Mobility Helps Security in Ad Hoc Networks

ACM MobiHoc 2003

2003.09.17

林佑青

Outline

- Introduction
- System model
- Security associations
- Mobility models
- Performance evaluation
- Conclusion

Introduction

- Mobility is usually perceived as a major security challenge, make security more difficult to achieve.
- Mobility can be useful to establish security associations between any two mobile nodes of a given network.

Introduction (cont.)

- The idea underpinning the solution that is extremely straightforward, as it simply mimics human behavior.
  - Face to face meetings
  - Transport of assets and documents
  - Authentication by physical presence
- Security associations between nodes are established, when they are in the vicinity of each other, by exchanging appropriate cryptographic material.

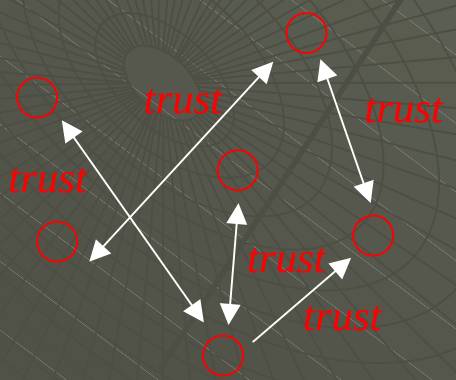
Two Scenarios

- **Fully self-organized mobile ad hoc networks**

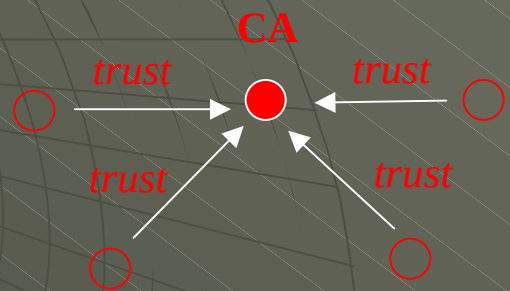
  - no central authority
  - each node generates its own keys and negotiates keys with others
  - membership and security controlled by users themselves

- **Mobile ad hoc networks with a central authority**

  - off-line or on-line authority
  - nodes or authorities generate keys
  - authorities certify keys and node identifies
  - authorities control network security settings and membership



Fully self-organized



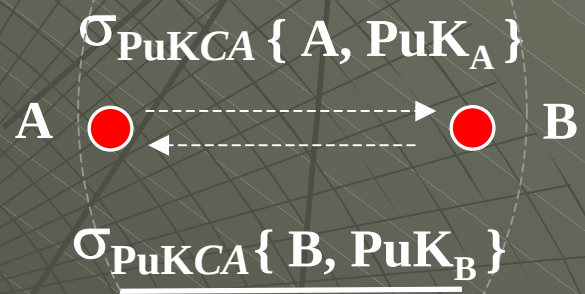
Authority-based

Secure routing and assumptions

- All security associations established between all nodes prior to protocol execution
- Routes are established between nodes with which a source and the destination have security associations
- Routing can not work until security associations are set up.

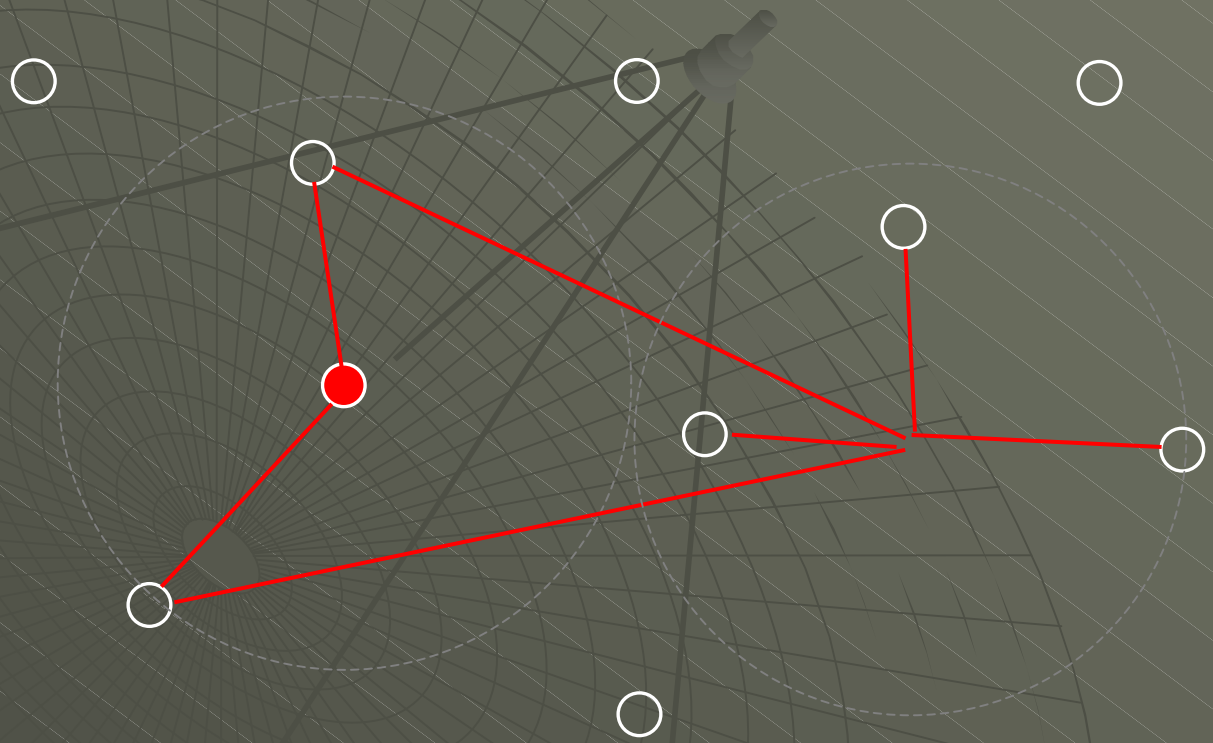
Establishment of security associations

- Each node holds a certificate that bind its ID with its public key, signed by the CA



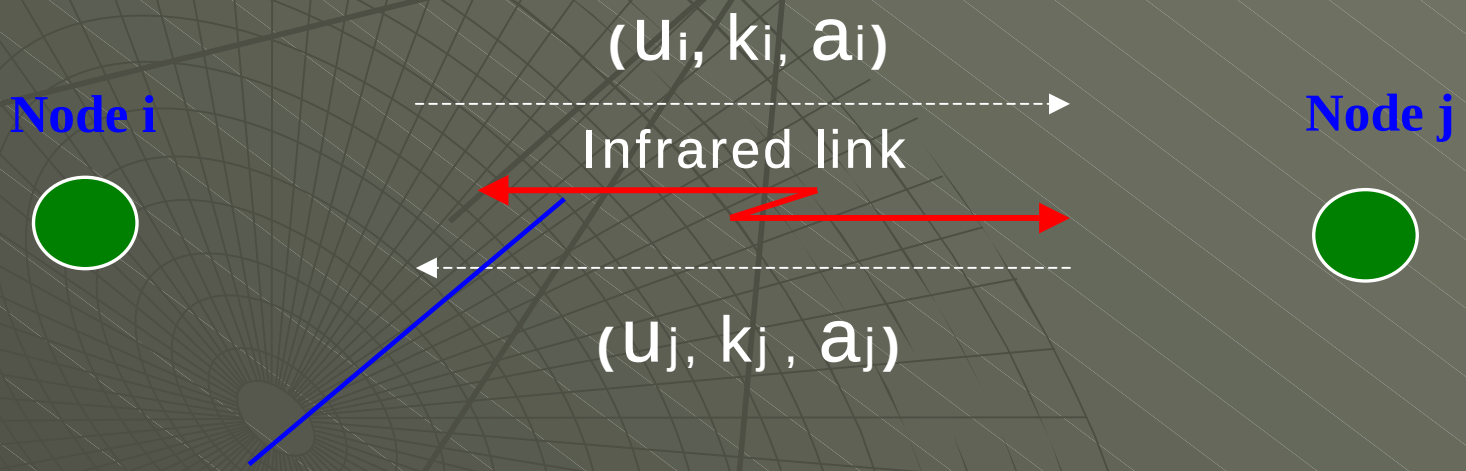
Certificate that binds B's
Public key with his id,
issued and signed by the central authority

Mobility helps security of routing



Fully self-organized scenario

Visual recognition, conscious establishment
of a two-way security association



Secure side channel
-Typically short distance
- Line of sight required
- Ensures integrity
- Confidentiality not required

u: name of the user

k: public key

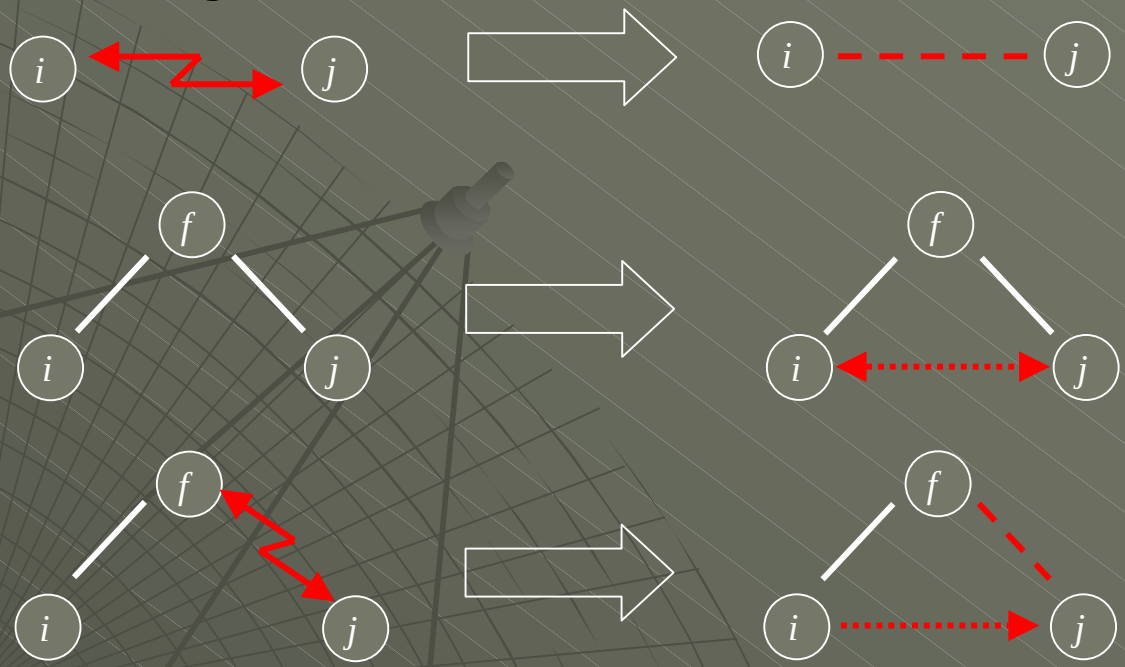
a: address of node

Mechanisms to establish Security Associations

a) Encounter and activation of the SSC

b) Mutual friend

c) Friend + encounter



Exchange of triplets over the secure side channel

Nodes know each others' triplet as a result of a physical encounter

Friendship : nodes know each others' triplets

i knows the triplet of *j* ; the triplet has been obtained from a friend of *i*

Implement the mechanisms

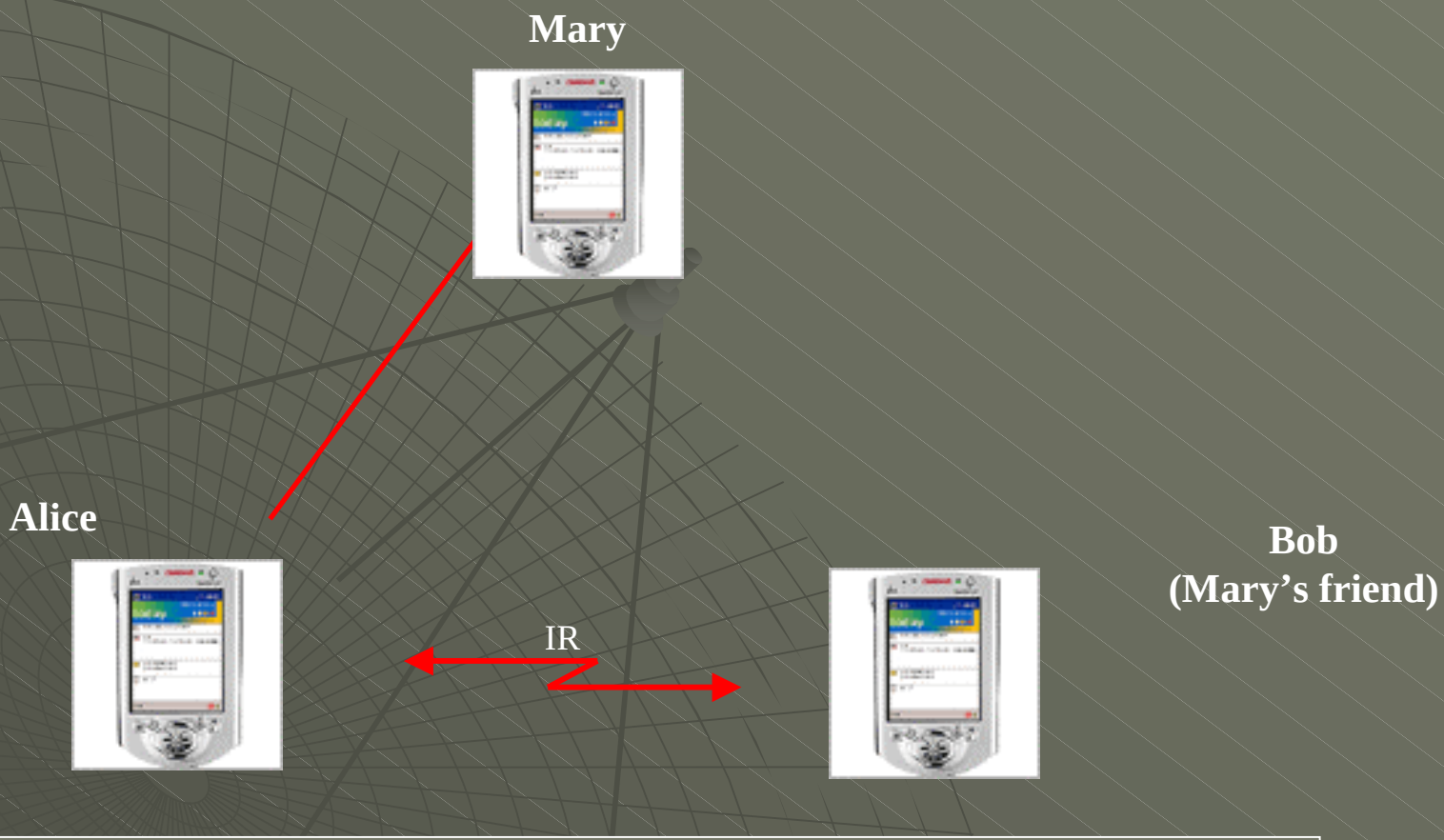
Protocol 1: Direct Establishment of a Security Association

msg1	$i \rightarrow j:$	$r_i \mid u_i \mid k_i \mid a_i$
msg2	$j \rightarrow i:$	$r_j \mid u_j \mid k_j \mid a_j$
	$i:$	$u_j?;\ match(k_j, a_j)?$
	$j:$	$u_i?;\ match(k_i, a_i)?$
msg3	$i \rightarrow j:$	$\sigma_i(r_j \mid u_i \mid u_j)$
msg4	$j \rightarrow i:$	$\sigma_j(r_i \mid u_j \mid u_i)$

Protocol 2: Friend-Assisted Establishment of a Security Association

msg1	$i \rightarrow f:$	$req : u_j \mid r_i$
msg2	$f \rightarrow i:$	$u_j \mid k_j \mid a_j \mid \sigma_f(r_i \mid u_j \mid k_j \mid a_j)$

Friends mechanism



Mary and Bob are friends:

- They have established a Security Association at initialisation
- They faithfully share with each other the Security Associations they have set up with other users

Advantages of the authority based scenarios

Mobile ad hoc networks with authority based security systems

- automatic establishment of security associations
- no user involvement
- only off-line authorities are needed
- straightforward rekeying

Advantages of the self-organized base scenarios

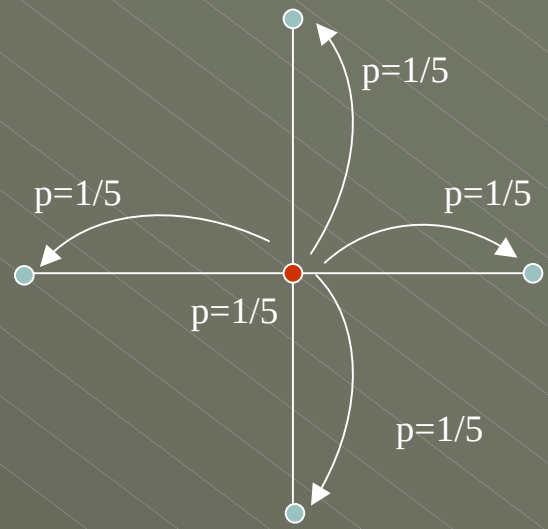
Fully self-organized mobile ad hoc networks

- There are no central authorities
- Each user/node generates its own public/private key pairs
- No trust transitivity
- Intuitive for users
- Can be easily implemented (vCard)
- Useful for setting up security associations for secure routing in smaller networks or peer-to-peer applications
-User/application oriented

Mobility models

Random walk

- discrete time
- simple, symmetric random walk
- area: Bounded and toroid grids



Random waypoint

- most commonly used in mobile ad hoc networks
- continuous time
- area size: 1000m x1000m
-security power range: 5m (SSC), 50m 100m (radio)

Common simulation settings

- simulations are run 20 times
- confidence interval: 95%

Terminology

Matrix F, the friend relationships between nodes:

$$f_{ij} = \begin{cases} 1 & \text{if } i \text{ trusts } j \text{ (i.e., } j \text{ is a friend of } i\text{)} \\ 0 & \text{otherwise} \end{cases}$$

Matrix P: Desired security associations :

$$p_{ij} = \begin{cases} 1 & \text{if } i \text{ wants to know the public key and address of node } j \\ 0 & \text{otherwise} \end{cases}$$

Matrix E(t), Established security associations :

$$e_{ij}(t) = \begin{cases} 1 & \text{if, at time } t, \ i \text{ knows the public key and address of node } j \\ 0 & \text{otherwise} \end{cases}$$

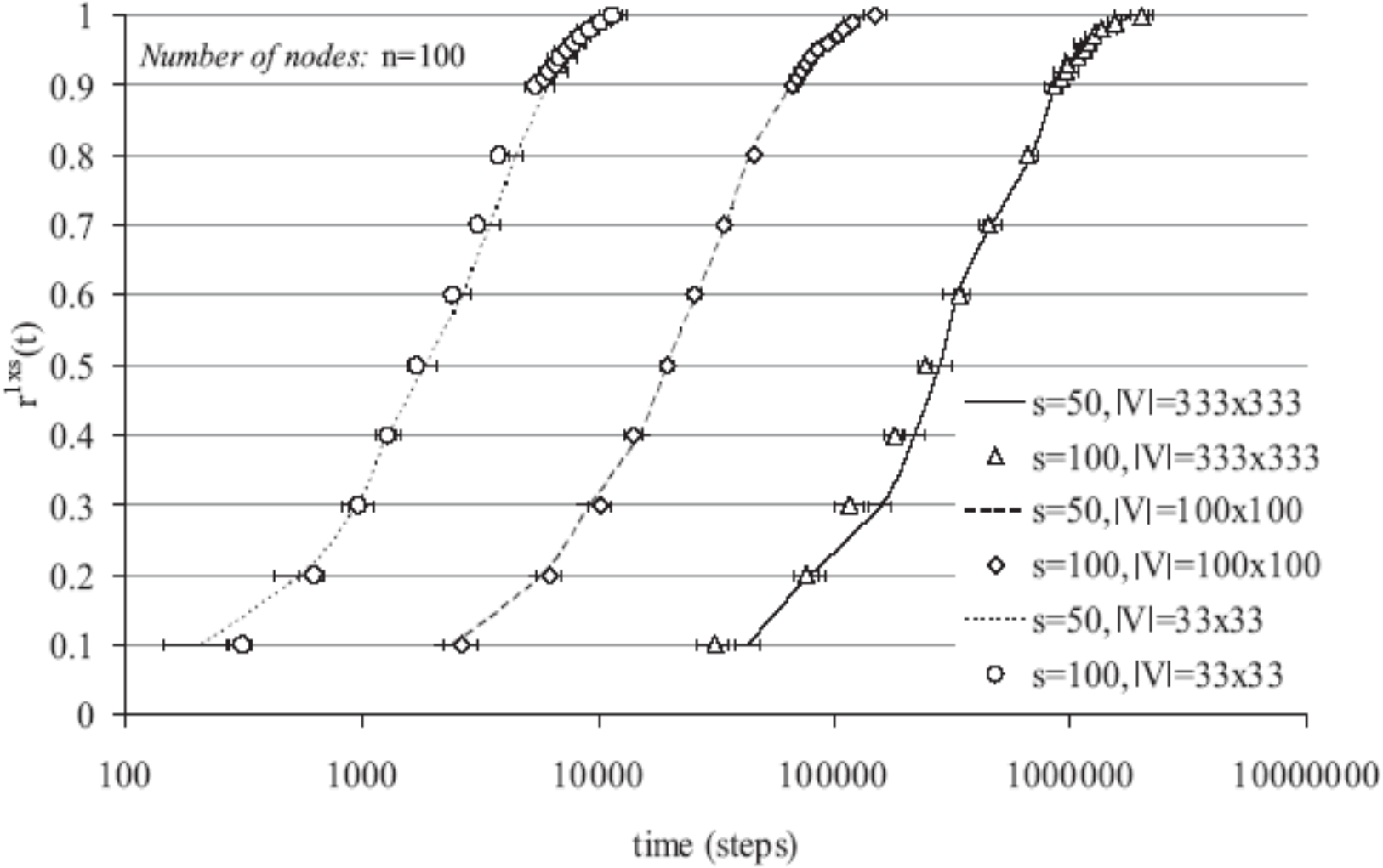
Convergence r(t) :

$$r(t) = \frac{\sum_{i,j}^{n} e_{ij}(t) \cdot p_{ij}}{\sum_{i,j}^{n} p_{ij}}$$

Pace of establishment of the security associations

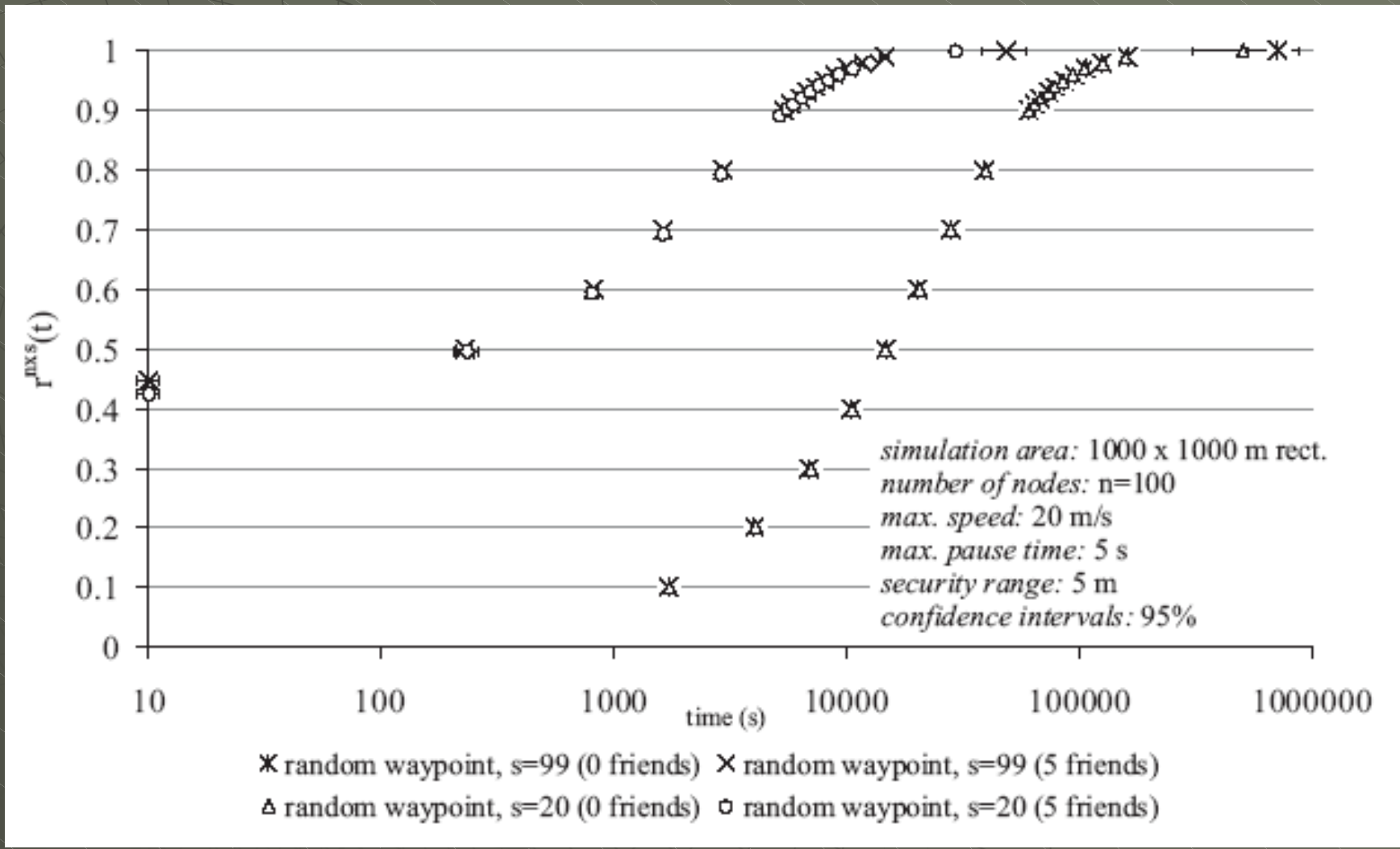
- Depends on several factors:
  - Area size
  - Number of communication partners: *s*
  - Number of nodes: *n*
  - Number of friends
  - Mobility model and its parameters (speed, pause times, ...)

Performance Evaluation (1)



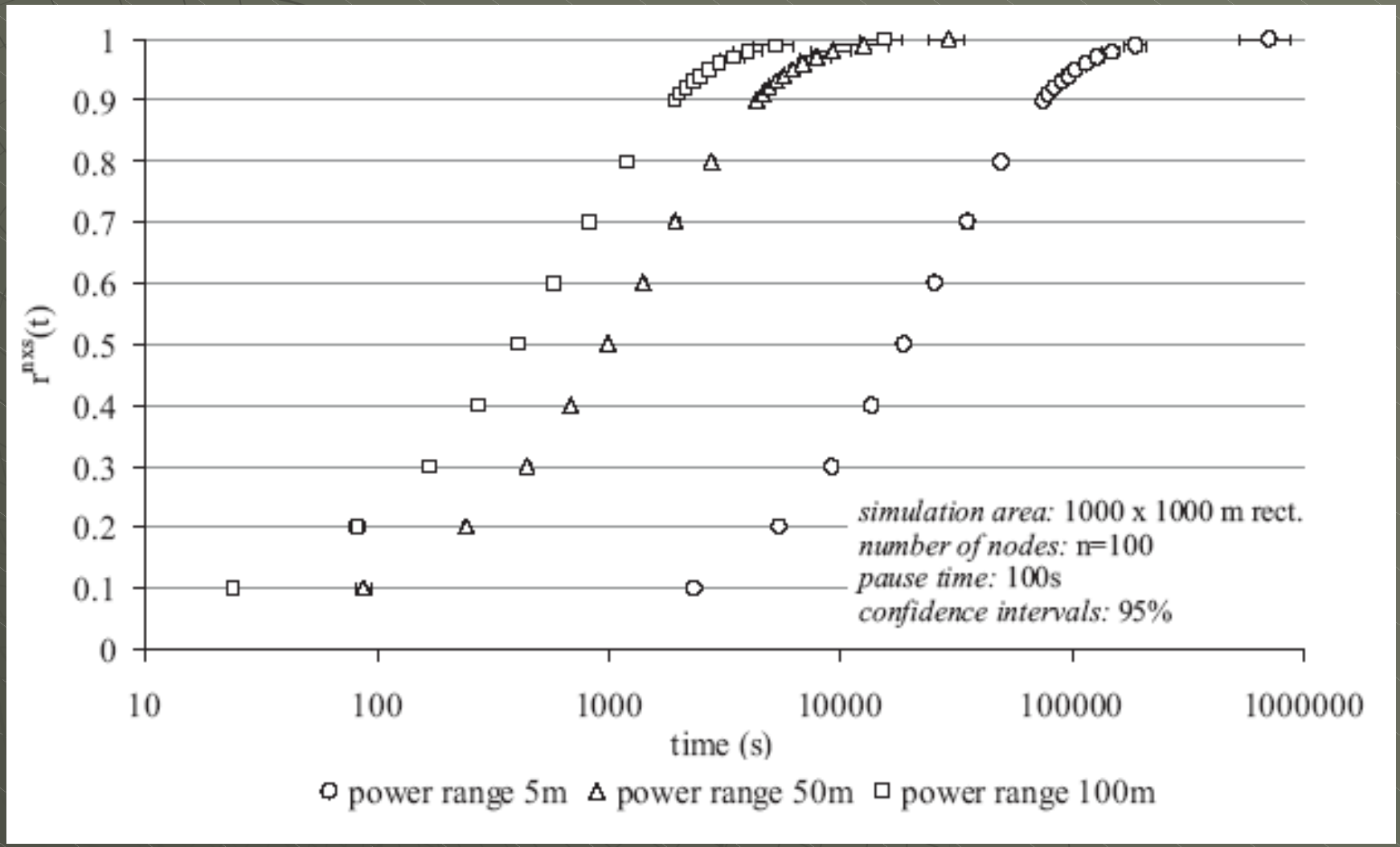
Convergence with random walk model for various sizes

Performance Evaluation (2)



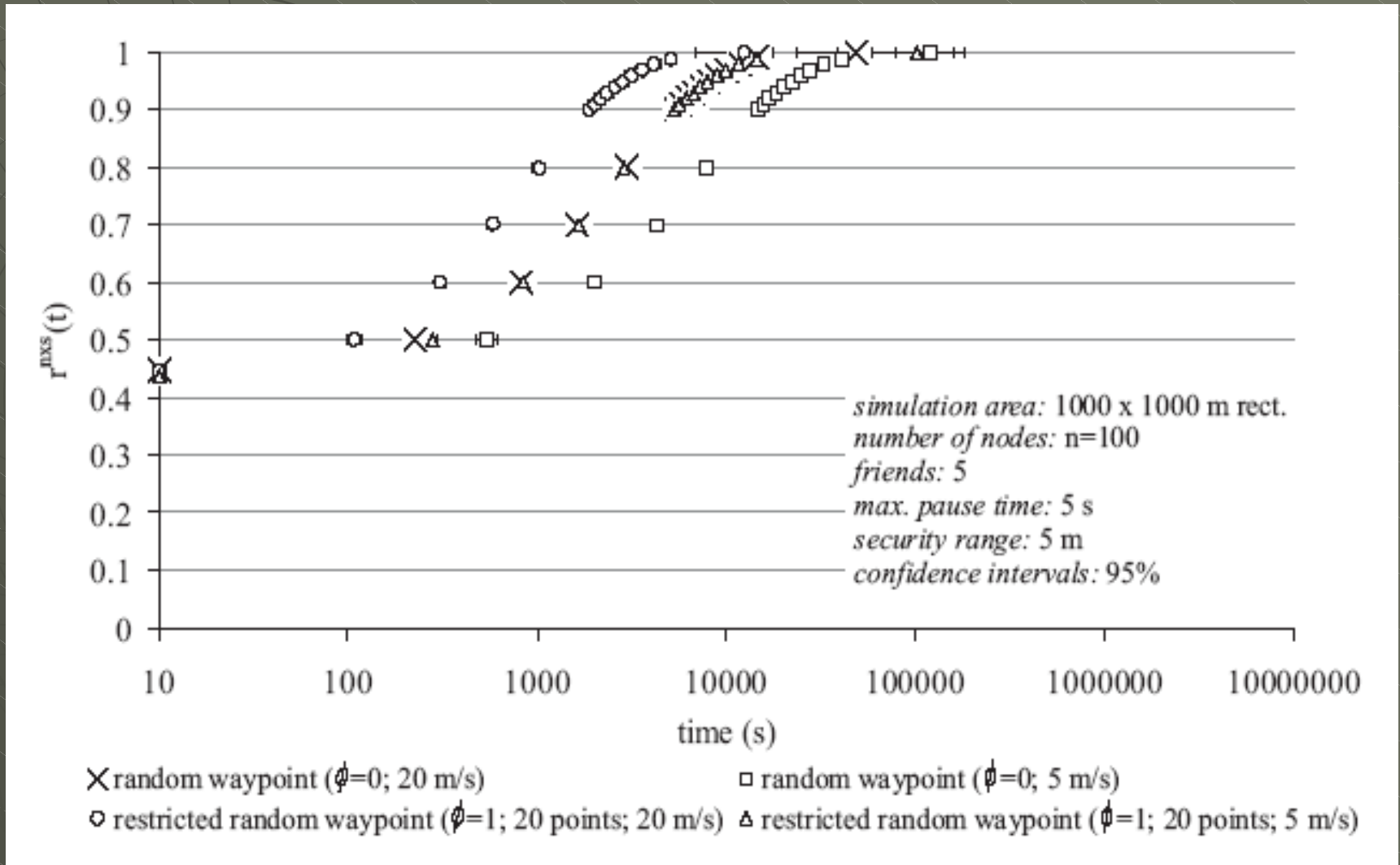
Convergence with random waypoint model

Performance Evaluation (3)



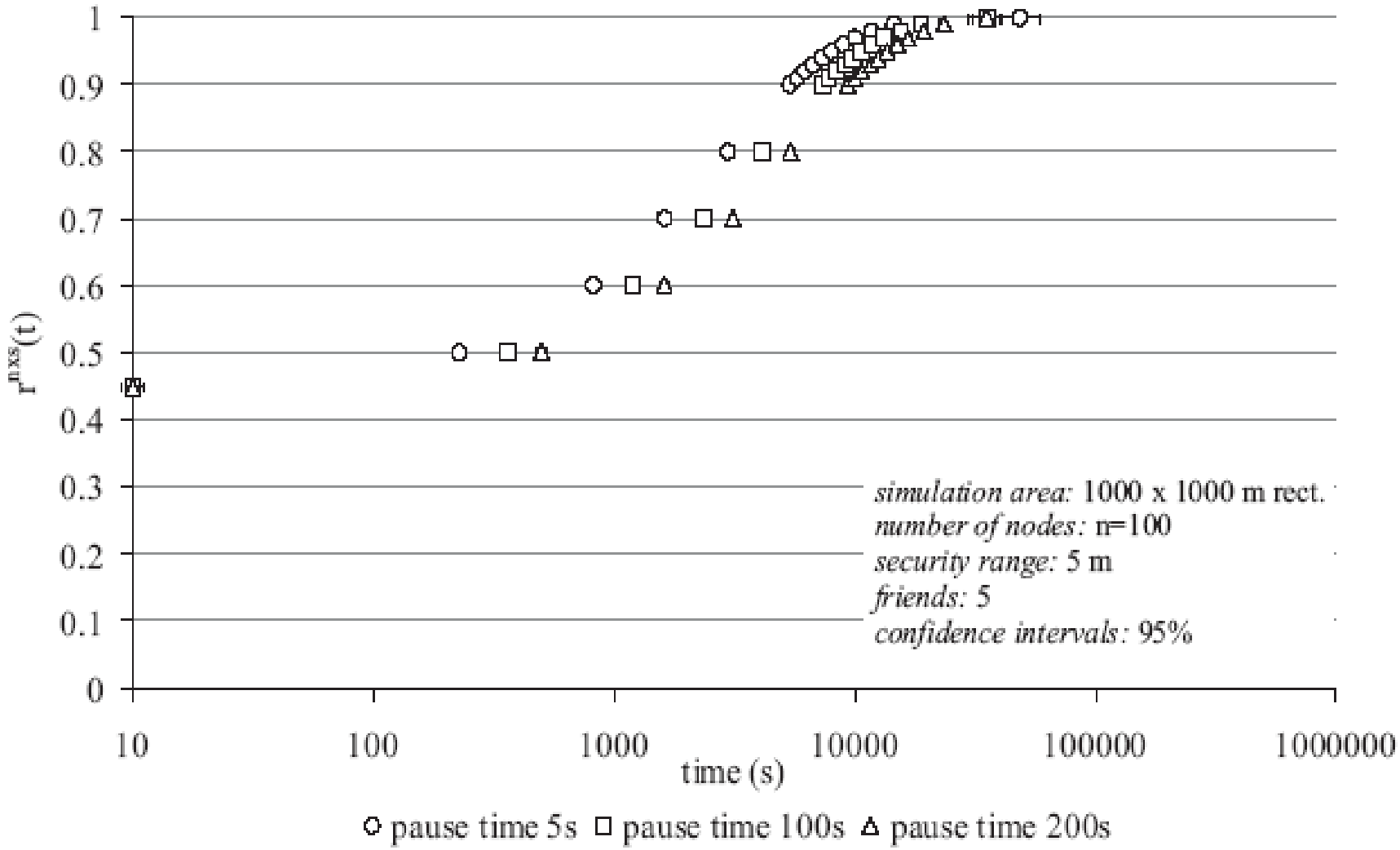
Convergence with random waypoint model for power ranges

Performance Evaluation (4)



Convergence with random waypoint model for speeds of node movement

Performance Evaluation (5)



Convergence with random waypoint model for pause time

Conclusion

- Mobility can help security in mobile ad hoc networks, from the networking layer up to the applications.
- The pace of establishment of the security associations depends on the area size, the number of friends, and the speed of the nodes.
- Higher mobility leads to a faster creation of the security associations.