Privacy and identity in context-aware services

NOKIA

NIS '09, Crete

Valtteri Niemi
Nokia Research Center
Lausanne, Switzerland

 © 2009 Nokia

Outline

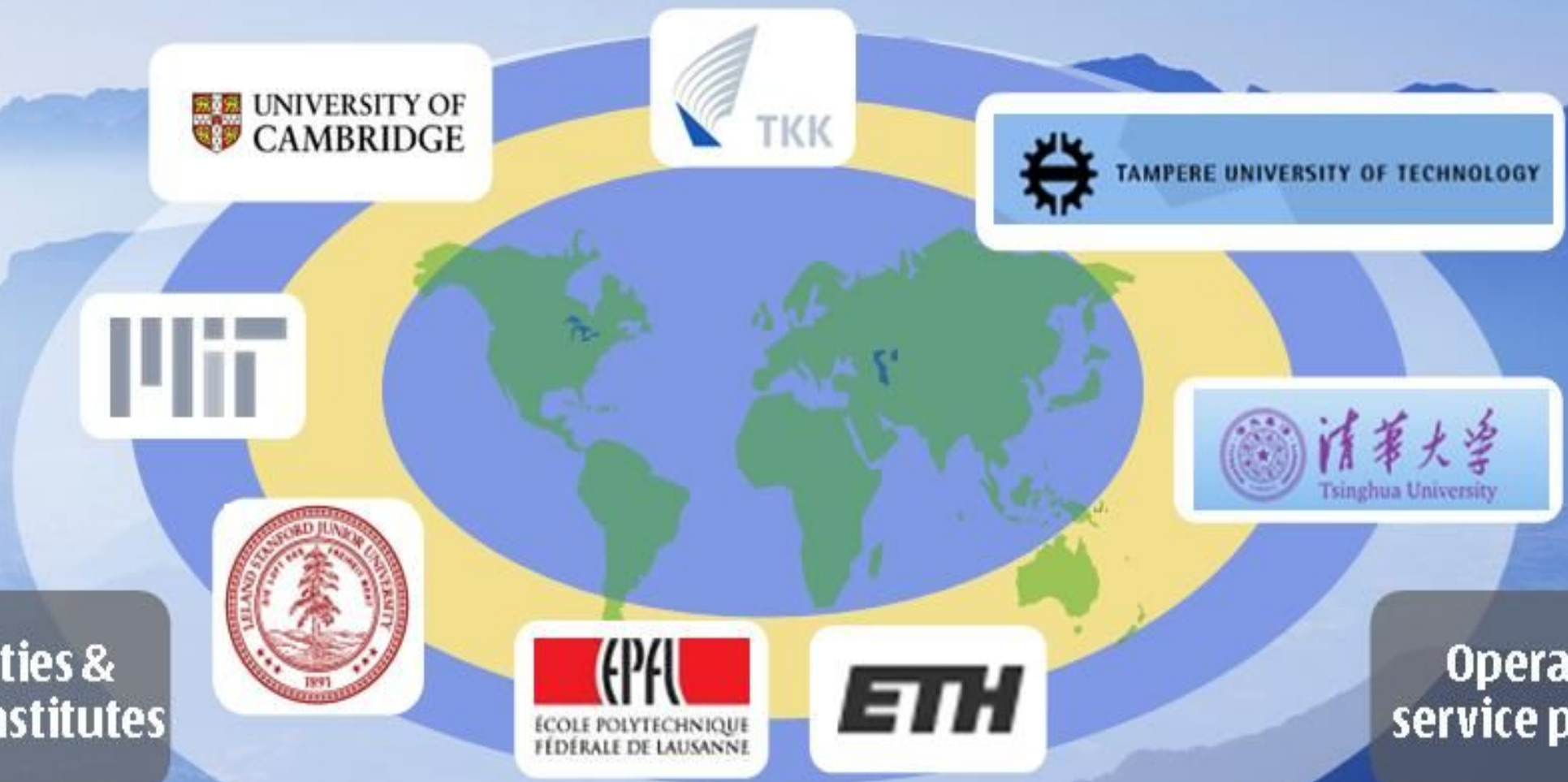
- Background
- Context-aware services
- Privacy
- Identity
- Privacy-enhancing technologies
  - Anonymisation
  - Multiparty computations
  - Usage control

NOKIA

Background

© 2009 Nokia

Nokia Research Center
Unique Network for Open Innovation



Universities & research institutes

Operators & service providers

Open source developers

International organizations

Corporations

Venture capital companies

NOKIA

Nokia Research Center

Overview on Industrial Ecosystem

Convergence & Mobile Internet



Windows Live Search

Google

skype

EA

myspace
a place for friends

flickr

YouTube

YAHOO!

CNN





All my connected services, always with me

NOKIA

Nokia Research Center

Context-aware services

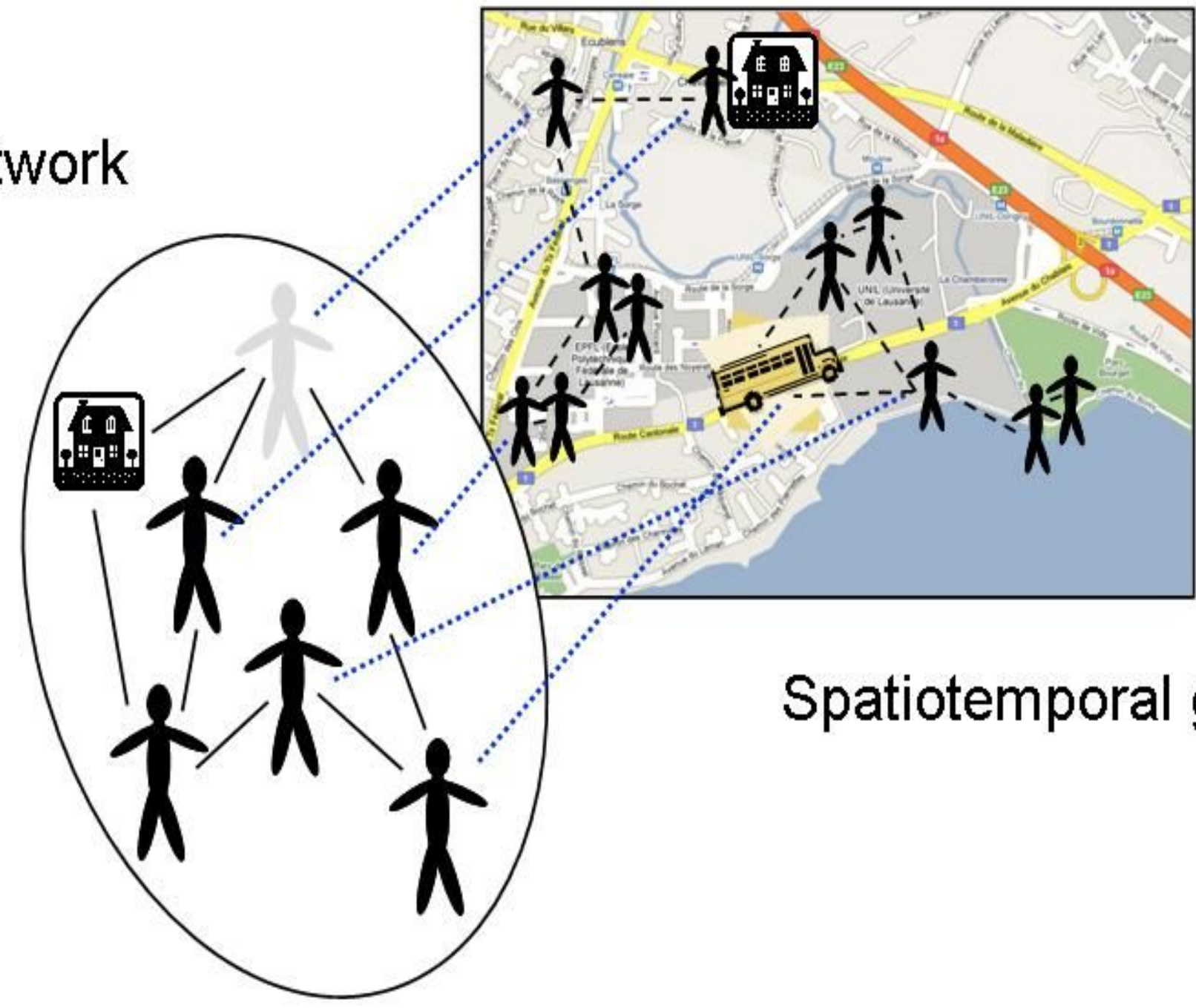
Spatiotemporal context



© 2009 Nokia

Context-awareness

Social network



Spatiotemporal graph

© 2009 Nokia

Sensing the context

- ~ 1 billion PC's in the world
- ~ 4 billion mobile devices
- ~ 40 billion mobile sensors
  - location, temperature, barometer, light, vibration,...

- Mobile device *automatically* knows user's context

NOKIA

Examples of context-aware services

- Classical examples:
  - Where is the nearest restaurant / grocery / ATM / bus stop / taxi station ... ?
  - How to get from *here* to *there* fastest / cheapest / easiest ... ?
  - Dating services
  - Presence
  - ...
- Augmented reality
- Targeted and mobile advertisement
- Using the social context:
  - Where are my friends ?
  - Where should a person like me go on this day on this city ?
  - ....
- Creation / sharing of *local* content can complement/enhance Internet services

© 2009 Nokia

Privacy

Security

- Confidentiality
- Authentication
- Integrity
- Availability
- Non-repudiation

Privacy vs. Security

- Narrow interpretation: Privacy = Confidentiality
  - Privacy Enhanced (e)Mail (PEM), Pretty Good Privacy (PGP), Wired Equivalent Privacy (WEP)
- Authentication = Verifying Identity
  - Seems to go inherently against privacy
- Integrity is needed whether data is public or private
  - Could be easier to provide if no privacy (e.g. by duplication)
- Availability is needed whether data is public or private
  - Challenges are different
- Non-repudiation e.g. by digital signatures
  - Seems to go against privacy

© 2009 Nokia

Privacy vs. Trust

- Trust – (extremely) multi-dimensional concept
- Here: trust ~ *predictability*
- No assumption of good intentions
  - Mafia
  - "He can be trusted to do the opposite than he is told to do"
  - Trust on machine / device, e.g. *trusted computing*
- Predictability seems to go against privacy
- On the other hand, privacy assumes trust
  - Others to respect one's privacy
  - *Trusted third party* could help in protecting privacy

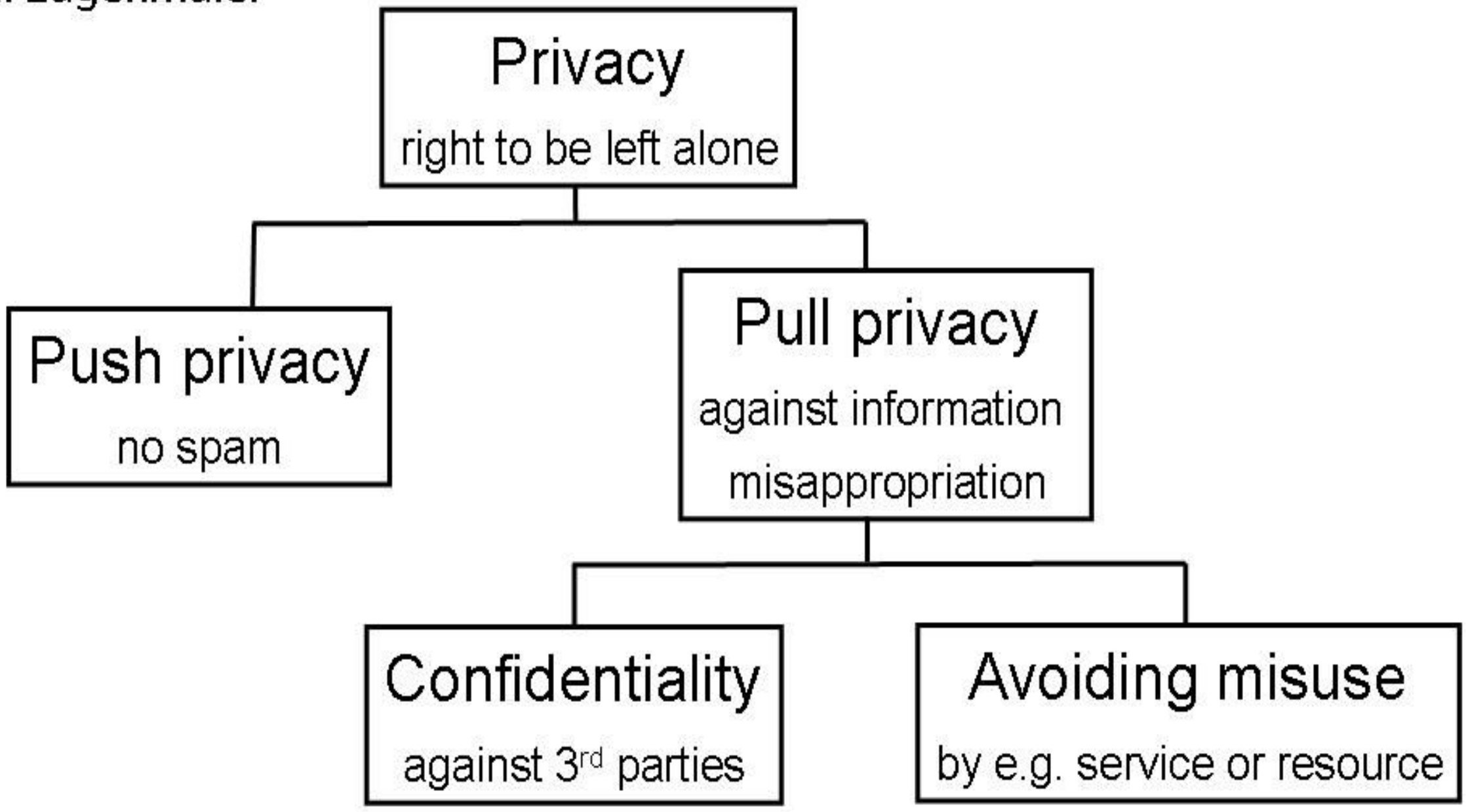
© 2009 Nokia

Privacy ~ Personally identifiable information

NOKIA

Taxonomy of privacy

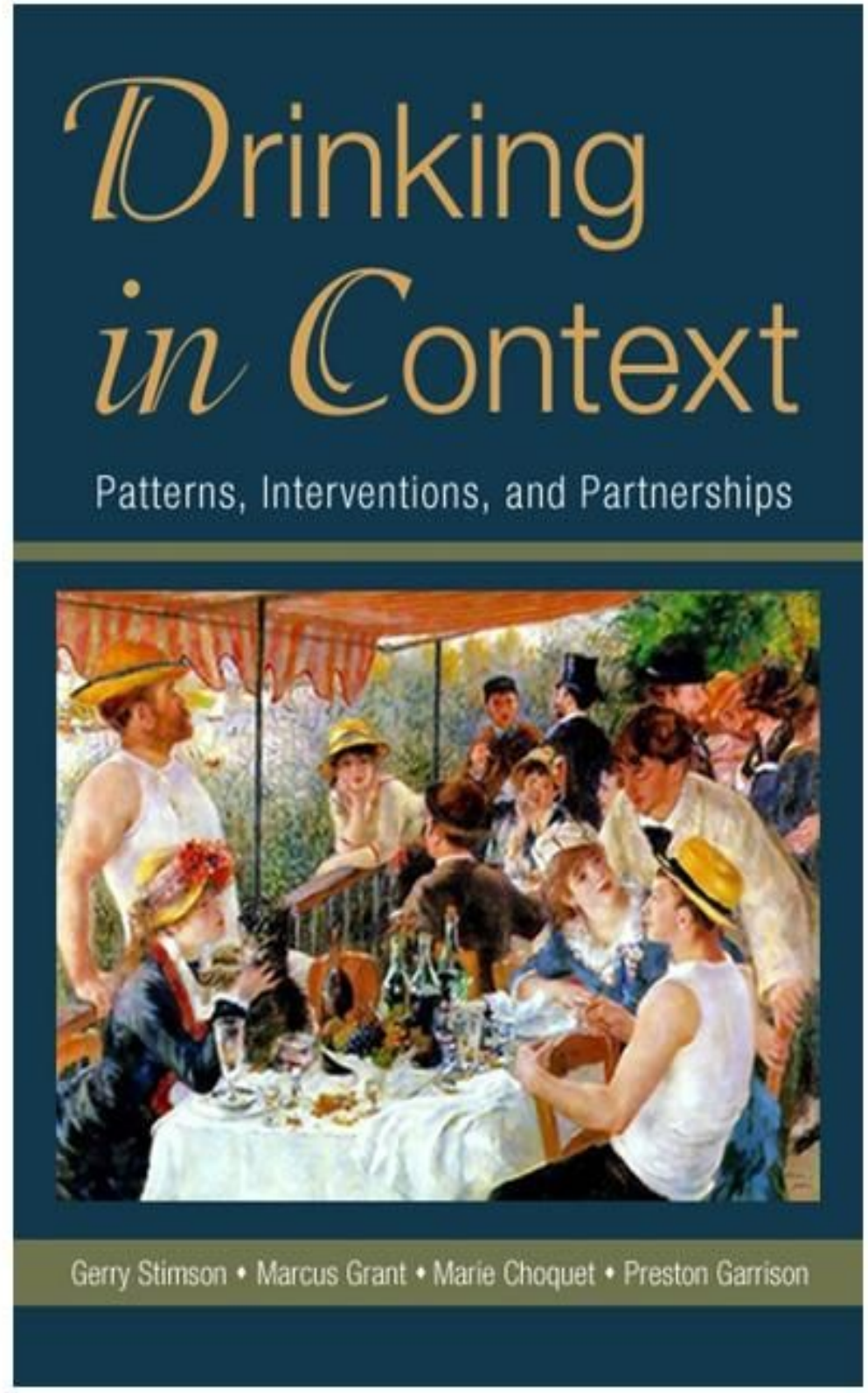
- By Alf Zugenmaier



© 2009 Nokia

Context vs. privacy

- Giving context away ~ giving privacy away
- Context history – privacy requirements vary over time



NOKIA

Identity

Digital identities

- Multiple roles – multiple identities
- Unlinkability
- Different privacy requirements

© 2009 Nokia

What is Identity ?

- Identifier
- Credentials
- Attributes
- Pattern

© 2009 Nokia

What is Identity ?

- Identifier e.g. Valtteri Niemi
- Credentials e.g. password
- Attributes e.g. male, Nokia employee
- Pattern e.g. reputation

NOKIA

Threats against identity privacy

- Identifiers in many layers / interfaces
  - MAC address (for WLAN, Bluetooth, cellular, ...)
  - IP address
  - Application layer identifiers (email address, SIP address, usernames, ...)
- Correlation between different identifiers
- Long-standing pseudonym = permanent identity
- Active attacks typically easy to do: “please identify yourself”
- Tracking person’s device = tracking person

© 2009 Nokia

Physical layer identification

- Instead of listening to identifiers, try to recognize a wireless device uniquely based on *characteristics* of physical layer (" radio fingerprint")
- Very difficult to change this characteristics because of dependence on the hardware
  - On the other hand, this is a good property for authentication purposes
- Well studied feature in military domain
- For commercial products:
  - *classification error* between equivalent radio transmitters from different manufacturers can be pushed down to a few per cent
  - Transmitters from same manufacturer can be identified with almost the same accuracy

© 2009 Nokia

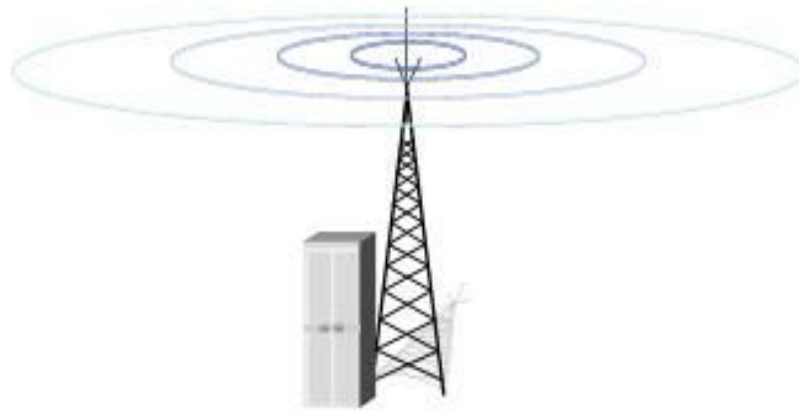
Example of identity protection: GSM

MS (SIM)
IMSI, Ki

VLR
and BTS

HLR
{{IMSI,Ki}}







IMSI / TMSI

IMSI

RAND

RAND, XRES, Kc

Kc

SRES

SRES=XRES ?

encrypted TMSI

© 2009 Nokia

NOKIA

Privacy enhancing technologies

Non-technological privacy enhancement

- Privacy policies
- Privacy laws
- Standards

Anonymity



- Anonymisation
  - How to anonymise *all* attributes ?
- Pseudonyms
- Anonymous authentication
  - Verifying authorization, not identity

© 2009 Nokia

NOKIA

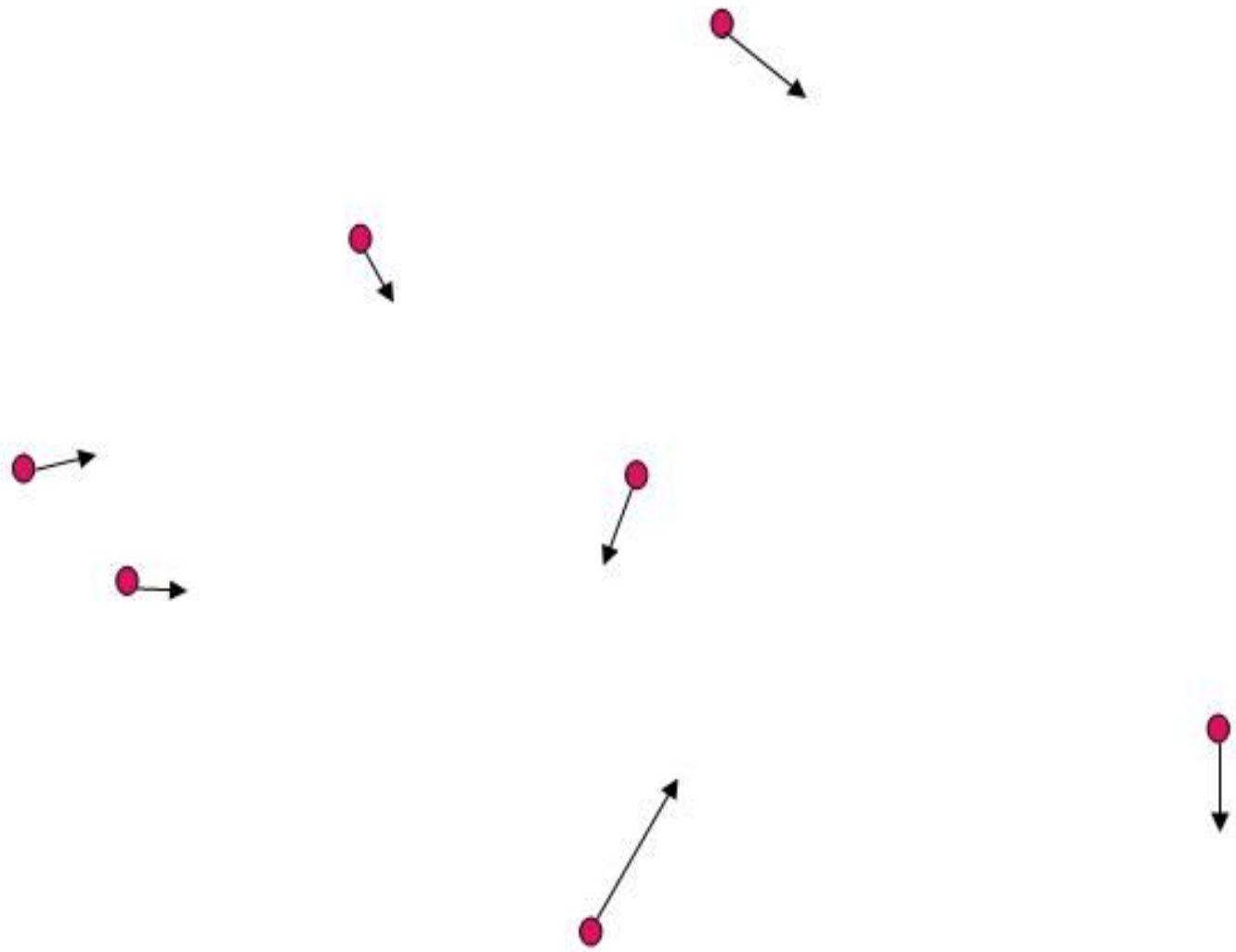
Anonymisation vs. tracking of devices

- Devices may exchange (permute) pseudonyms when sufficiently many in proximity to each other
- Some services are "*privacy-friendly*" by nature
  - e.g. for observing / predicting traffic jams, no need to identify individual cars
- For many services, exact location is not needed
  - e.g. device could add "*noise*" to its location before revealing it (see next slides)
  - statistical distribution of devices could remain

© 2009 Nokia

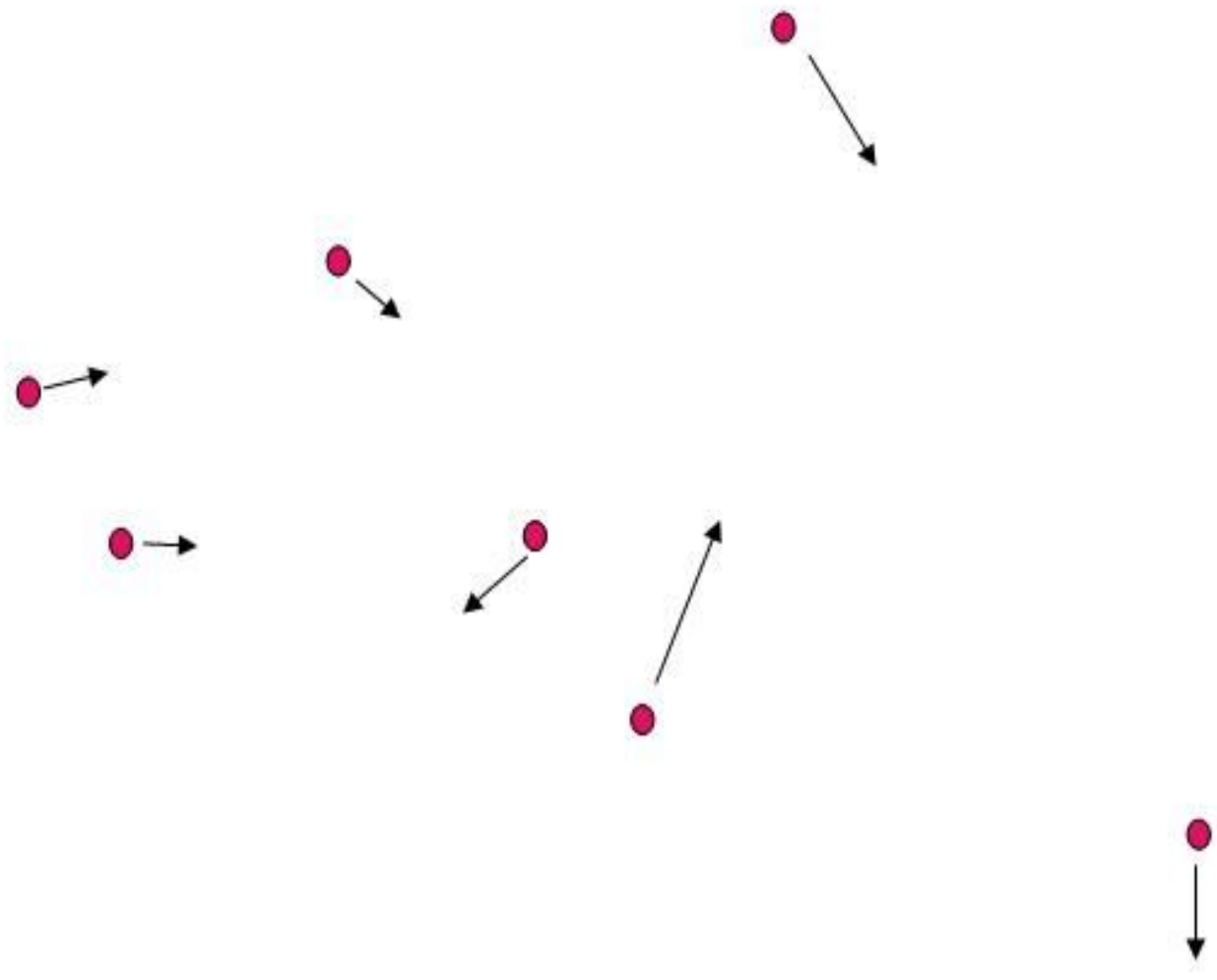
Tracking location of anonymous devices

Tracking location of anonymous devices

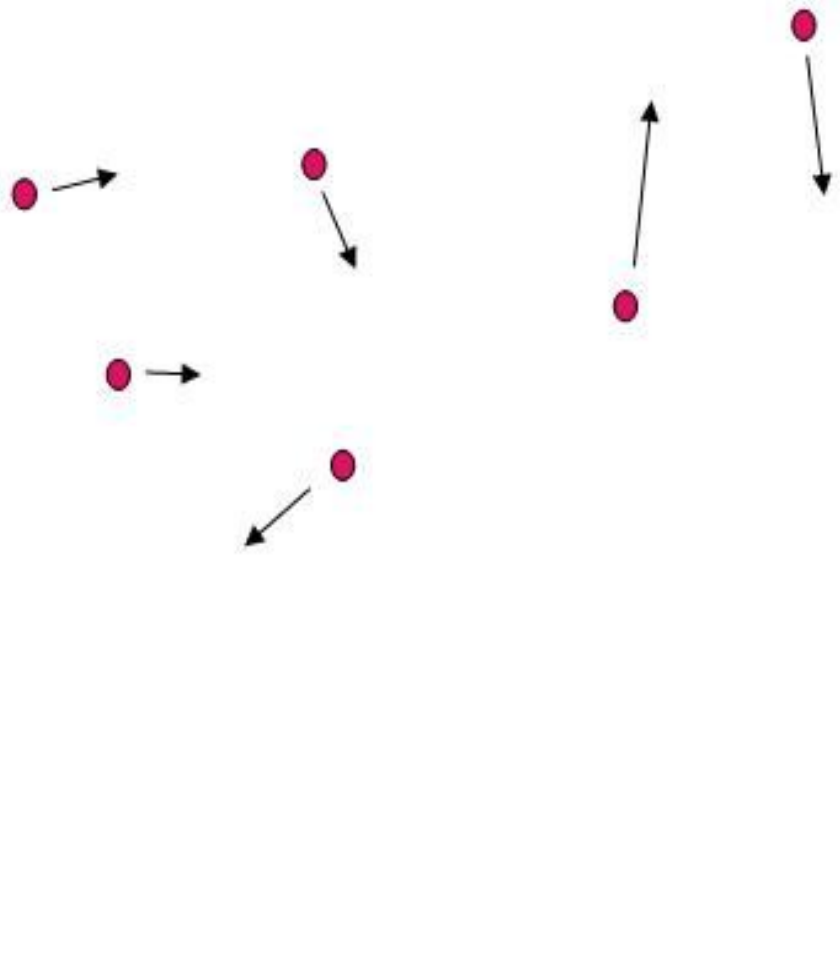


NOKIA

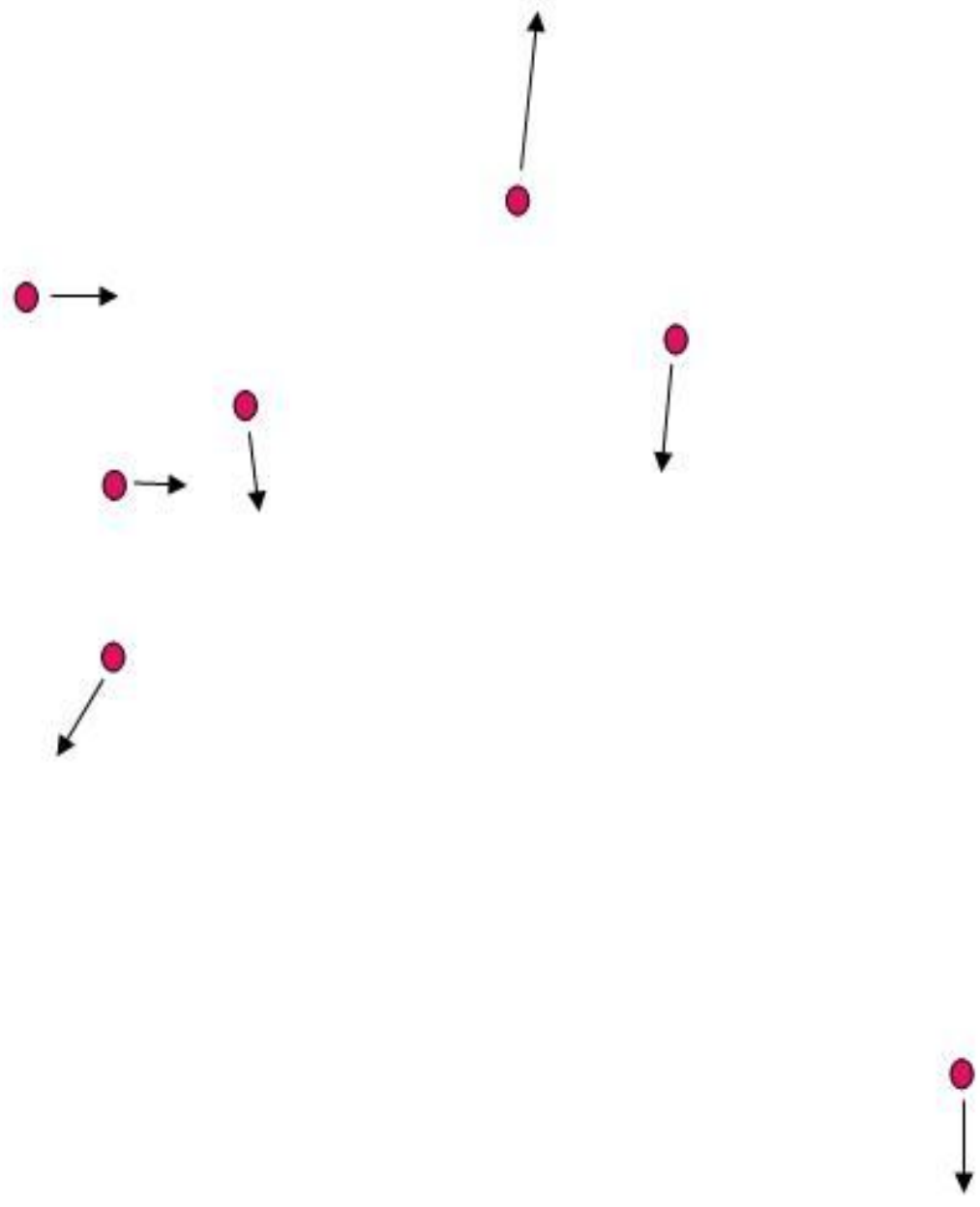
Tracking location of anonymous devices



Tracking location of anonymous devices



Tracking location of anonymous devices

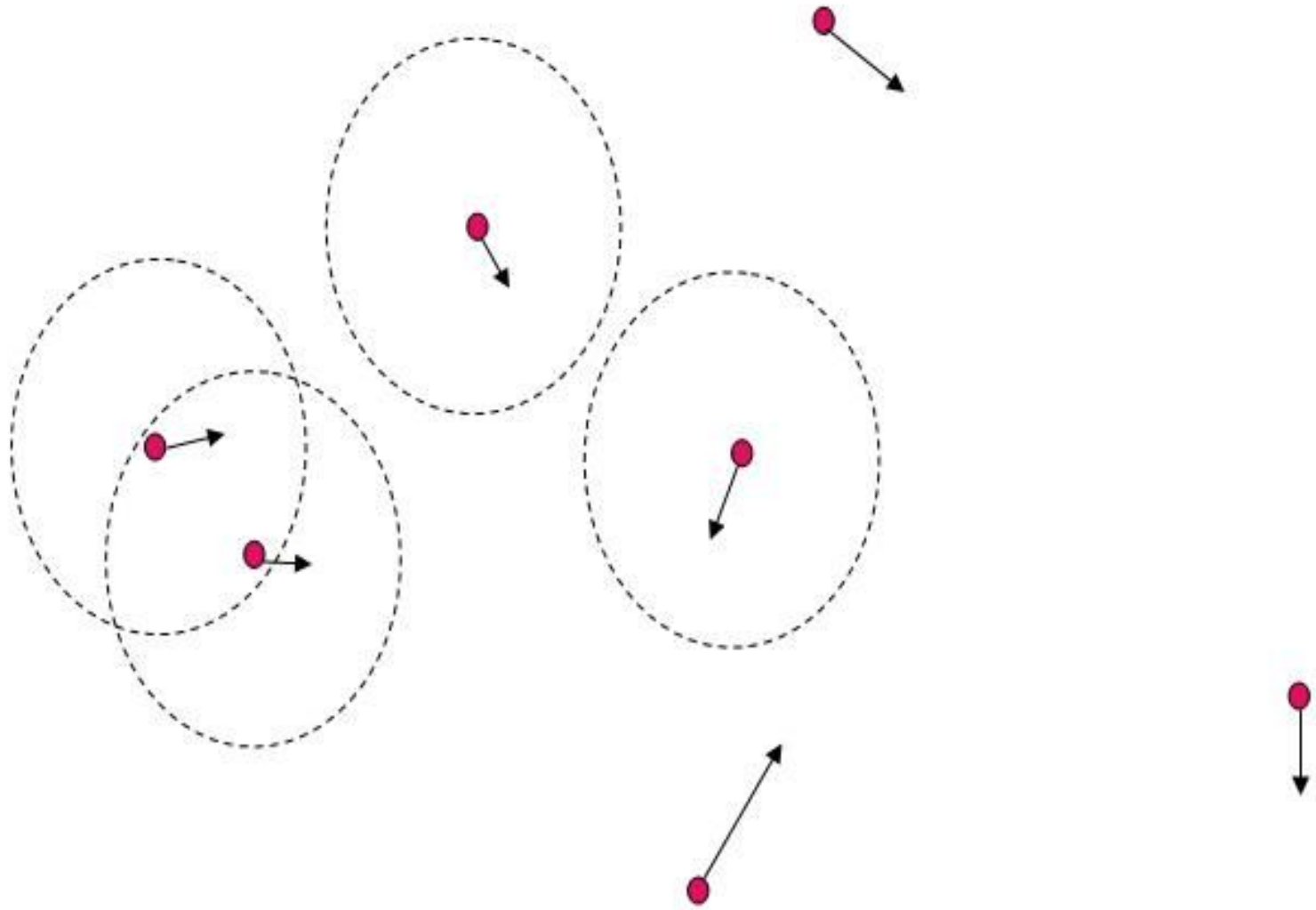


NOKIA

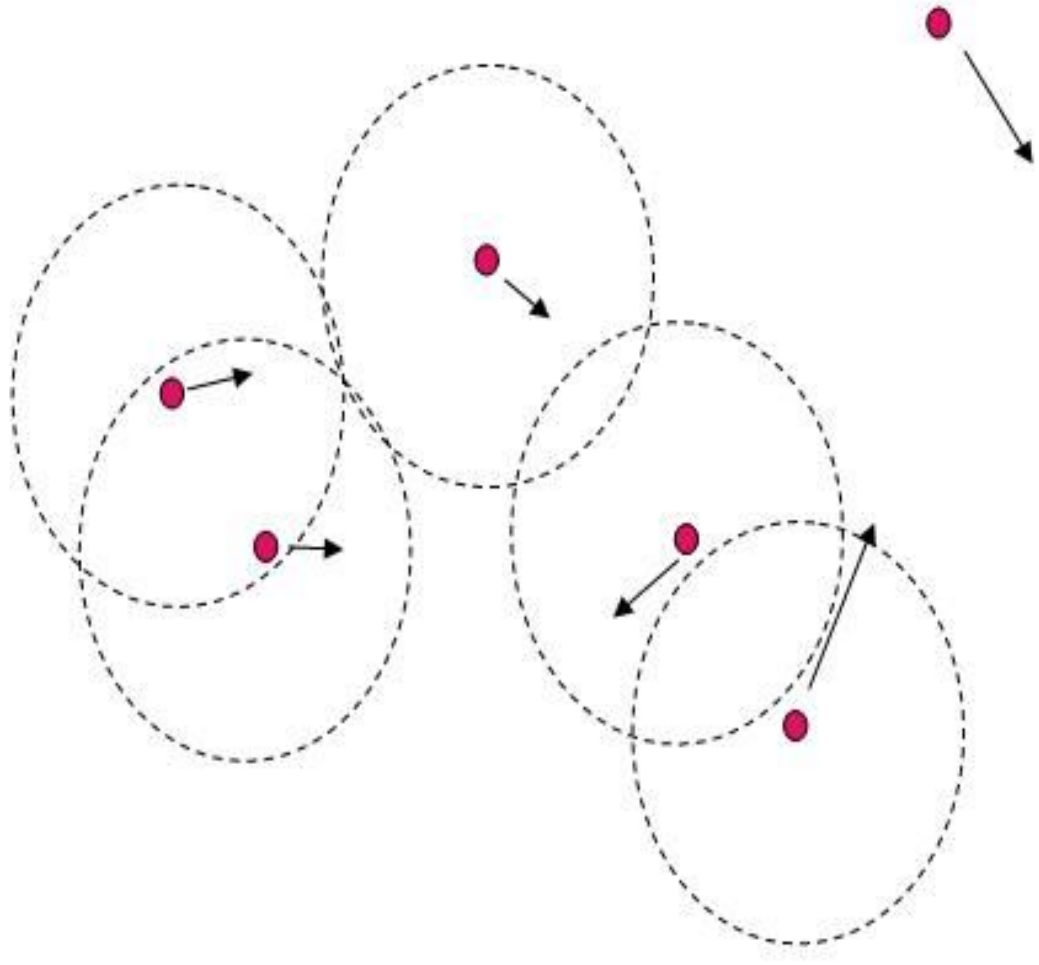
Adding "noise" to the location

© 2009 Nokia

Adding "noise" to the location



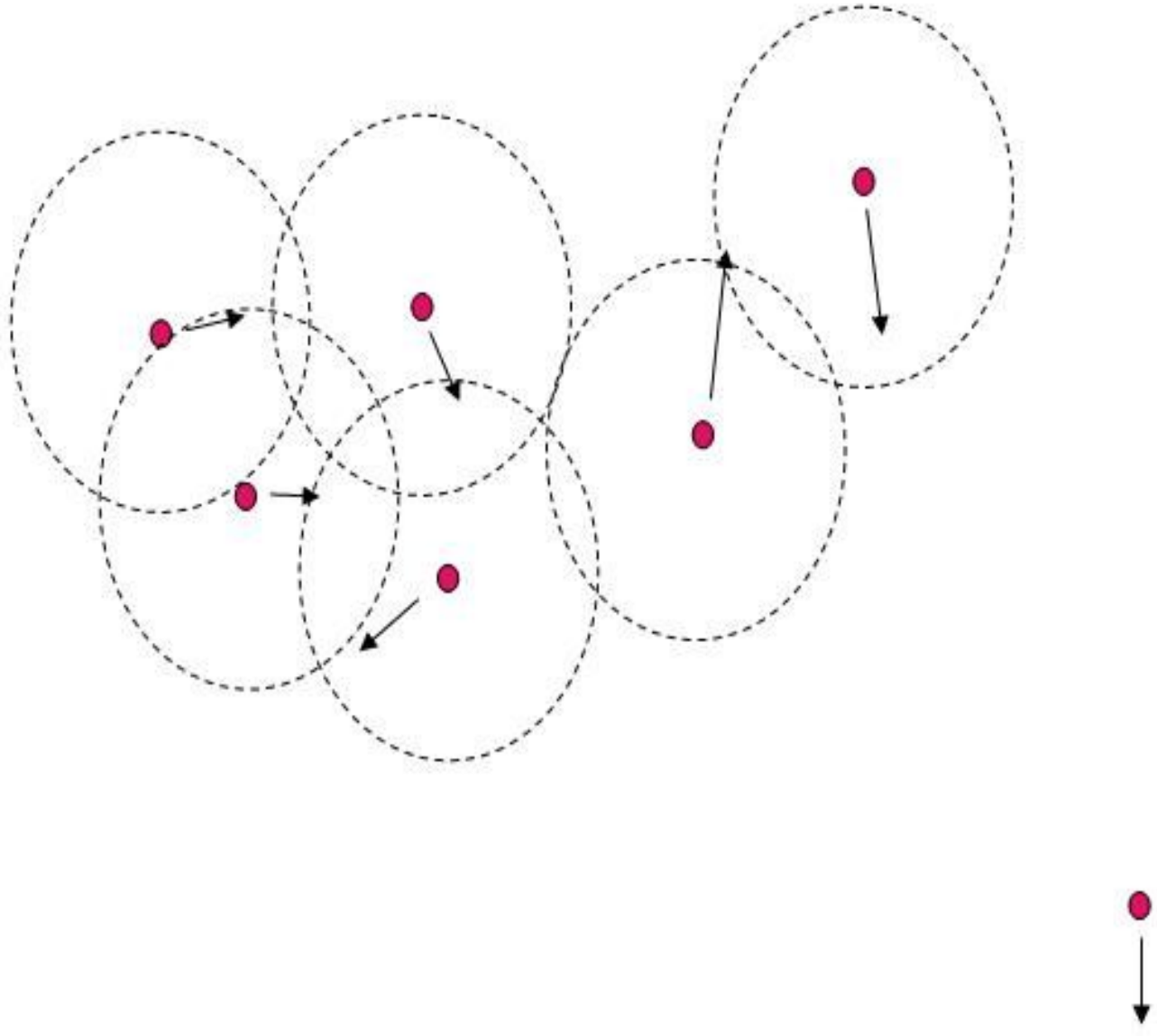
Adding "noise" to the location





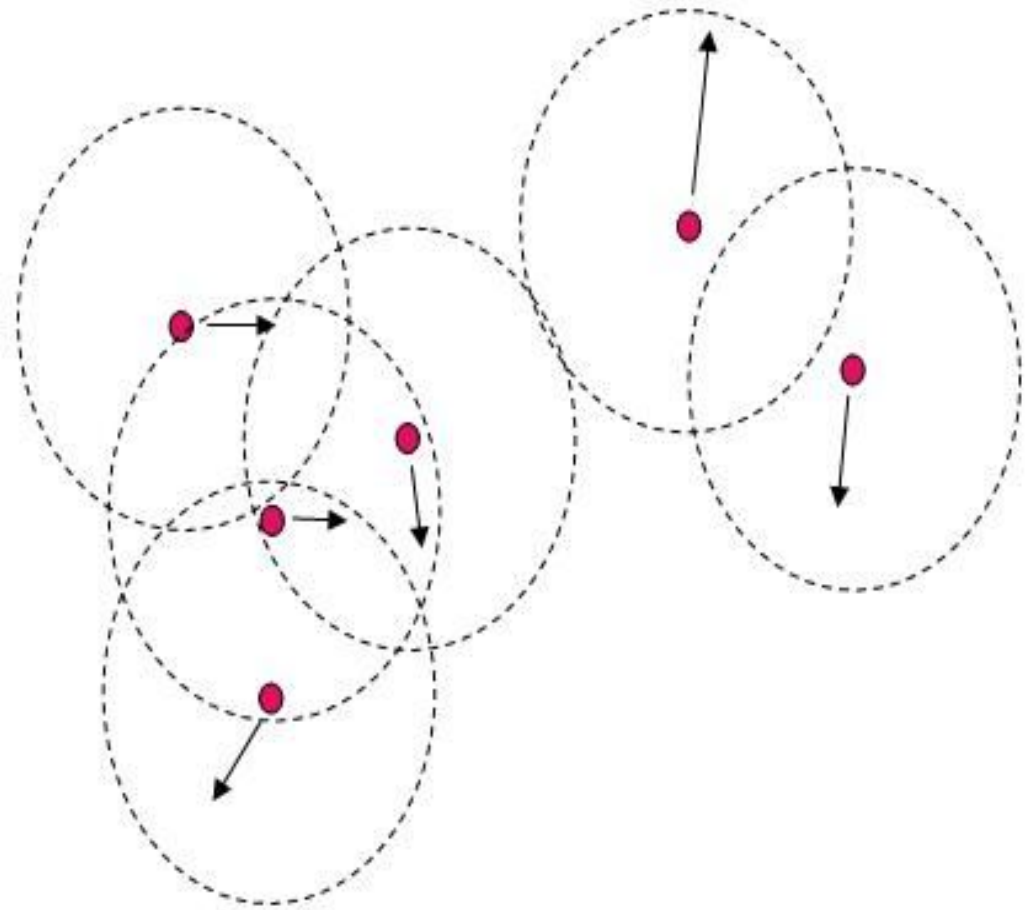
NOKIA

Adding "noise" to the location



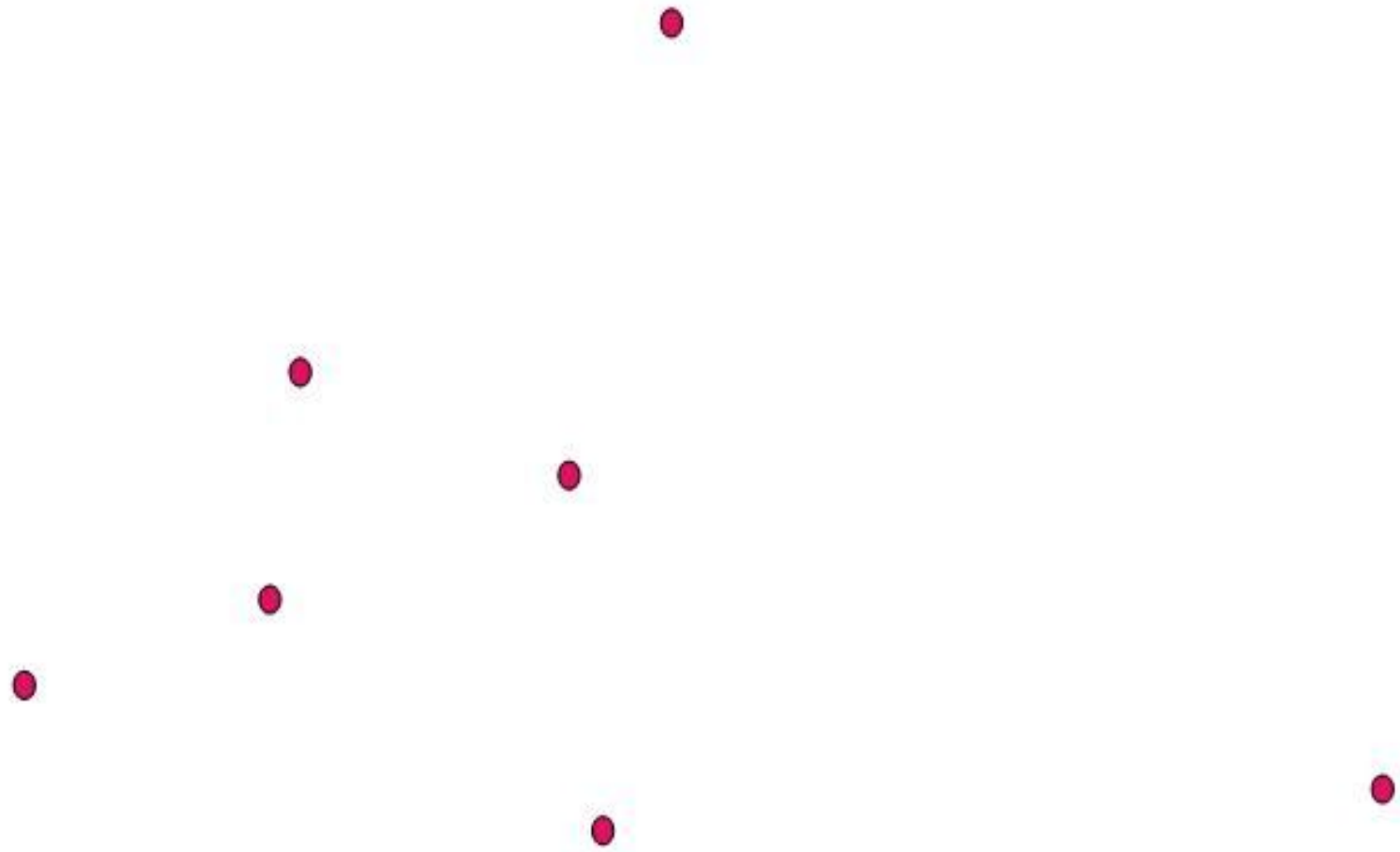
NOKIA

Adding "noise" to the location



Randomized locations

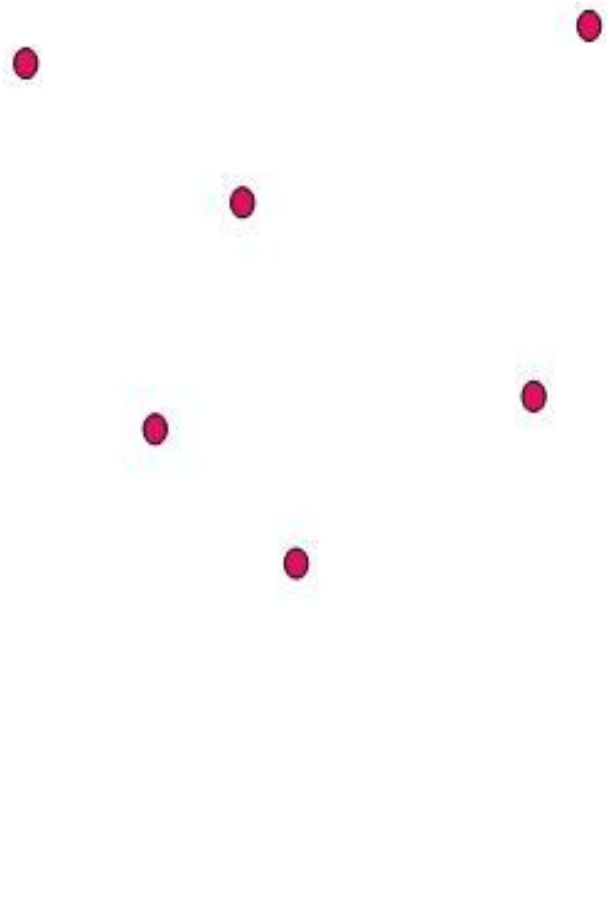
Randomized locations



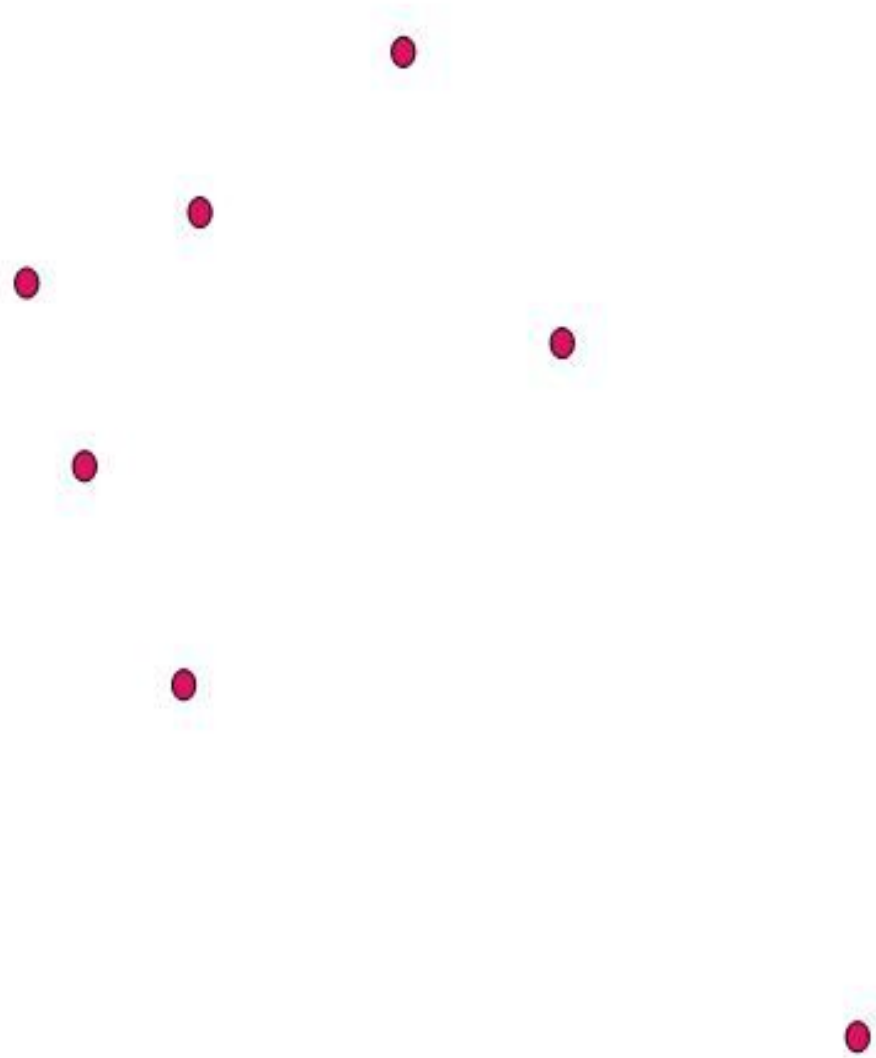
Randomized locations



Randomized locations



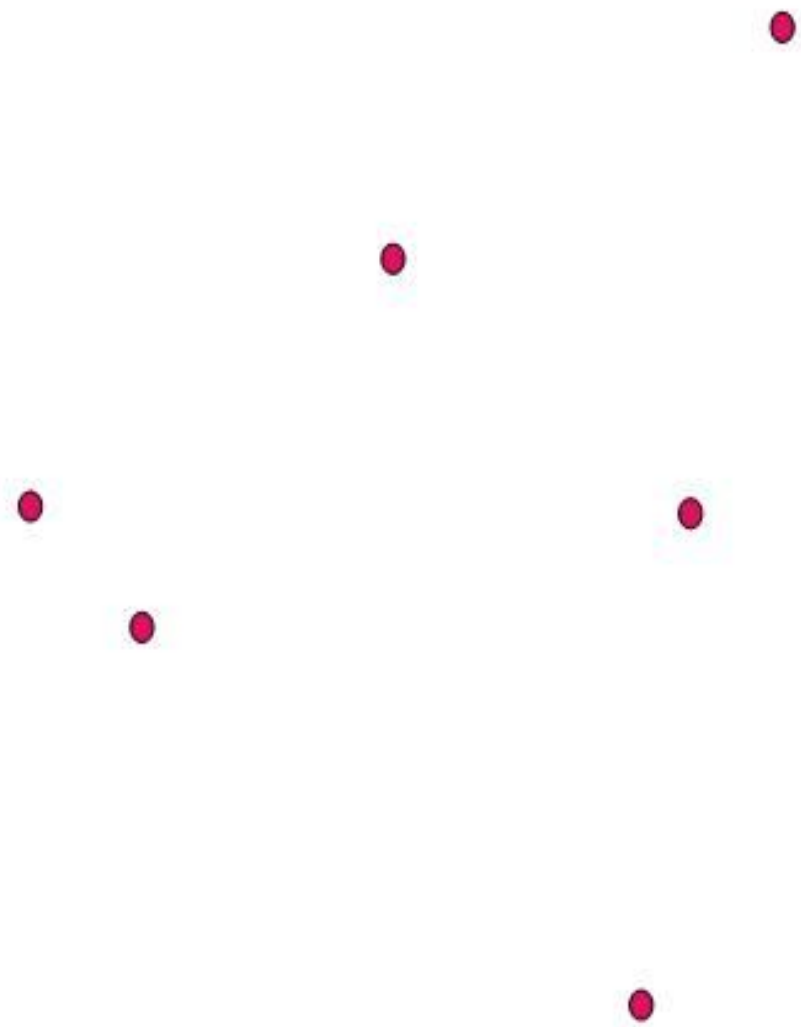
Randomized locations



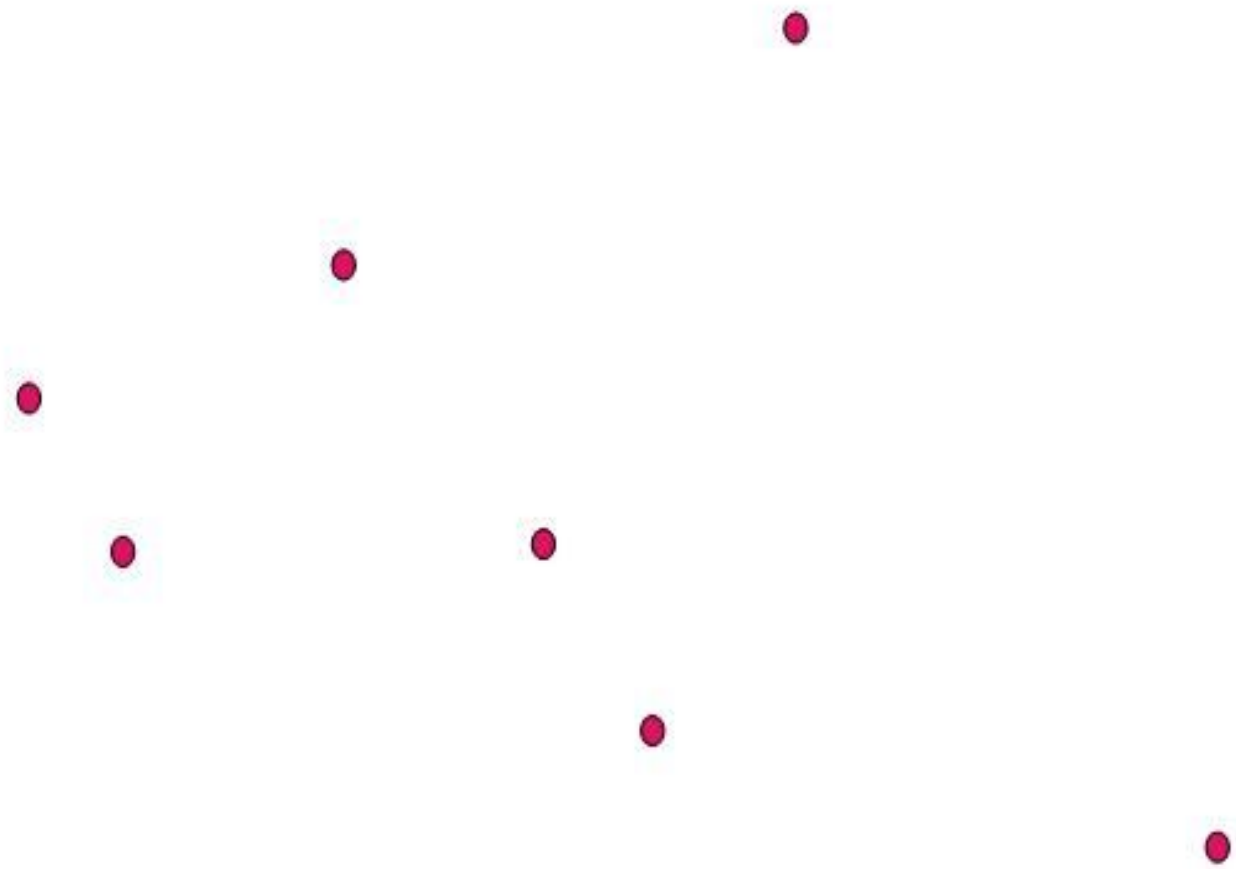
© 2009 Nokia

Original locations

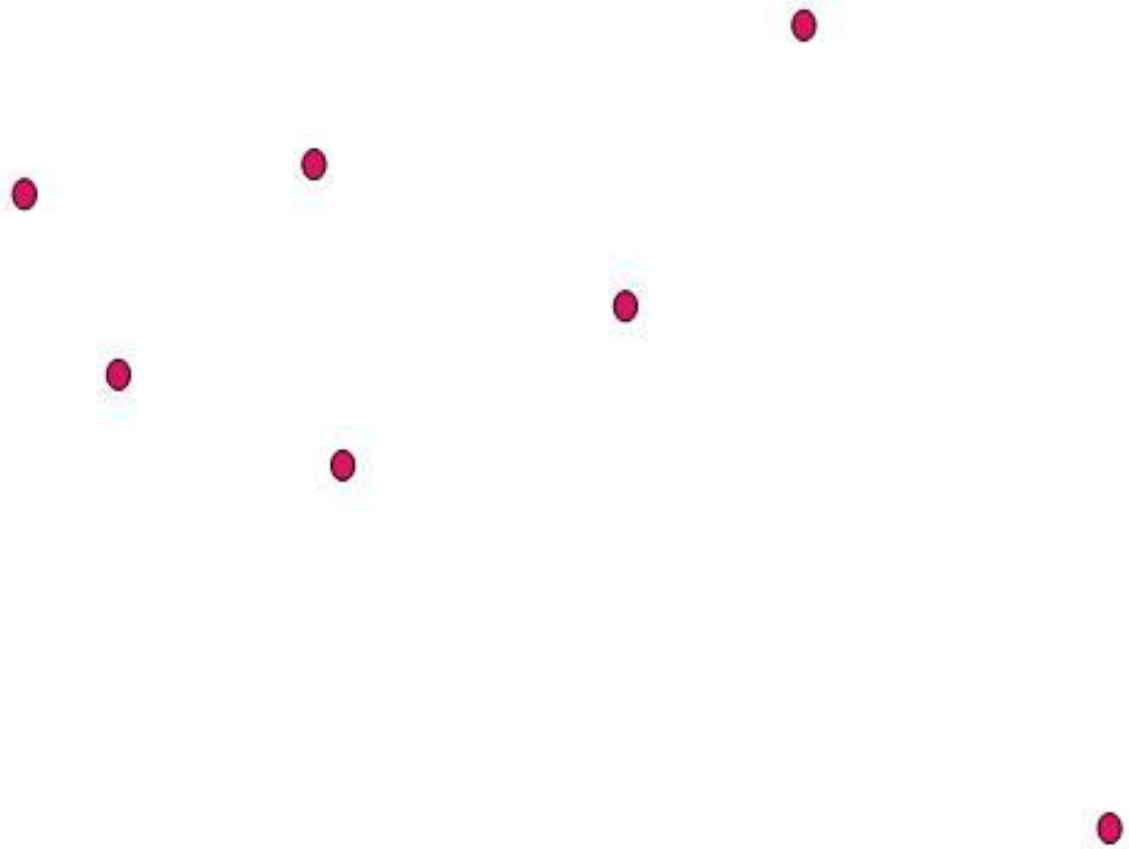
Original locations



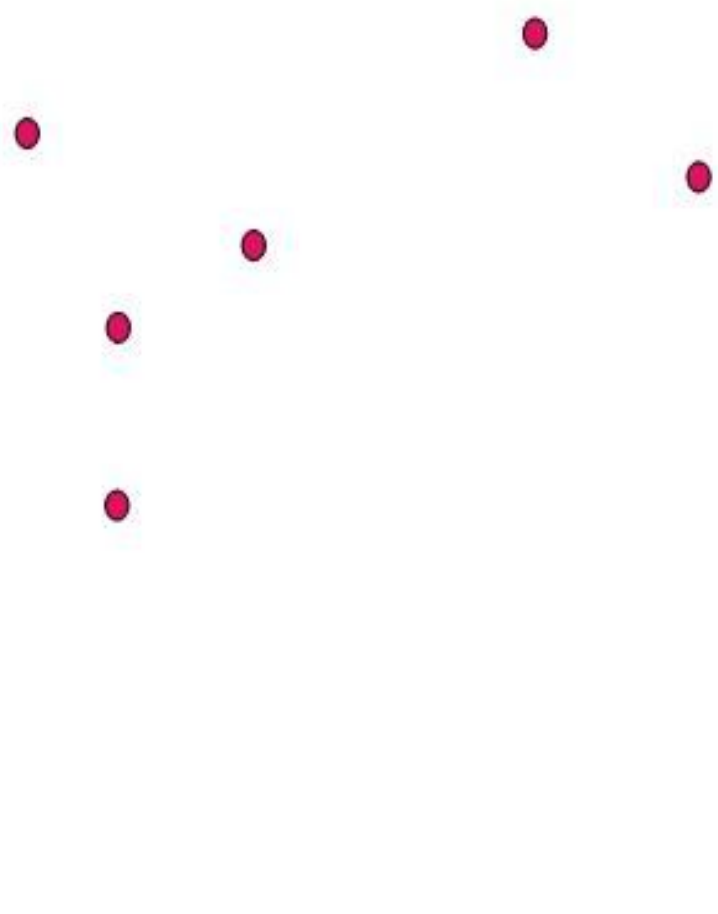
Original locations



Original locations



Original locations



Multiparty computations

- Limit information exchange to minimum
- Applied cryptology

NOKIA

Millionaires' problem

- Origin for theory of *secure multiparty* computations (Yao '82)
- Two millionaires want to find out who is richer *without* revealing anything more about their wealth to the other side
- In principle, anything that can be computed can also be computed without revealing any additional information, e.g. from the intermediate steps
- Setup:
  - Parties $P_1, P_2, \ldots, P_n$ each have an input (X_i for P_i) and they want to compute function $Y = f(X_1, X_2, \ldots, X_n)$
  - During the procedure, nobody learns anything about other parties' input (except what can be learnt from Y alone)
  - In millionaires' case:
    - X_1 is the wealth of the first millionaire
    - X_2 is the wealth of the second millionaire
    - $Y = f(X_1, X_2) = sign(X_1 - X_2)$

NOKIA

Solution to millionaires' problem (sketch)

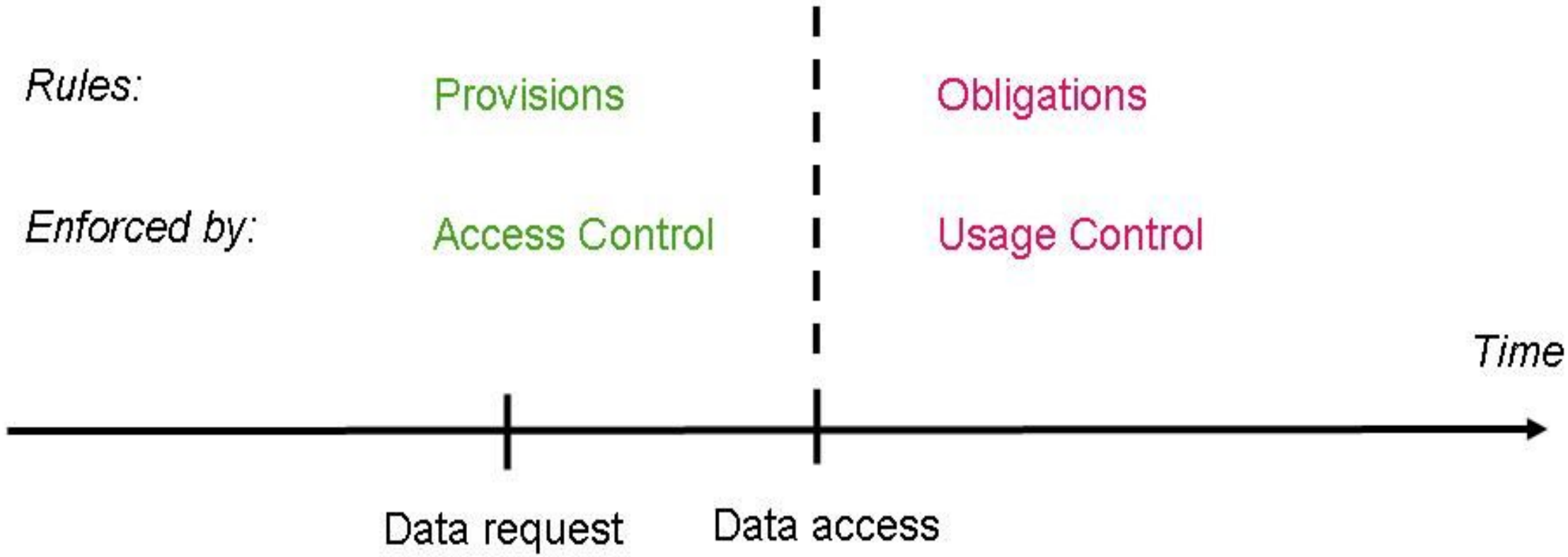
- Setup:
  - Millionaire A (resp. B) has wealth a (resp. b)
  - (both agree that $max(a,b) < n$)
  - A has private key to decryption function d
  - B has public key to encryption function e
- Procedure
  - B chooses *random* x and sends $y = e(x) - b$ to A
  - A chooses *random* p and computes:
    - (for $i = 1, ..., a$): $z_i = d(y + i) \pmod p$
    - (for $i = a+1, ..., n$): $z_i = d(y + i)+1 \pmod p$
  - A sends to B all values $z_1, ... , z_n$
  - B looks only at value z_b:
    - (if $b <= a$): $z_b = d(y+b) = d(e(x)) = x \pmod p$
    - (if $b > a$): $z_b = d(y+b) + 1 = d(e(x)) + 1 = x + 1 \pmod p$

© 2009 Nokia

Usage control

- Control usage of personal data
- Not only access to it

Usage control vs. access control



- Examples of obligations:
  - Credit card details to be deleted after payment received
  - Data about product purchase to be kept until warranty period is over
  - Picture may be viewed maximum five times

© 2009 Nokia

Usage control mechanisms

- Monitoring
  - Only reactive enforcement possible: e.g. penalties if violations detected
  - Relies on monitors working correctly (e.g. trusted computing)
- Run-time control
  - Prevents violations
  - Example: Digital Rights Management (DRM)

Summary

- Mobile devices increasingly *sensing* their (and user's) *context*
- → new kind of *context-aware services*
- → these services tend to be *privacy-sensitive*
- Tricky interplay between *privacy – security – trust - identity*
- Technology helps in *enhancing* privacy but a lot depends on policies, laws etc.
- Threats against identity privacy in all layers, from *physical layer* to *application layer*
- Mechanisms to enhance privacy:
  - Various ways to *anonymise identities* and *data*
  - Minimize the need for private data exchange – *secure multiparty computations*
  - Control the *usage* of data – also the future use

© 2009 Nokia