FFI Forsvarets forskningsinstitutt

Truverdige mobile trådlause ad hoc-nett – ein illusjon?

Eli Winjum

seniorforskar FFI

Seminar

21. september 2006

Abelia Innovasjons Fagnettverk for Informasjonssikkerhet

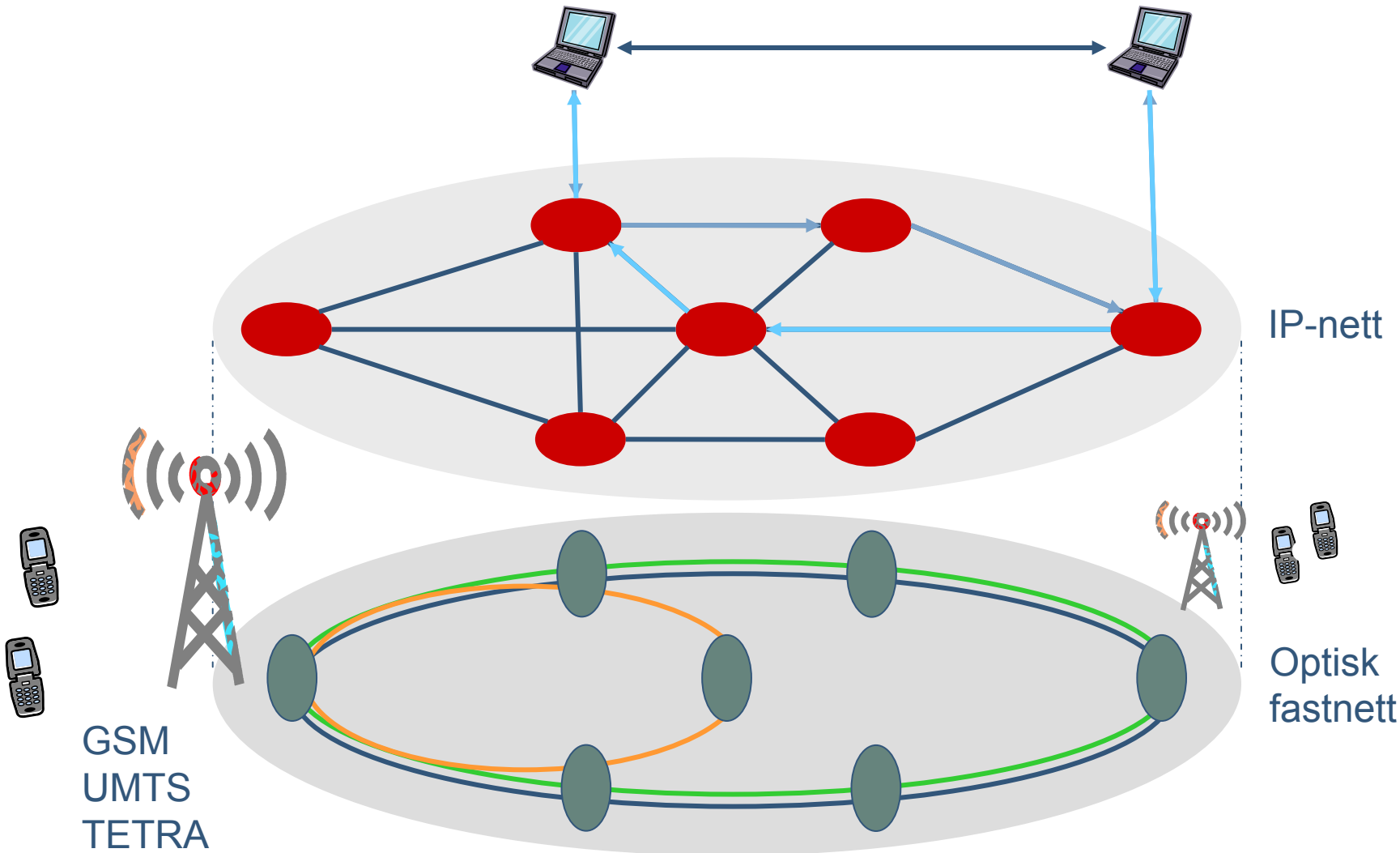
Skal snakka om

- Kva gjer eit kommunikasjonsnett truverdig?
- Mobile trådlause ad hoc-nett
  - kva er det?
  - kvar og til kva vil slike nett kunna brukast?
- Den trådlause kanalen er usikker
- Kan tillit etablerast?
  - grunnlag for tillit
  - knappe ressursar
  - integritet og konfidensialitet
- Utfordringar

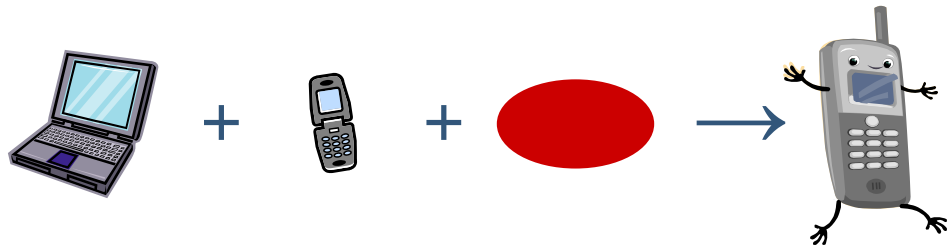
Eit truverdig kommunikasjonsnett

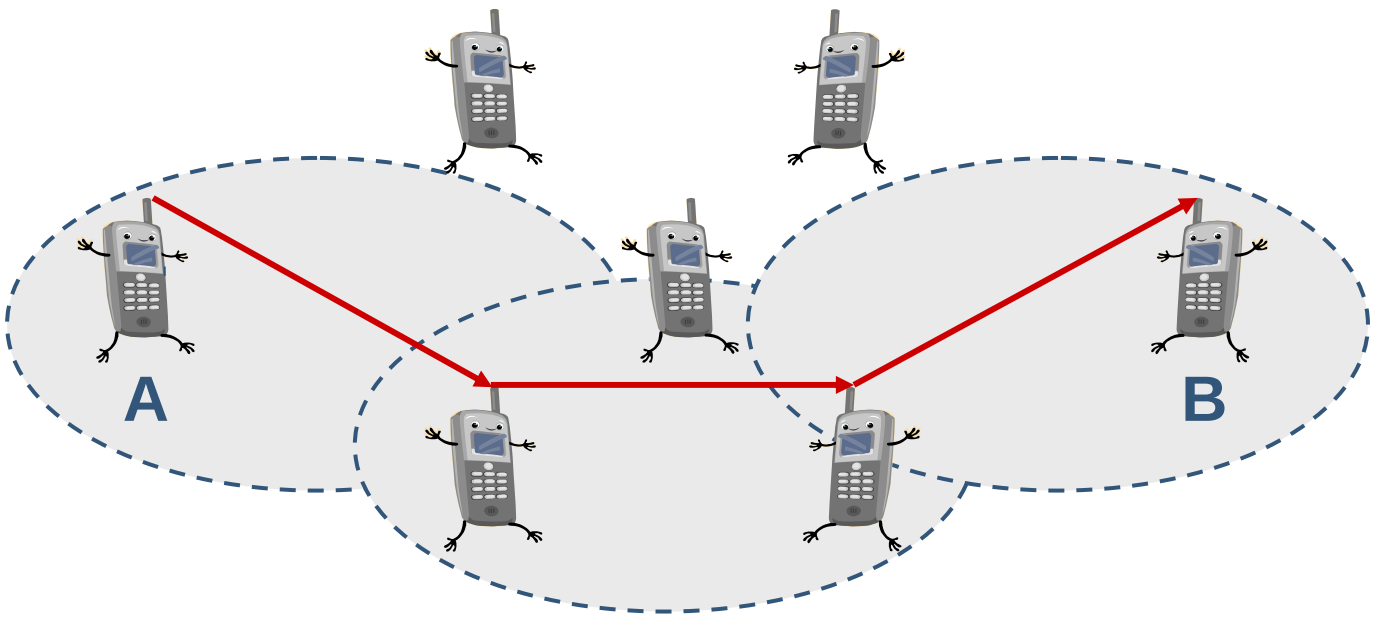
- Yter som spesifisert i tekniske standardar
- Yter som spesifisert i kontraktar
- Har styrbar teknisk infrastruktur
- Er tilgjengeleg for autoriserte – utilgjengeleg for ikkje-autoriserte
- Har utprøvde tenester og mekanismar for
  - integritet, til dømes autentisering
  - konfidensialitet, til dømes kryptering
- Organisasjon(ar) som eig, driv, tek mot klager og søksmål
-
- Tillitverdig – truverdig – påliteleg – sikkert .....

Kva er eit mobilt trådlaust ad hoc-nett?



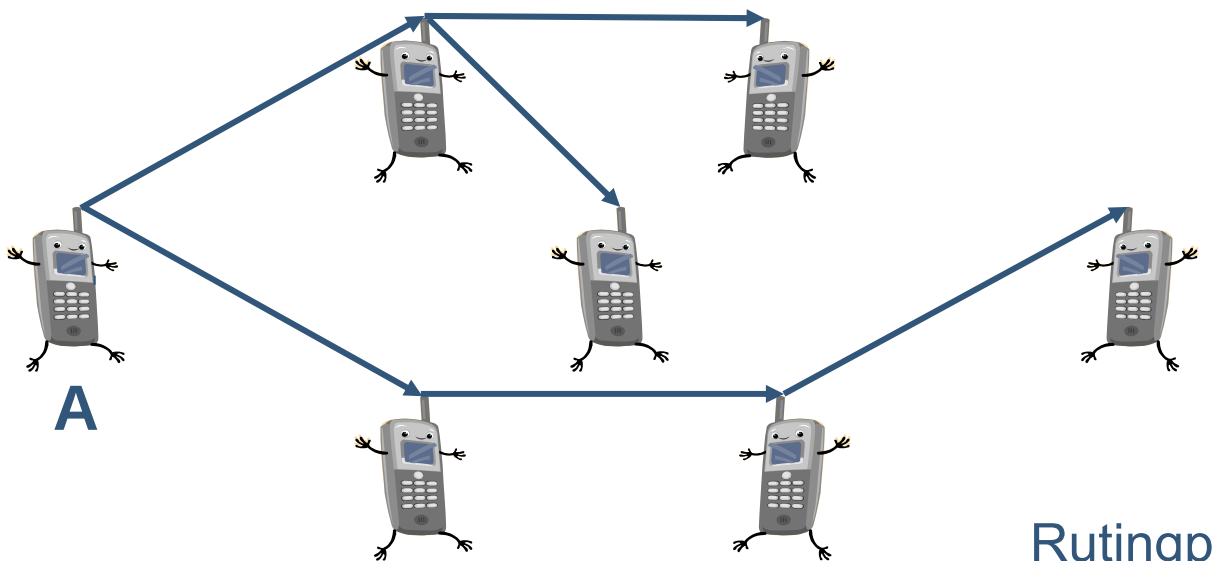
Kva er eit mobilt trådlaust ad hoc-nett?





Kva er eit mobilt trådlaust ad hoc-nett?

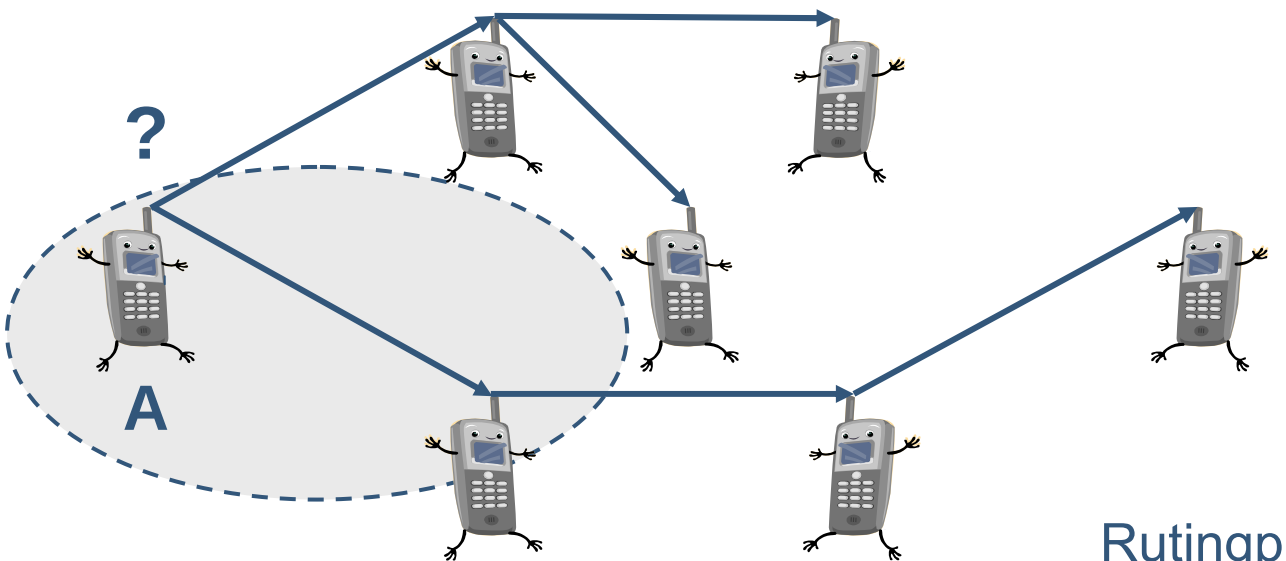
Dette:



Rutingprotokollen er limet

Kva er eit mobilt trådlaust ad hoc-nett?

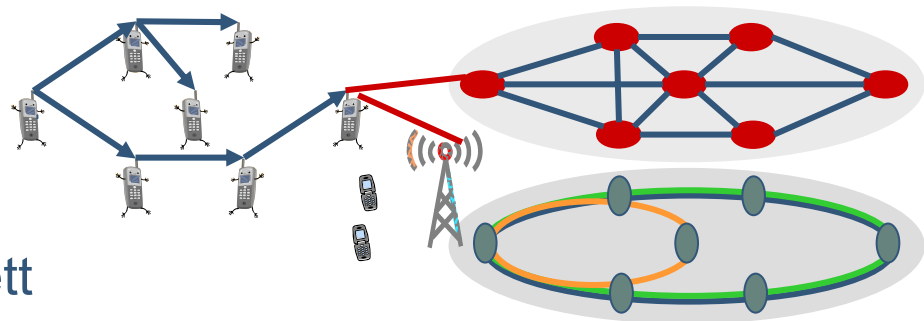
Truverdig?



Rutingprotokollen er limet

Framtidig bruk

- Sentrale i 4. generasjons (4G) trådlause kommunikasjonsnett
- Kan utvida eksisterande nett
  - offentlege
  - private
  - militære
- Kan innlema nye typar nett
  - Personal Area Networks (PANs)
  - Body Area Networks (BANs)
  - robotar og sensorar
- Kan vera eit isolert nett
- Døme: Redningsoperasjonar



Fordeler og ulemper

- Viktige fordeler
  - treng ikkje fysisk infrastruktur
  - treng ikkje sentral styring

- Viktige ulemper
  - har ikkje fysisk infrastruktur
  - har ikkje sentral styring

Den trådlause kanalen er usikker

- Kvaliteten varierer – kan ikkje garanterast
- Interferens
- At kanalen er tilgjengeleg for alle, gjer det lett å
  - avlytta
  - planta falsk informasjon
  - endra informasjon
  - “jamma”
- … og når nodane er mobile
  - endrar nett-topologien seg heile tida
  - nodar kjem og går
  - og det er ikkje lett å identifisera eit angrep

The Perfect Match

- Eigenskapar ved tradisjonelle løysingar for sikring av trådbaserte kommunikasjonsnett
  - krev stor bandbreidde
  - krev stor reknekraft
  - krev stor lagringskapasitet
  - basert på sterk infrastruktur
  - basert på sentraliserte protokollar, prosessar, maskiner
- Eigenskapar ved mobile trådlause ad hoc-nett
  - avgrensa bandbreidde
  - avgrensa reknekraft
  - avgrensa lagringskapasitet
  - kan ikkje garantera tilgang til sentraliserte tenester
  - “single-point-of-failure” – løysingar er særleg sårbare

Grunnlag for tillit?

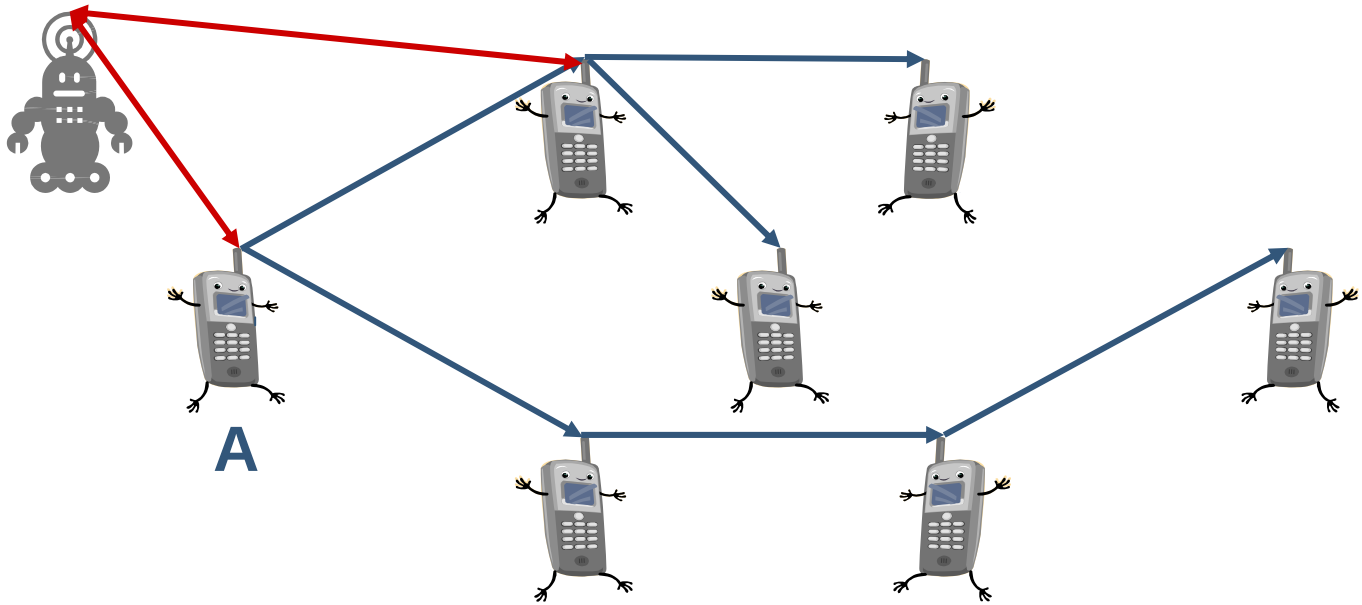
- Opererer som spesifisert i opne tekniske standardar
- Tilgjengeleg for autoriserte – utilgjengeleg for ikkje-autoriserte
- Utprøvde tenester/mekanismar for integritet og konfidensialitet
  - brukardata
  - nettdata
- Korleis få det til?
  - sikker ruting
  - robust ruting
  - intrusjonsdeteksjon – intrusjonstoleranse
  - autentisering
  - effektiv nøkkelhandtering
  - tenestekvalitet
- Kva er godt nok?

Sikring av rutingprotokoll

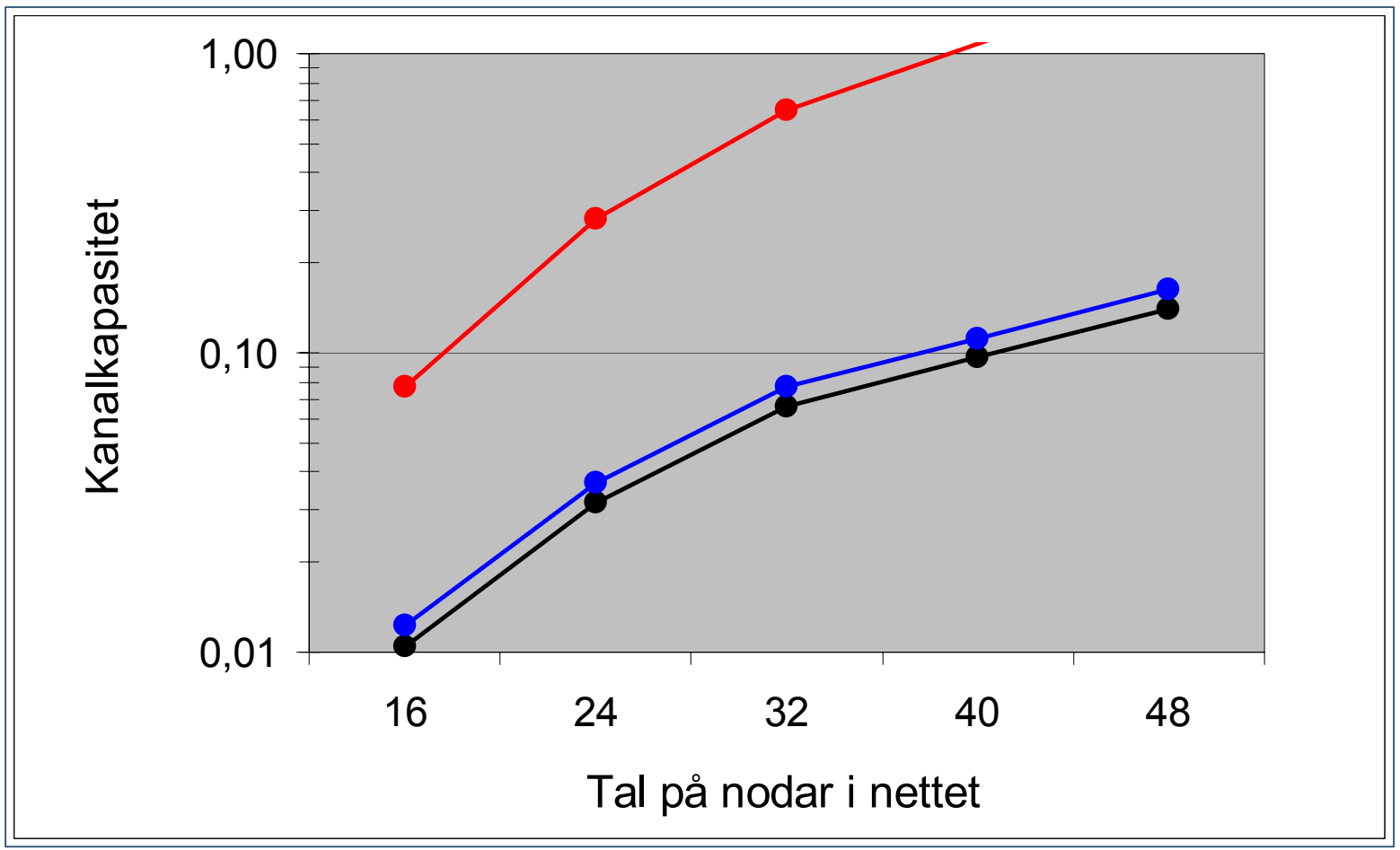
Ei autentiseringsteneste må detektera

- uautoriserte meldingskjelder
- uautoriserte endringar av meldingar
- gamle meldingar (replays)

ekstern
angripar

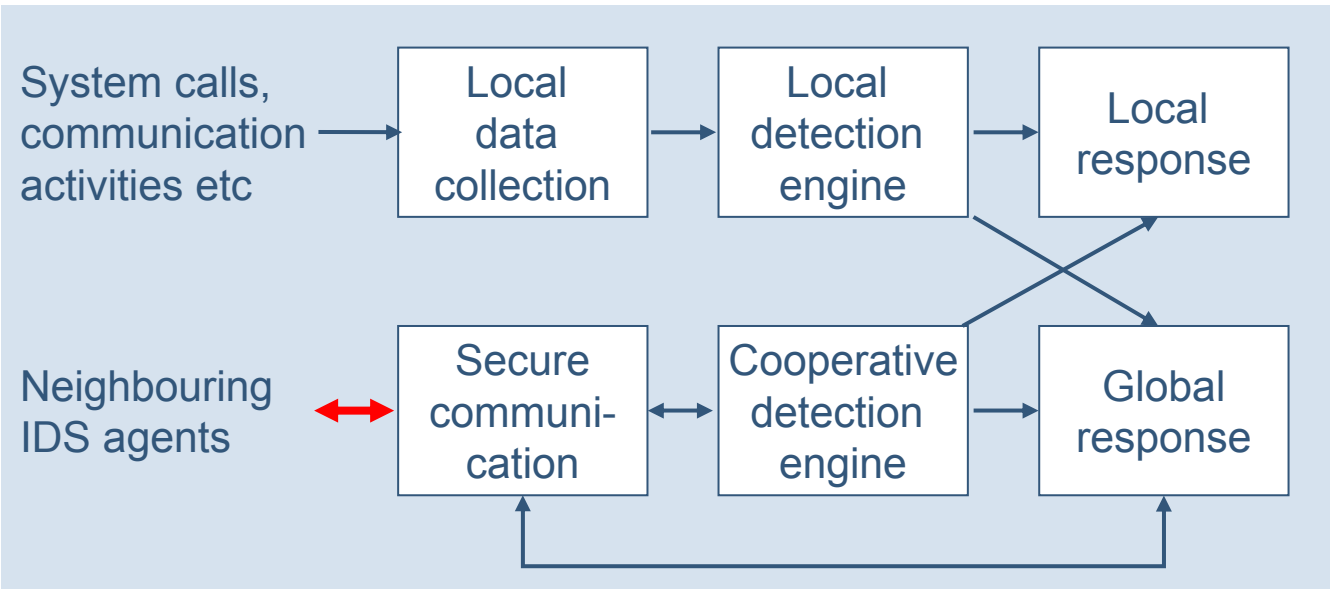


Eit rekne-eksempel: Rutingprotokoll med autentisering av kjelde, data og tid



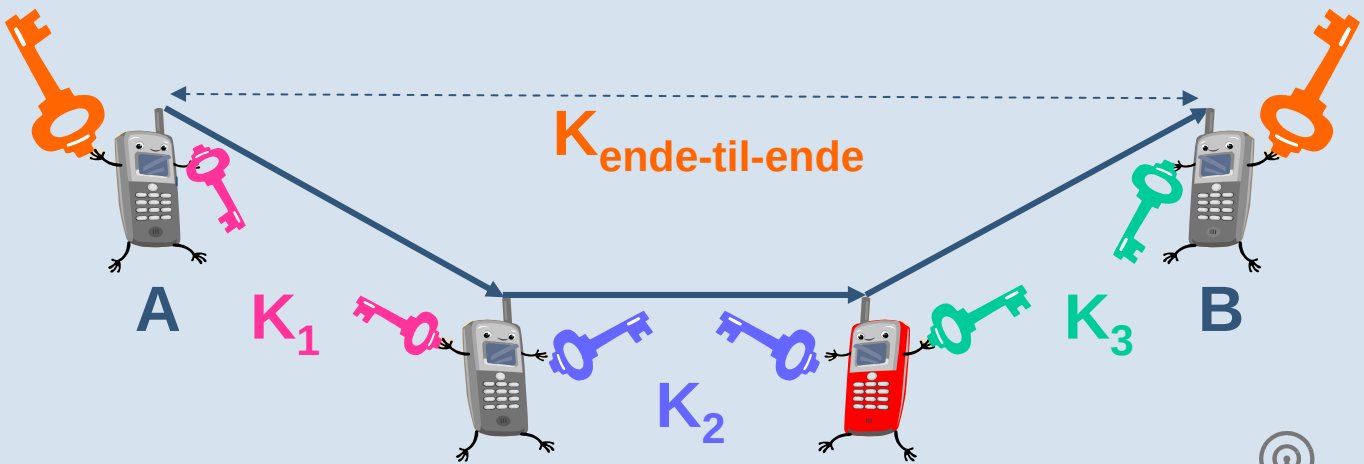
Distribuert intrusjonsdeteksjon

- Detektera misbruk
  - angrep vi kjenner
- Detektera anomali
  - avvik frå etablert normalaktivitet
- Omdøme-generator



Zhang and Lee, 2000

Distribuert nøkkelforhandling



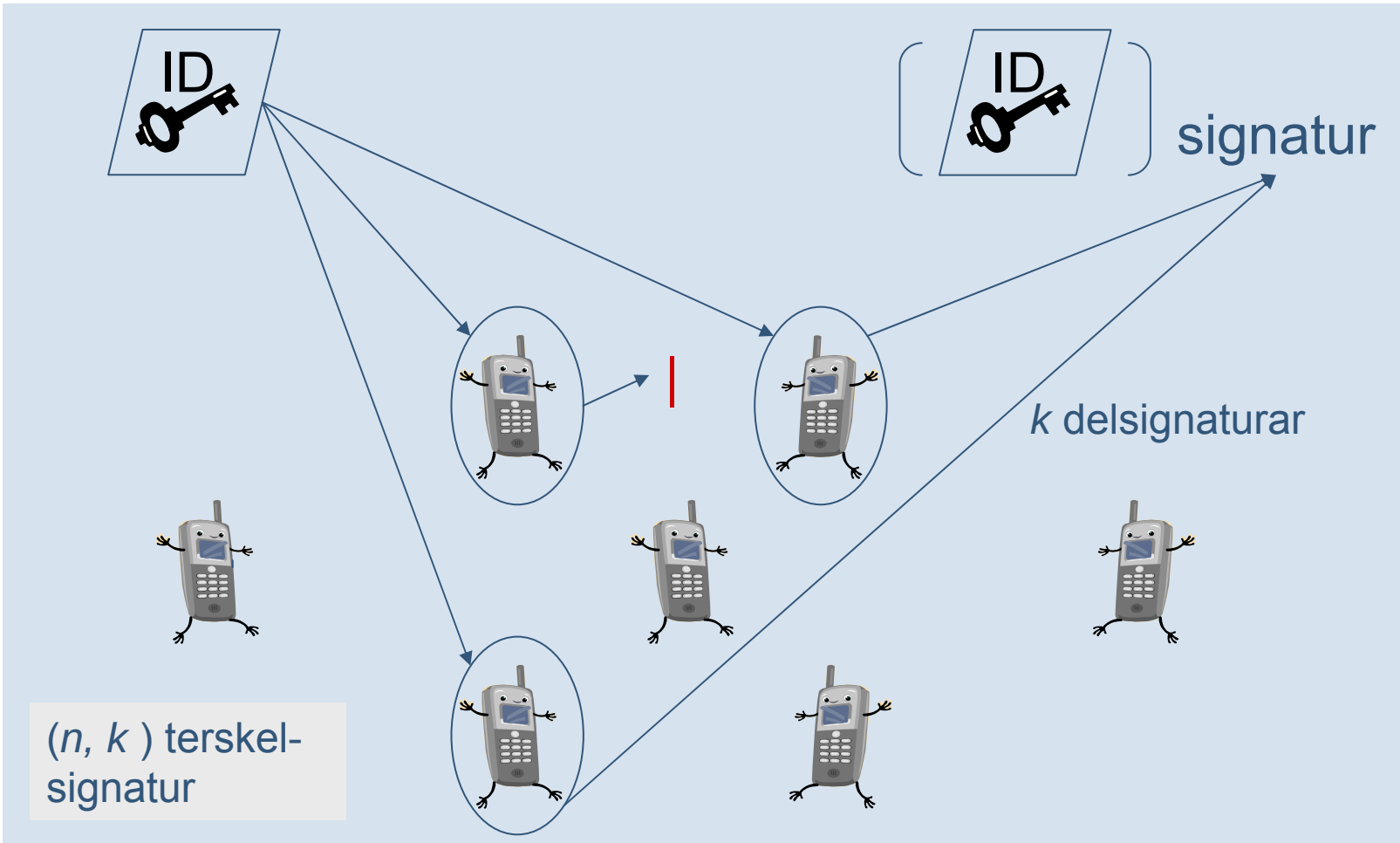
intern angripar

ekstern angripar

$K = Y^X = X^Y$ Diffie and Hellman, 1976

Verma et al, 2001

Distribuert sertifiseringsteneste for PKI



Zhou and Haas, 1999

Utfordringar

- Sikringstenester/mekanismar i ad hoc–nett må vera
  - distribuerte og redundante, men lite ressurskrevjande
  - effektive og skalerbare, men sikre
- Tenestekvalitet
- Trussel og risiko er scenarioavhengig
  - men interoperabilitet med eksisterande nett kan gjera ad hoc-netta til svake ledd i gjennomgåande nett-tenester
- Policy som tek omsyn til at risiko varierer
  - tid/rom
  - multi-nivå
  - multi-domene