Ad hoc networks and information security

- temporary formed on the spot for a specific purpose for a short time

- wireless communications

- mobile in relation to each other and/or as a whole

... servers, certificate authorities...

... infrastructureless: no central services such as fixed routers, name

... infrastructure to keep the network connected

Ad hoc network="collection of nodes that do not need a pre-defined
Properties of the ad hoc devices

A device can lose connection to the rest of the network for several reasons: it can move out of the network's reach, be compromised, be broken, run out of batteries...

- Weak physical security
- Limited battery life
- Limited memory and computational capacities
- Small, portable
Properties of ad hoc networks

- Connections can be sparse
- Unreliable connections, network may even be split temporarily
- Information outdated rapidly
- Network topology and routes change frequently, hence route nodes
- Connections are formed by jumping from point to point via other
Consequences

- no previously agreed-on secrets
- security: no trusted third parties, weak physical security, sometimes
- communications should be as fast as possible
- broadcast not always possible
- the time
- the other party/parties (a database for example) is not reachable all
- one cannot rely on algorithms that require a fixed topology
• Solutions

- Ad hoc networks
- Wireless networks
- Distributed algorithms based on local information
- Carry-on documents (certificates for example)
- Off-line solutions
- Piggy-back the information to bigger packets
Scenarios

- Rescue operation: police officers, firefighters have portable devices, cell phones or such
- Battlefield scenario
- Wearable computing
- Household appliances
- Office: computers, printers, phones
- Business meetings: connecting laptops to form a network
portable devices: memory, computational capacity: state of the art - small,

physical security: easy - difficult

administration: support personnel etc. - "self-administering"

services: name services, certificate authorities etc - none

routing: routers - peer-to-peer

topology: fixed - dynamic

connections: copper or optical cable - wireless connections

time: long term - (often) short term