Ad hoc networks and information security

Ad hoc network=”collection of nodes that do not need a pre-defined infrastructure to keep the network connected”

- *infrastructureless*: no central services such as fixed routers, name servers, certificate authorities ...
- *mobile* in relation to each others and/or as a whole
- *wireless* communications
- *temporary* formed on the spot for a specific purpose for a short time

Properties of the ad hoc devices

- small, portable
- limited memory and computational capacities
- limited battery-life
- weak physical security

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 ...

Properties of ad hoc networks

- connections are formed by jumping from point to point via other nodes
- network topology and routes change frequently, hence route information outdates rapidly
- unreliable connections, network may even be split temporarily
- connections can be sparse

Consequences

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

Solutions

- piggy-bag the information to bigger packets
- off-line solutions
- carry-on documents (certificates for example)
- distributed algorithms based on local information

Scenarios

- business meeting: connecting laptops to form a network
- office: computers, printers, phones
- household appliances
- wearable computing
- battlefield scenario
- rescue operation: police or firemen have portable devices, cell phones or such

Conventional network - Ad hoc network

- time: long term - (often) short term
- connections: copper or optical cable - wireless connections
- topology: fixed - dynamic
- routing: routers - peer-to-peer
- services: name services, certificate auctorities,etc - none
- administration: support personnel etc. - “self-administering”
- physical security: easy - difficult
- devices: memory, computational capacity: state of the art - small, portable