{ij}(x, y|k \in G_{i,j}) = \frac{1}{2\pi\sigma^2} e^{-[(x-x_i)^2+(y-y_j)^2]/2\sigma^2}$$

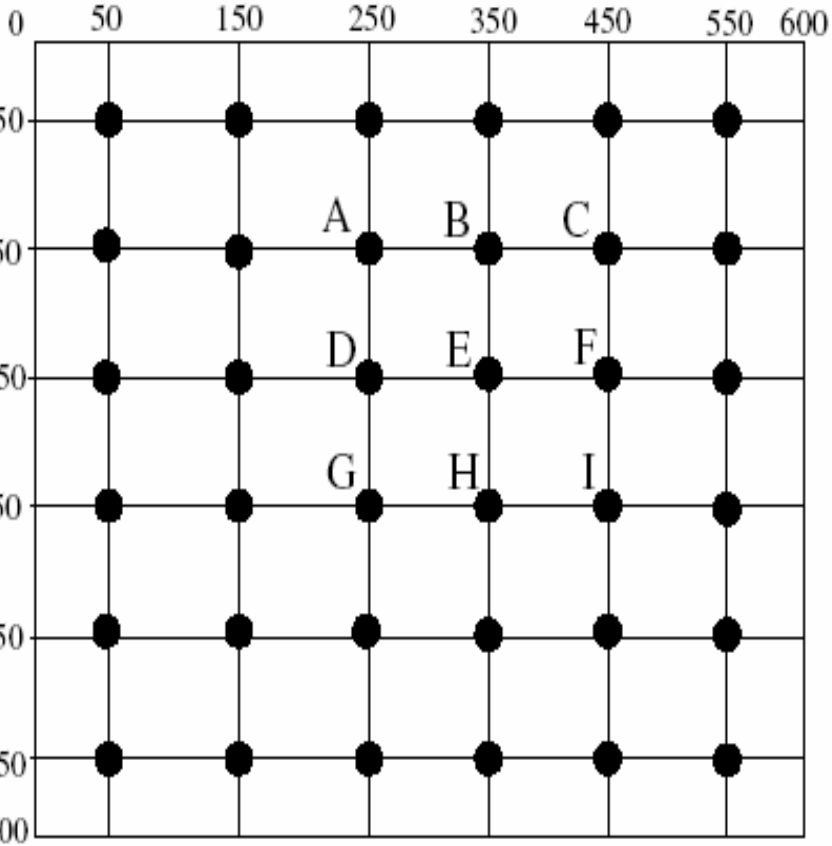
$$f_{overall}(x, y) = \sum_{i=1}^{t} \sum_{j=1}^{n} \frac{1}{t \cdot n} \cdot f_k(x, y|k \in G_{i,j})$$

Deployment Distribution

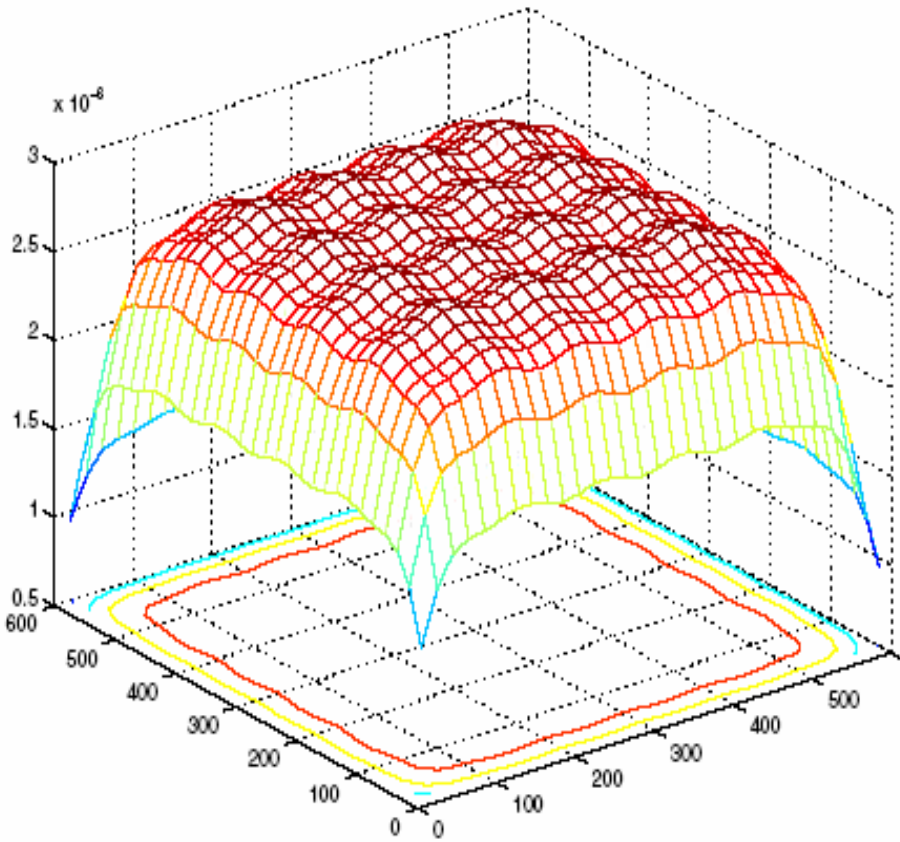
- Normal distribution



Node Deployment



(a) Deployment points (each dot represents a deployment point).

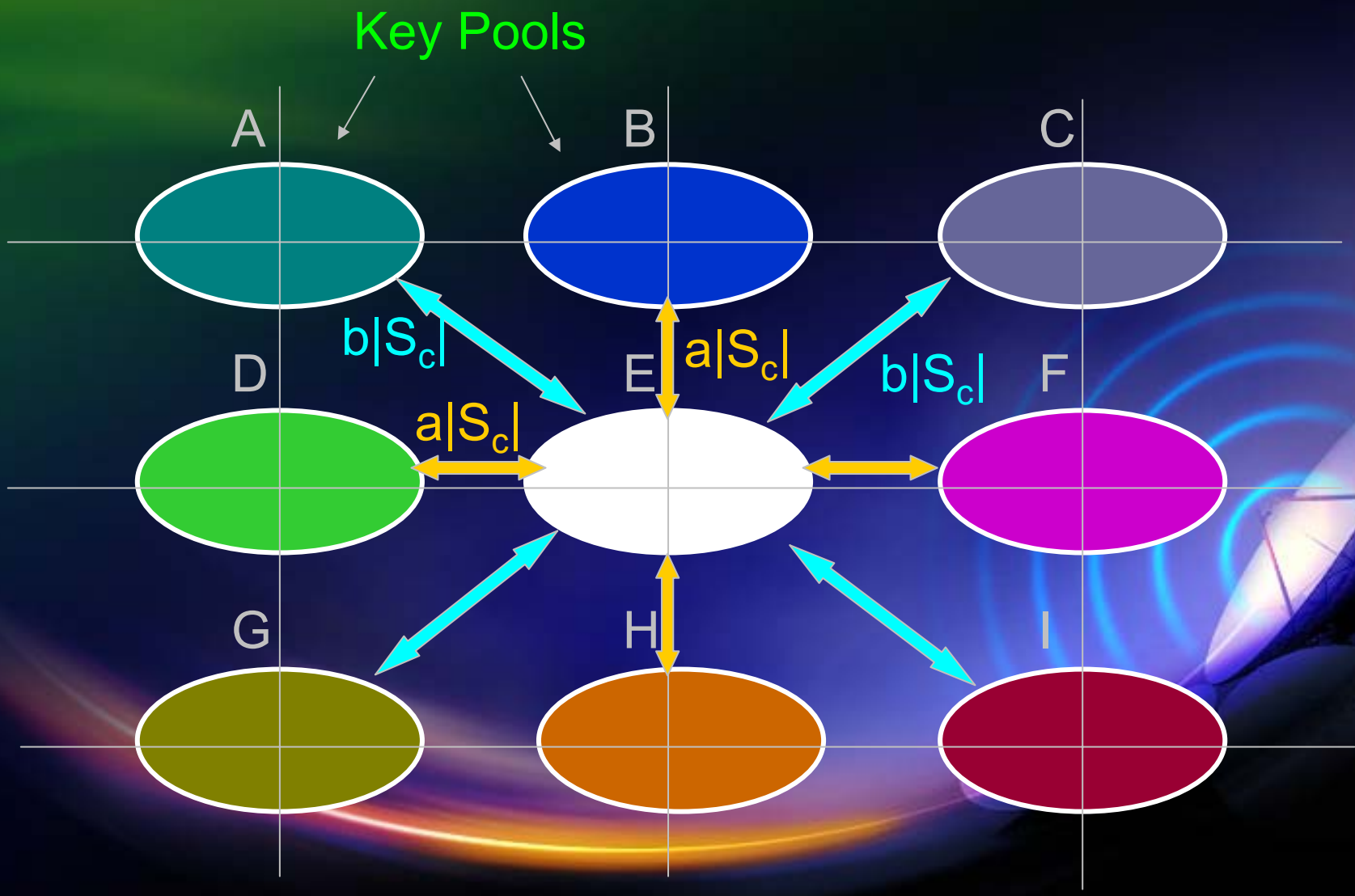


(b) Deployment distribution on the entire region using the deployment strategy modeled by (a).

Key Pre-distribution Scheme

- Dividing the global key pool S into t*n key pools $S_{i,j}$, with $S_{i,j}$ corresponding to the deployment group $G_{i,j}$
- Setting up key pools
  - Horizontally or vertically neighboring key pools share $a|S_c|$ keys, where $0 \leqq a \leqq 0.25$
  - Diagonally neighboring key pools share $b|S_c|$ keys, where $0 \leqq b \leqq 0.25$

Key Pre-distribution Scheme (cont.)



Key Pre-distribution Scheme (cont.)

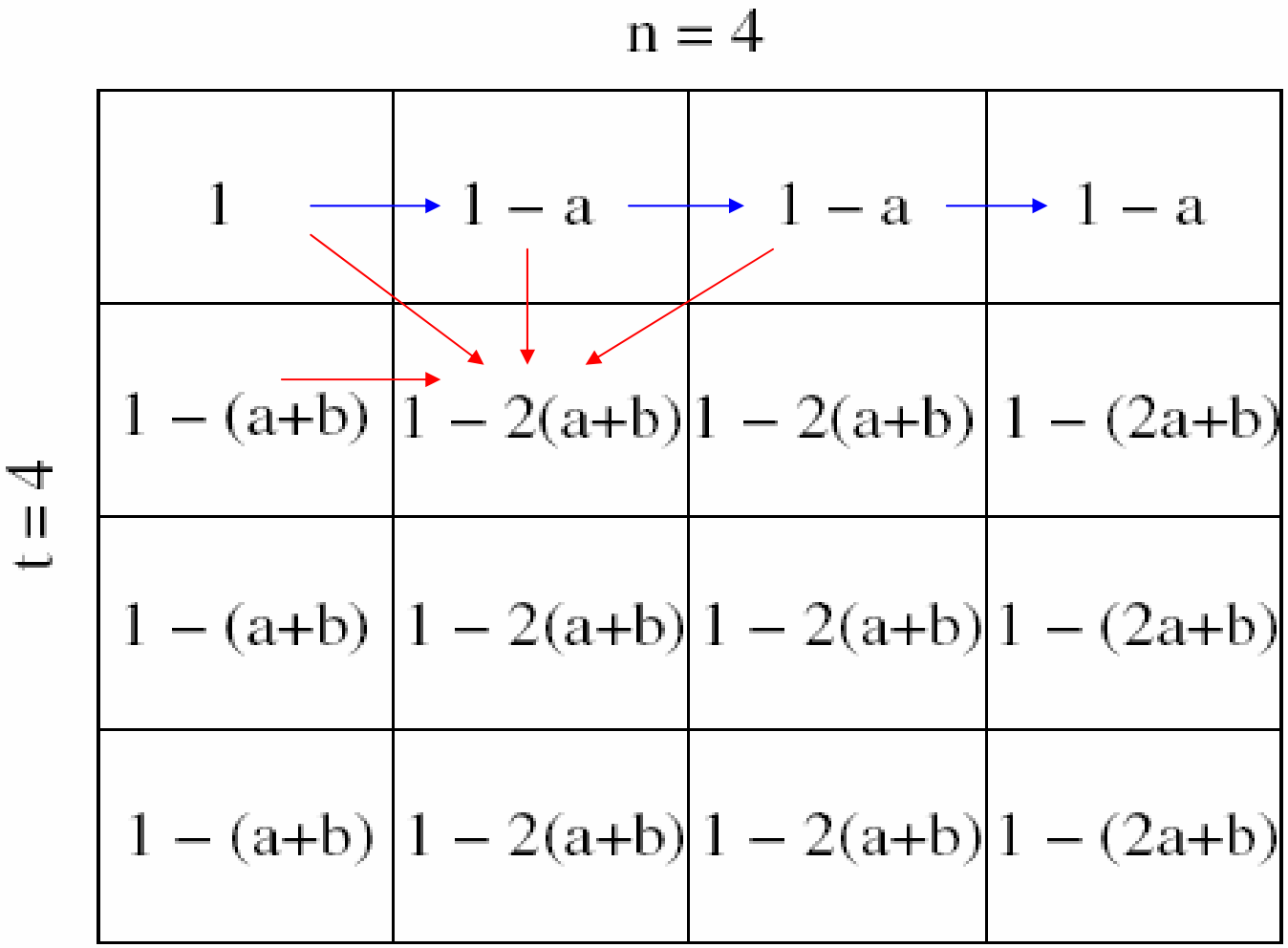


Fig. 3. Key assignment for all the key pools

Determining $|S_c|$

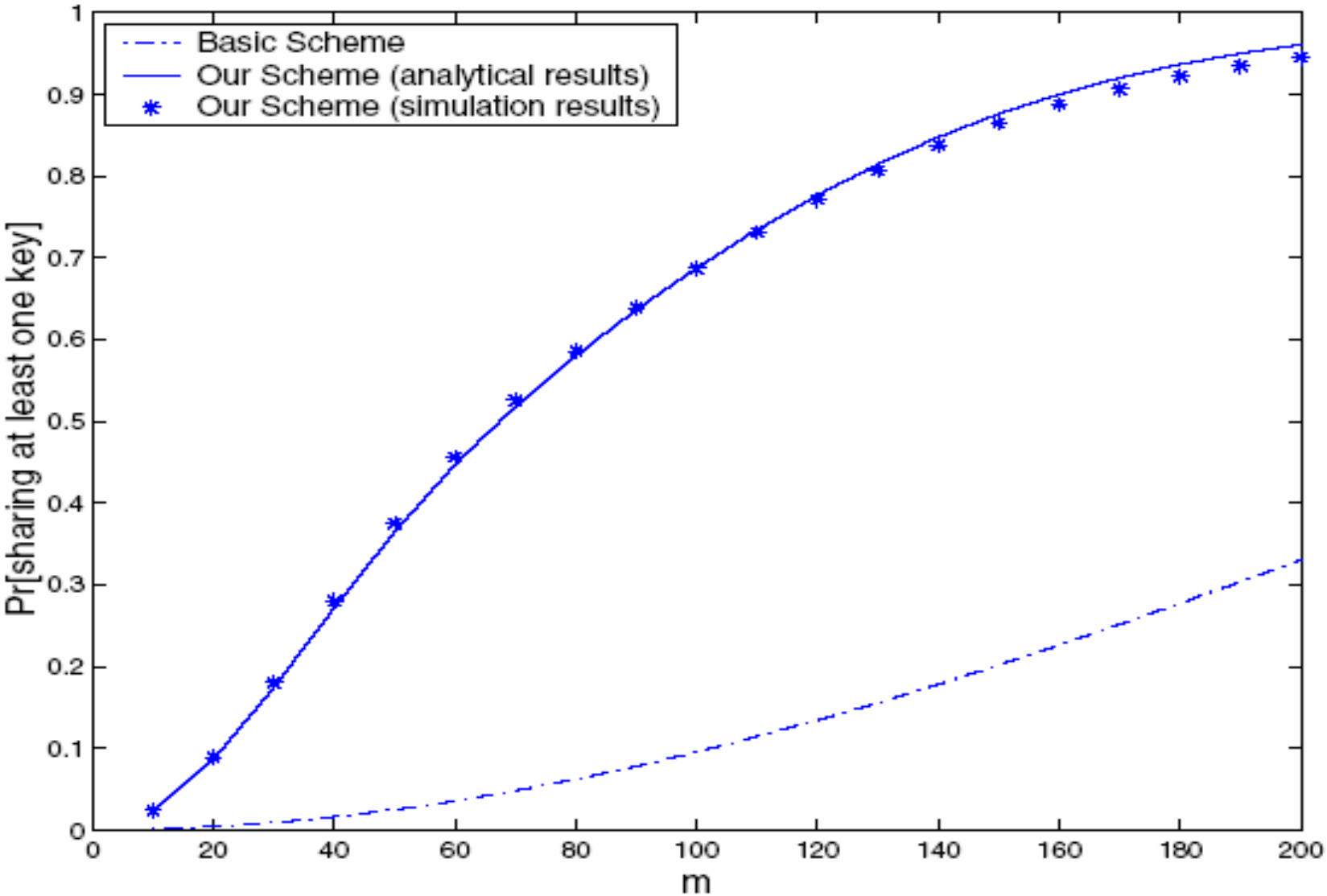
$$|S_c| = \frac{|S|}{tn - (2tn - t - n)a - 2(tn - t - n + 1)b}$$

- For instance, when $|S|=100{,}000$, $t=n=10$, $a=0.167$ and $b=0.083$, $|S_c|=1770$

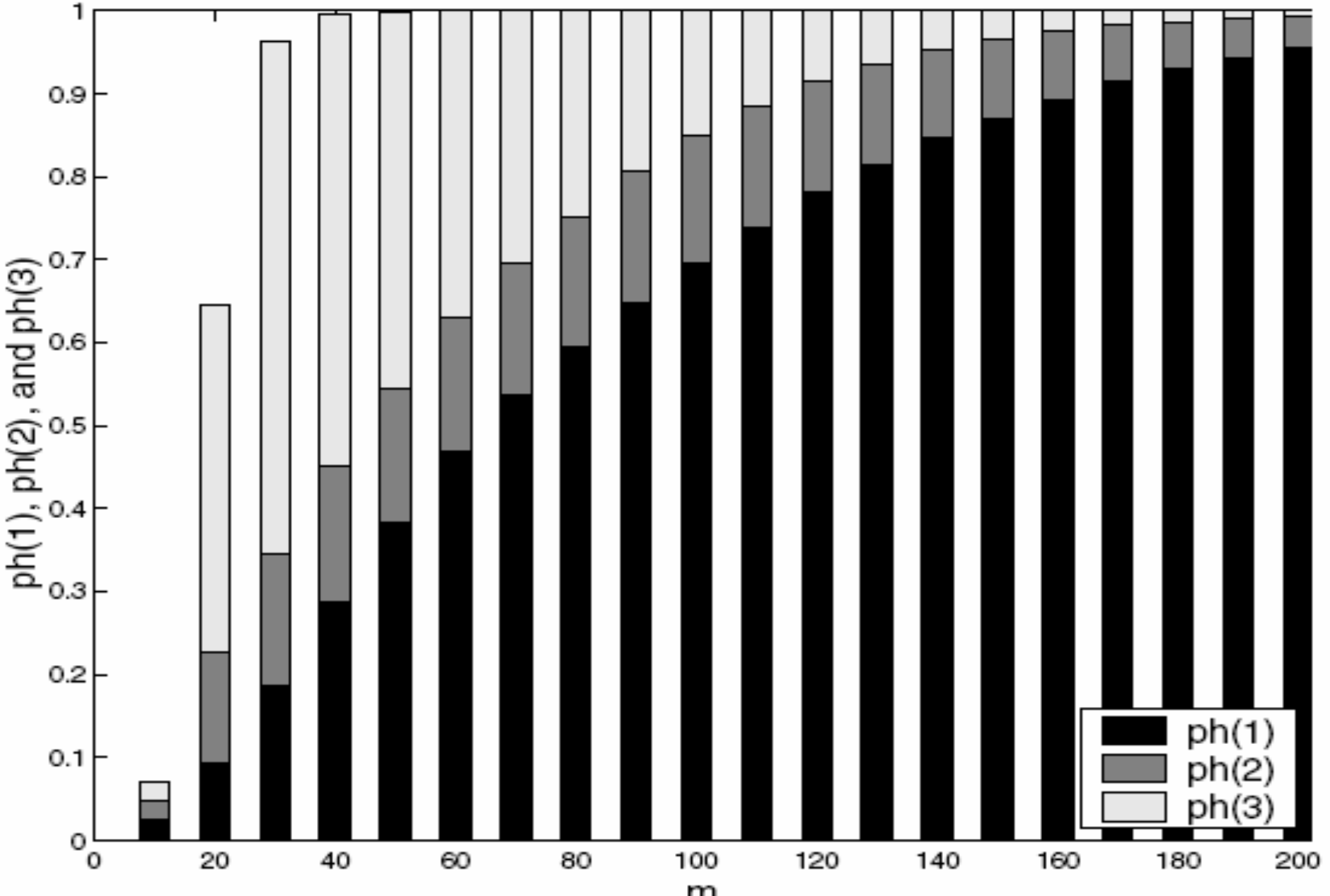
Evaluation

- Connectivity
  - P_{local} = the probability that two neighboring nodes can find a common key
- Communication overhead
  - The neighboring nodes are not connected
- Resilience against node capture
  - Fraction of communications compromised

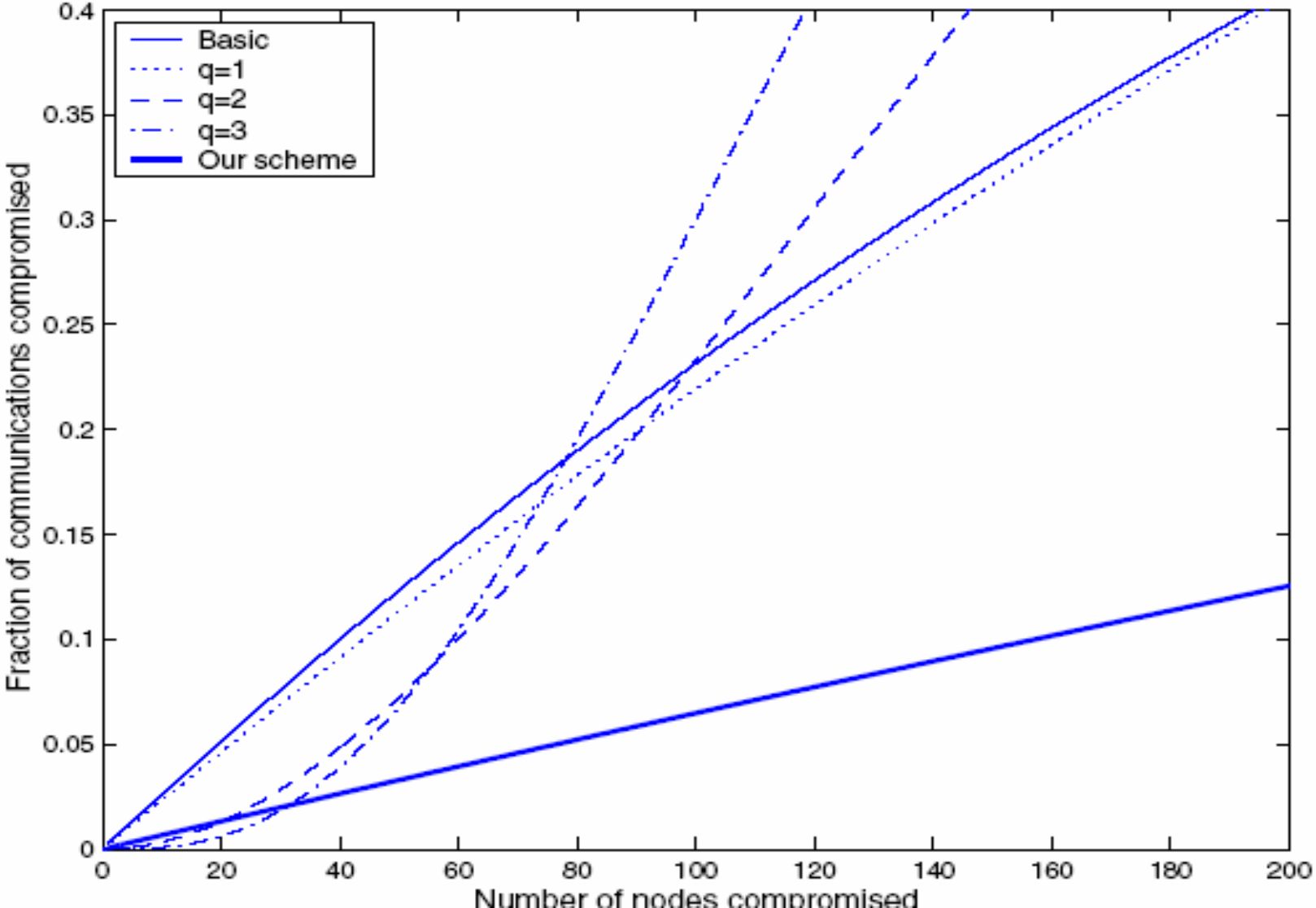
Local Connectivity



Communication Overhead



Network Resilience



Conclusion

- With deployment knowledge, the scheme improves the performance of key pre-distribution in sensor networks.
  - Each node only needs to carry fewer keys while achieving the same level of connectivity
  - Reduce the memory usage
  - Network resilience