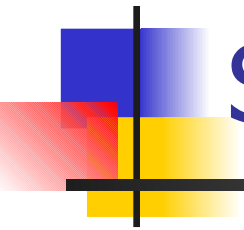
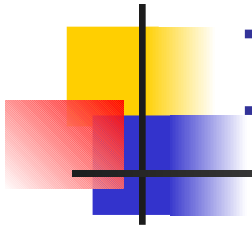


Privadesa en Xarxes Vehiculars i Serveis Basats en la Localització

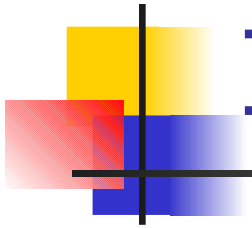
Francesc Sebé Feixas
Grup de recerca CRISES

Universitat Rovira i Virgili
Juny 2007



Index

- Introducció
- Privadesa en xarxes vehiculars
- Privadesa en serveis basats en la localització



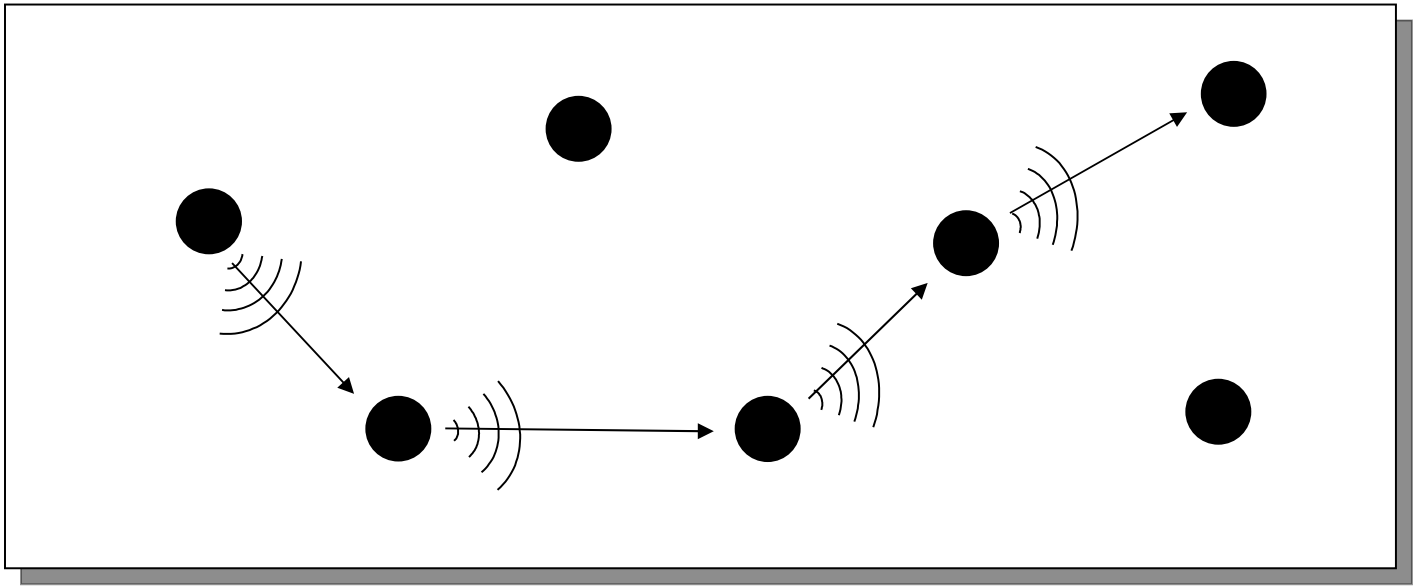
Introducció

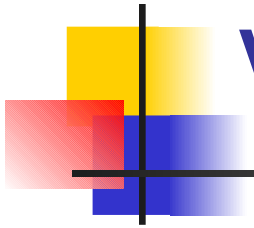
- Privadesa de localització
  - "Habilitat per evitar que altres coneguin la nostra posició actual o passada"
- No és problema en GPS
  - Receptor passiu
- A considerar en
  - Telefonia mòbil
  - Computació ubiqua
  - Xarxes vehiculars

Privadesa en xarxes vehiculars

MANET

- MANET (*Mobile Ad-hoc Network*)
  - Xarxa formada per nodes mòbils auto-organizats sense infraestructura



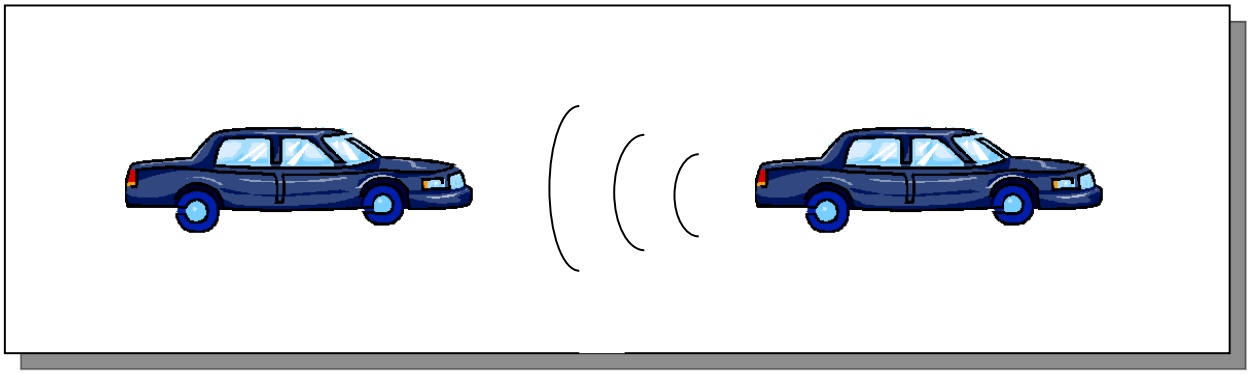


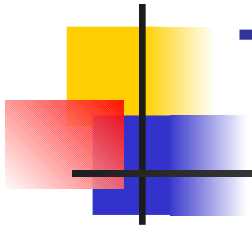
VANET

- VANET (*Vehicular Ad-hoc Network*)
  - Nodes mòbils situats en vehicles
  - Nodes fixes sobre infraestructura de trànsit (senyals, semàfors, etc)

Tipus de comunicacions

- Missatges “d’alerta”
  - Adverteixen d’accions perilloses
    - Frenades



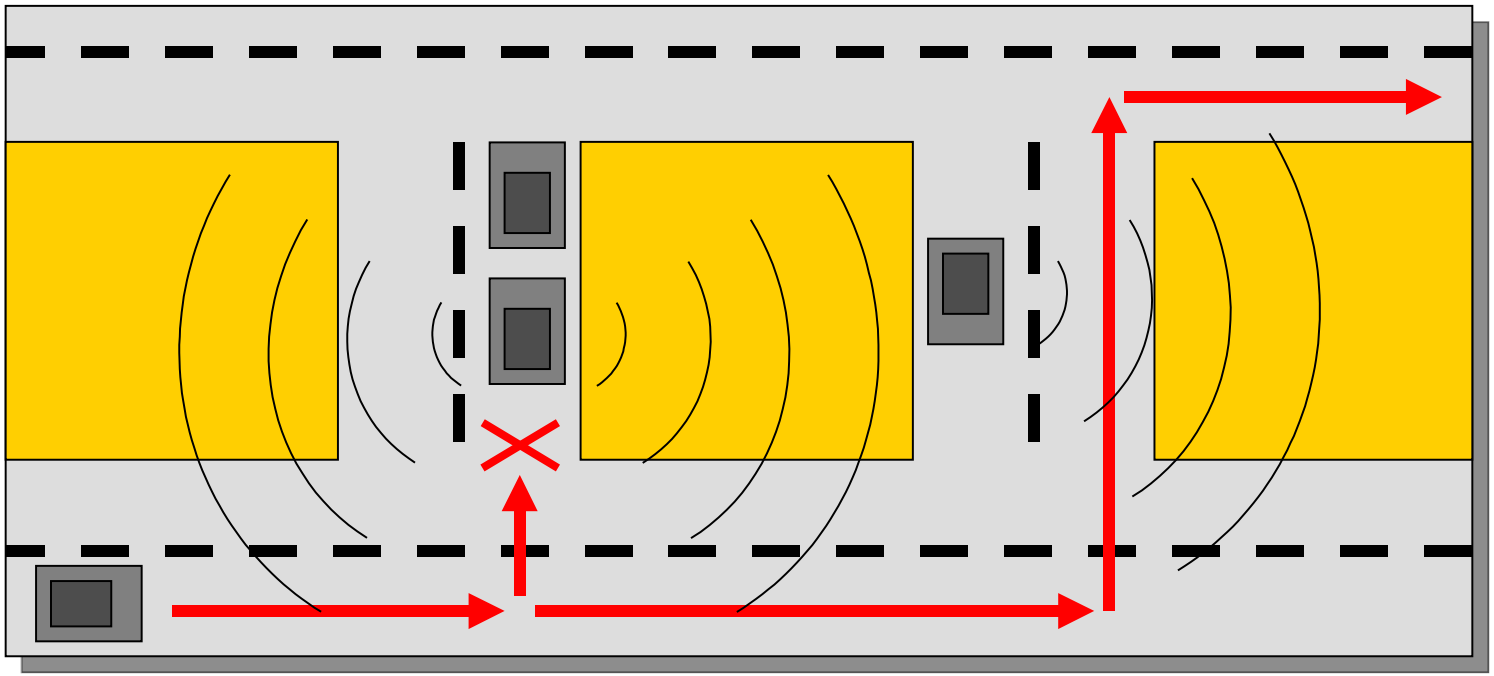


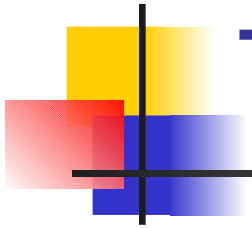
Tipus de comunicacions

- Missatges “d’alerta”
  - Adverteixen d’accions perilloses
    - Frenades
  - Disseminació limitada
  - Requisits durs de temps real
  - Prevenció d’accidents

Tipus de comunicacions

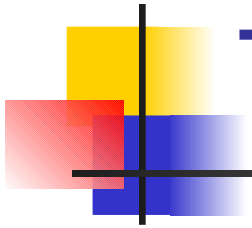
- Missatges “d’anunci”
  - Informen sobre fets que entorpeixen el trànsit





Tipus de comunicacions

- Missatges “d’anunci”
  - Informen sobre fets que entorpeixen el trànsit
    - Embussos, accidents
  - Disseminació àmplia
  - Requisits de temps real poc estrictes
  - Permeten l’elecció de rutes alternatives per evitar els punts conflictius



Tipus de comunicacions

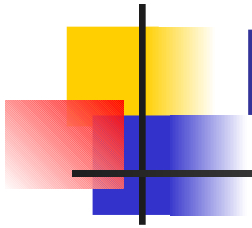
- Comunicacions TCP/IP
  - Accés a Internet
  - Missatgeria instantània entre vehicles

Privadesa en VANET

- La informació sobre els hàbits de conducció és molt confidencial
  - Llocs freqüentats
  - Horaris
  - Personalitat
  - Infraccions

Encaminament en VANET

- Els nodes d'una VANET són molt dinàmics
  - Canvi constant de localització
  - Arribada i sortida de nodes
- Encaminament basat en posició
  - Missatges 'hello beacon' $\rightarrow$ De forma periòdica cada node indica la seva posició

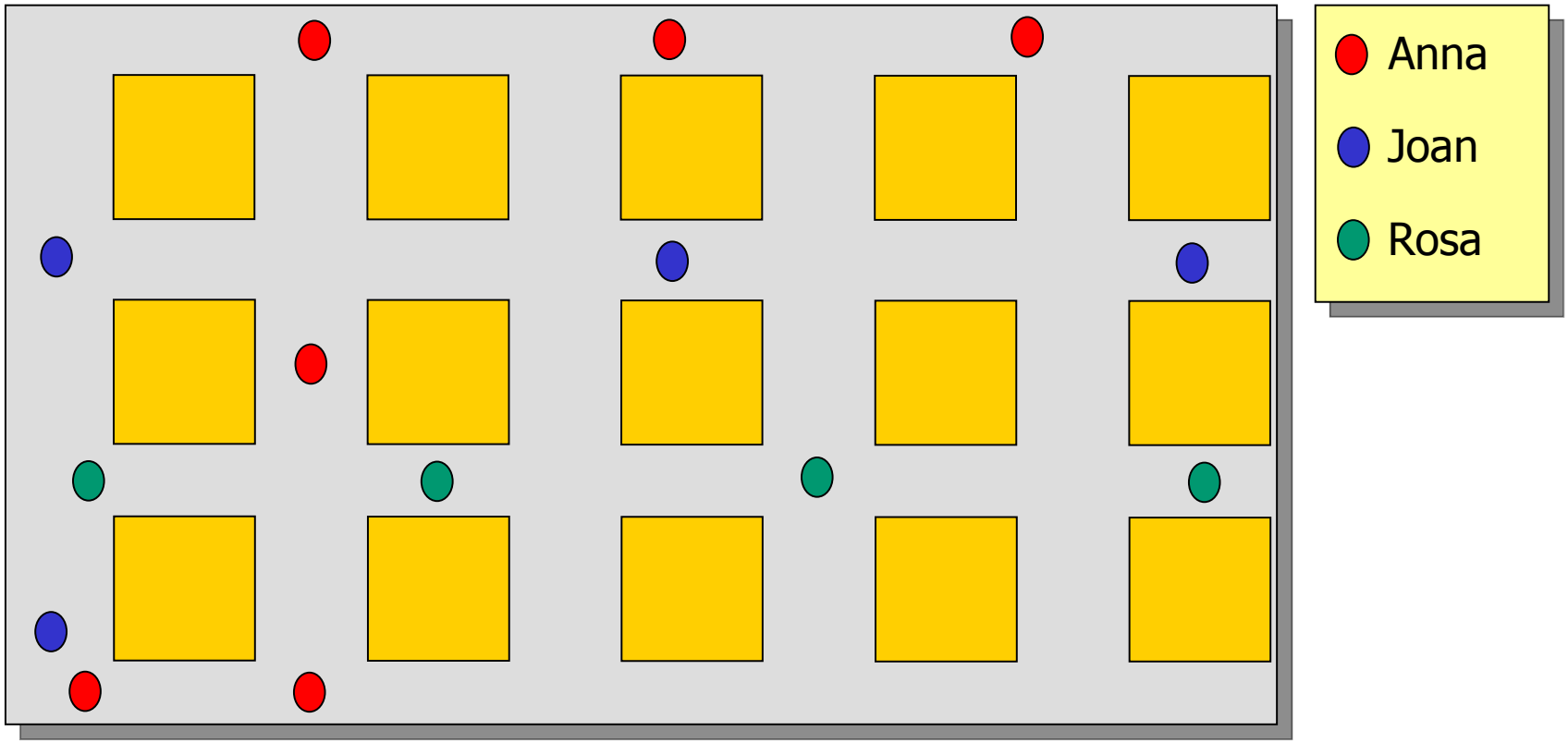


Privadesa en VANET

- Anonimat
  - No es coneix la identitat d'un node
  - Us de pseudònims
- No enllaçabilitat
  - Diferents interaccions no relacionables
  - Requereix canvi periòdic d'adreces, identificadors, etc

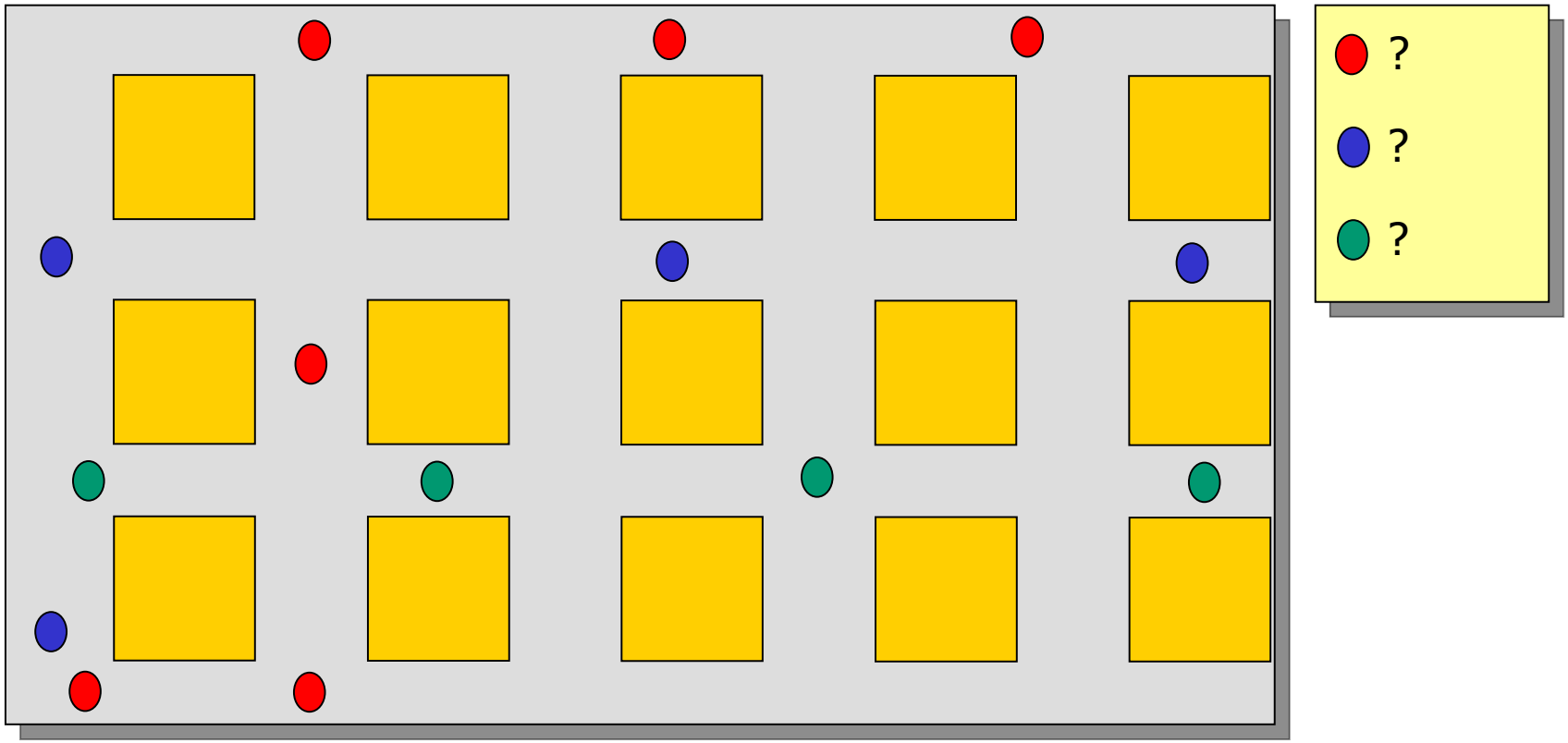
Privadesa en VANET

- VANET sense privadesa



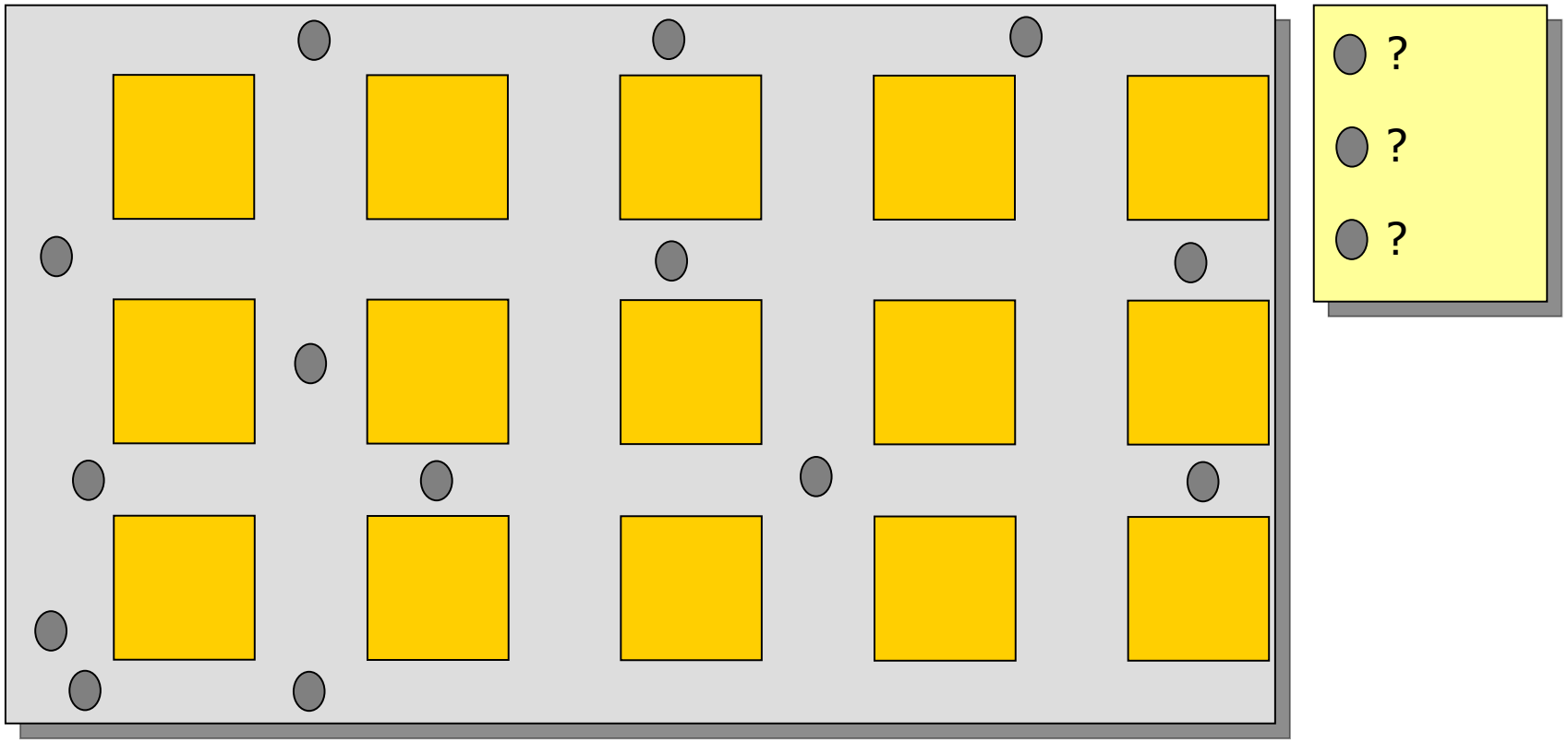
Privadesa en VANET

- Anonimat (permet seguiment)



Privadesa en VANET

- Anonimat i no enllaçabilitat

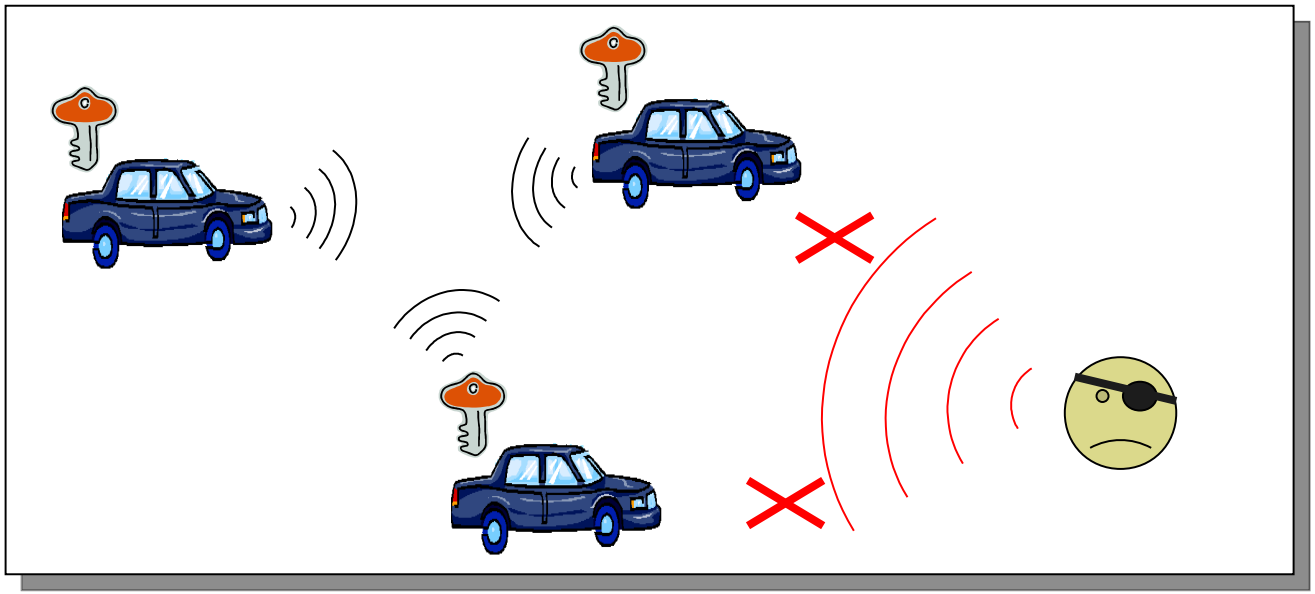


Seguretat en VANET

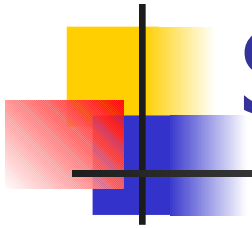
- La seguretat és clau en una VANET
- Missatges malintencionats
  - Accidents
  - Complicacions per al trànsit

Seguretat en VANET

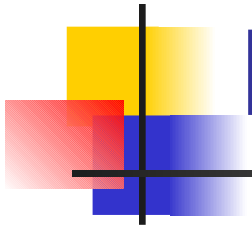
- Atacants externs
  - Prevenció utilizant criptografia
    - Nodes autoritzats coneixen una clau secreta



Seguretat en VANET

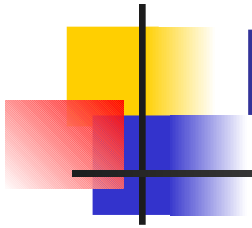


- Nodes autoritzats afegeixen un codi d'autenticació als missatges enviats
  - El codi demostra coneixement sobre clau secreta
  - Verificable a partir d'un certificat de clau pública
  - Permet traçabilitat
  - Pseudònims intercanviables
    - Gestió costosa



Privadesa vs Seguretat

- Anonimat
  - No se sap qui ha realitzat certa acció
  - Com prendre mesures contra usuaris que han actuat de forma fraudulenta ?
    - Atacants interns
  - Anonimat revocable
    - TTP pot revocar l'anonimat

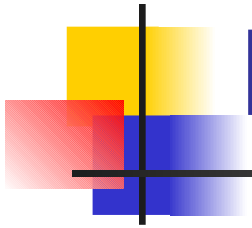


Privadesa vs Seguretat

- Mesures a priori
  - Evitar que un node autoritzat enviï informació fraudulenta
  - Missatge vàlid si és avalat per un número mínim de vehicles

Estàndards

- IEEE 1609
  - Estats Units
    - Finançat pel Dept. de Transport
  - Sistema WAVE
    - *Wireless Access in Vehicular Environments*
  - Format per quatre estàndards
    - Un d'ells encara en desenvolupament
    - Vehicles equipats de fàbrica el 2011

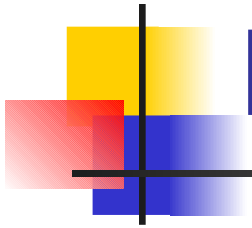


Estàndards

- Seguretat en IEEE 1609 (1609.2)
  - Clau pública + Certificats digitals
  - Criptografia semànticament segura
- Privadesa
  - Esmenten que cal evitar seguiment per adreça MAC
    - Mitjançant canvi freqüent
  - Esmenten que cal mecanisme per enviar missatges autenticats de forma anònima
  - Ho deixen per treball futur

Estàndards

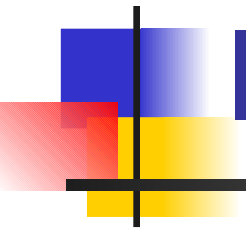
- C2C-CC (*Car to Car – Communication Consortium)*
  - Àmbit europeu
  - Consorci de fabricants de vehicles i subministradors de components electrònics
  - En desenvolupament



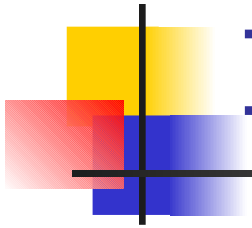
Estàndards

- Requeriments de seguretat C2C-CC
  - Informació correcta i fiable
  - Robustesa (DoS)
  - Privadesa
- Privadesa (tema obert)
  - Certificats anònims (signatura cega)
  - Certificats de durada curta
  - Proves de coneixement nul

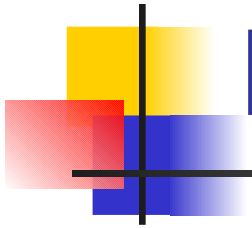
Privadesa en serveis basats en la localització



Introducció LBS

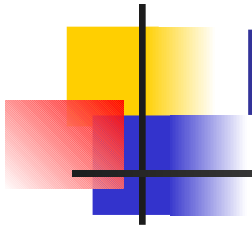


- *LBS=Location-Based Services*
- Usuari rep informació a partir de la seva localització
  - Assistència en cas d'emergència
  - Informació turística: hotels, restaurants, monuments
  - Itineraris



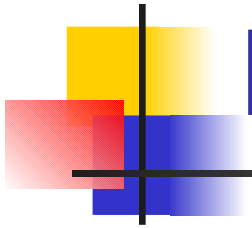
Privadesa en LBS

- El proveïdor de serveis, a partir de les consultes, sap la localització
- Podrà inferir
  - Llocs freqüentats
  - Horaris
  - Costums, aficions



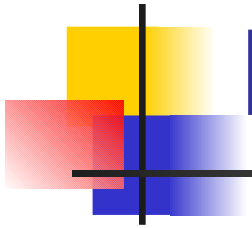
Privadesa en LBS

- Aplicacions on és necessari revelar la identitat
  - Serveis amb subscripció
  - No vull revelar **on** sóc
  - Distorsiono la meva localització
  - Compromís entre privadesa i qualitat de la informació rebuda



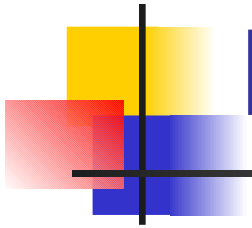
Privadesa en LBS

- Aplicacions que permeten anonimat de l'usuari
  - No se sap **qui** sóc
  - Puc revelar la meva posició



Privadesa en LBS

- Com aconseguir anonimat
  - Sense TTP
    - Difícil a nivell tècnic (adreces, identificadors, claus)
    - Situació en VANET
  - Amb TTP
    - Usuari envia consulta a un anonimitzador en qui confia

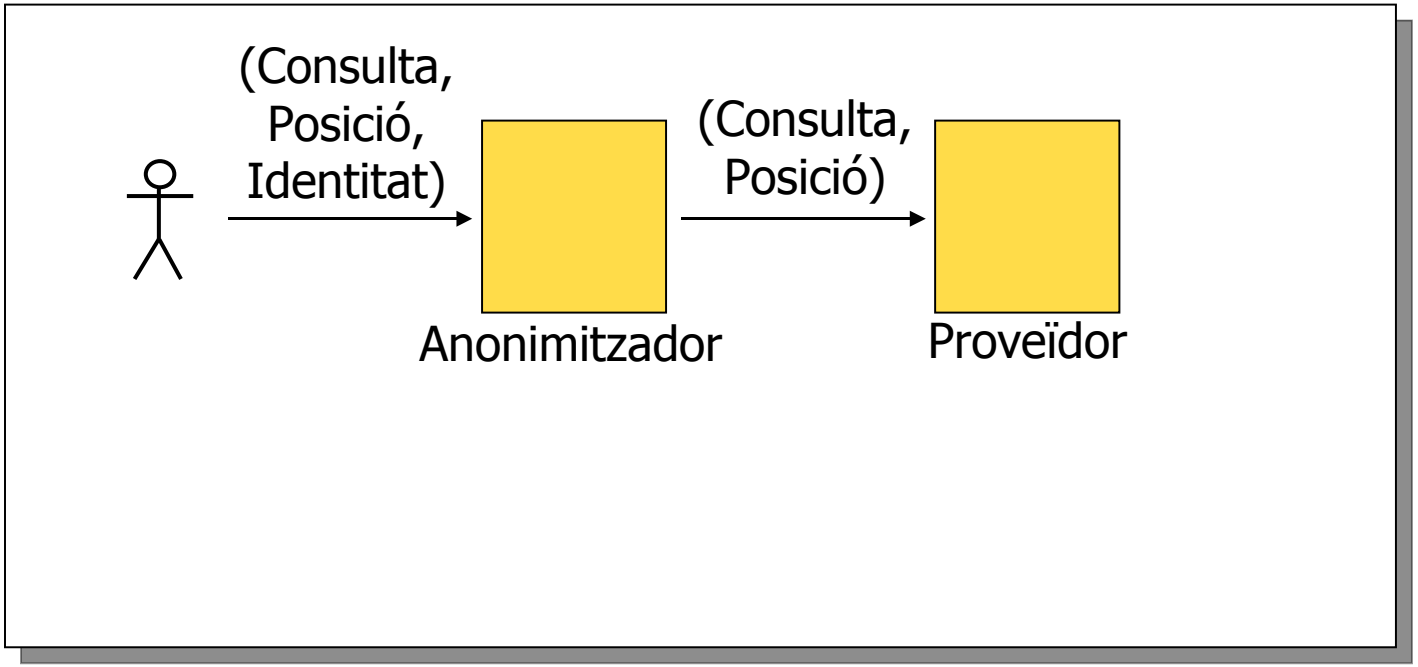


Privadesa en LBS

- Anonimat amb TTP
  - Anonimitzador rep la consulta
  - Elimina l'identificador
  - Possiblement distorsiona la posició
  - Envia la consulta al proveïdor de serveis

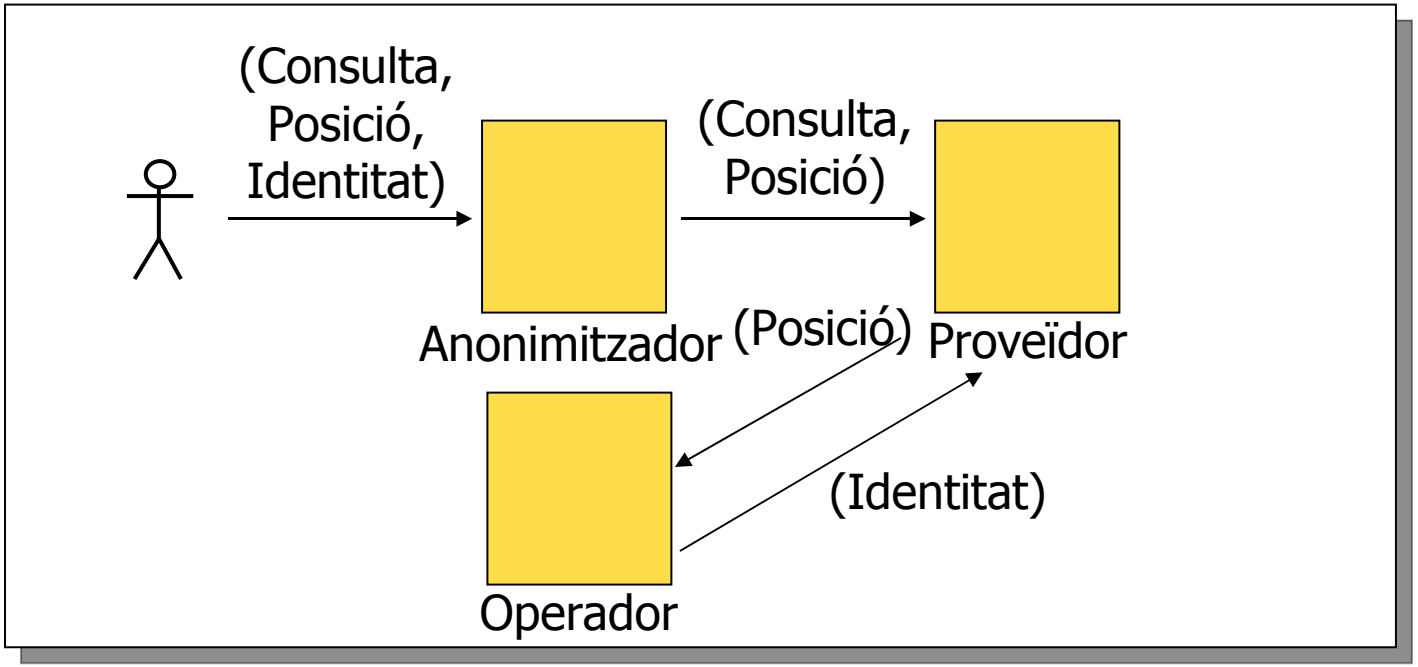
Privadesa en LBS

- Per què cal que l'anonimitzador distorsioni la posició ?



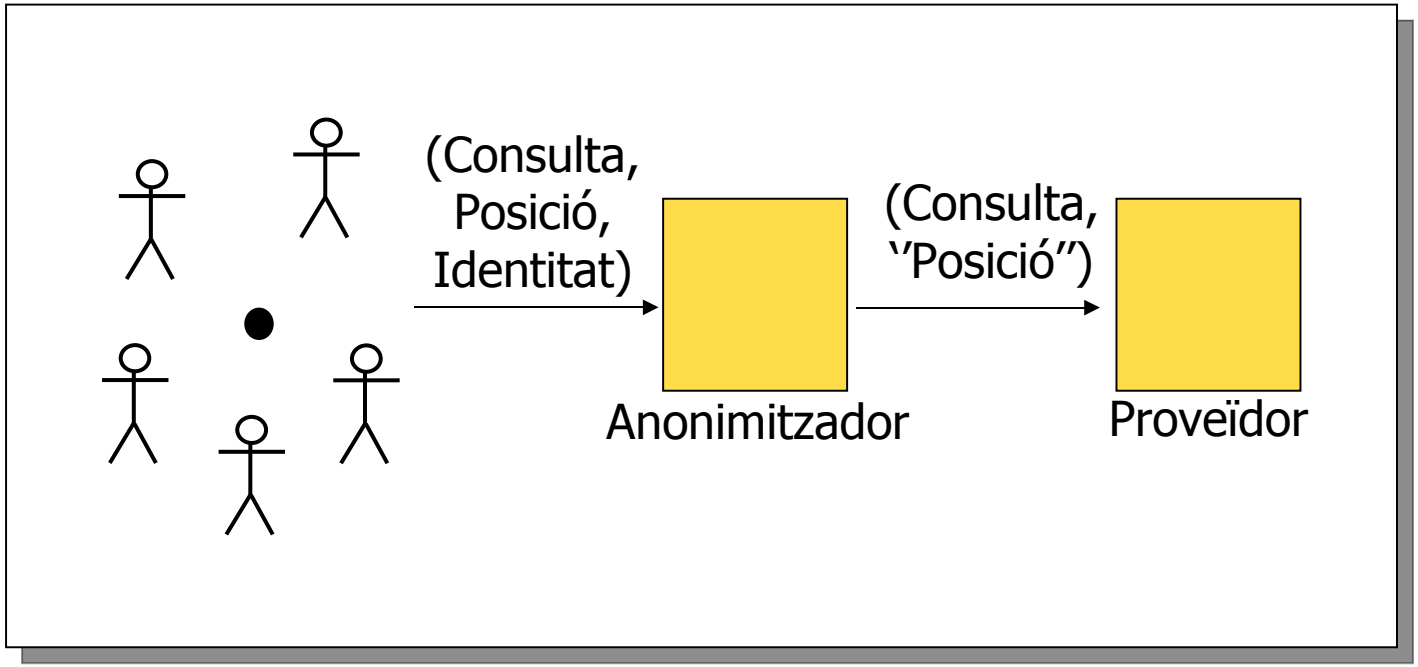
Privadesa en LBS

- Per què cal que l'anonimitzador distorsioni la posició ?



Privadesa en LBS

- k-Anonimat
  - "Posició" assignable almenys a *k* usuaris

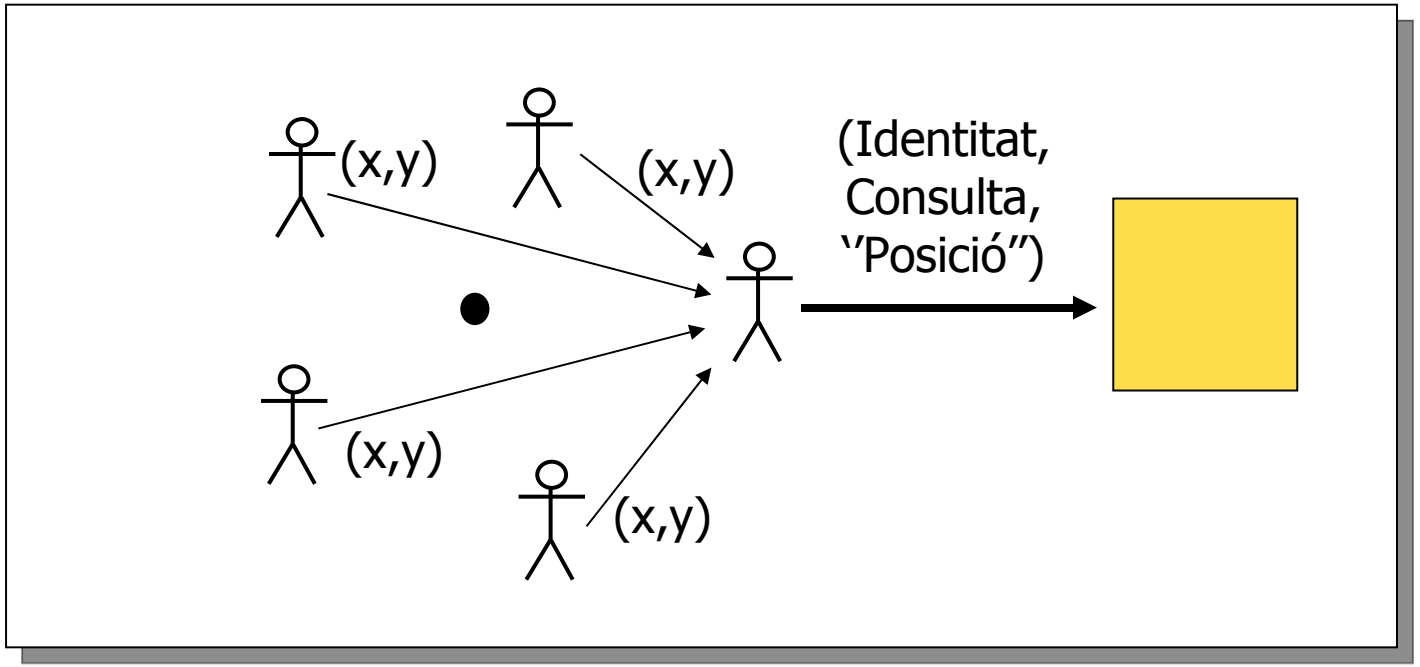


k-Anonimat

- Què passa si no confiem en l'anonimitzador?
  - Sistema distribuït d'emmascarament de posició
  - Els usuaris, de forma col·laborativa calculen "posició"

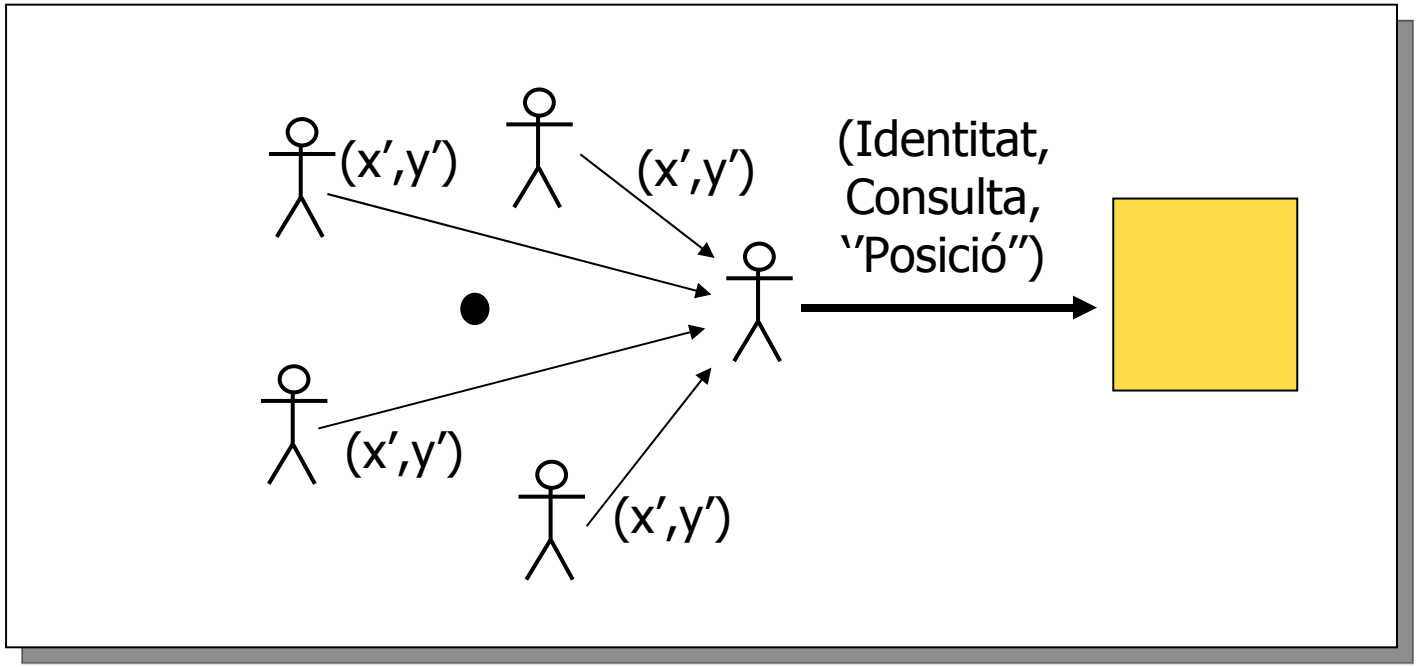
k-Anonimat

- Usuaris confien entre sí
  - Comparteixen posició



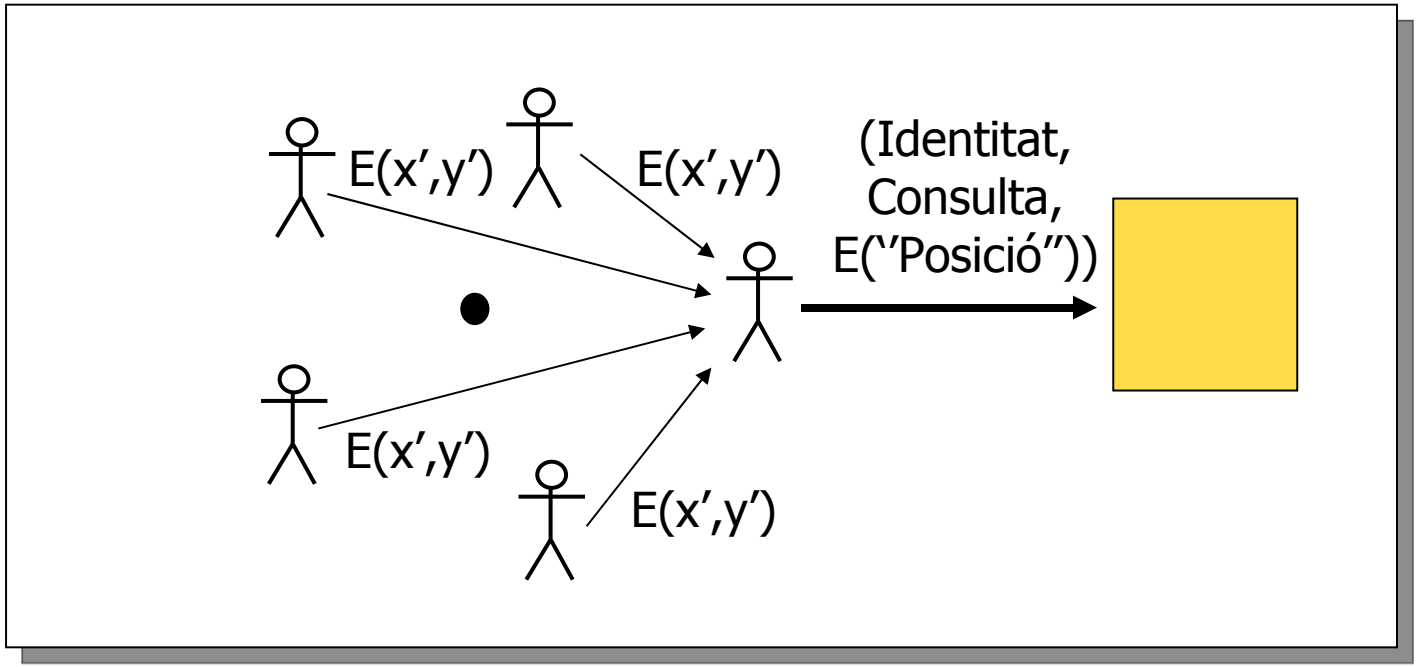
k-Anonimat

- Reduïm confiança
  - Comp. posició amb soroll $(x,y)+(N^x,N^y)$



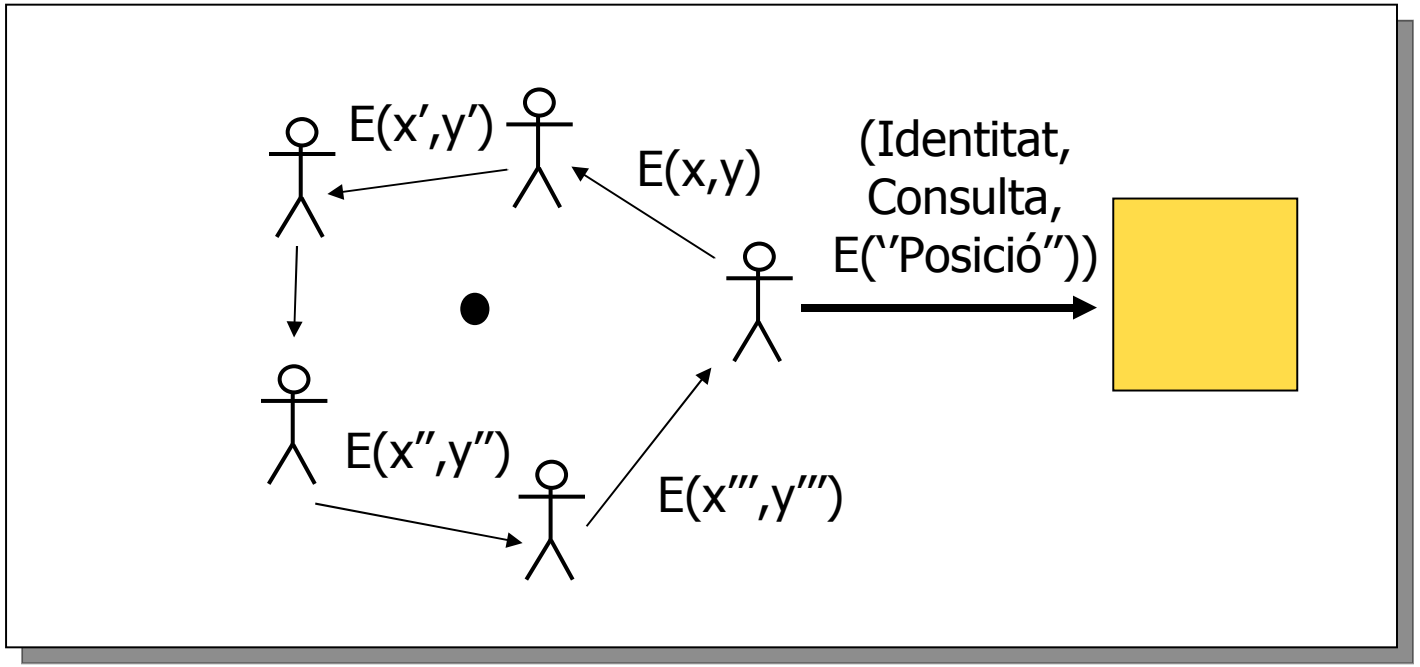
k-Anonimat

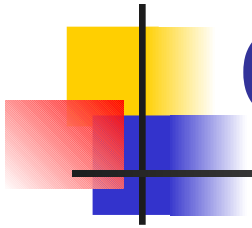
- Reduïm confiança
  - Utilització d'homomorfismes de privacitat



k-Anonimat

- Reduïm confiança
  - Homomorfismes + Camins





Conclusions

- Xarxes vehiculars i serveis basats en localització
  - Revelen informació sobre la localització dels usuaris
  - Informació molt confidencial
  - Cal prendre mesures
  - Tema obert de recerca