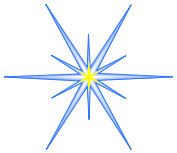
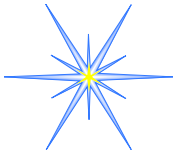


Advanced Topics in Cyber-Physical Systems

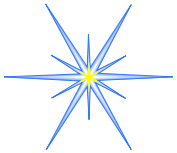
Jack Stankovic
BP America Professor
Department of Computer Science
University of Virginia
Fall 2011

University of Virginia



Outline (first 2 classes)

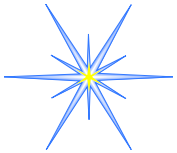
- Course Logistics/Goals
- Intro to Cyber Physical Systems (CPS)
  - Nothing less than the future!!!
- Motivating Exemplars of Required Research
- Proposed approach: *-aware solution



Lament from Industry

- …we can't hire students trained in the multi-disciplinary areas we require …

mainly control, SP, and CS



Class Structure

- Part I
  - Introduction/Background
- Part II
  - Medical Applications
  - Energy-Based Applications
- Part III
  - Run Time Validation
  - Anomaly Detection
  - Role of Control Theory

Reading Assignments

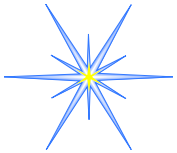
- Part I - Introduction
  - 2 background papers on CPS
- Part II - Applications
  - 7 papers on WH and BSN
  - 6 papers on Saving Energy
- Part III – Technology Topics
  - 4 papers on Runtime Validation
  - 2 papers on Anomaly Detection
  - 4 papers on Role of Control Theory

Grading

- *Selected* Reading Summaries – 25%
- Paper Presentation – 50%
- Class Participation – 25%

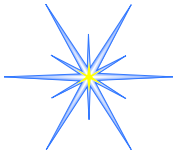
Course Goals

- Basis for improved CPS understanding and research
- Capability to simultaneously address multiple issues
- Significant exposure to advanced topics in a new research area



Prerequisites

- Recommended
  - Computer Networking
- Questions for Class
  - OS?
  - Computer Architecture?
  - Control Theory?
  - Real-time?
  - Sensors?
  - WSNs?



Intro - Outline

- What are Cyber Physical Systems?
- Exemplars of Required Research
  - Components
  - Lightweight Security
  - Robustness and Diversity
  - Systems of Systems
- *-aware solution approach

Acknowledgements/Info

- CPS Program (3 years in the making)
  - Core of about 10 people
  - Expanded to more than 30 researchers
  - Expanded to 100s of researchers

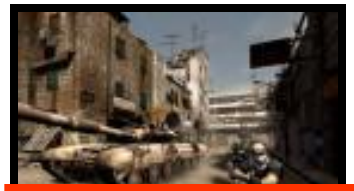
  - NSF CPS ($30,000,000 per year)
  - PCAST 2007 report: #1 priority for Federal Investment
  - Expanding to other agencies
  - European Union - $7B (ARTEMIS)

Definition

- CPS is the co-joining of computation and communication with physical processes.
- Functionality and salient system characteristics are realized through the coordination and interaction of networked physical and computational objects.
- CPS exhibits an intimate coupling between the cyber and physical that manifests itself from the nano world to large-scale wide-area systems of systems.

Computing in Physical Systems

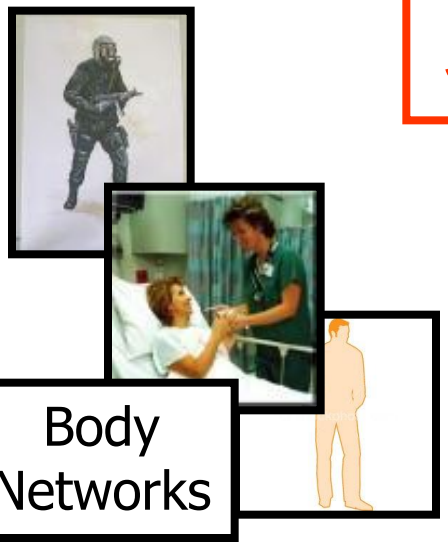
Environmental Networks



Road and Street Networks

dustrial etworks

Heterogeneous Wireless Networks with Sensors and Actuators



Body Networks

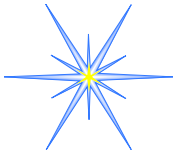
Vehicle Networks

ng Networks

University of Virginia

Important?

- US Auto - $500B in annual revenue
  - By 2015 40% of auto value in CPS
- Aerospace - $125B
- Medical – 20% of US economy by 2020
- Energy, infrastructures (electric power grid, defense, agriculture, …)



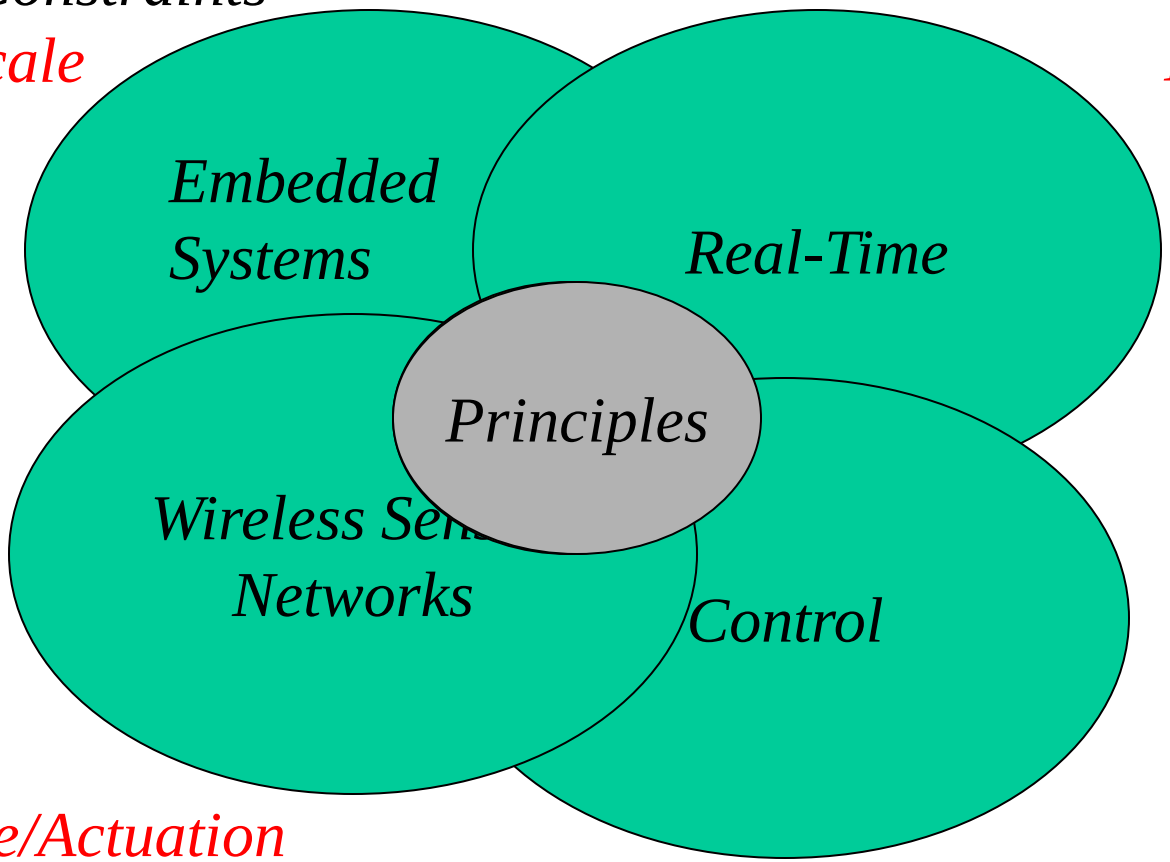
What is a CPS?

- Isn't is just an embedded system?
- Not the main question
- Simply parsing "CPS" -> Many systems are CPS, but that is not the issue
- REALLY INTERESTED IN
  - New research needed for the next generation of physical-cyber systems

Confluence of Key Areas

Cost
Form Factor
Severe Constraints
Small Scale
Closed

Scheduling
Fault Tolerance
Wired networks
Level of Uncertainty



Noisy C.
Sensing
Scale
Real-Time/Actuation
Open

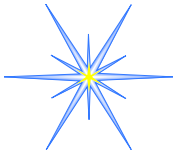
Linear
Adaptive
Distributed
Decentralized
Open
Human Models

What's New

- Scale
- Systems of systems
- Confluence of physical, wireless and computing
- Human Participation in Loop

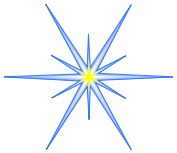
- Open

Level of Uncertainty



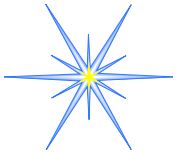
Question

- Define "open"



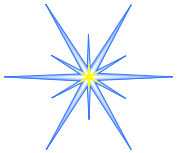
CPS

- Are CPS simply embedded systems on steroids?
  - Interact with the physical world
  - Constraints on cpu, power, cost, memory, bandwidth, …
  - Control actuators



- Is the Internet just a LAN on steroids?

- Confluence of the right technologies at the right time can result in
  - Fundamental paradigm shift
  - Totally new systems
  - Revolutionize business, science, entertainment, …
  - Transform how we interact with the physical world



More Areas

- Signal Processing
- AI
- Data Mining
- Robotics
- Security and Privacy
- Formal Methods
- Software Engineering

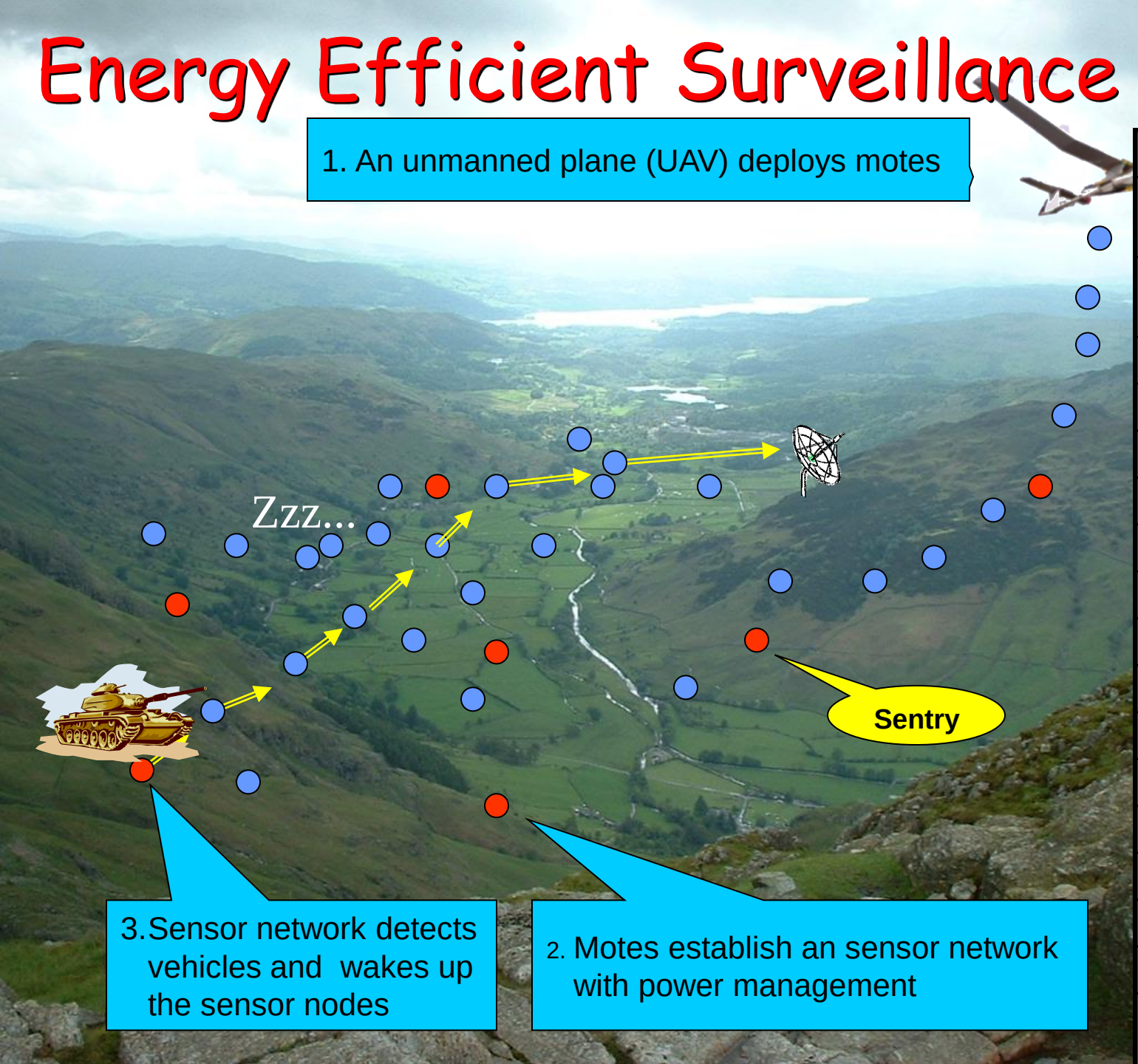
Physical Affects Cyber

- Can we develop a science?

- Examples?

Energy Efficient Surveillance System

1. An unmanned plane (UAV) deploys motes



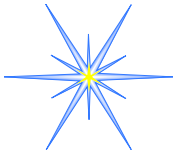
3. Sensor network detects vehicles and wakes up the sensor nodes

2. Motes establish an sensor network with power management

- Ad-Hoc Network
- Neighbor Discovery
- Time Synchronization
- Parameterization
- Sentry Selection
- Coordinate Grid
- Data Aggregation
- Data Streaming
- Group Management
- Leader Election
- Localization
- Network Monitor
- Power management
- Reconfiguration
- Reliable MAC
- Leader Migration
- Scheduling
- State Synchronization

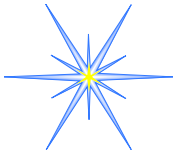
What Physical Things Affect the Cyber?

- In the sensing?
- In the wireless?
- In the environment?



Tracking Example (1)

- Sensing:
  - Magnetic sensor takes 35 ms to stabilize
    - affects real-time analysis
    - affects sleep/wakeup logic
  - Physical properties of targets affect algorithms and time to process (uncertainty fundamental)
    - Use shape, engine noise, …
    - Environmental factors must be addressed such as wind, obstacles, …



Tracking Example (2)

- Sensor Fusion:
  - Sensor fusion to avoid false alarms
    - power management may have sensors in sleep state (affects fusion algorithms and real-time analysis)
  - Location of nodes, target properties and environmental conditions affect fusion algorithms
    - Target itself might block messages needed for fusion algorithms

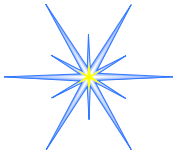
Tracking Example (3)

- Wireless:
  - Missing and delayed control signals alters FC loops; impossibility results for hard real-time guarantees *(new notions of guarantees)*
- Humans:
  - Don't follow nice trajectories; active avoidance in tracking examples
  - Social models, human models

Realistic (Integrated) Solutions

- CPS must tolerate
  - Failures
  - Noise
  - Uncertainty
  - Imprecision
  - Security attacks
  - Lack of perfect synchrony
  - Disconnectedness
  - Scale
  - Openness
  - Increasing complexity
  - Heterogeneity

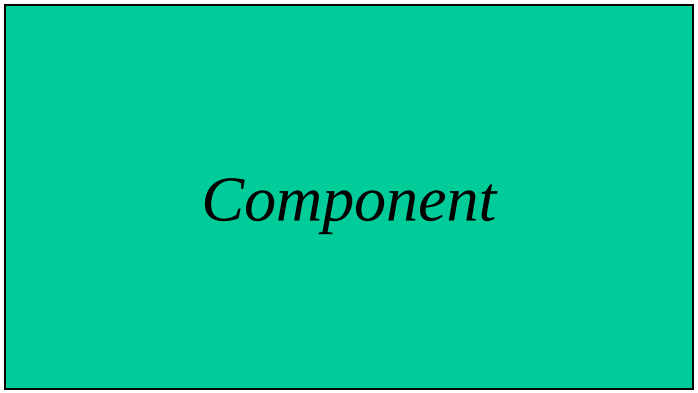
ROBUSTNESS



Research Ideas/Exemplars

1. New Components/Compositional Theory
2. Lightweight, Adaptive, Reactive Security
3. Robustness and Diversity
4. Systems of Systems

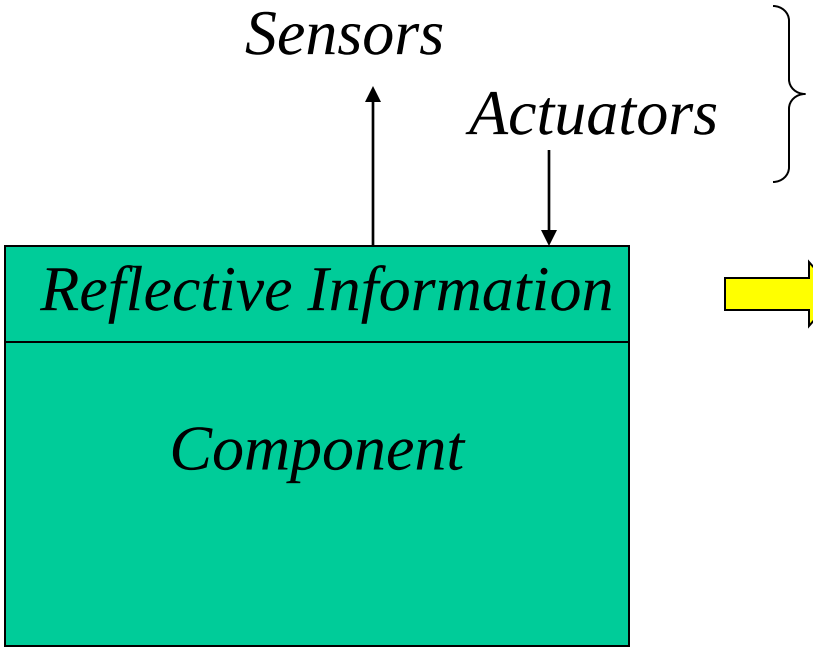
Component-Based (today - mostly)



Reuse
Modularity
Portability
Reconfigure

Beginning to consider performance

Component-Based (Tomorrow)

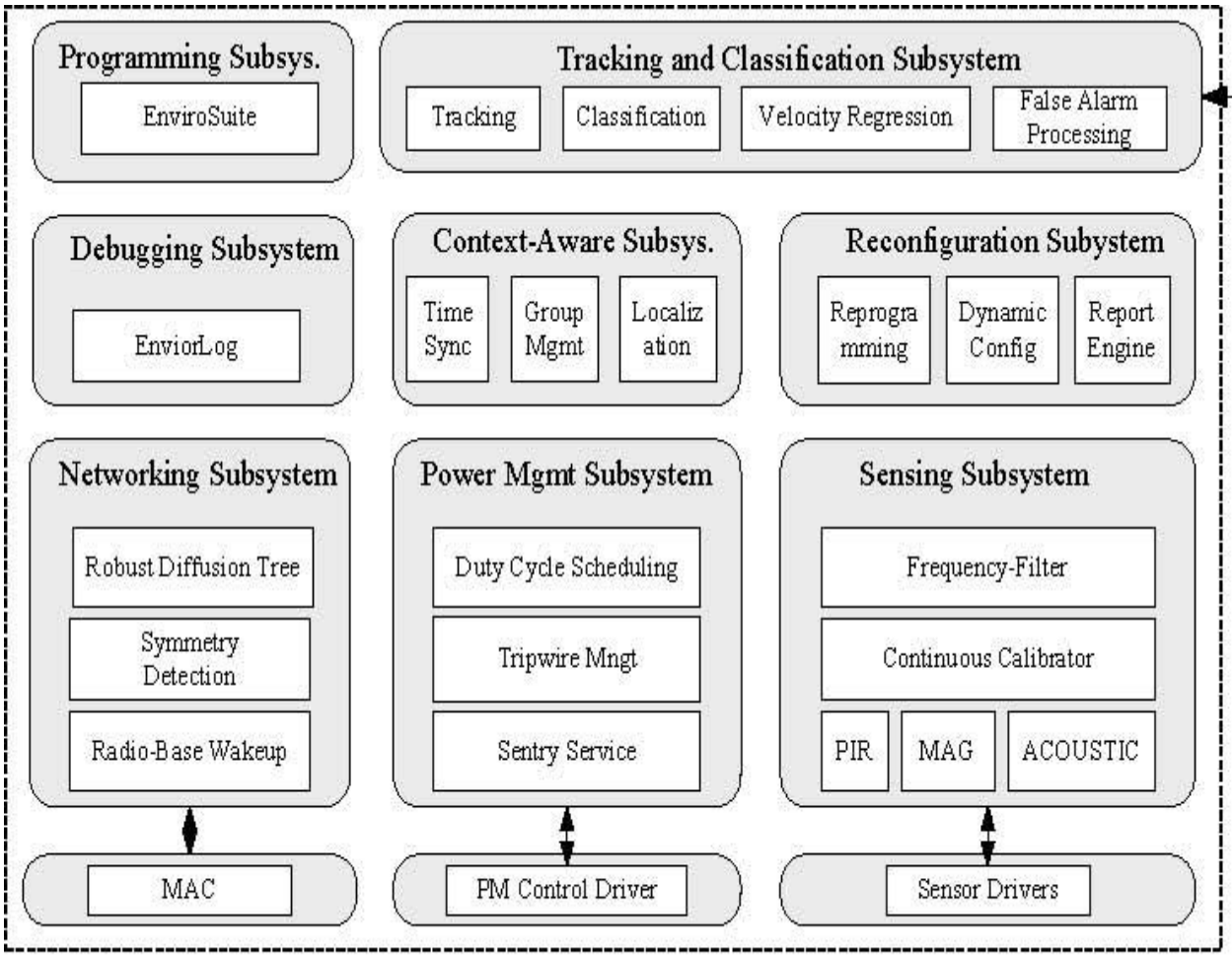


Support for control

Support for

- *cross cutting performance*
- *security*
- *mobility*
- *dependability*
- *costs*
- *real-time*
- *power*
- *dynamics*
- *openness*

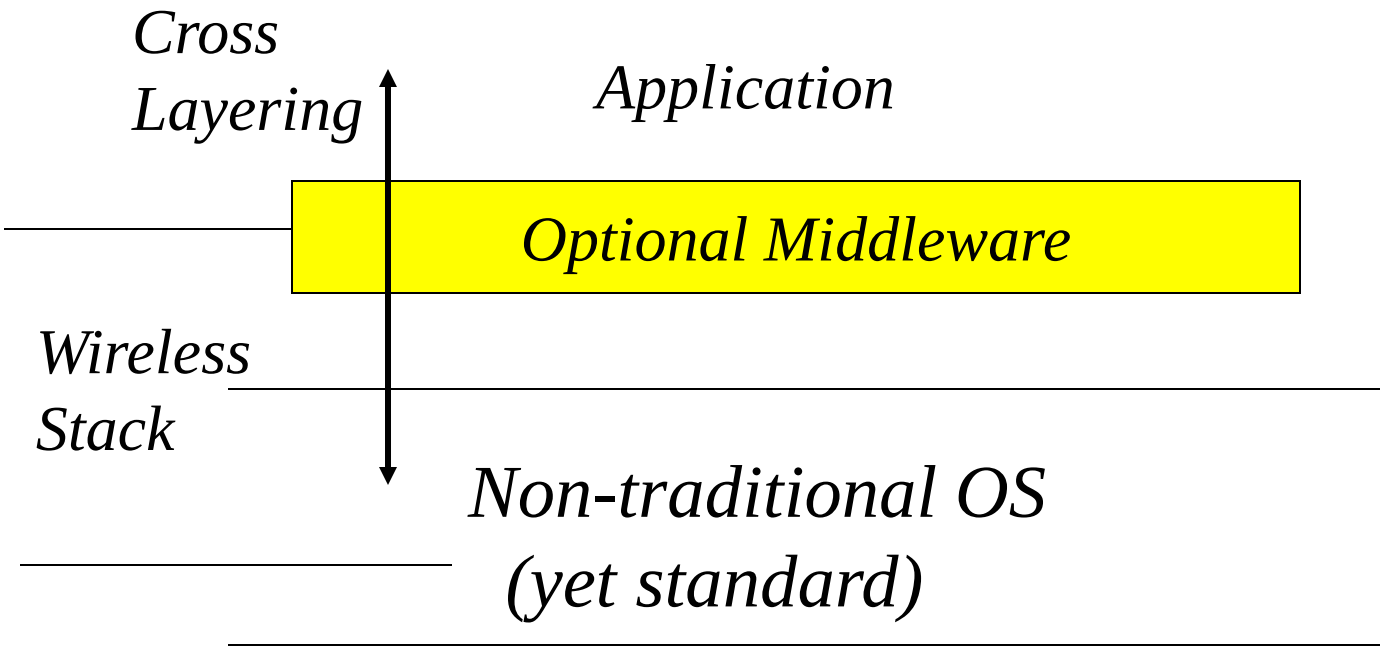
Component Architecture



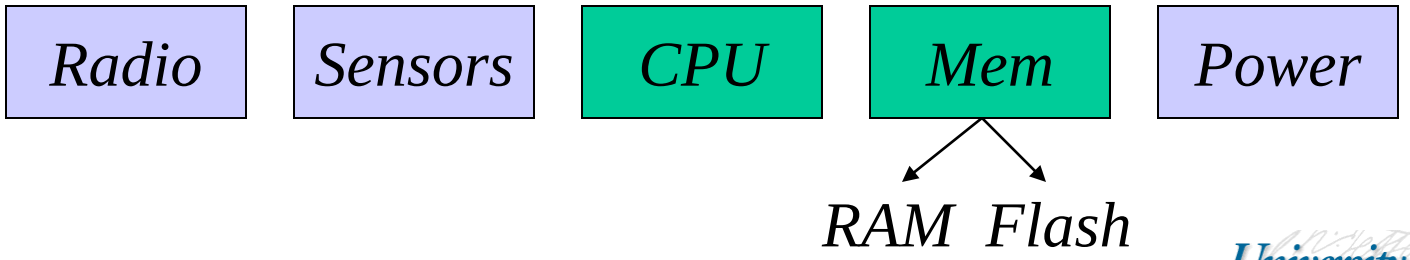
User Interface & Control Subsystem

University of Virginia

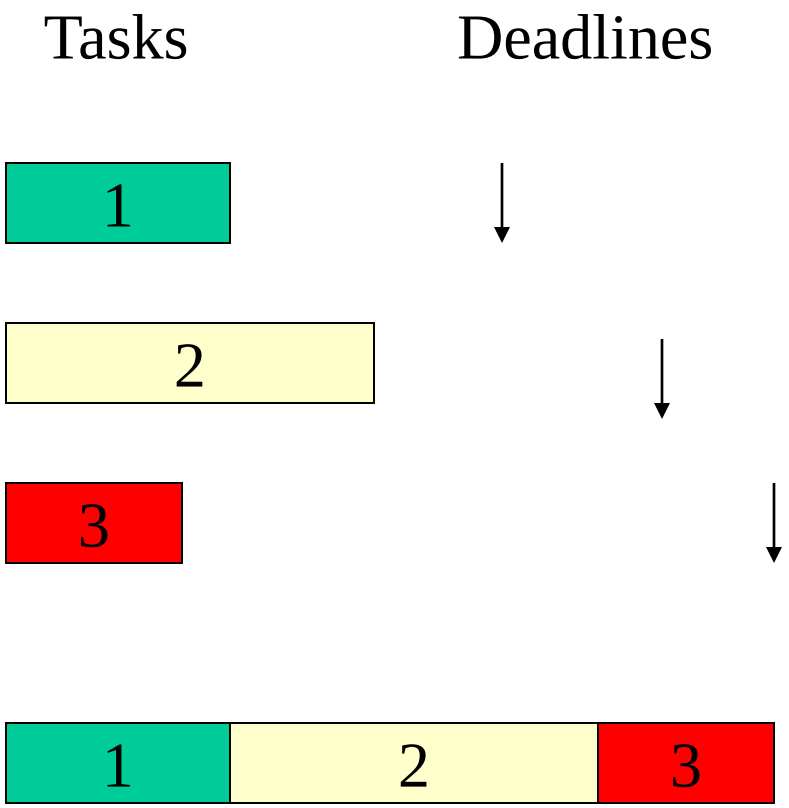
Component Architecture 2



Cyber Physical Hardware Abstraction Layer



Tasks in Architecture
Robust Scheduling



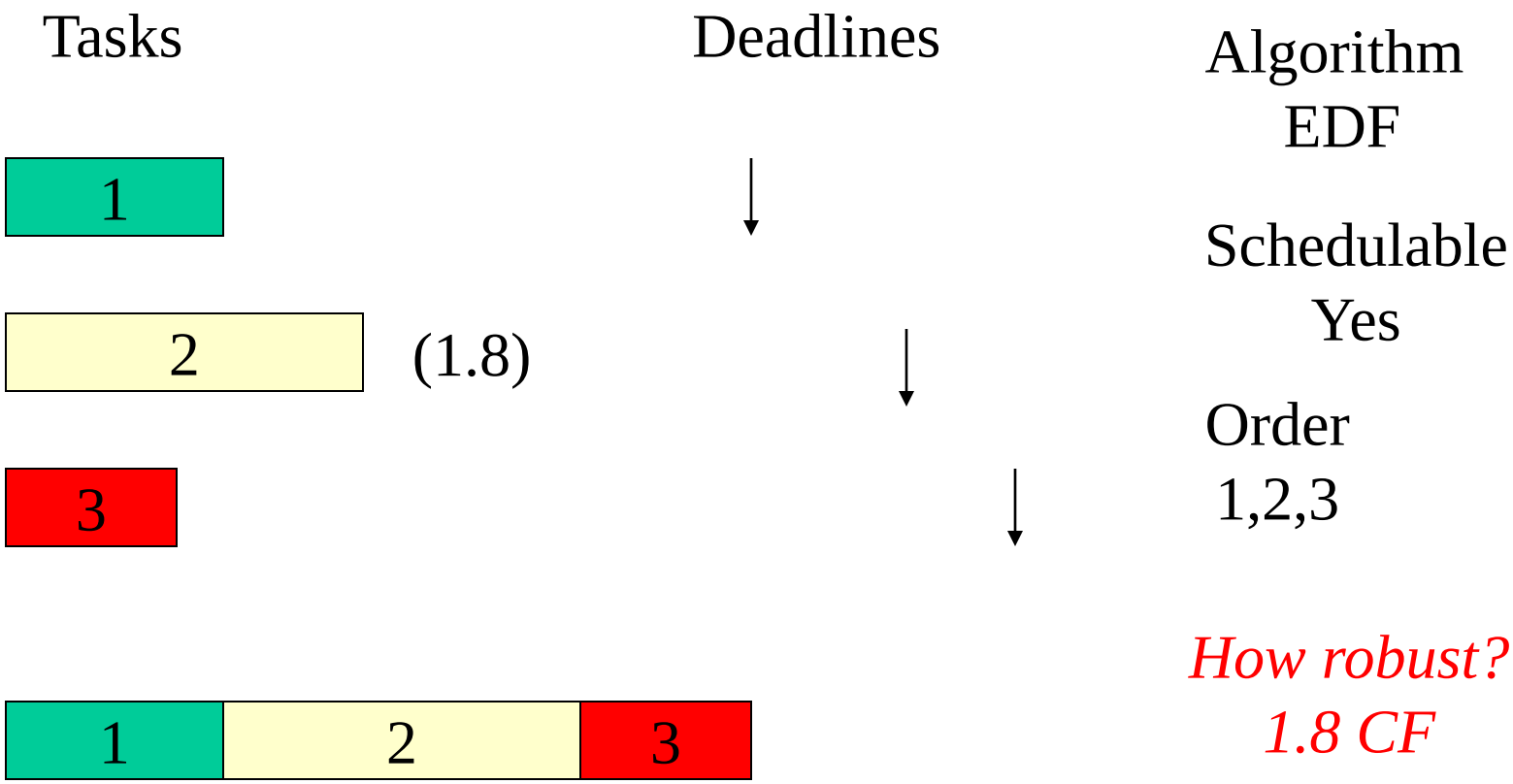
Algorithm
EDF

Schedulable
Yes

Order
1,2,3

How robust?
CF=1

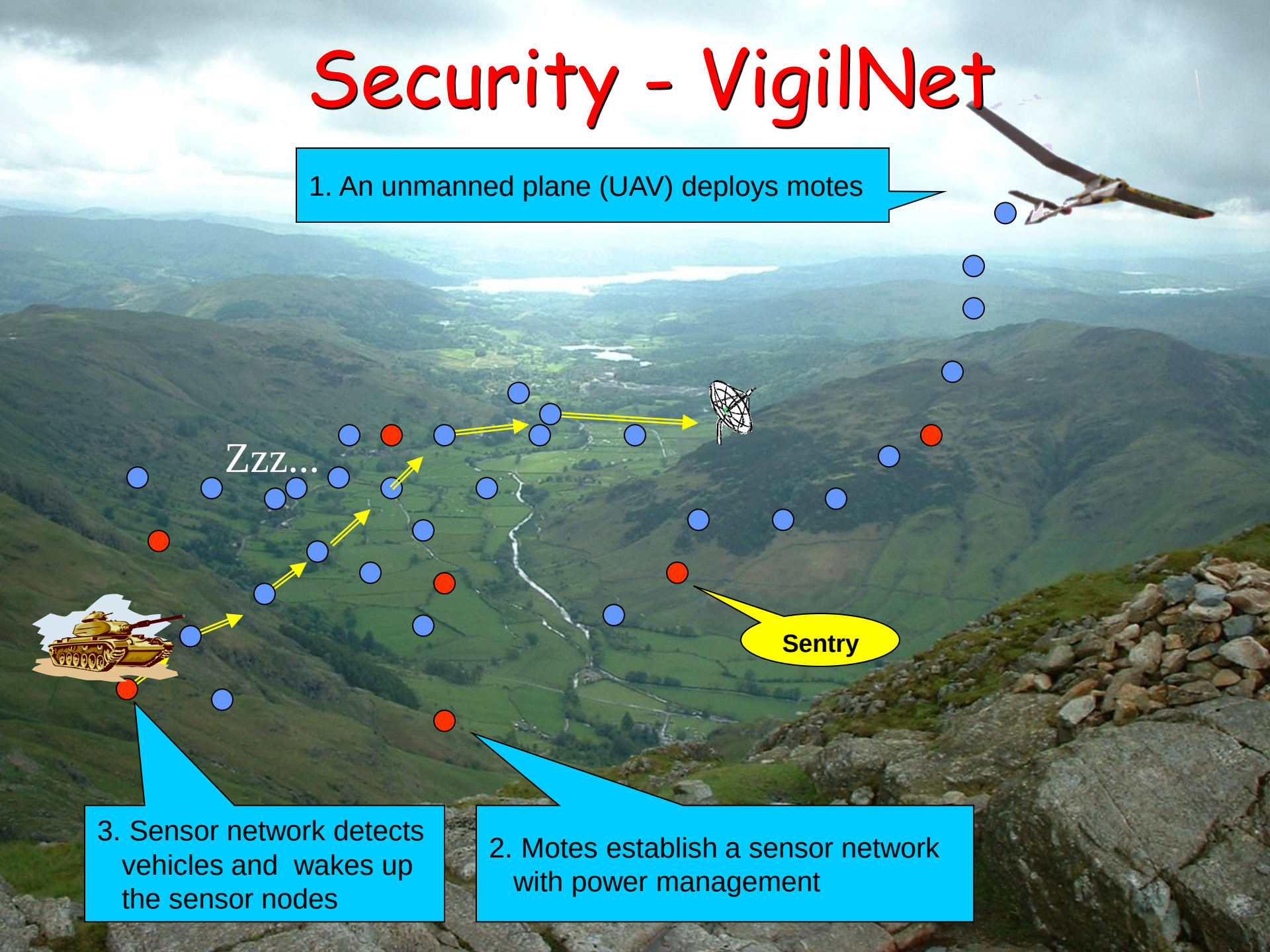
Robust Scheduling For Real World CPS



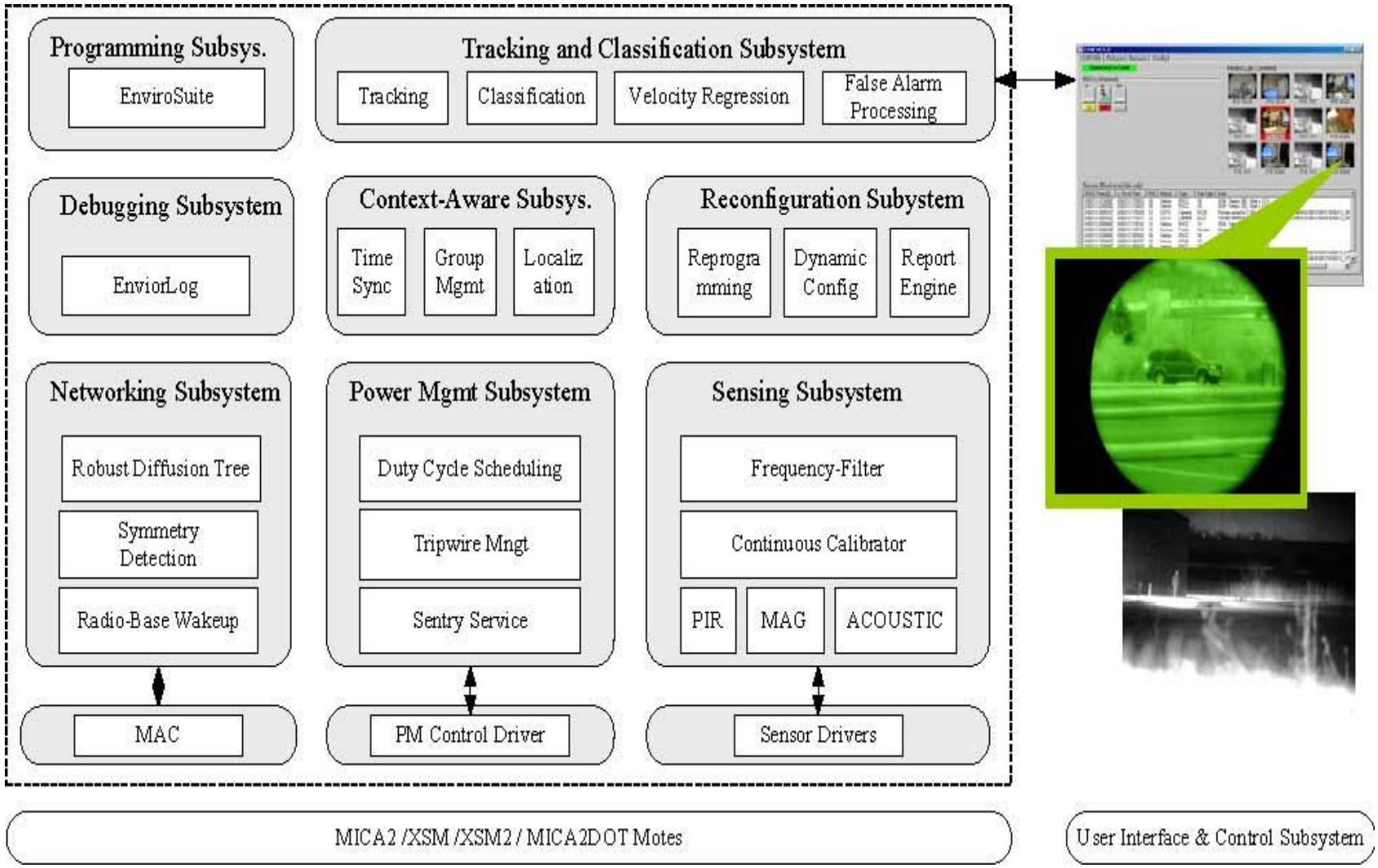
Required

- Robust, Real-Time, Dynamic, Open, Heterogeneous Compositional Theory
  - Based on underlying physical realities
  - Real-Time scheduling is dynamic (based on current instances of CPS constraints)

Security - VigilNet



VigilNet Architecture

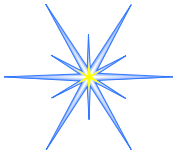


Security Issues

- Every one of the 30 services can be attacked
- Too expensive to make every service attack-proof
- Attacks will evolve anyway
- Cannot collect, re-program, and re-deploy

MICAz mote:

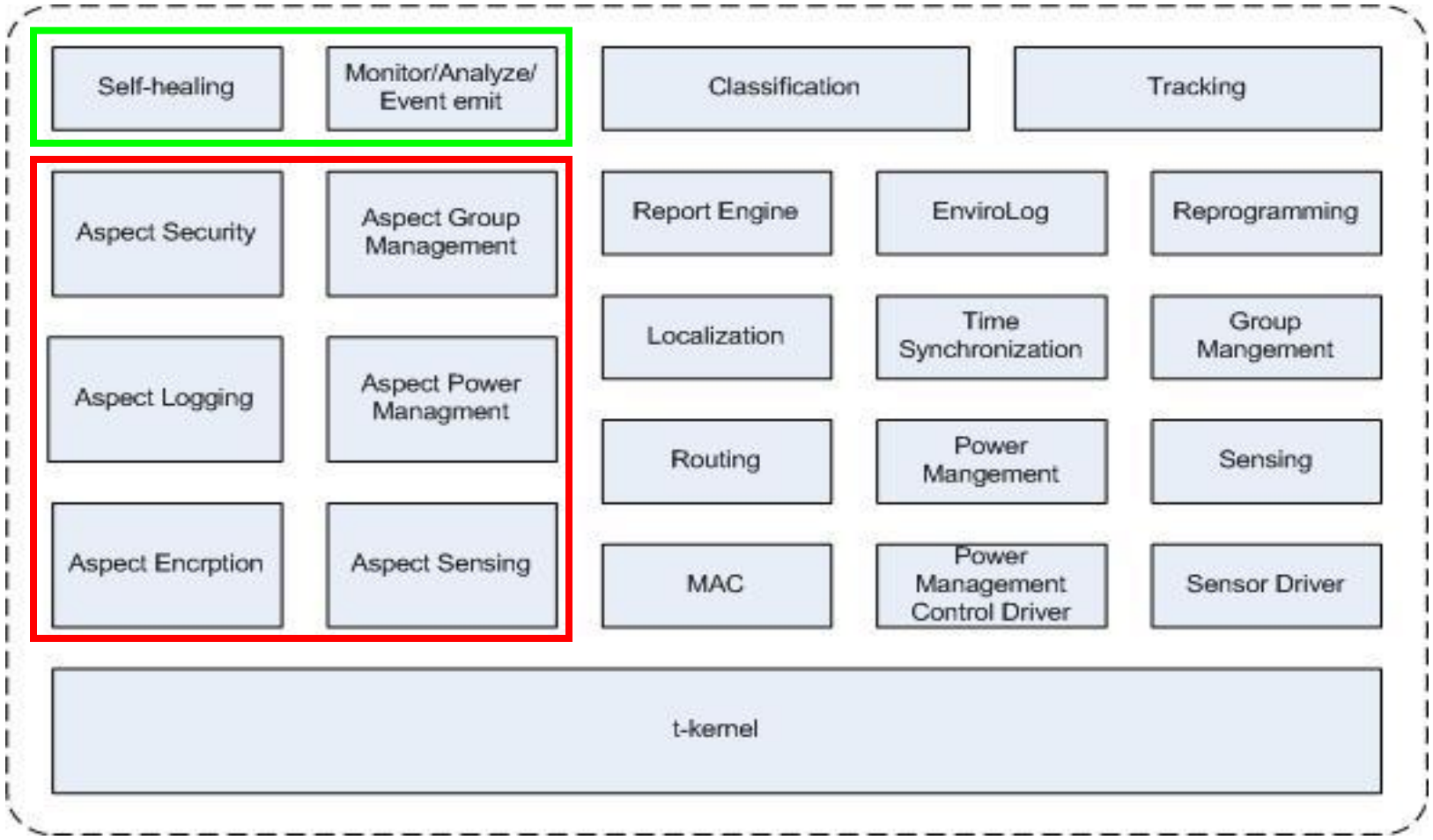
8 MHz 8-bit uP
128 MB code
4 KB data mem
250 Kbps radio



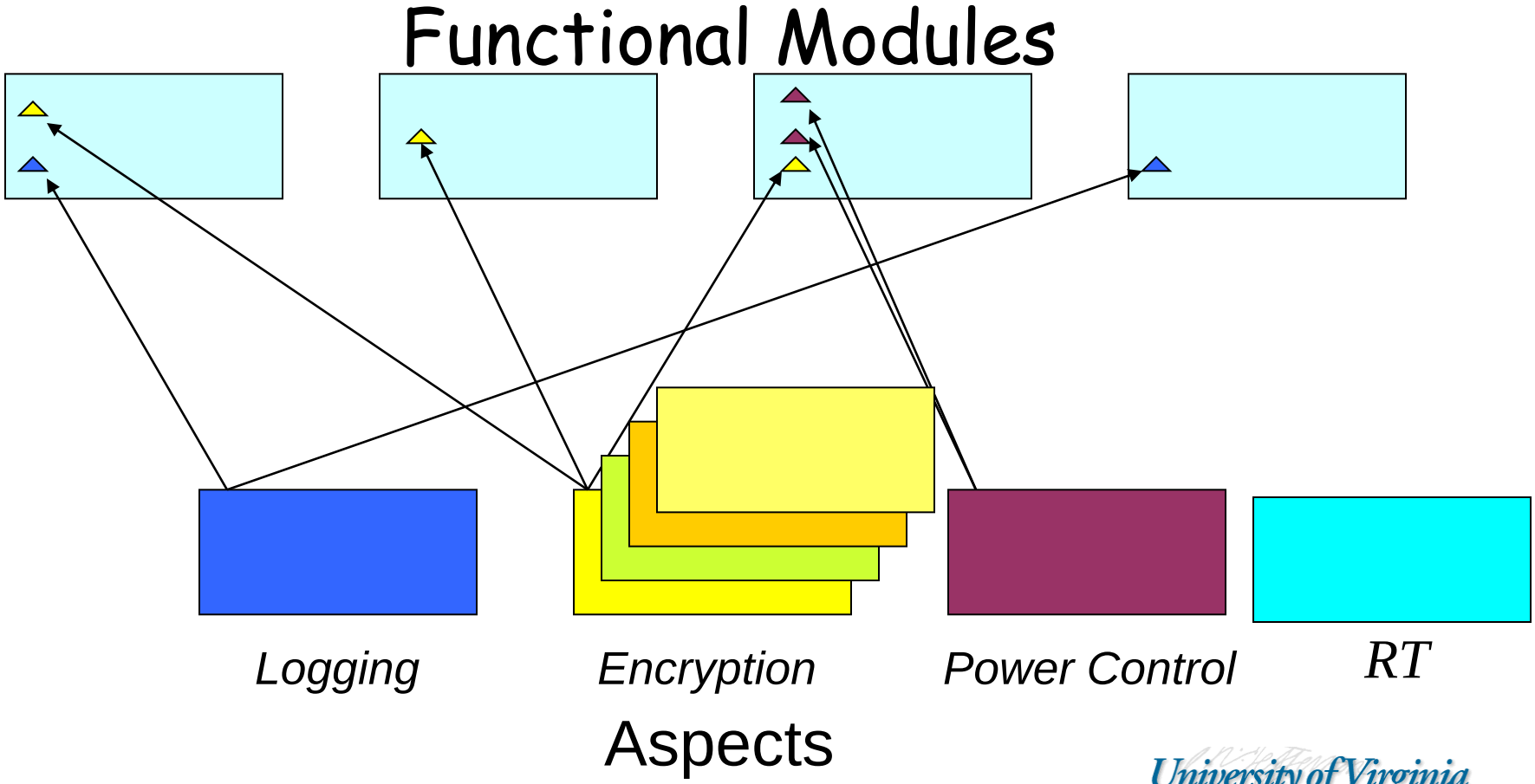
Security Approach

- Operate in the presence of security attacks
  - Robust decentralized protocols
  - Runtime control of security vs. performance tradeoffs
- Self-healing architecture
- Evolve to new, unanticipated attacks
  - Recall – open system!
- Lightweight solutions required due to severe constraints

Self-Healing Architecture



Aspect Oriented Programming (AOP)

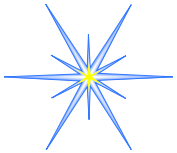


SIGF: Secure Routing

- The SIGF family provides incremental steps between stateless and shared-state protocols.

Protocol	General Approach	Corruption	Wormhole	HELLO flood	Black hole	Sybil	Replay DoS
IGF	Dynamic Binding	☑	☑	☑	–	–	–
SIGF-0	Nondeterminism	☑	☑	☑	☑	–	–
SIGF-1	Local Reputation	☑	☑	☑	☑	☑	–
SIGF-2	Cryptography	☑	☑	☑	☑	☑	☑

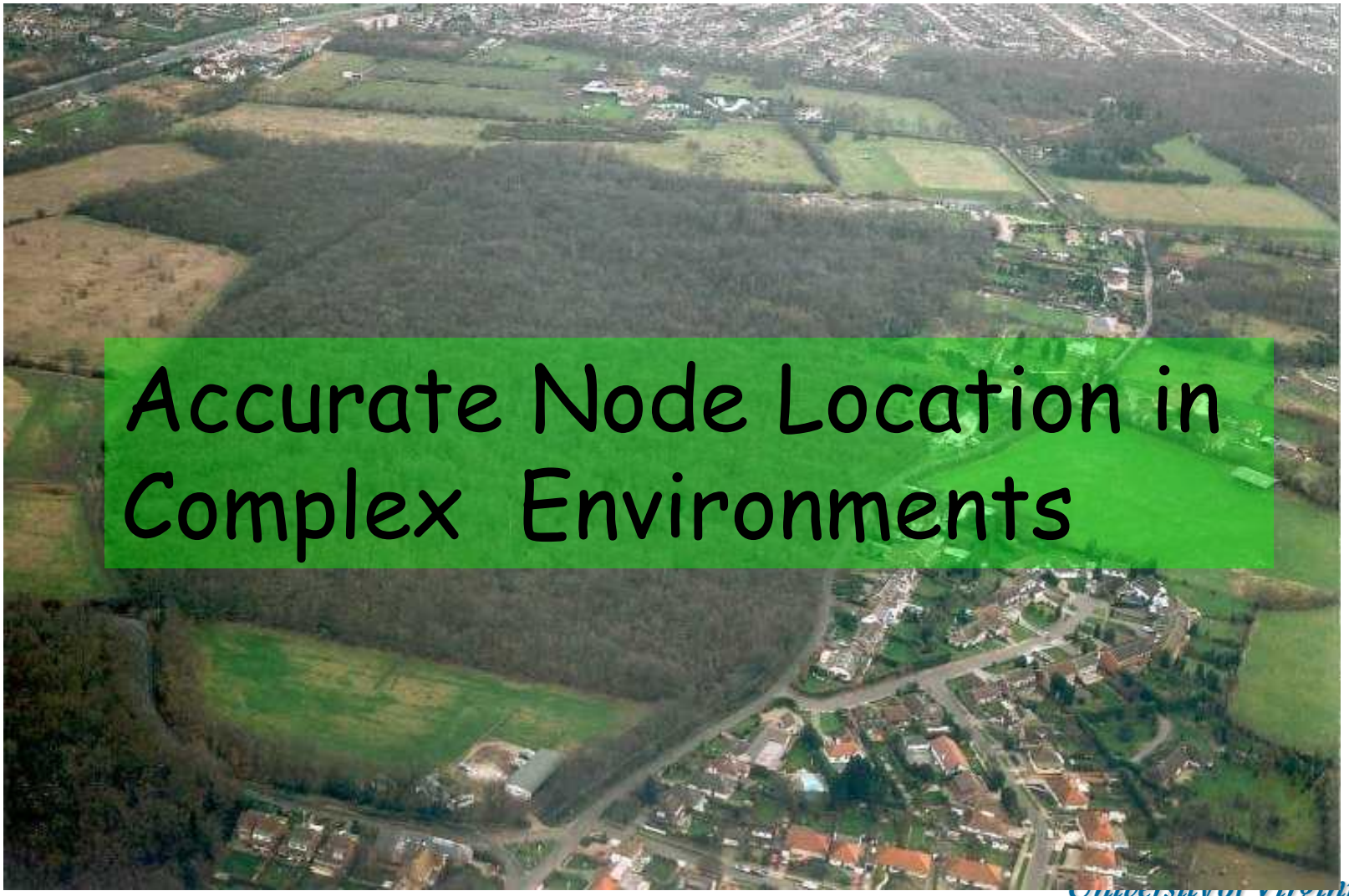
- SIGF allows efficient operation when no attacks are present, and good enough security when they are.



Robustness and Diversity

- Good for security
- Good for real world systems
- Good for uncertainties of physical interactions

Example Problem

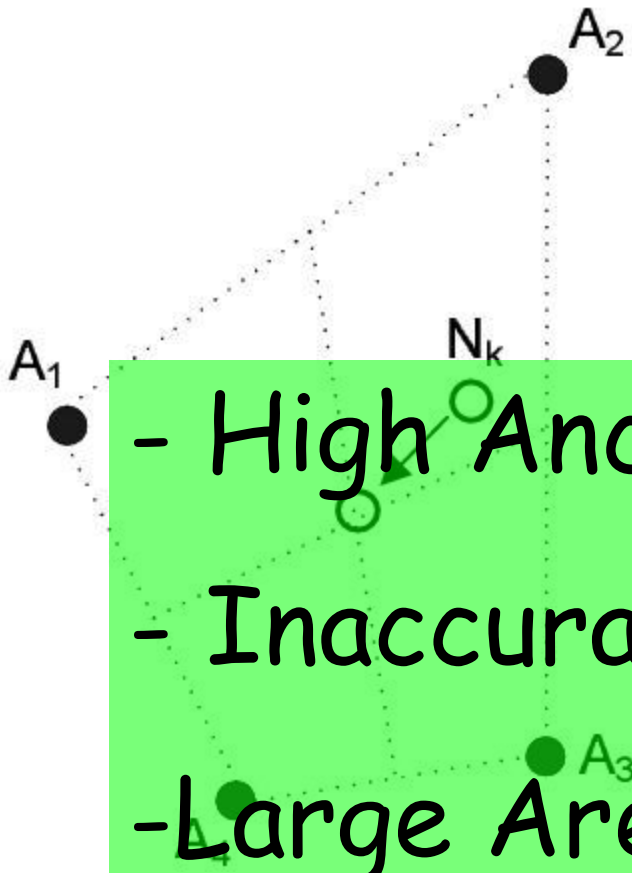


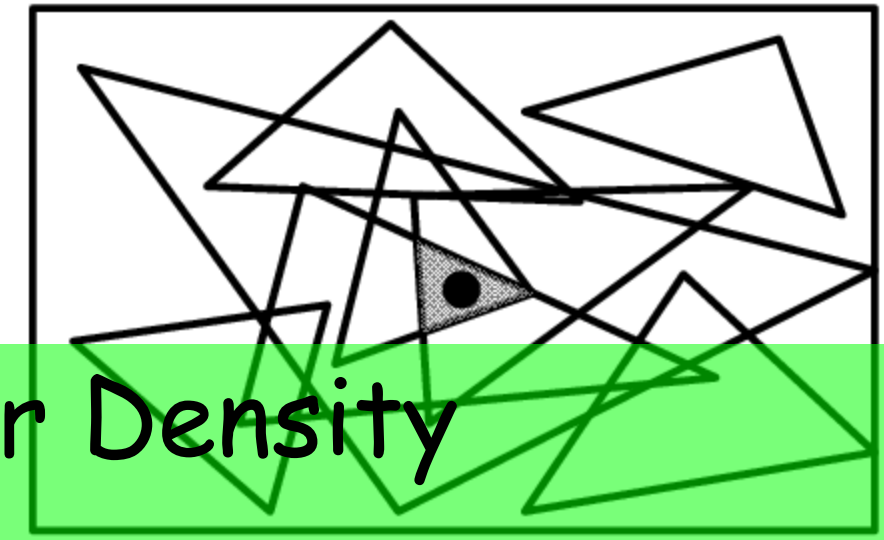
GPS

Range Free

Centroid

APIT

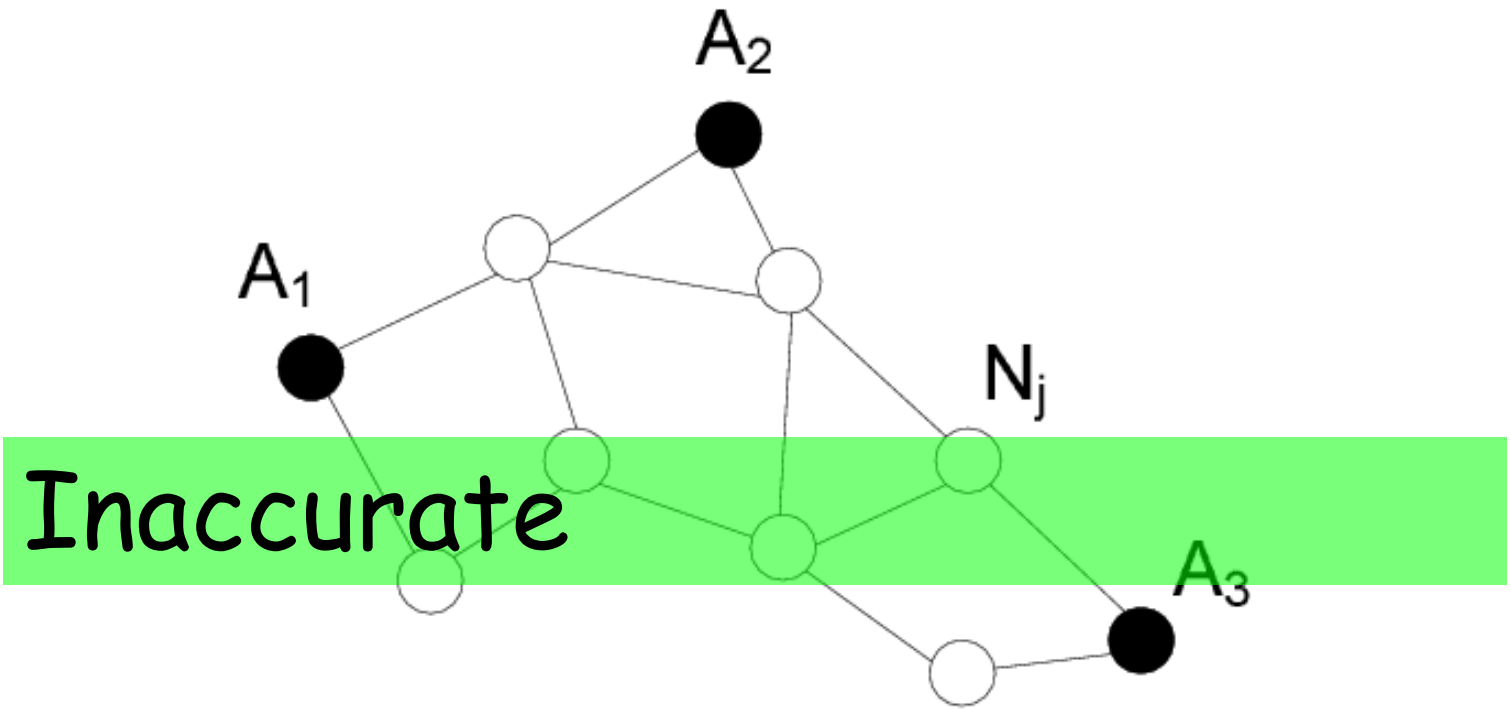




- High Anchor Density
- Inaccurate
- Large Areas without anchors

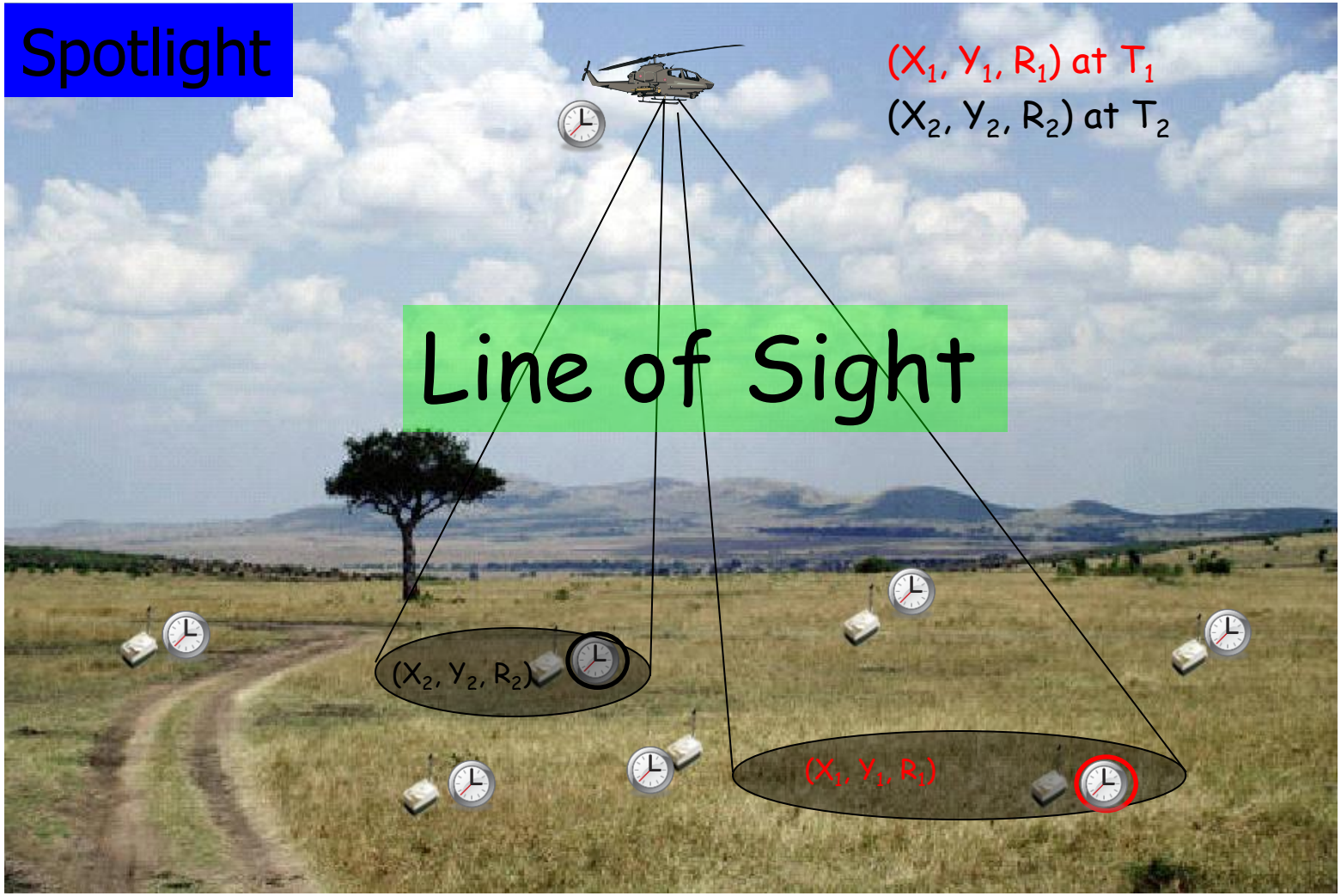
Range Free

DV-Hop

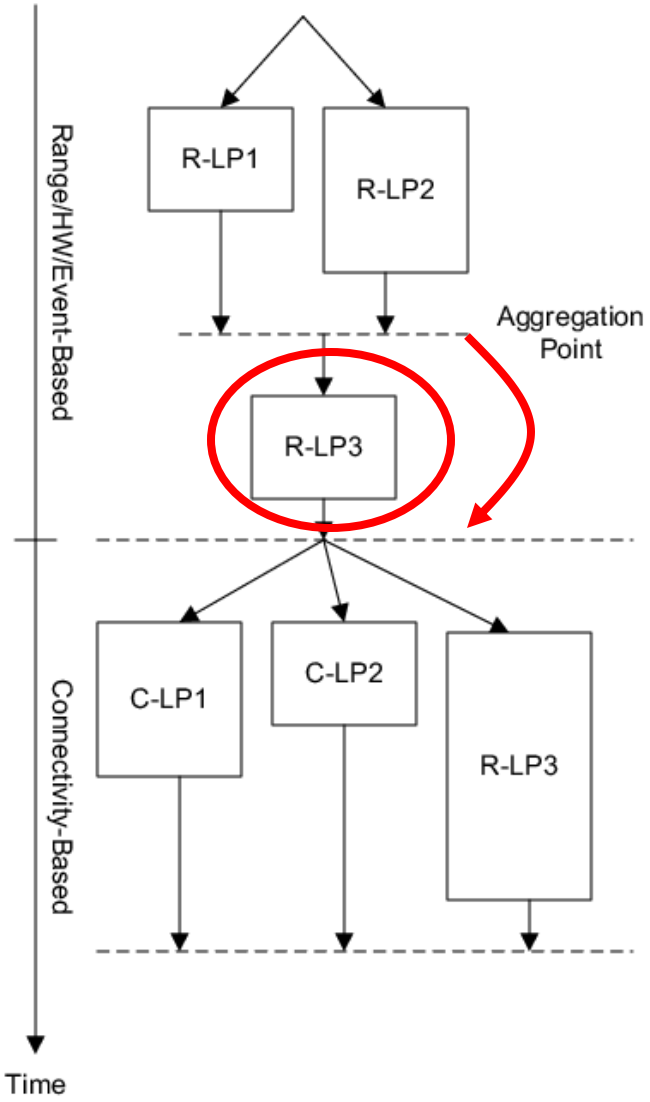


Inaccurate

Low Cost - Accurate



Hierarchical Framework

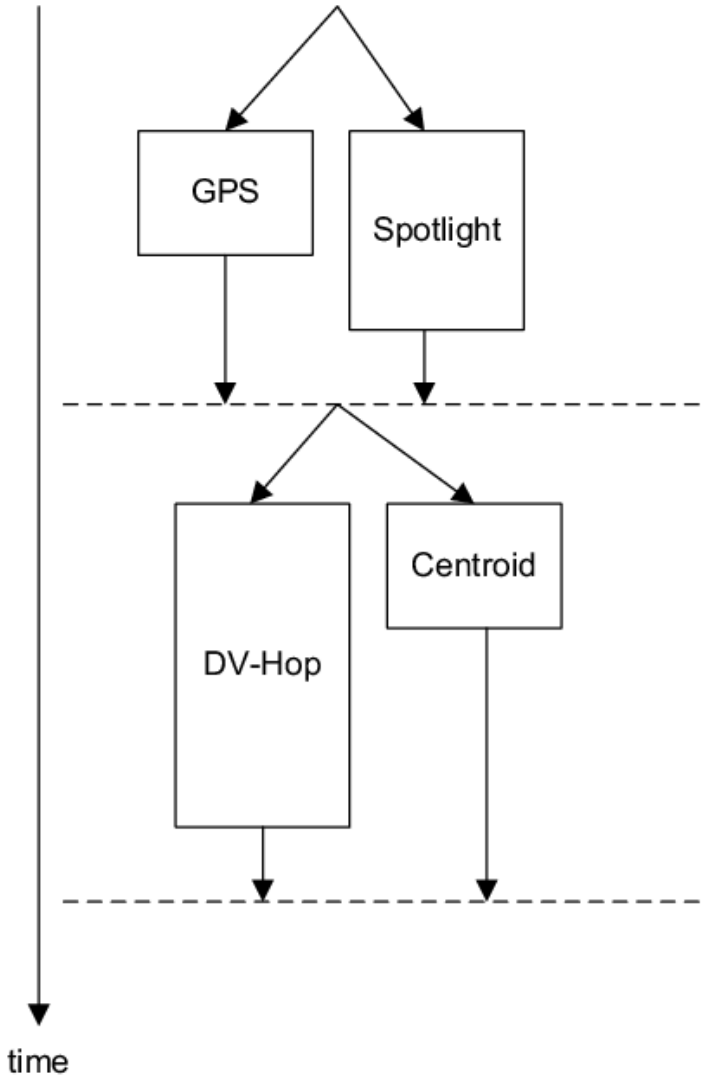


- Choose best / Weighted average
- If not localized – try another algorithm
- All nodes have a location at this point.

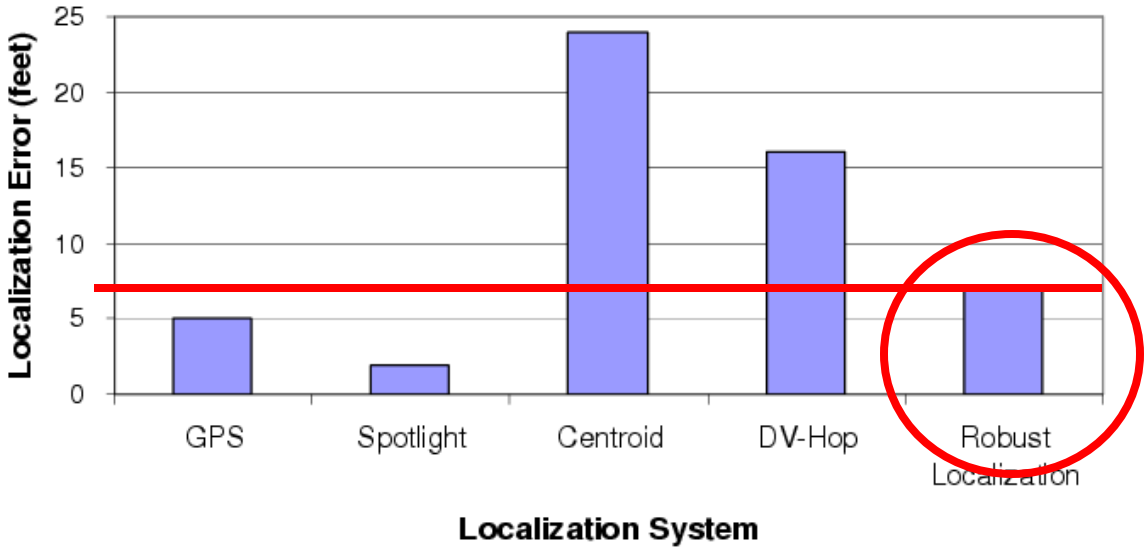
Evaluation

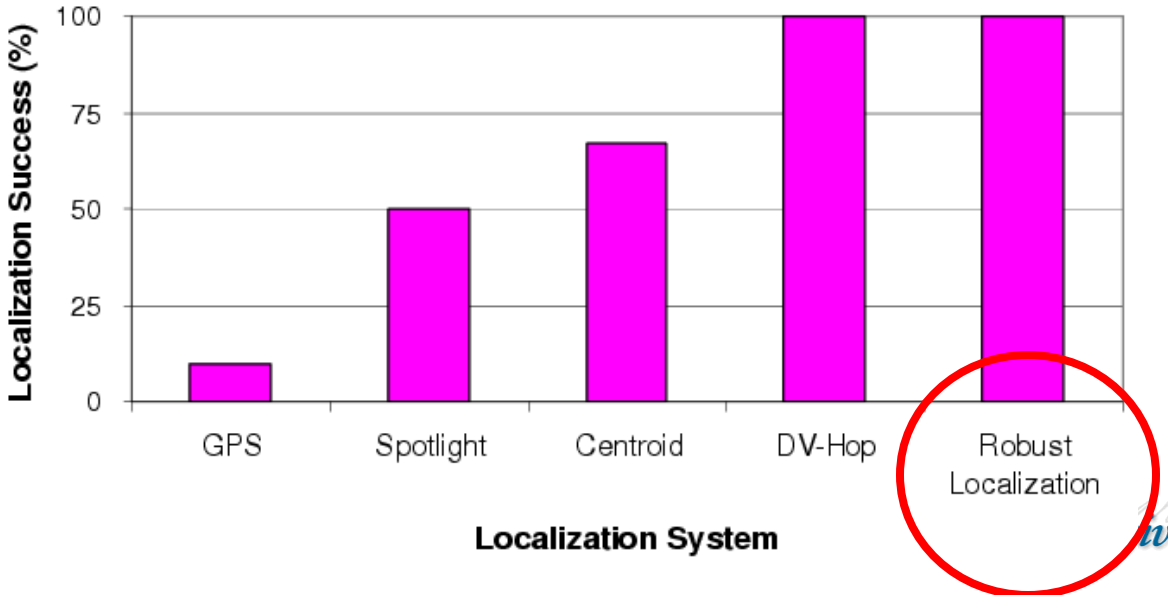
- TOSSIM
  - 400 nodes in 300x300ft2
  - 200x200ft^2 obstructed area
  - 50ft radio range
  - 10% nodes have GPS
  - 15% nodes in open area can't be localized

Evaluation



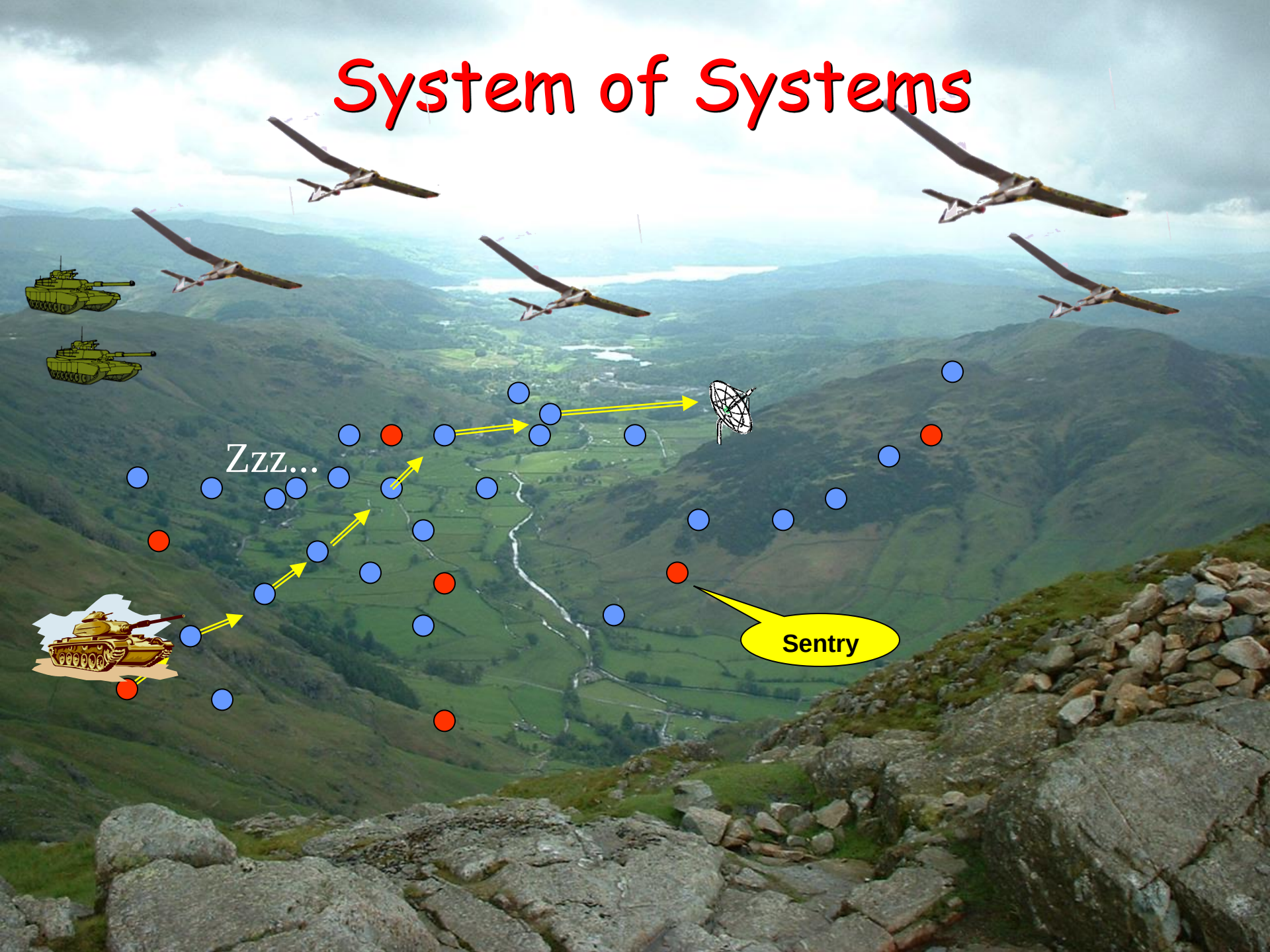
Evaluation

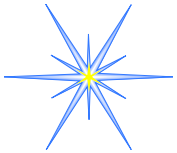




All nodes are localized

System of Systems

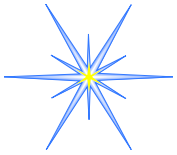




Systems of Systems

- Example of Openness

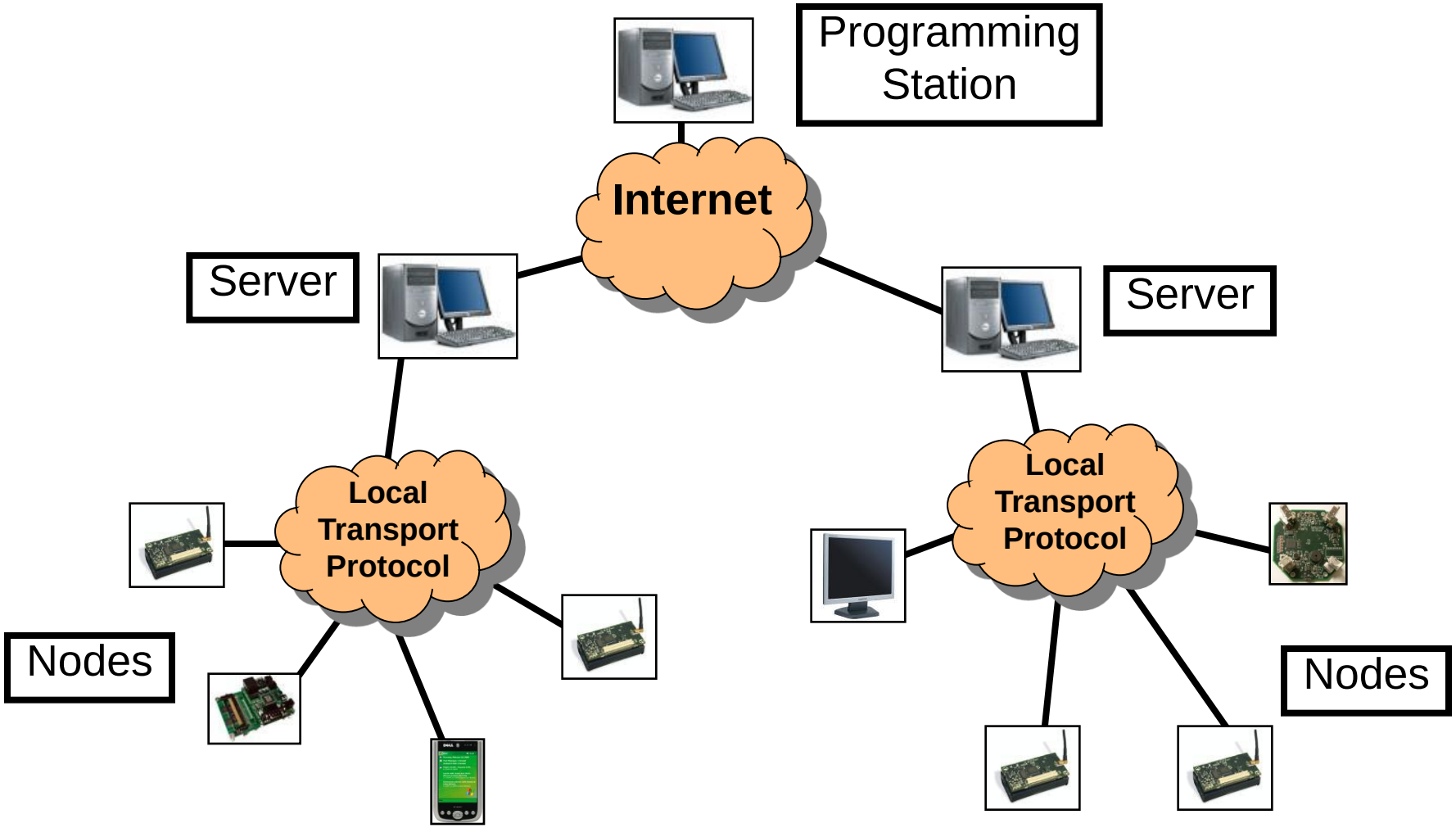
- Control loops across systems
- RT constraints across systems
- Human Participation



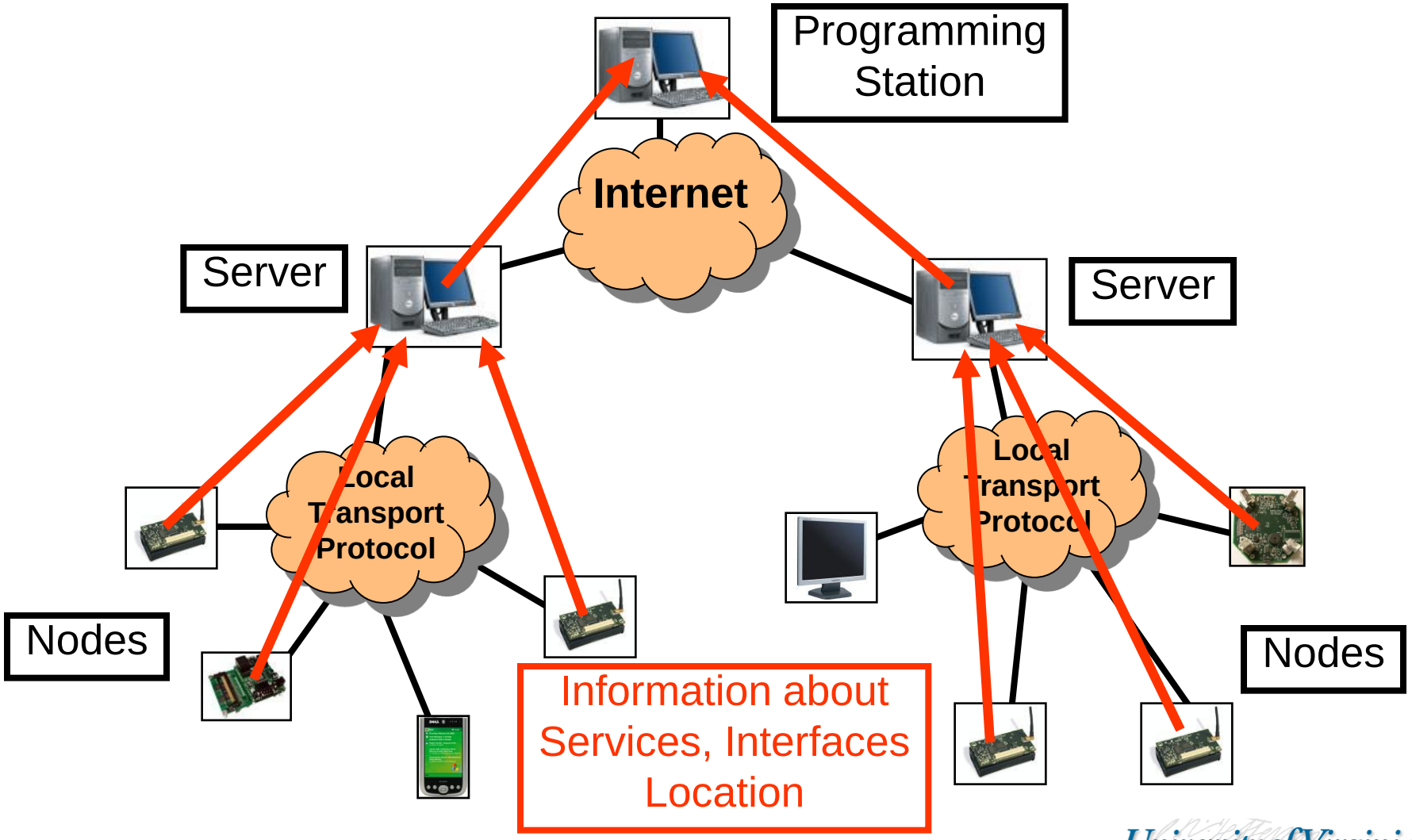
Adaptive/Decentralized Control

- Missing messages
- Delayed messages
- Wrong messages
- Real-time constraints

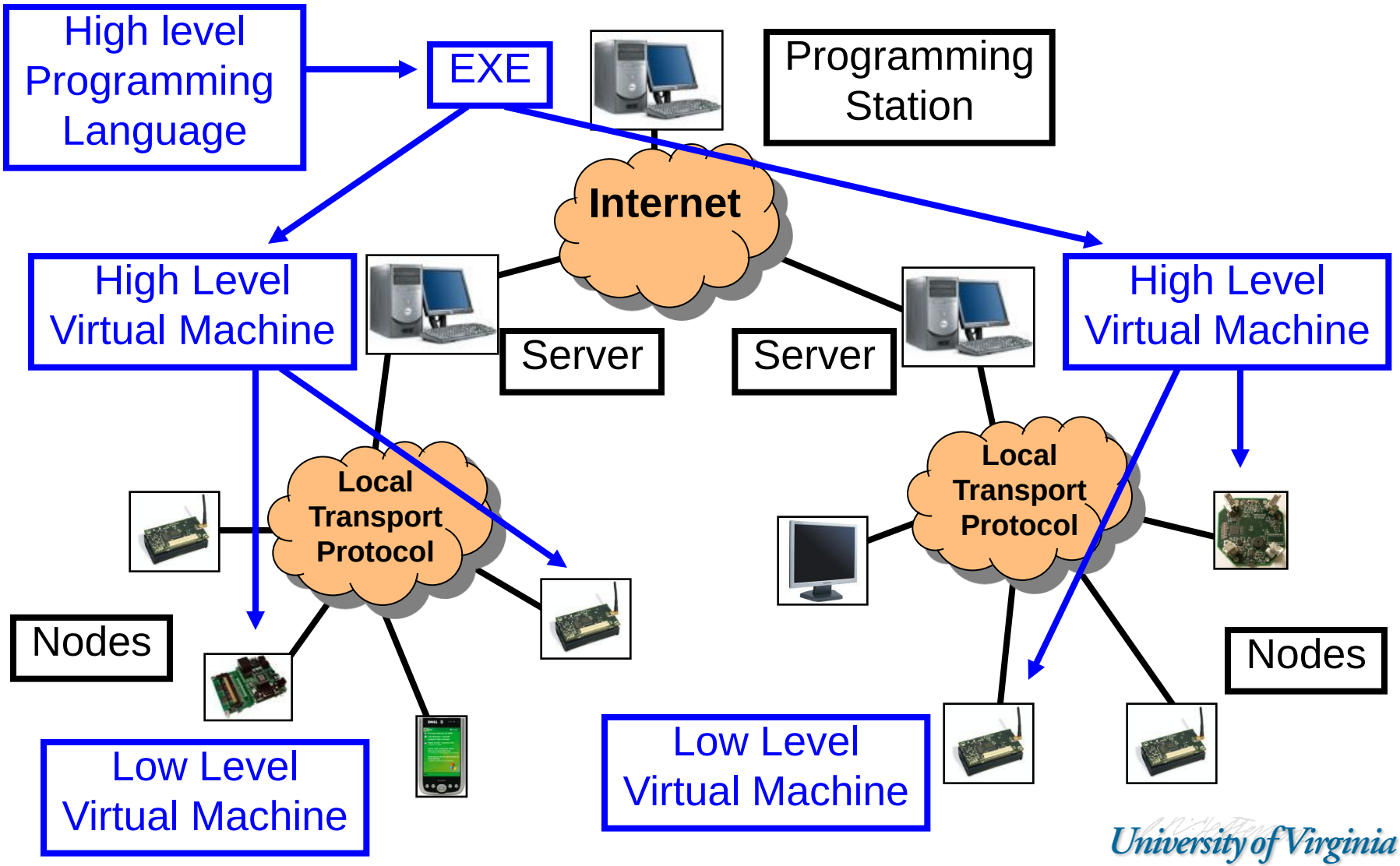
System Architecture



System Architecture



System Architecture

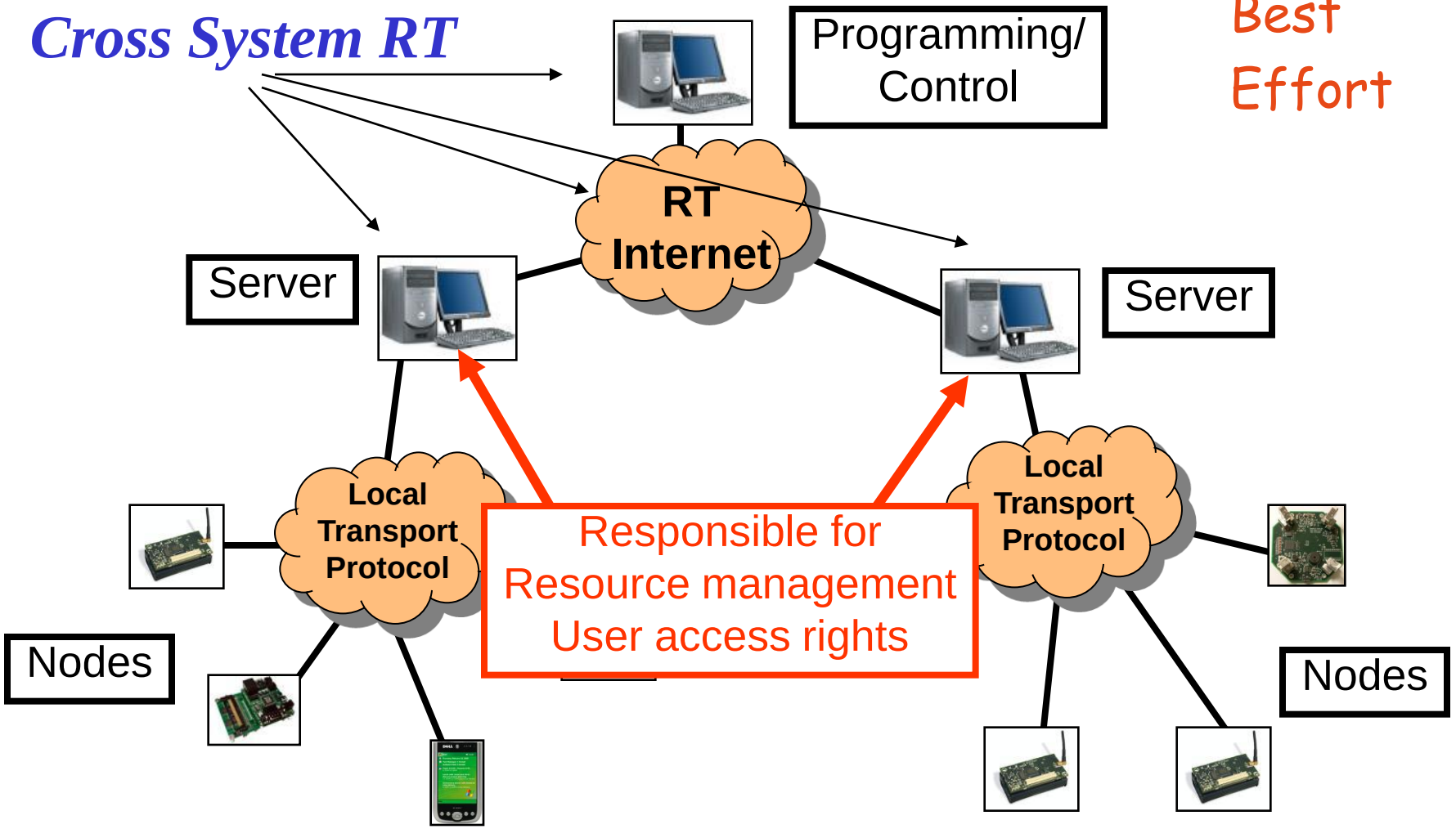


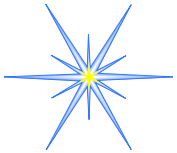
System Architecture

Cross System Control

Cross System RT

Beyond Best Effort



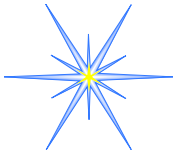


Correct Architecture?

- 6LoWPAN based
- WEB services based

CPS - Enabler for Dramatic Innovation

- New global-scale, personal medical delivery systems
- New paradigms for scientific discovery
- Smart (Micro) Agriculture
- Towards the end of terrorism
- Wireless Airplanes
- Next Generation Internet



Key Point

- Connection to the physical world will be so pervasive that systems will be *open* even if you think they are not