Information security
Wireless sensor networks and civil security
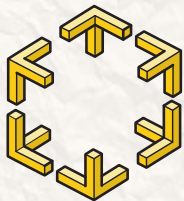
Andreas Larsson

2011-04-13

Our research

- Three research areas
  - Security metrics
  - Wireless sensor networks
  - Denial of service

- Focus on this presentation
  - Wireless sensor networks

Security metrics and denial of service
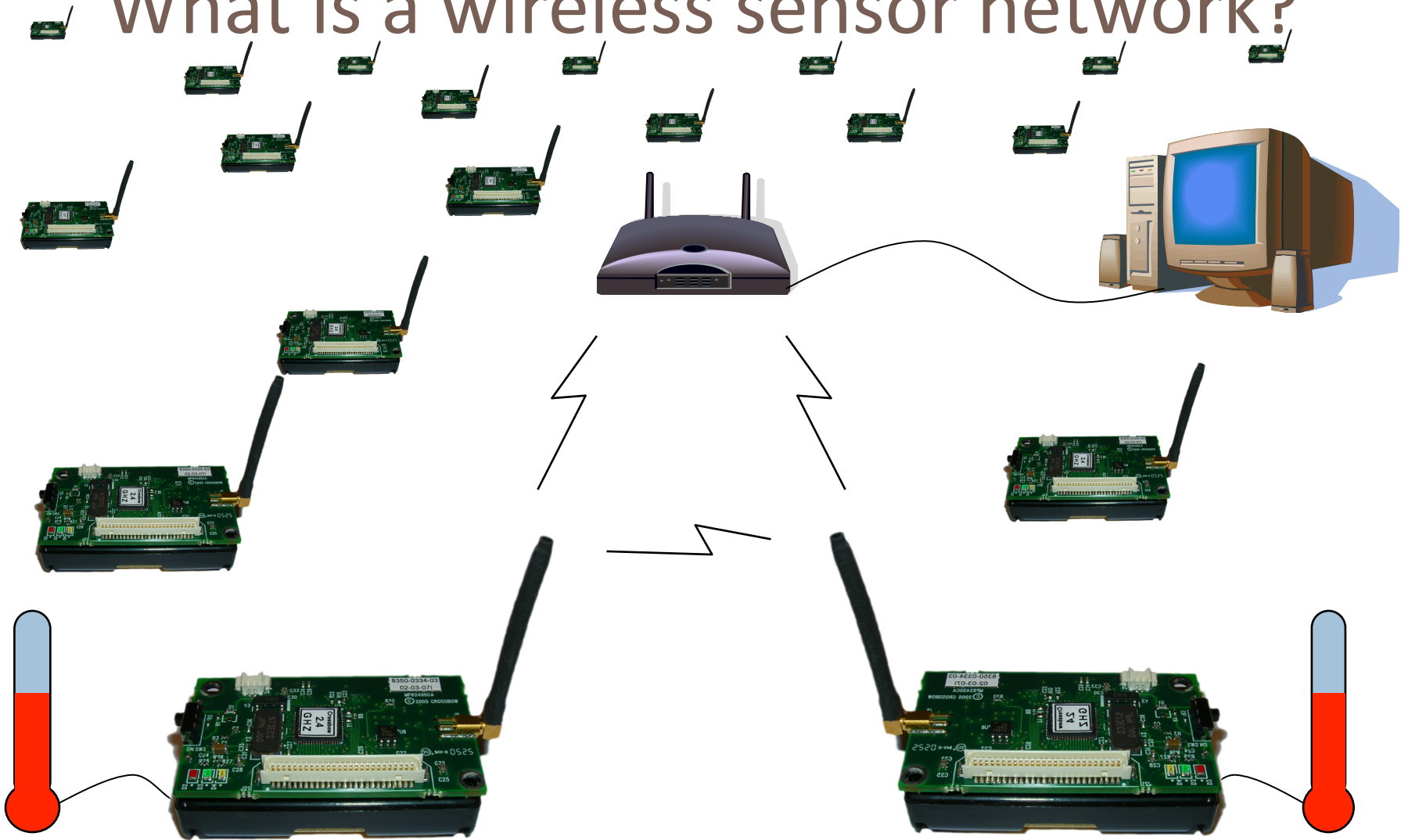
Sensor networks and civil security

Distributed Computing and Systems
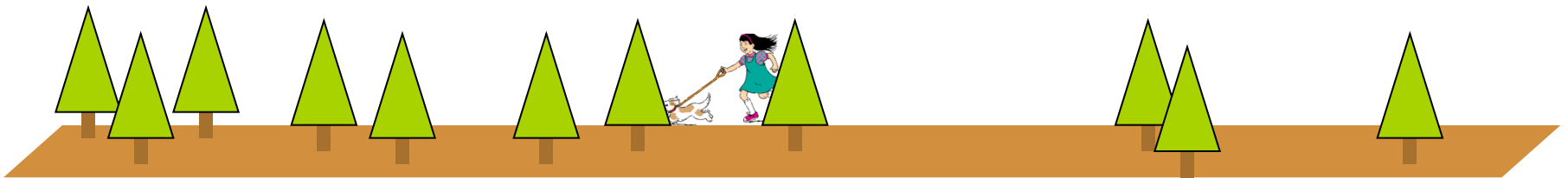**Chalmers university of technology**
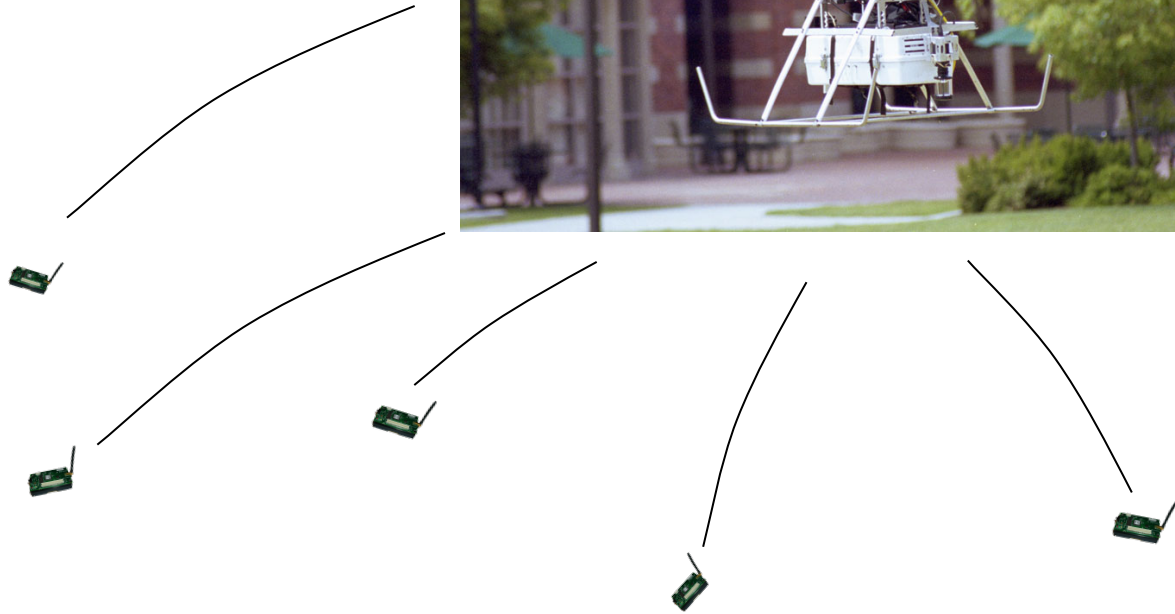
Talk outline

- **Sensor networks**
- Security in sensor networks
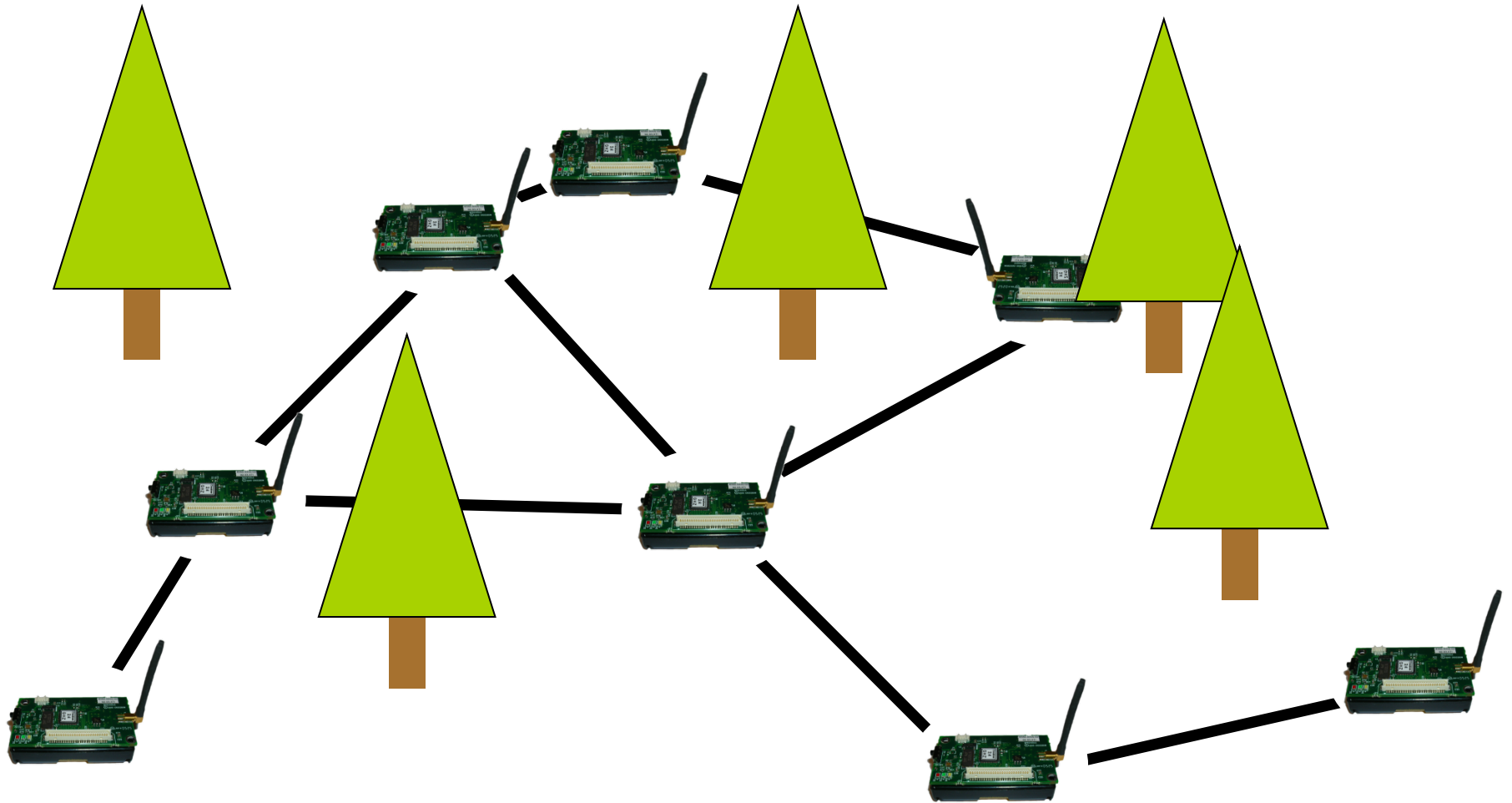- Clock synchronization
- Clustering
- Conclusions

What is a wireless sensor network?

Deployment
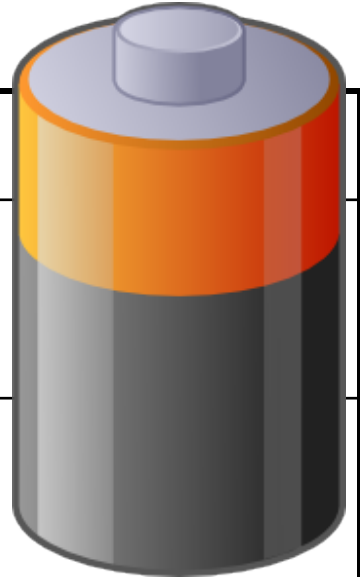
Wireless ad-hoc networks

Sensor node limitations
MicaZ sensor node example

CPU	7MHz
Program Memory	128 kB
RAM	4 kB
Storage Memory	512 kB

Bandwidth	
Indoor Range	
Outdoor Range	

Battery Life	Much more!

Agriculture – water monitoring
The COMMONsense project, India

Internet
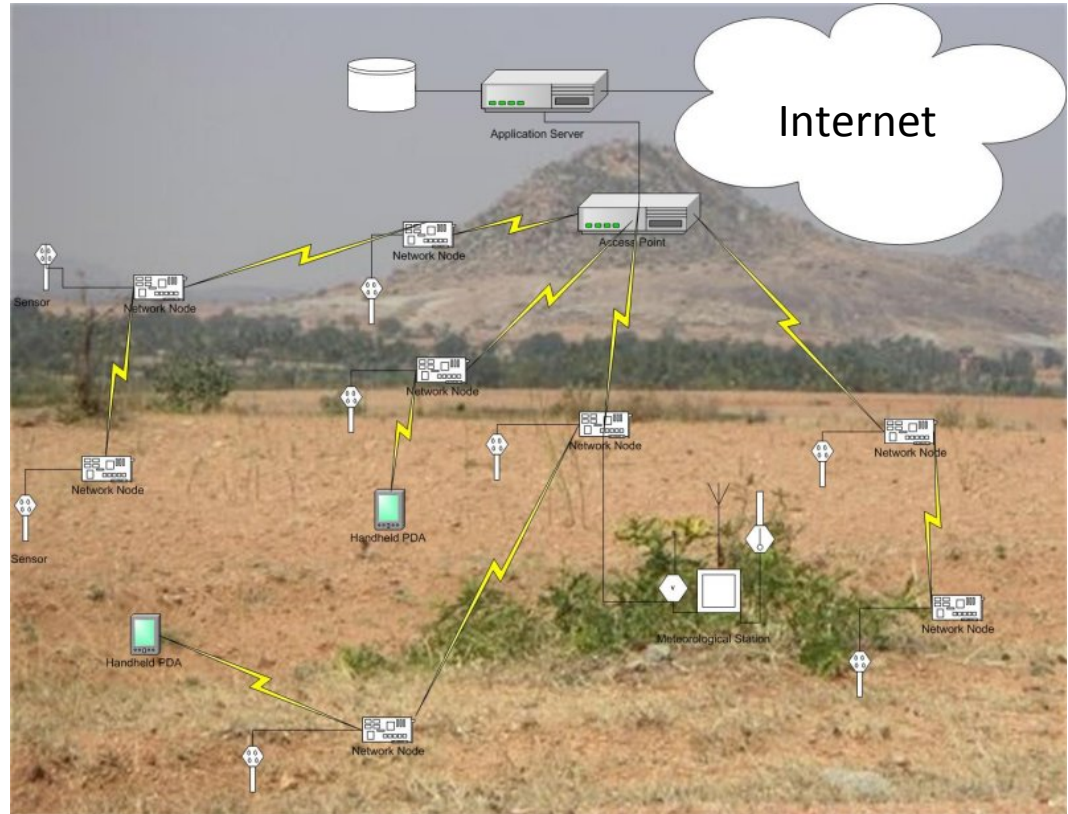
Structural health monitoring
The Stork bridge, Switzerland

Volcanic research – seismic activity Tungurahua, Ecuador

Civil security possibilities

- Disaster area networks
  - Situational awareness
  - Getting communications up
- Forest fire detection
  - Early warning
  - Follow the sequence of events
- Border and perimeter security
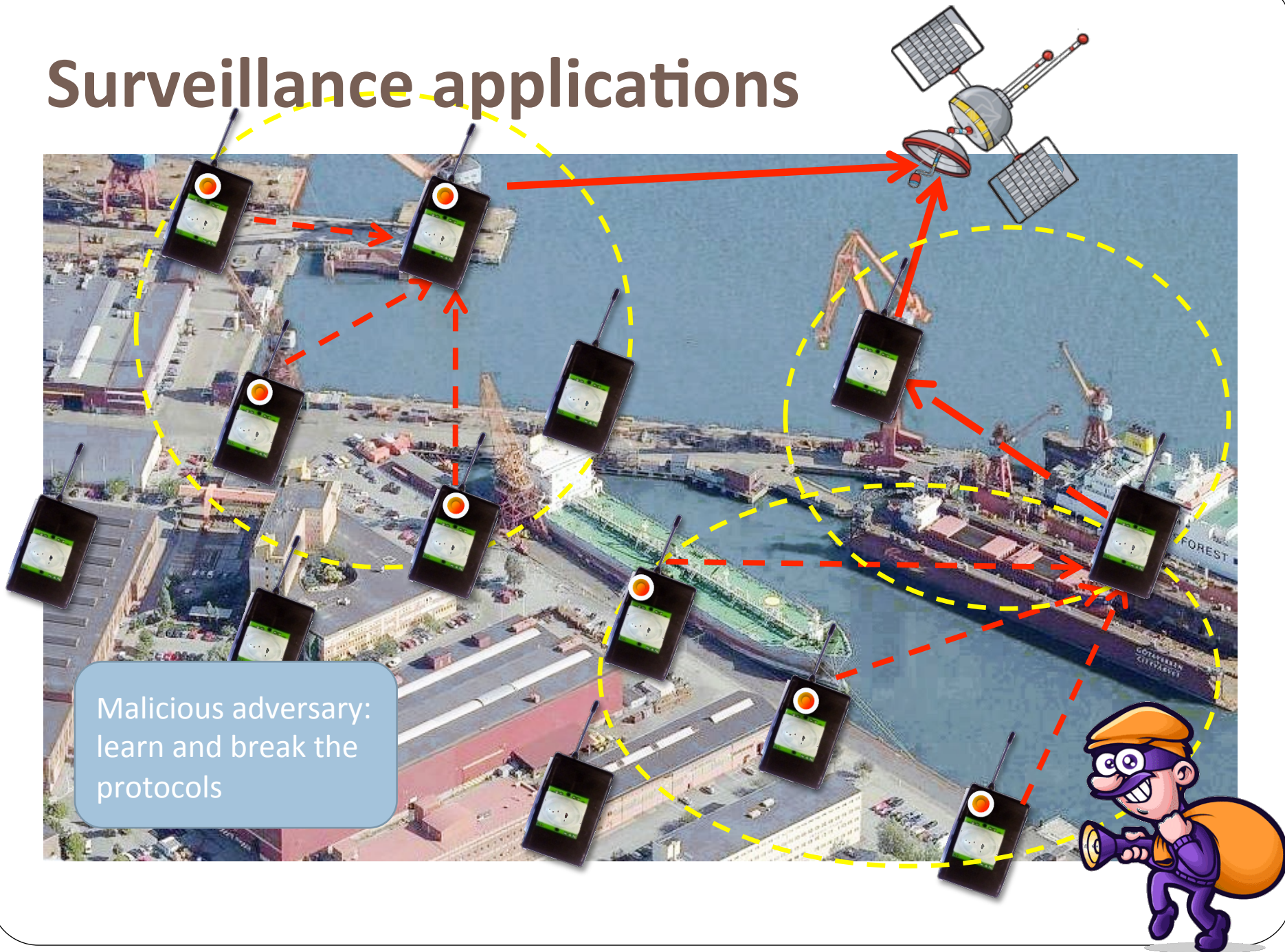 - Intrusion detection

Swedish Civil
Contingencies
Agency

Talk outline

- Sensor networks
- **Security in sensor networks**
- Clock synchronization
- Clustering
- Conclusions

Surveillance applications

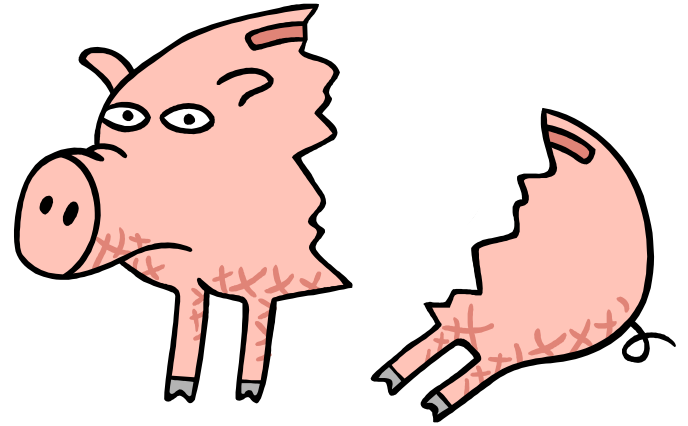Malicious adversary: learn and break the protocols

Security compared to normal networks

- Limitations
  - Public key expensive
  - Key sizes limited
- Threats
  - Compromises
    - Extract information
    - Take over nodes
    - Destroy nodes
  - Denial of Service
   - Jam radio

Fault tolerance

- Nodes get lost
  - Harsh environments
  - Batteries run out
  - Adversarial attacks

Possibility to withstand lost nodes
Possibility to refill the network

Robustness and self-stabilization

- Harsh environments
  - Sensor readings go bad
  - Node states go bad
- Incorrect input
  - Data from compromised nodes
  - Messages corrupted in transmission
- Temporary deviations from assumptions
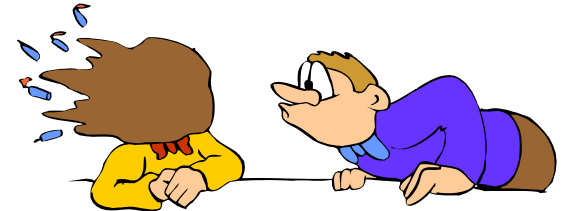
Need to cope with unexpected data
Stabilization from arbitrary state is powerful

Security in sensor networks

- A secure sensor network is not only about secure communications

- We also need
  - Fault tolerance
    - Attacks destroying nodes
  - Robustness
    - Compromised nodes sending bad data
  - Self-stabilization
    - Recover from being overwhelmed

Many services to secure
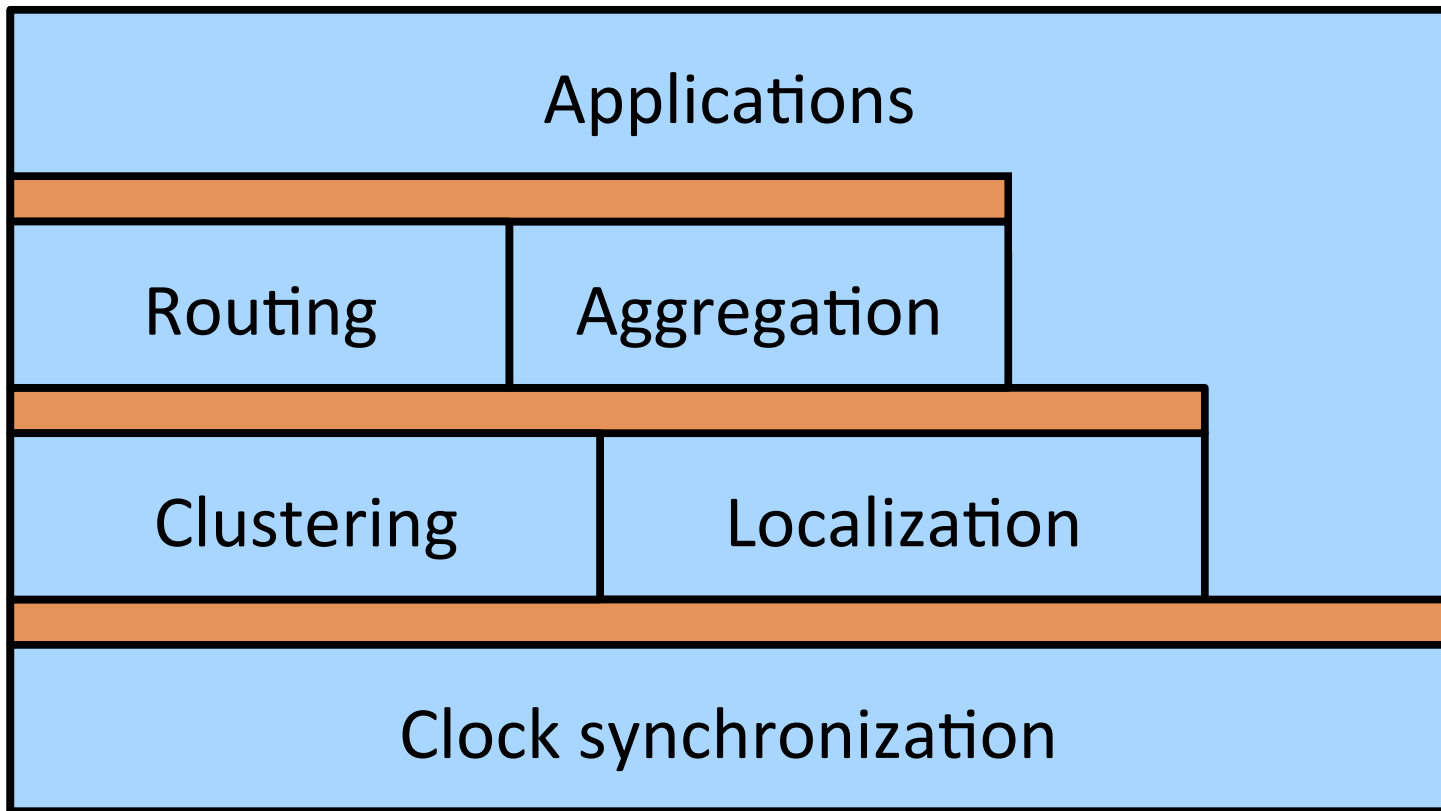
Applications

Routing | Aggregation

Clustering | Localization

Clock synchronization

Talk outline

- Sensor networks
- Security in sensor networks
- **Clock synchronization**
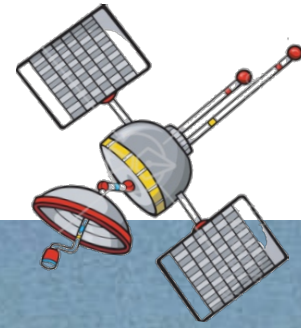- Clustering
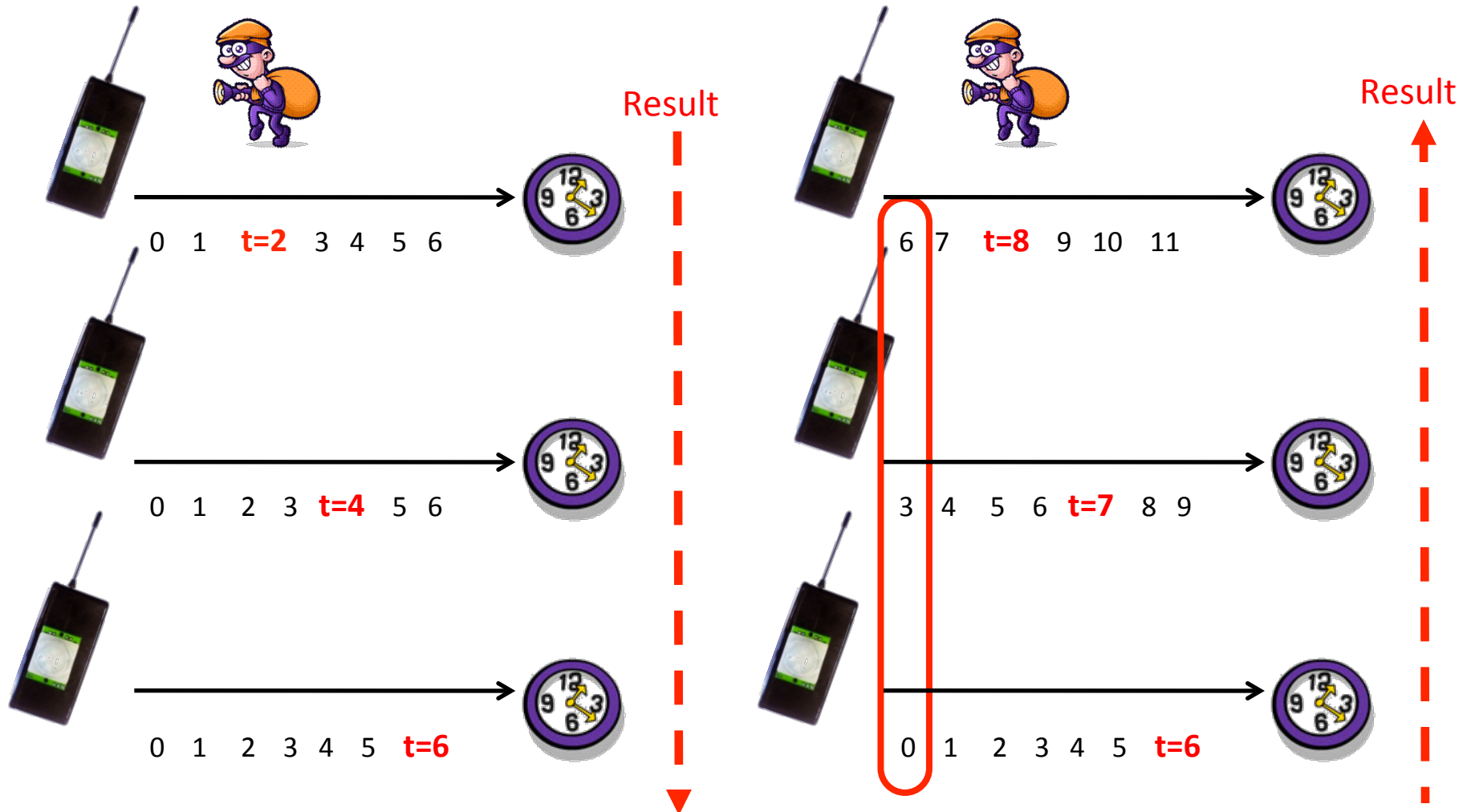- Conclusions

The need for clock synchronization

- Following movements
- Pinpointing events geographically
- TDMA radio scheduling
- Ordering sensor data
- Detecting duplicate events
- Coordinating sleep cycles
- …

Remember this guy?

Errors in clock synchronization

Result

0   1   **t=2**   3   4   5   6

0   1   2   3   **t=4**   5   6

0   1   2   3   4   5   **t=6**

Result

6   7   **t=8**   9   10   11

3   4   5   6   **t=7**   8   9

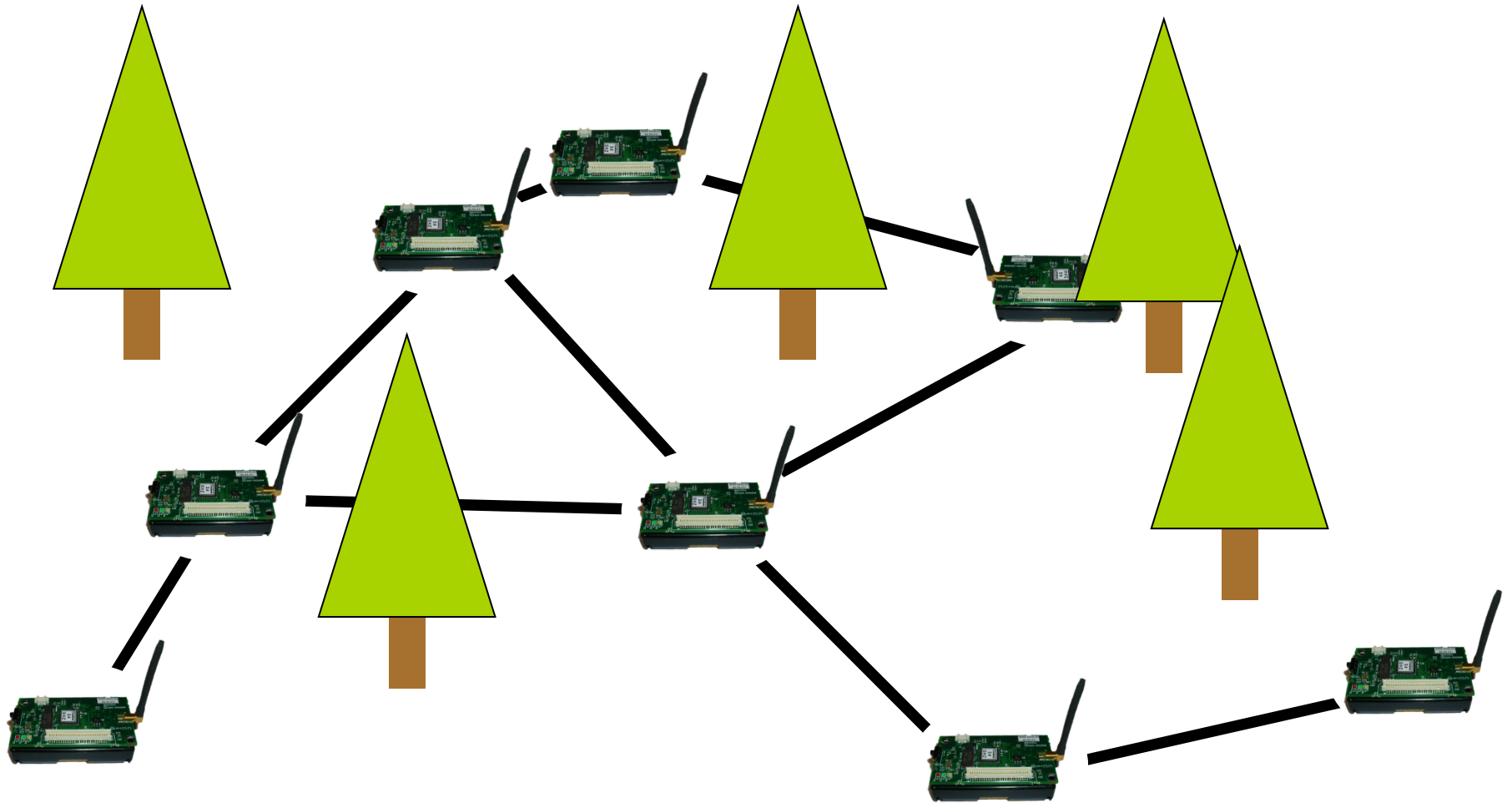0   1   2   3   4   5   **t=6**

Contributions

- Clock Synchronization
  - Secure
  - Self-stabilizing
- Deals with
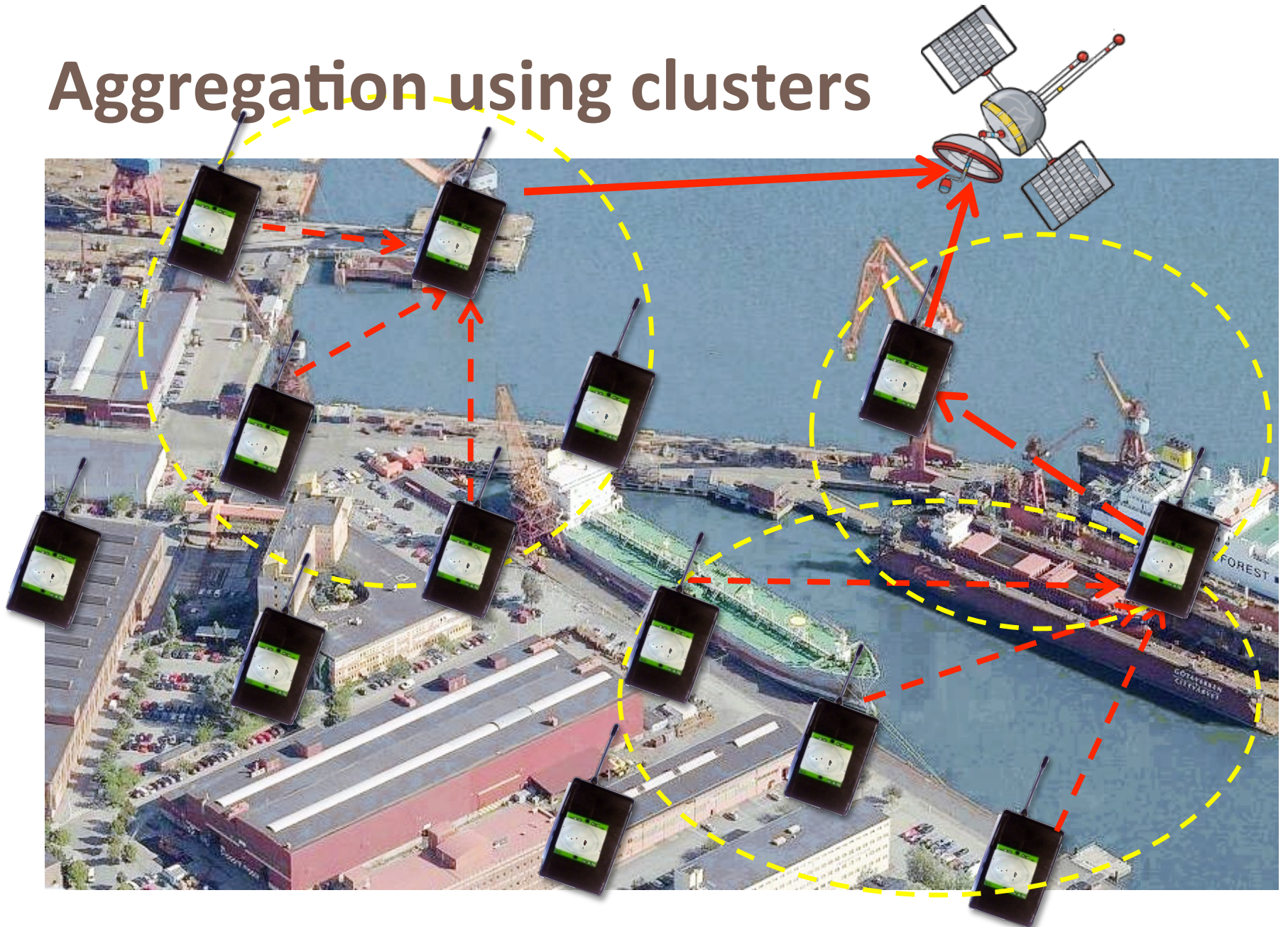 - Outside attacks
  - Compromised nodes

Talk outline

- Sensor networks
- Security in sensor networks
- Clock synchronization
- **Clustering**
- Conclusions

Clustering – organize ad-hoc networks

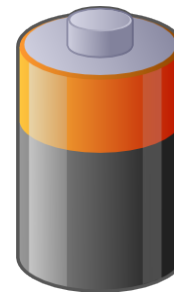# Aggregation using clusters
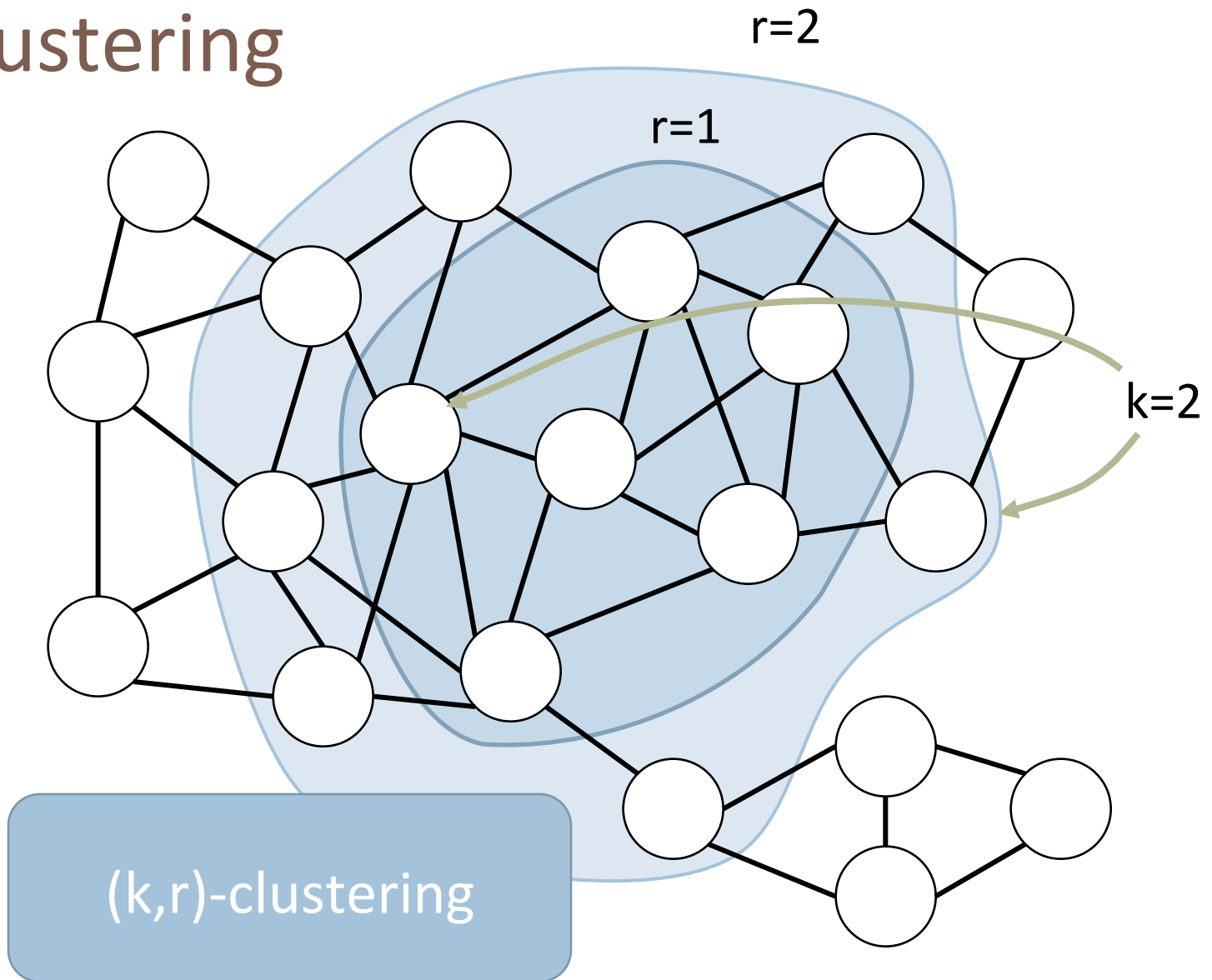
Uses of clustering

Backbones

Scaling

Routing

Saving power

Clustering

r=2

r=1

k=2

(k,r)-clustering

Contribution

- Clustering
  - Self-stabilizing
  - Provides redundancy
- Multiple cluster heads and multiple paths
  - Help withstand attacks
  - Increased fault tolerance

Talk outline

- Sensor networks
- Security in sensor networks
- Clock synchronization
- Clustering
- **Conclusions**

Conclusions

- Many possible civil security-related applications
  - Fault-tolerance and security is needed
  - Insider nodes are a serious threat

- We provide fundamental services
  - Clock synchronization
  - Clustering
  - Routing
  - Cryptography

Thank you for your attention!