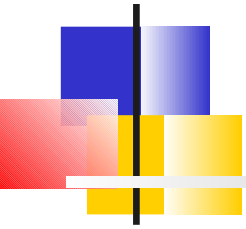
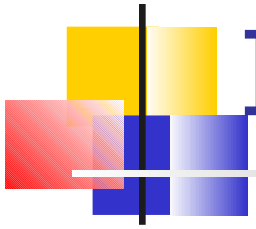


Privacy in Vehicular Networks and Location-Based Services

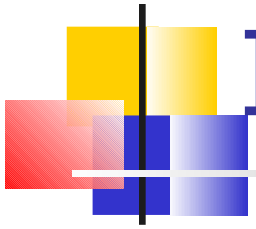
Francesc Sebé Feixas
CRISES research group

Rovira i Virgili University of Tarragona
June 2007



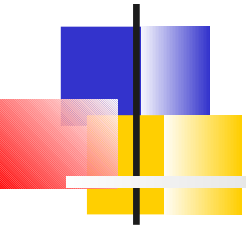
Index

- Introduction
- Privacy in vehicular networks
- Privacy in location-based services



Introduction

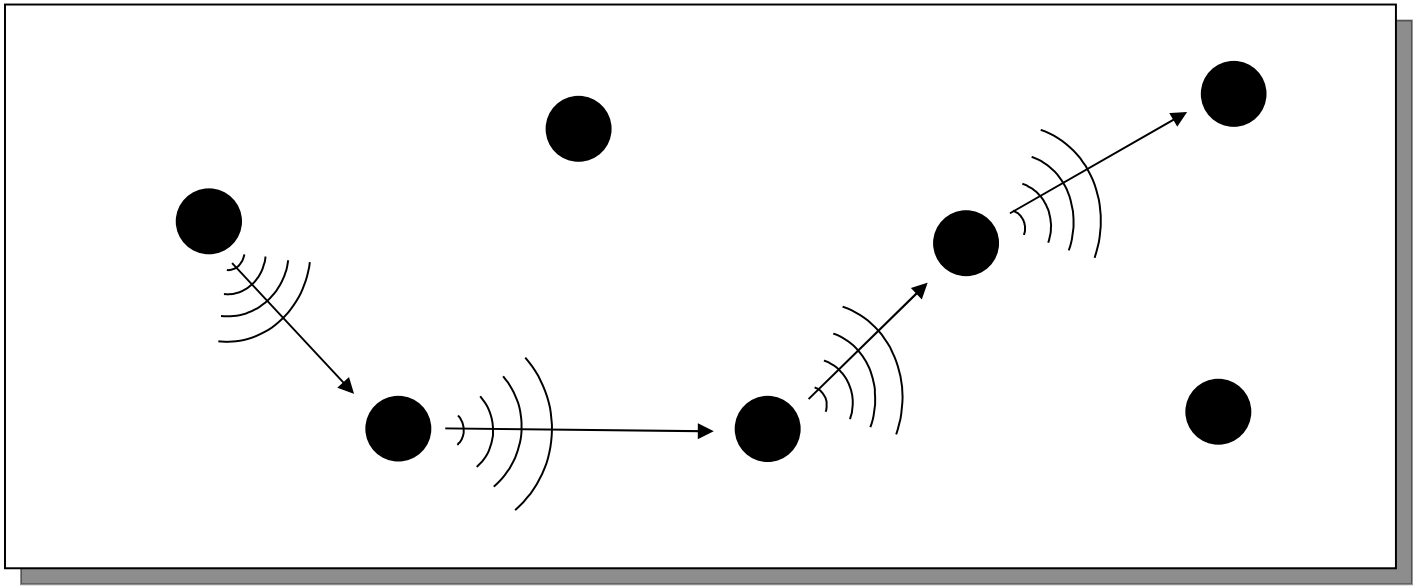
- Location privacy
  - "Ability to prevent other parties from learning one's current or past position"
- Not a problem in GPS
  - Passive receiver
- To consider in
  - Mobile telephony
  - Ubiquitous computing
  - Vehicular networks

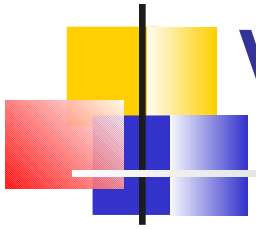


Privacy in Vehicular Networks

MANET

- MANET (*Mobile Ad-hoc Network*)
  - Network formed by self-organized mobile nodes without infrastructure



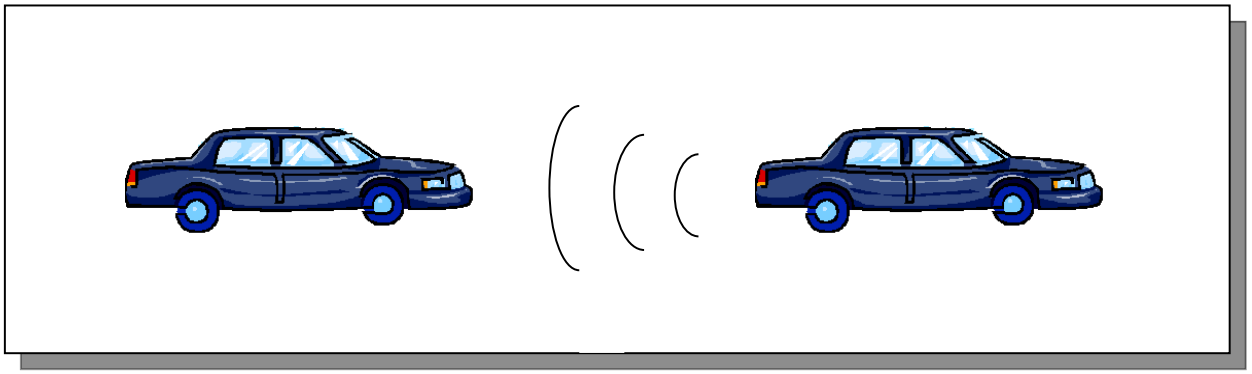


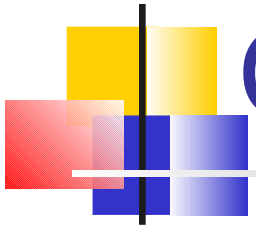
VANET

- VANET (*Vehicular Ad-hoc Network*)
  - Mobile nodes placed in vehicles
  - Fix nodes located on traffic infrastructure (signals, semaphores, etc)

Communication types

- "Alert" messages
  - Warn about dangerous actions
    - Braking



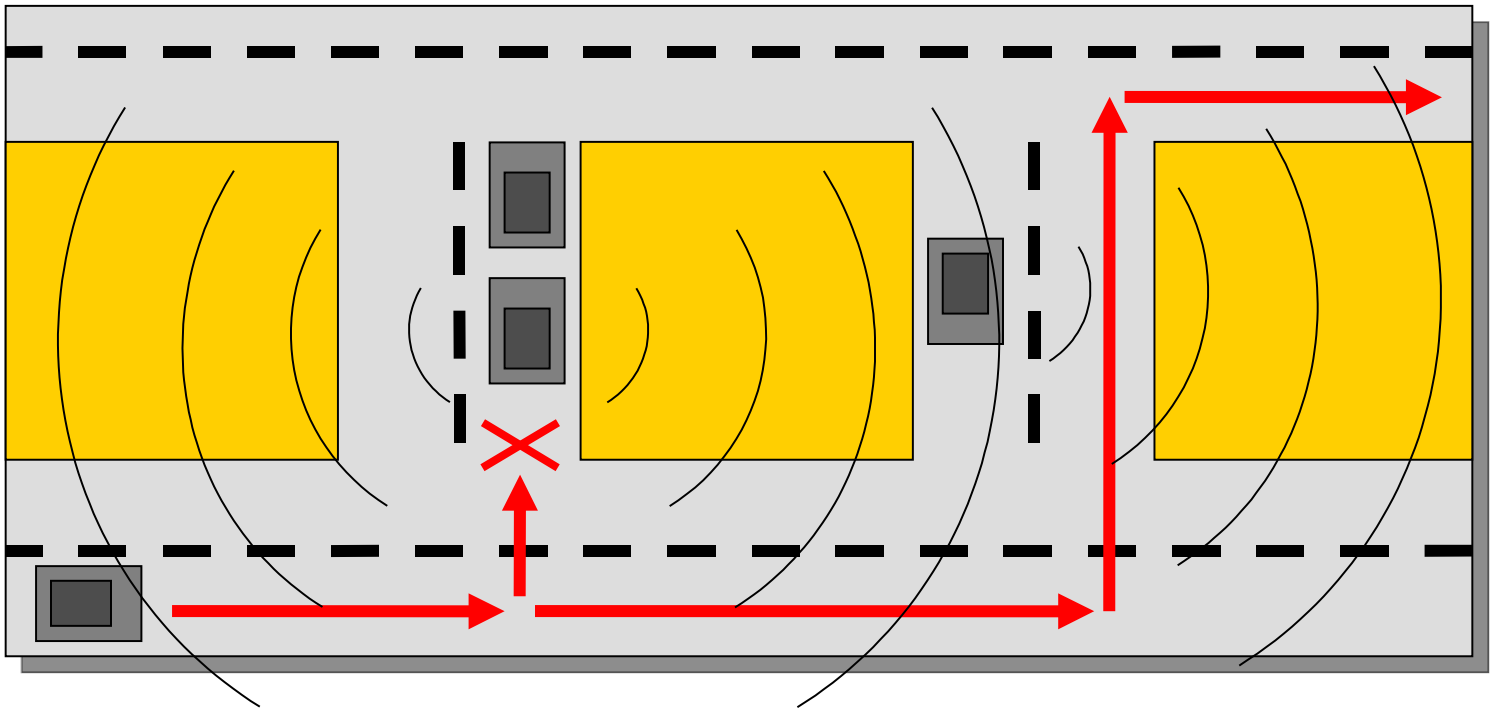


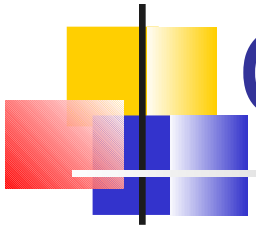
Communication types

- "Alert" messages
- Warn about dangerous actions
  - Braking
  - Limited dissemination
  - Hard real time requirements
  - Accidents prevention

Communication types

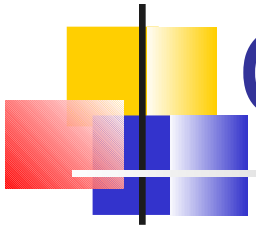
- "Announcement" messages
  - Inform about facts that disrupt the traffic





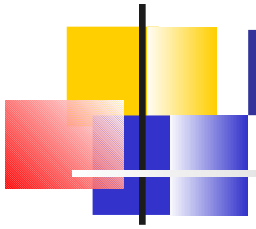
Communication types

- "Announcement" messages
  - Inform about facts that disrupt the traffic
    - Traffic jams, accidents
  - Wide dissemination
  - Soft real time requirements
  - They permit to choose alternative routes to avoid the troubled points



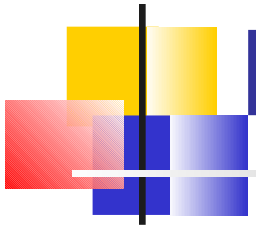
Communication types

- TCP/IP communications
  - Internet access
  - Instantaneous messages among vehicles



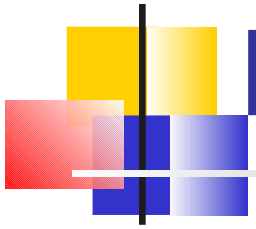
Privacy in VANET

- Information about driving habits is highly confidential
  - Frequented places
  - Timetables
  - Personality
  - Offenses



Routing in VANET

- The nodes of a VANET are very dynamic
  - Constant change of location
  - Arrival and departure of nodes
- Location-based routing
  - ‘Hello beacon’ messages $\rightarrow$ Each node periodically indicates its position

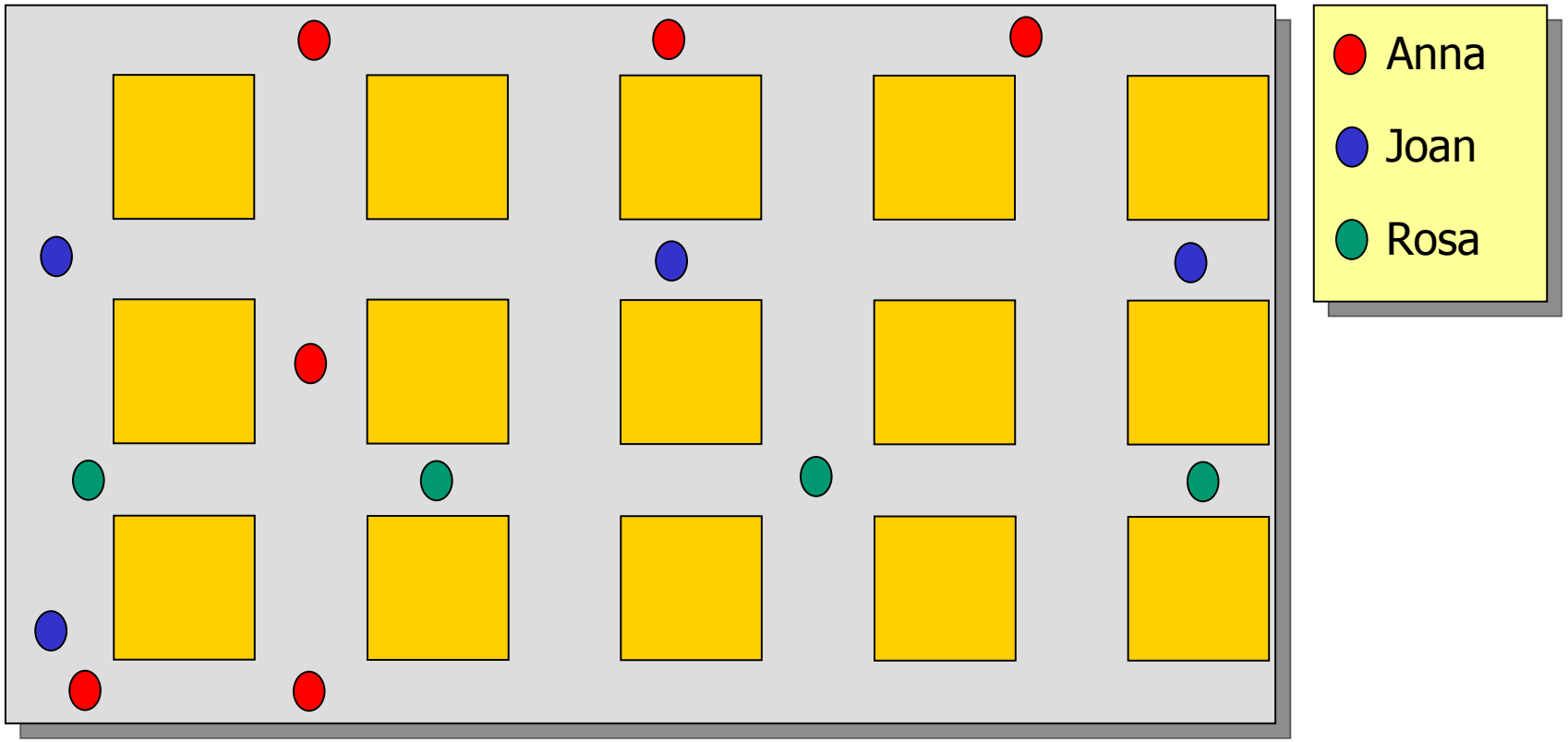


Privacy in VANET

- Anonimity
  - The identity of a node is not known
  - Use of pseudonyms
- Unlinkability
  - Different interactions can't be linked
  - Requires periodic change of addresses, identifiers, etc.

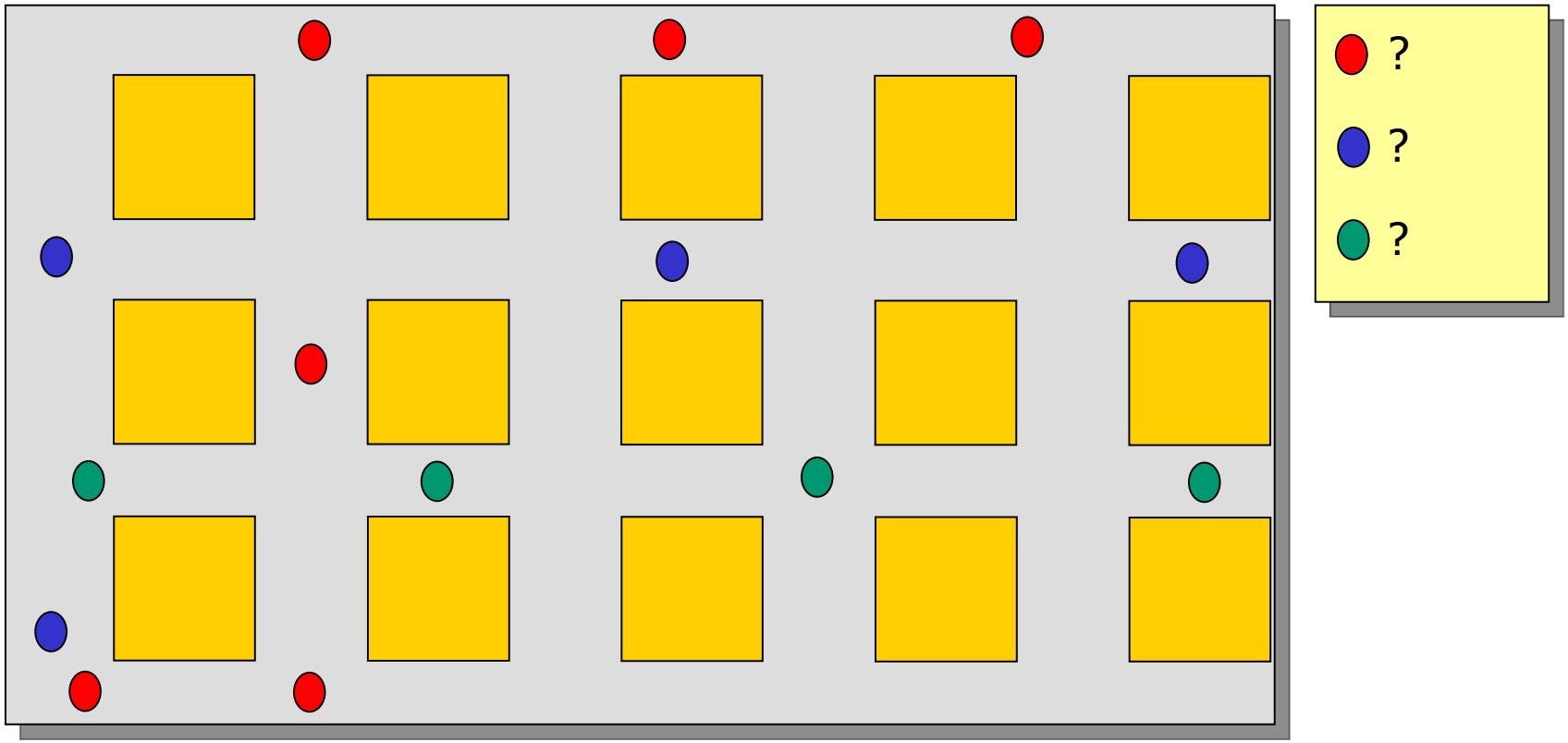
Privacy in VANET

- VANET without privacy



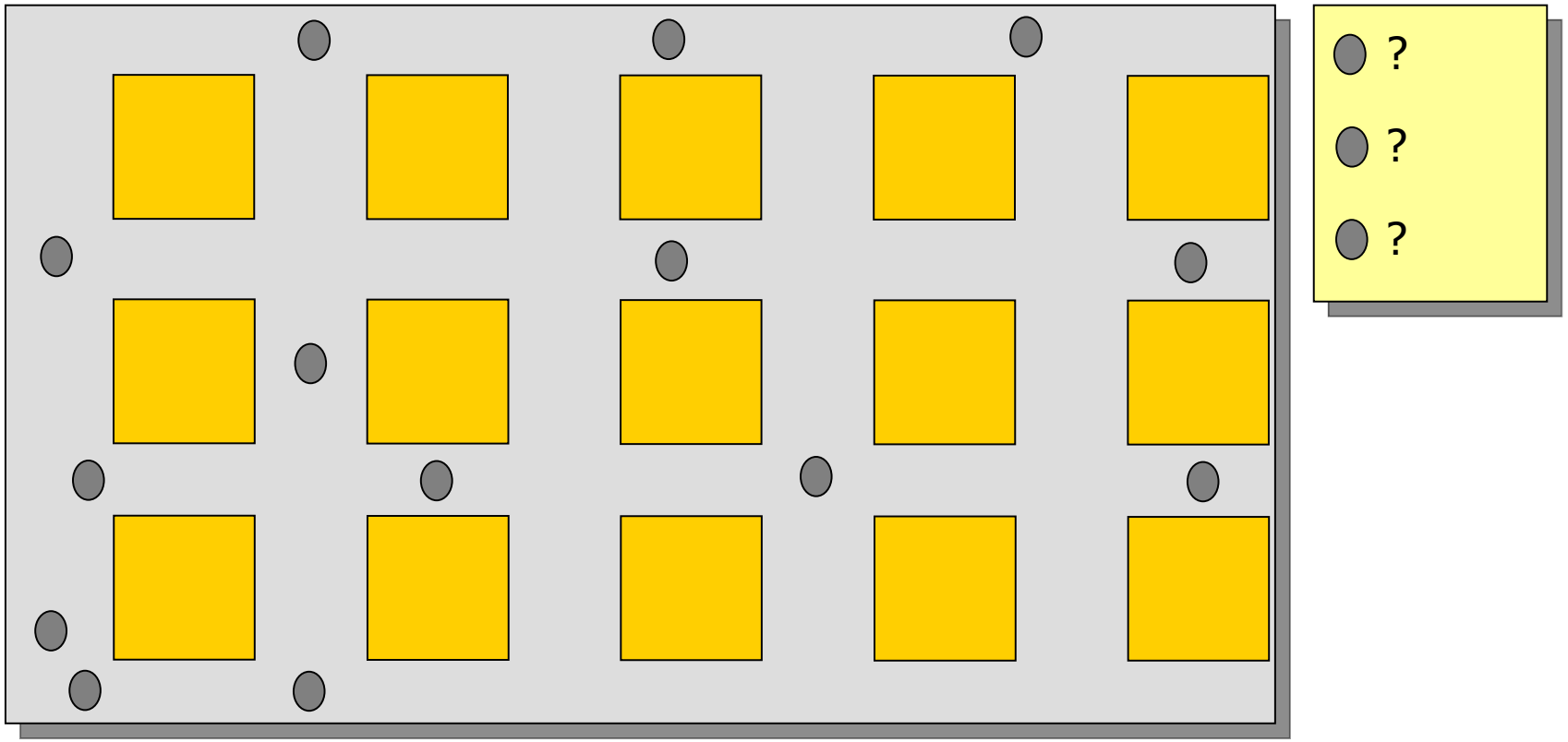
Privacy in VANET

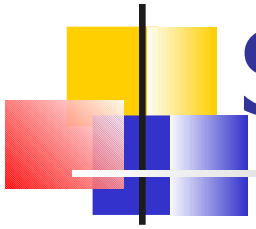
- Anonimity (permits tracking)



Privacy in VANET

- Anonimity and unlinkability



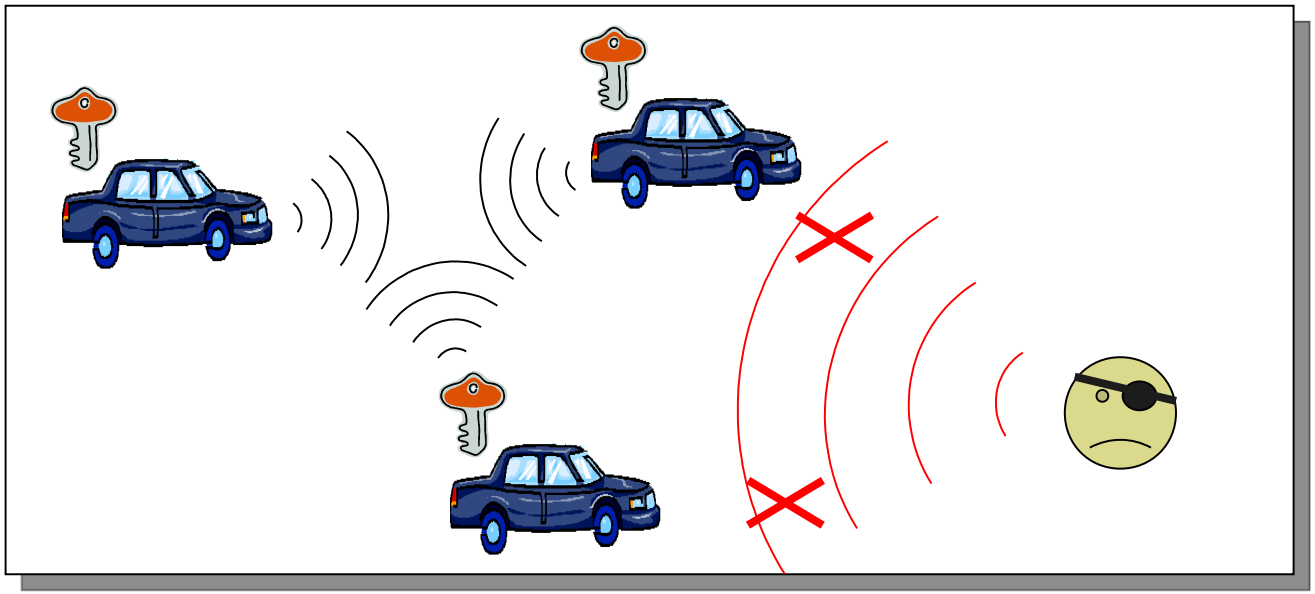


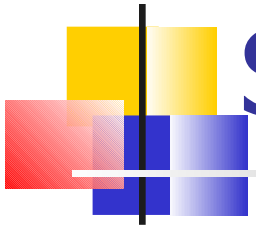
Security in VANET

- Security is basic in a VANET
- Malicious messages can cause
  - Accidents
  - Traffic complications

Security in VANET

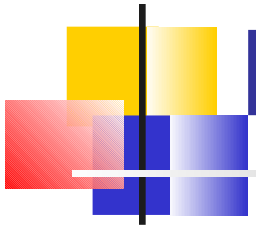
- External attackers
  - Prevention using cryptography
    - Authorized nodes know a secret key





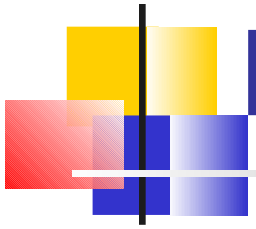
Security in VANET

- Authorized nodes add an authentication code to messages
  - The code demonstrates knowledge on the secret key
  - Verifiable from a public key certificate
  - Allows tracking
  - Interchangeable pseudonyms
    - Costly management



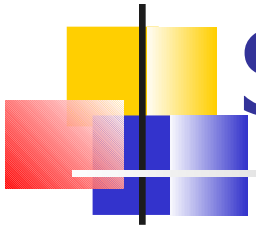
Privacy vs Security

- Anonimity
  - It is not known who has carried out a certain action
  - How to take measures against users who have performed in a fraudulent way?
    - Internal attackers
  - Revocable anonimity
    - TTP can revoke anonimity



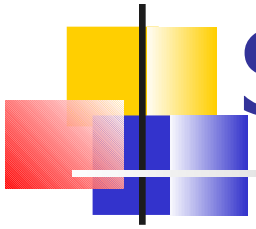
Privacy vs Security

- A priori measures
  - Prevent authorized nodes from sending fraudulent information
  - A message is considered valid if it has been supported by a minimum number of vehicles



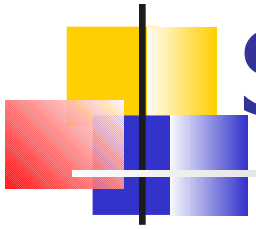
Standards

- IEEE 1609
  - United States
    - Funded by the Dept. of Transport
  - WAVE system
    - *Wireless Access in Vehicular Environments*
  - Composed of four standards
    - One of them is still being developed
    - Vehicles equipped by default in 2011



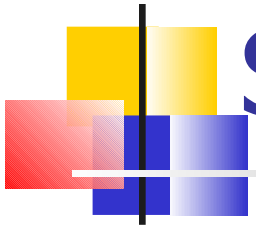
Standards

- Security in IEEE 1609 (1609.2)
  - Public key + Digital certificates
  - Semantically secure cryptography
- Privacy
  - They mention it is necessary to avoid tracking by MAC address
    - Through frequent change
  - They mention the need for a mechanism to send authenticated messages in an anonymous way
  - Privacy issues are left for future work



Standards

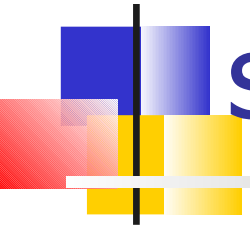
- C2C-CC (*Car to Car – Communication Consortium)*
  - European area
  - Consortium of vehicle manufacturers and suppliers of electronic components
  - Under development

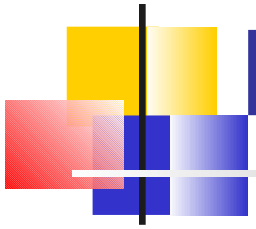


Standards

- Security requirements C2C-CC
  - Correct and reliable information
  - Robustness (DoS)
  - Privacy
- Privacy (open topic)
  - Anonymous certificates (blind signatures)
  - Short time certificates
  - Zero-knowledge proofs

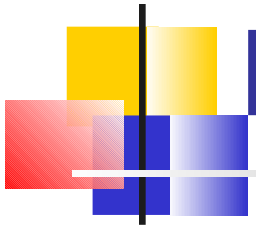
Privacy in location-based services





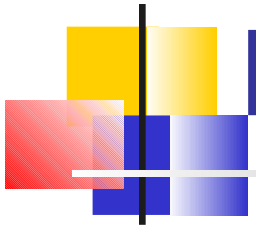
LBS introduction

- *LBS=Location-Based Services*
- User receives information depending on its location
  - Emergency assistance
  - Touristic information: hotels, monuments, restaurants...
  - Itineraries



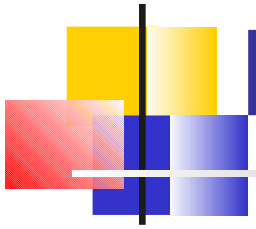
Privacy in LBS

- Service provider learns the location from user queries
- He will be able to infer
  - Frequented places
  - Timetables
  - Habits, hobbies



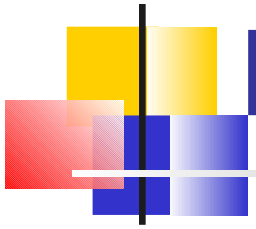
Privacy in LBS

- Applications where it is necesari to reveal identity
  - Subscription services
  - I don't want to reveal **where** I am
  - I distort my location
  - Tradeoff between privacy and the quality of the received information



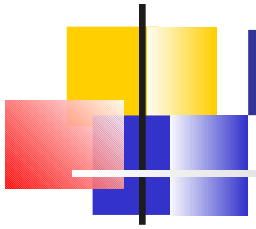
Privacy in LBS

- Applications that provide anonymity to the user
  - It is not known **who** I am
  - I can reveal my location



Privacy in LBS

- How to achieve anonymity
  - Without TTP
    - Technically difficult (addresses, identifiers, keys)
    - Situation in VANET
  - With TTP
    - User sends the query to a trusted anonymizer

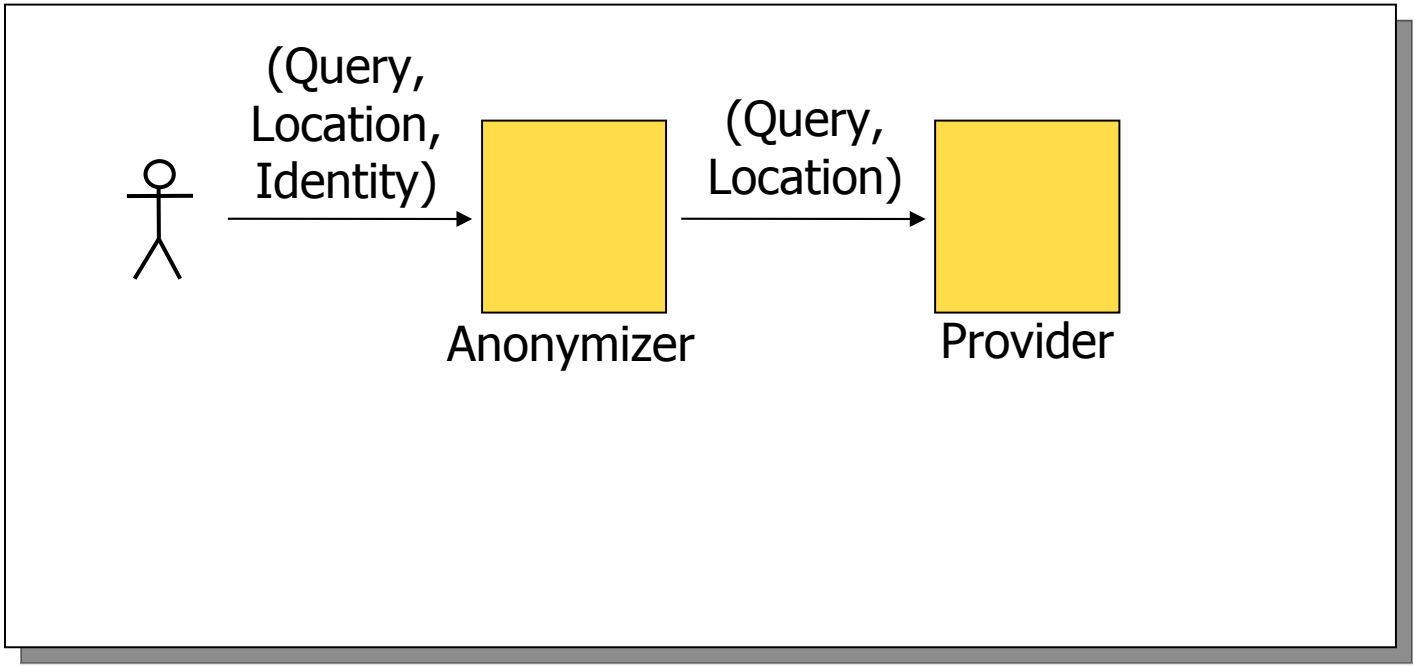


Privacy in LBS

- Anonymity with TTP
  - The anonymizer receives the query
  - Eliminates the identifier
  - Possibly distorts the position
  - Sends the query to the service provider

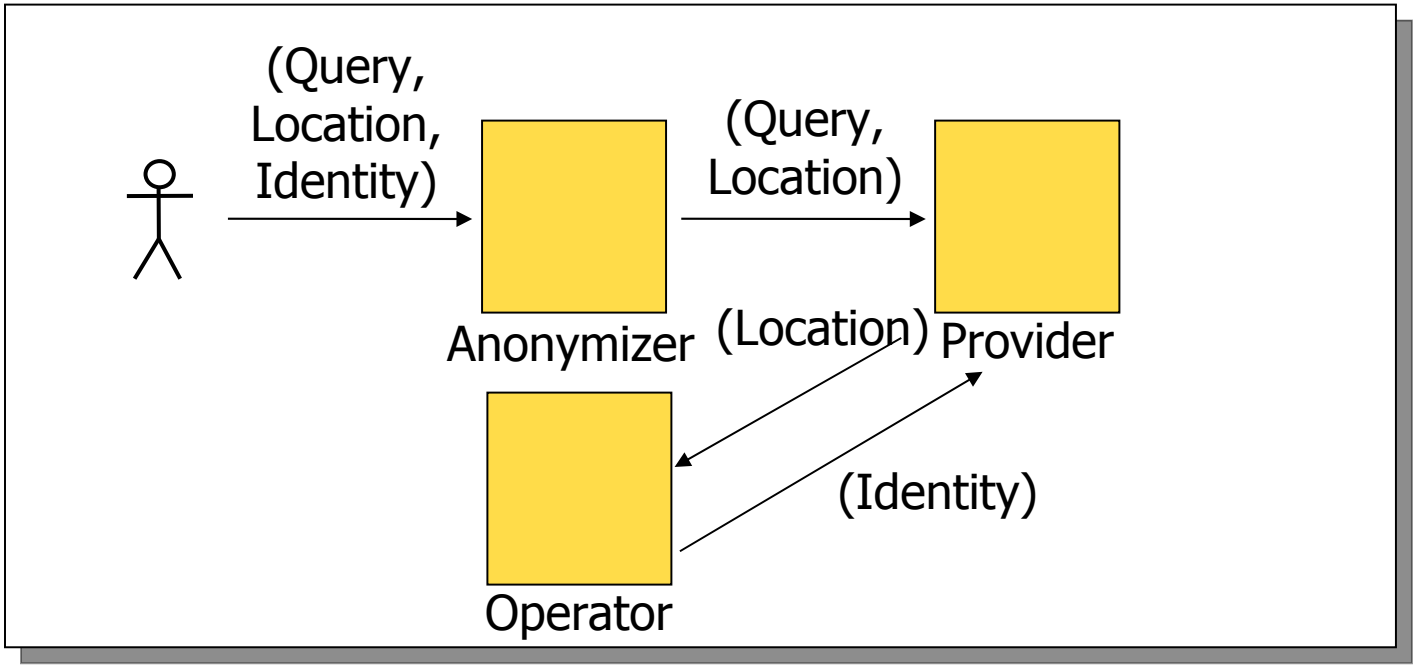
Privacy in LBS

- Why is it necessary that the anonymizer distorts the location?



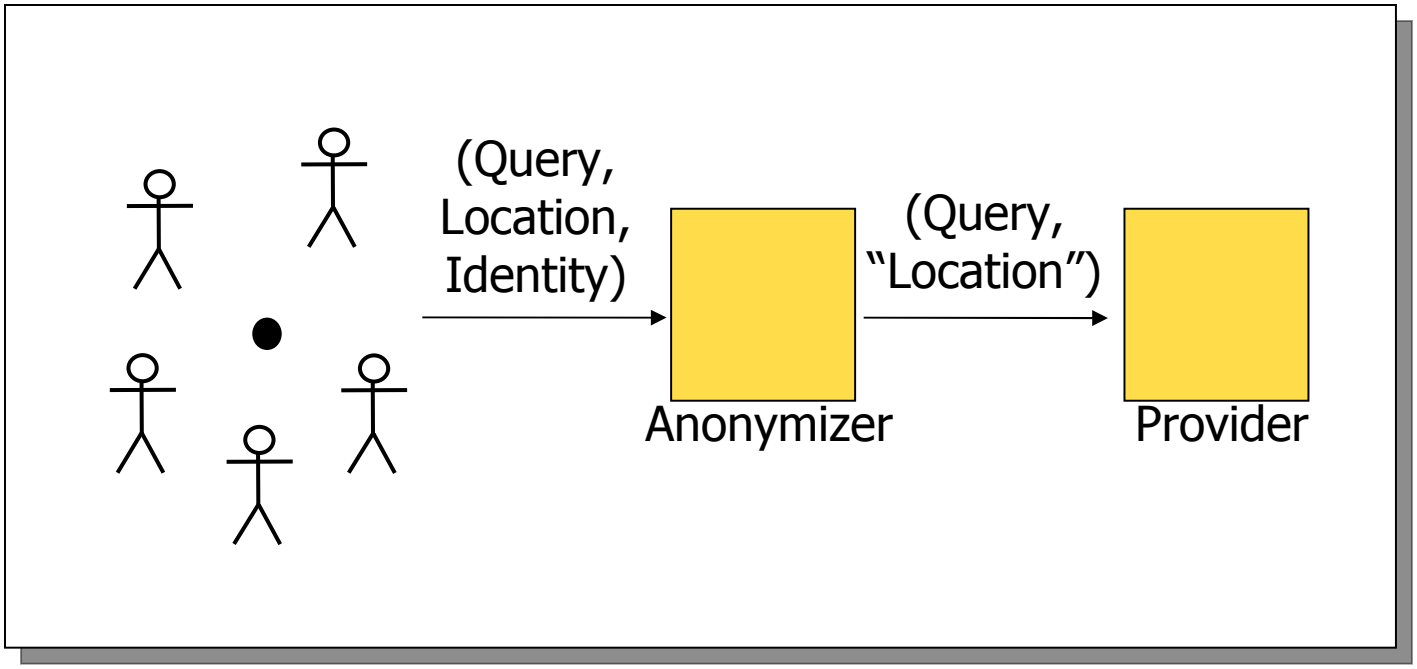
Privacy in LBS

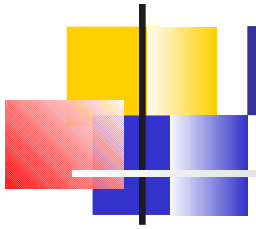
- Why is it necessary that the anonymizer distorts the location?



Privacy in LBS

- k-Anonymity
  - "Location" assignable to at least *k* users



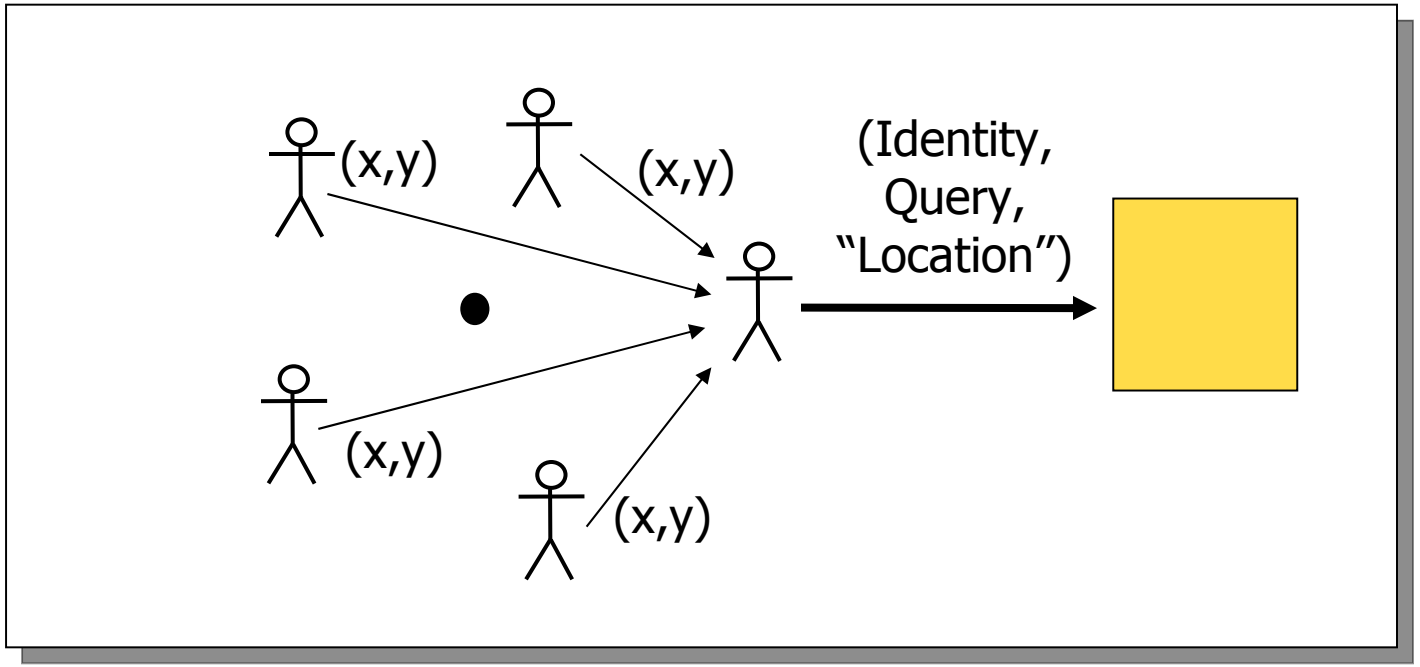


k-Anonymity

- What happens if we don't trust the anonymizer?
  - Distributed system to mask the location
  - Users calculate the “location” in a collaborative way

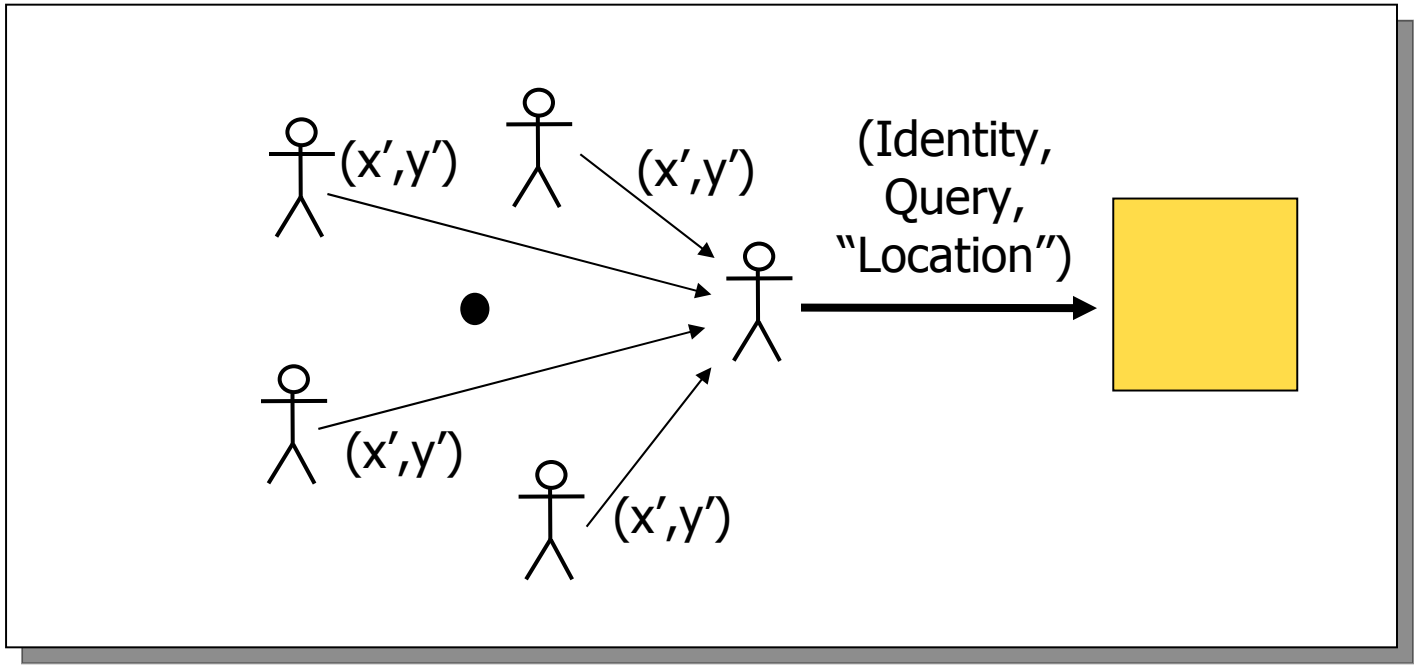
k-Anonymity

- Users trust each others
  - They share location



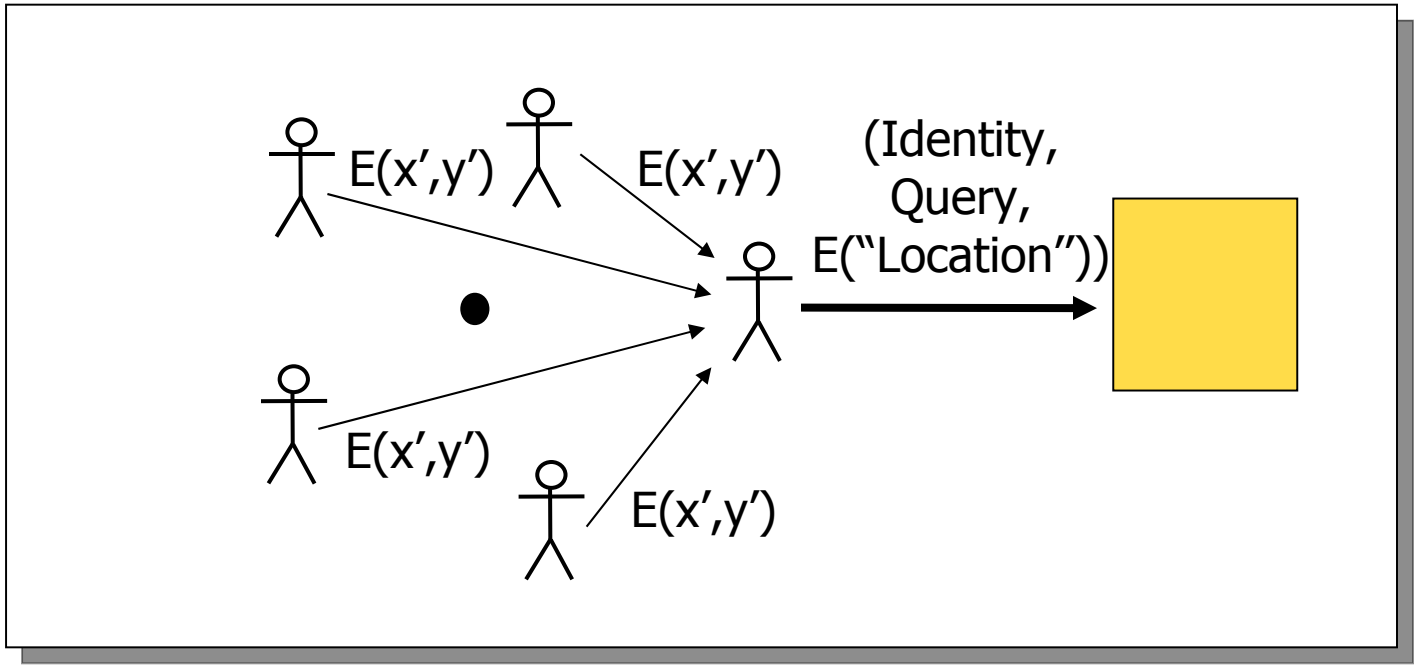
k-Anonymity

- We reduce confidence
  - Share location with noise $(x,y)+(N^x,N^y)$



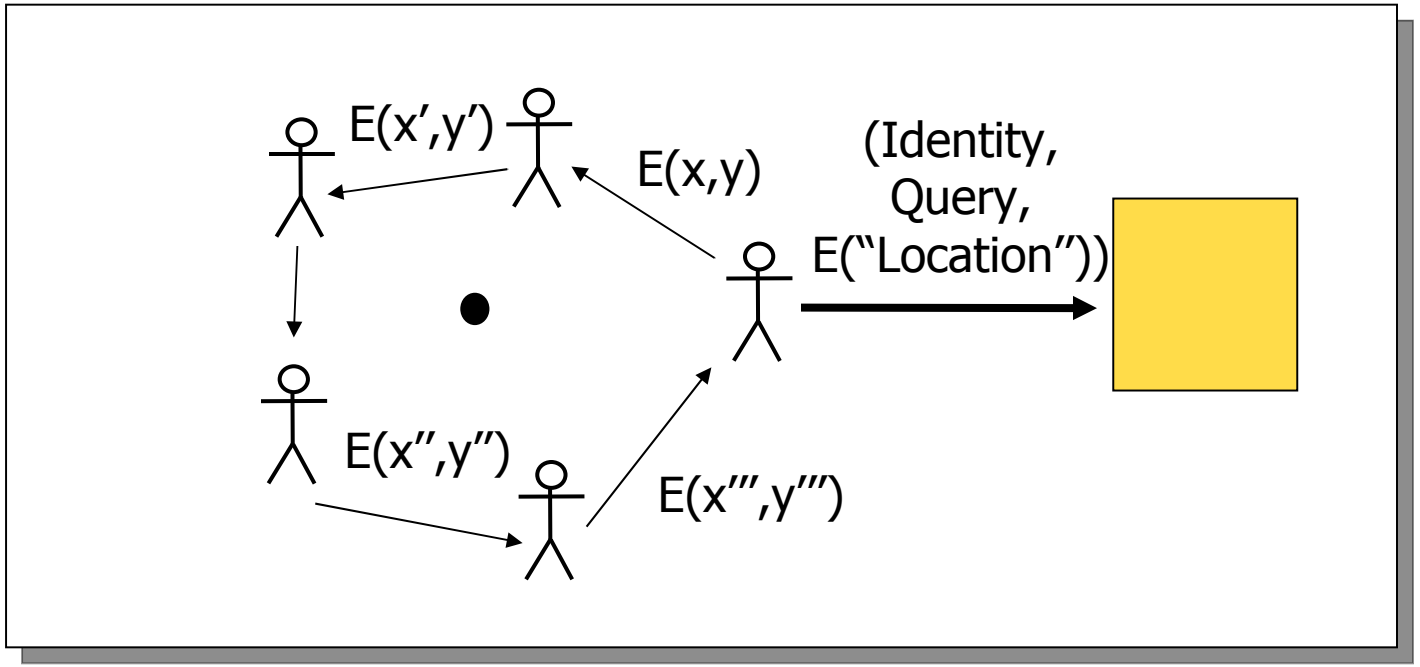
k-Anonymity

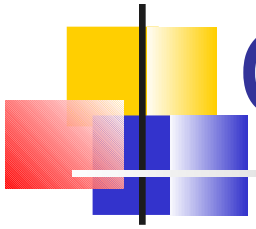
- We reduce confidence
  - Use of privacy homomorphism



k-Anonymity

- We reduce confidence
  - Homomorphism + Paths





Conclusions

- Vehicular networks and location-based services
  - Reveal information about user's location
  - Very confidential information
  - Measures have to be taken
  - Open research topic