Cyber-Physical Systems:
Aspects as a Basis for Robustness and Openness

John A. Stankovic
Department of Computer Science
University of Virginia

March 2009

University of Virginia

How does this 67-year old doctor have the body of a 30-year old?

Cyberphysical Systems Research

BENEFITS MAY INCLUDE:

Improved Muscle Tone
Decreased Body Fat
Increased Energy
Increased Sex Drive/Libido
Sharper Thinking
Improved Outlook on Life

Outline

- What are Cyber Physical Systems (CPS)

- Aspects in CPS (cross cutting concerns)
  - Logging
  - (Reactive) Security
  - Robust Localization
  - Power Management
  - Feedback Control

Acknowledgments/Info

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

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

Definition

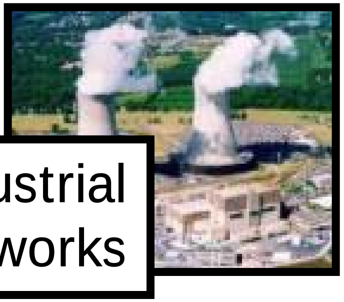
- CPS is the co-joining of computation and communication with physical processes.

- 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

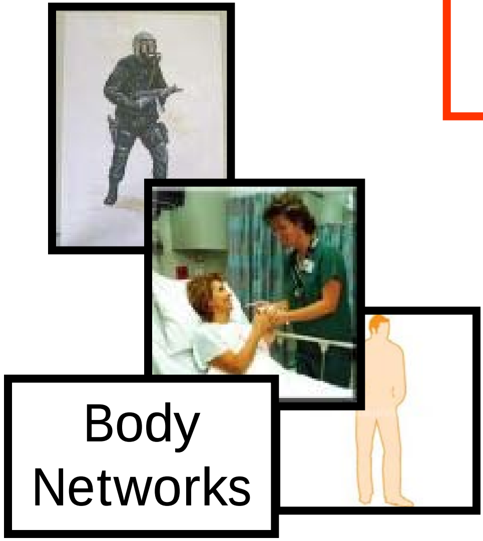
Environmental
Networks

Road and Street
Networks



dustrial
etworks

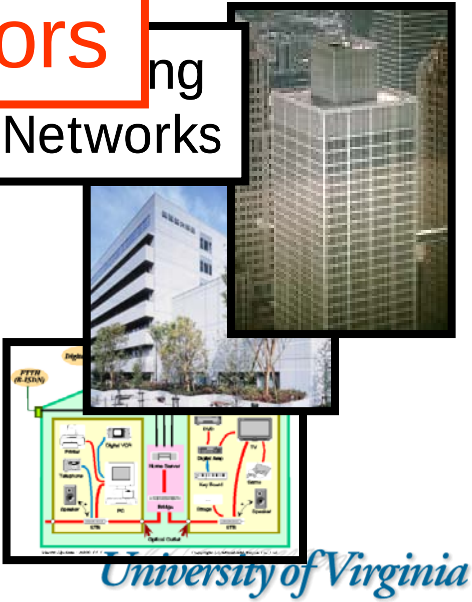
Heterogeneous
Wireless Networks with
Sensors and Actuators



Body
Networks

Vehicle
Networks

ng
Networks



What's New

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

CPS

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

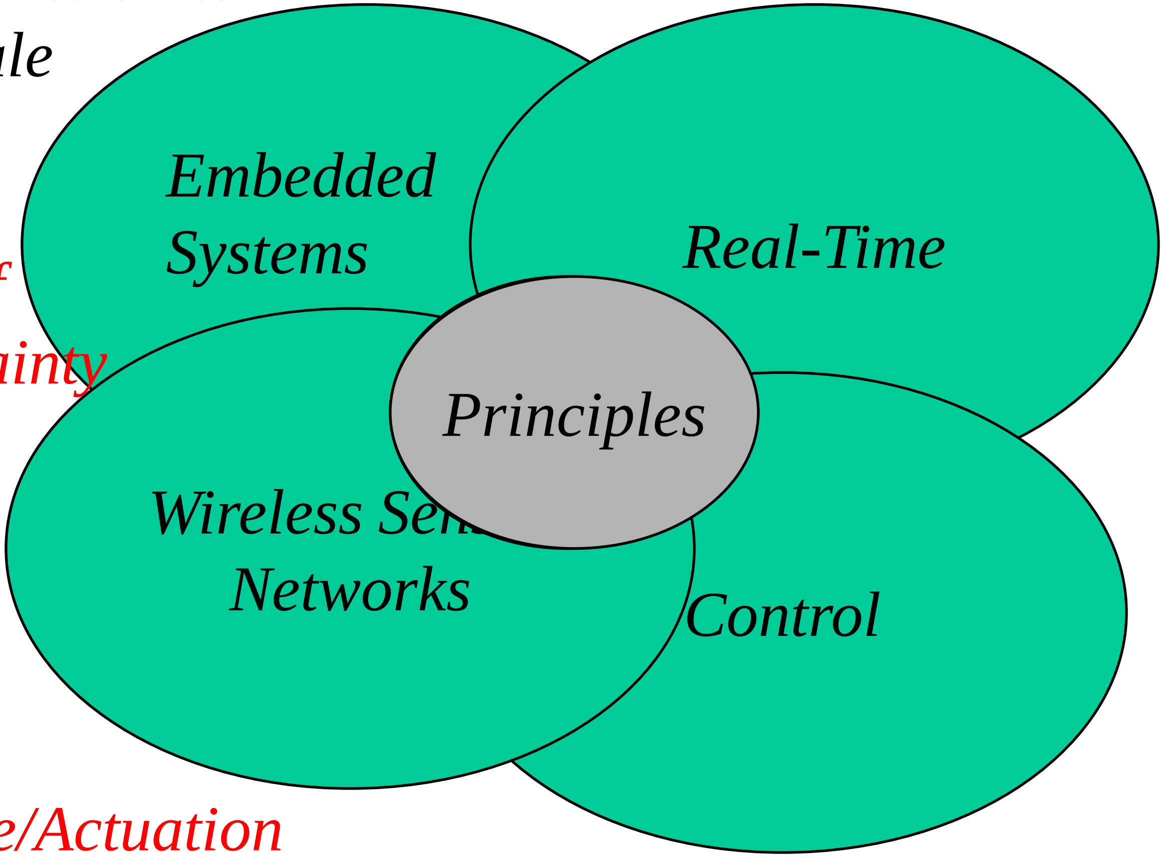
- Is the Internet just a LAN on steroids?

- 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

Confluence of Four Key Areas

Cost
Form Factor
Severe Constraints
Small Scale
Closed
Open
Degree of
Uncertainty

Scheduling
Fault Tolerance
Wired networks
Wireless
Degree of
Uncertainty



Noisy C.
Sensing
Scale
Real-Time/Actuation
Open

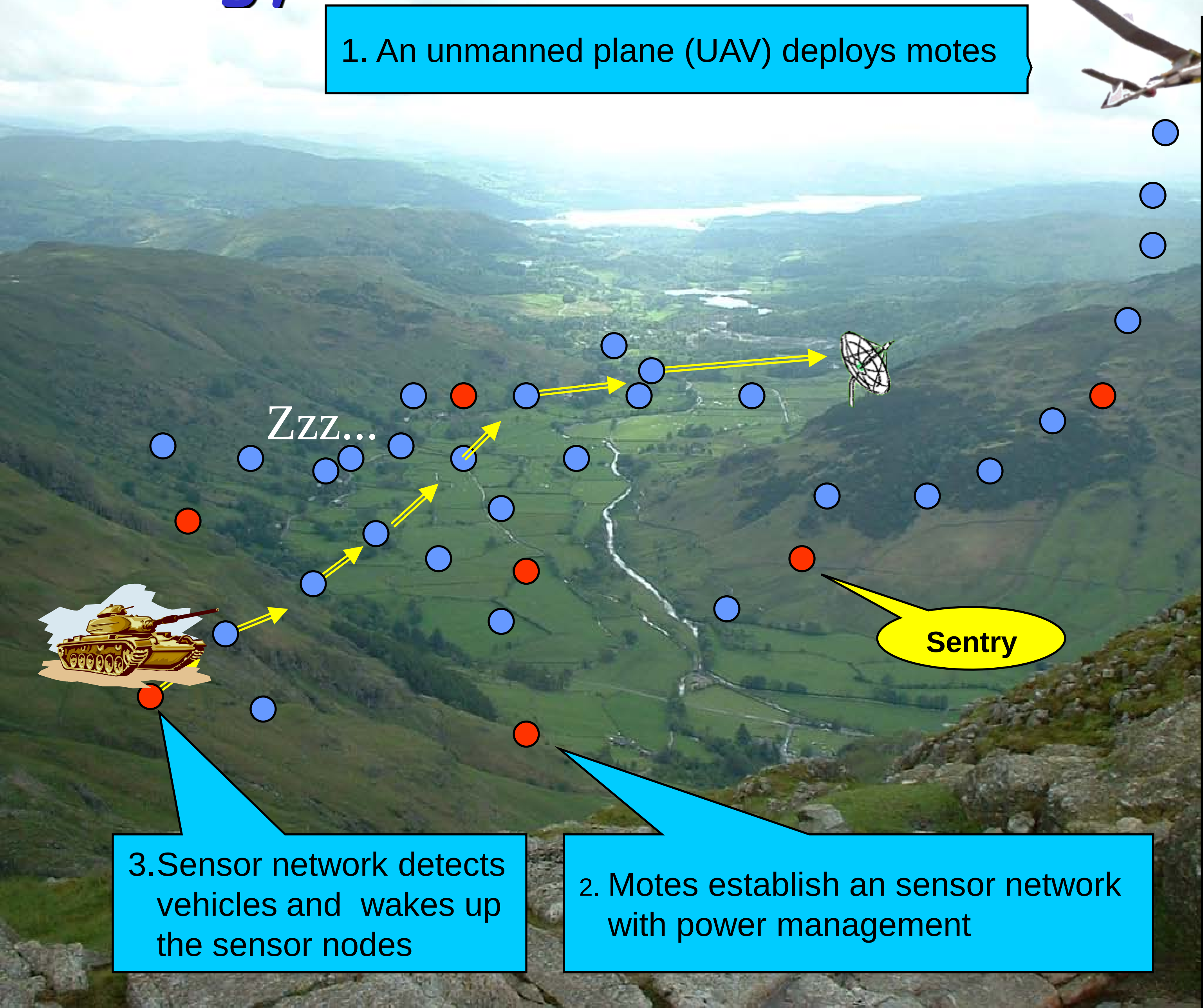
Linear
Adaptive
Distributed
Decentralized
Open
Human Models

University of Virginia

Motivating Example

- Cyber – Physical Interactions
  - Influence on each other
  - Cross disciplinary

Energy Efficient Surveillance System



1. An unmanned plane (UAV) deploys motes

2. Motes establish an sensor network with power management

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

- 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

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, …
- Sensor Fusion:
  - Sensor fusion to avoid false alarms, but 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

Tracking Example (2)

- 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 attempts
  - 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

R
O
B
U
S
T
N
E
E
S

Aspects in CPS

- Logging
- (Reactive) Security
- Robust Localization
- Power Control
- FC Loops

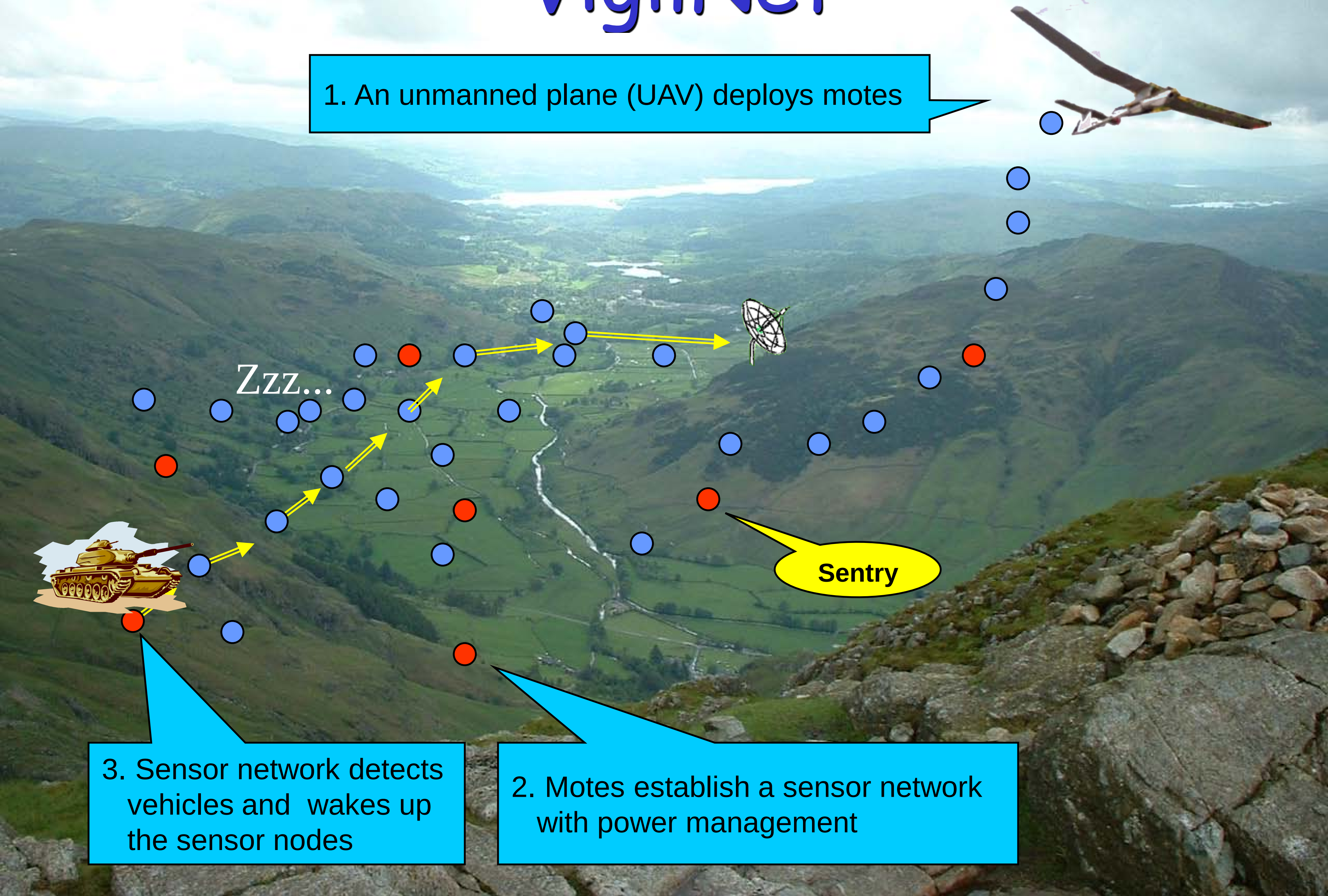
Themes

- Requirements of Robustness and Openness
  - Minimal capacity devices

- Adaptive Systems (Dynamic Aspects)

- Produce Consistent Changes Across
  - Protocols
  - Nodes
  - Control Loops

VigilNet

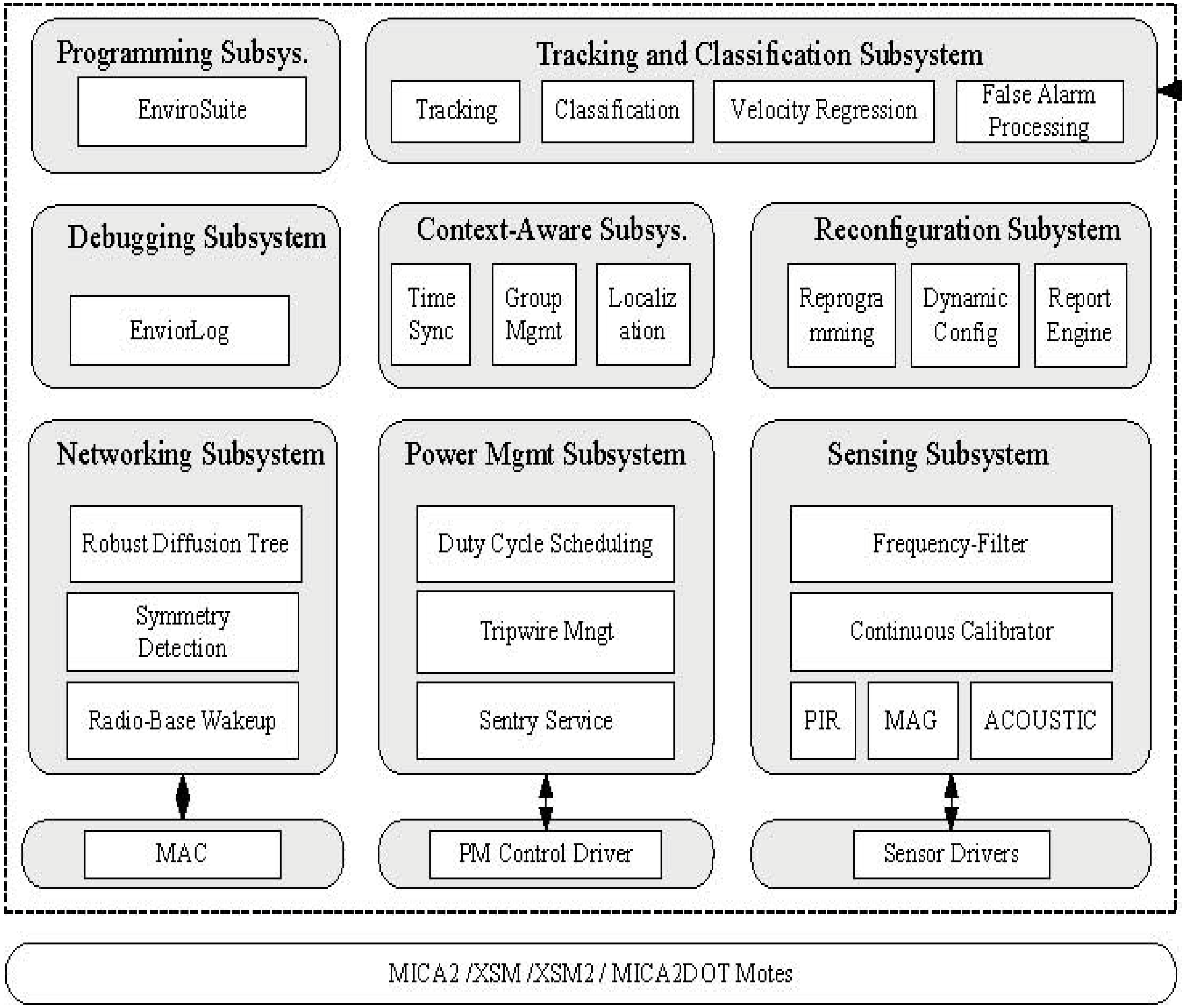


1. An unmanned plane (UAV) deploys motes

2. Motes establish a sensor network with power management

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

VigilNet Architecture



Programming Subsys.

EnviroSuite

Tracking and Classification Subsystem

Tracking

Classification

Velocity Regression

False Alarm Processing

Debugging Subsystem

EnviorLog

Context-Aware Subsys.

Time Sync

Group Mgmt

Localiz ation

Reconfiguration Subystem

Reprogra mming

Dynamic Config

Report Engine

Networking Subsystem

Robust Diffusion Tree

Symmetry Detection

Radio-Base Wakeup

Power Mgmt Subsystem

Duty Cycle Scheduling

Tripwire Mngt

Sentry Service

Sensing Subsystem

Frequency-Filter

Continuous Calibrator

PIR

MAG

ACOUSTIC

MAC

PM Control Driver

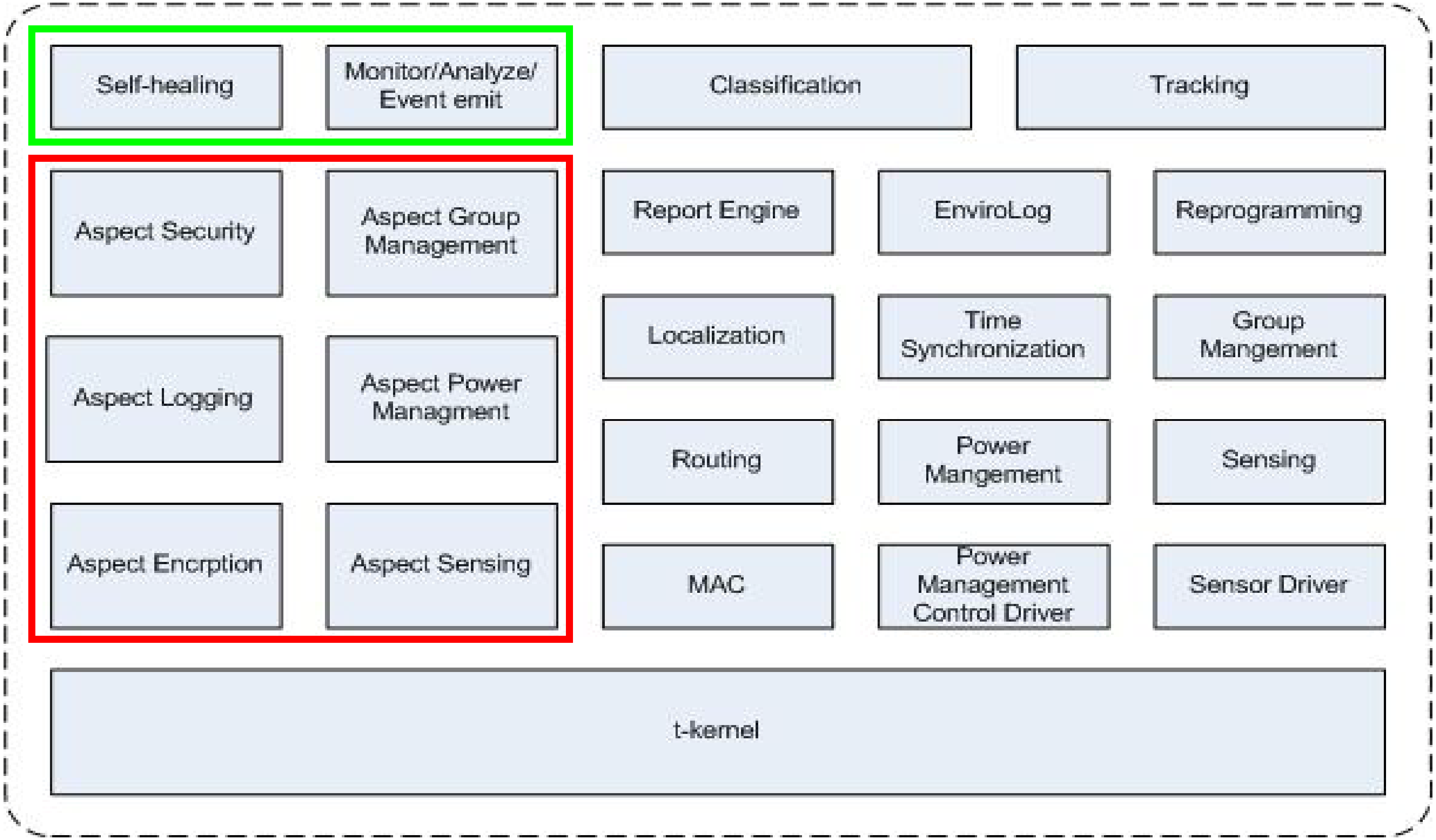
Sensor Drivers

MICA2 /XSM /XSM2 / MICA2DOT Motes

User Interface & Control Subsystem

University of Virginia

Dynamic Aspect Architecture



Logging

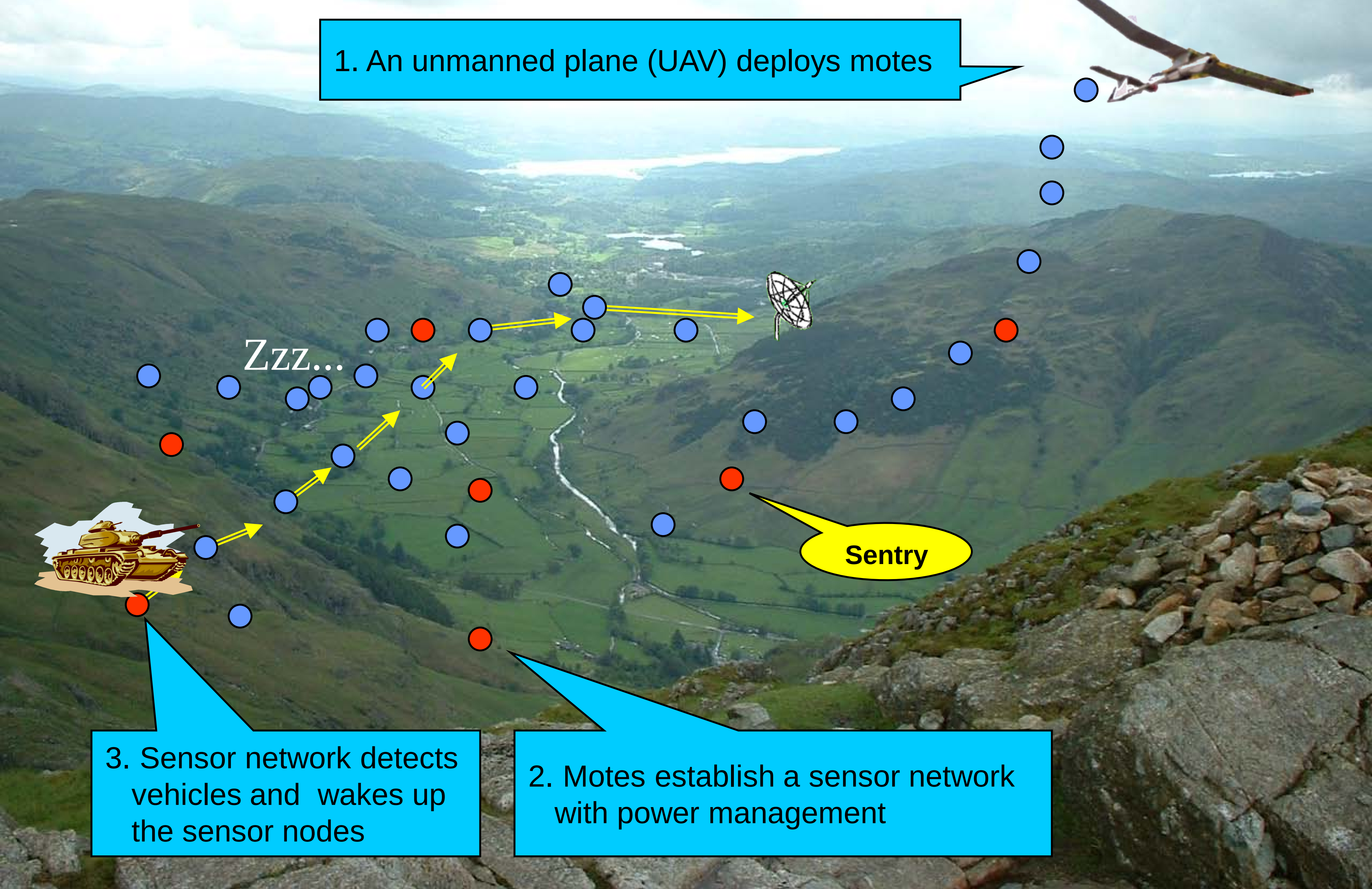
- Open and noisy/uncertain environments
- Limited storage and energy (must be selective)

- Examples:
  - Activate (logging) advice at all MAC and routing protocol entries when E2E comm. performance drops
  - Activate periodically to assess state of system

Logging

- Surprising performance
  - Routes used?
  - Congestion and why?
  - Current topology?
  - Hotspots?
  - How much traffic generated by a node?
  - …
- Turn on/off
  - Coordinated across CPS to get coverage
  - By area

Security - VigilNet

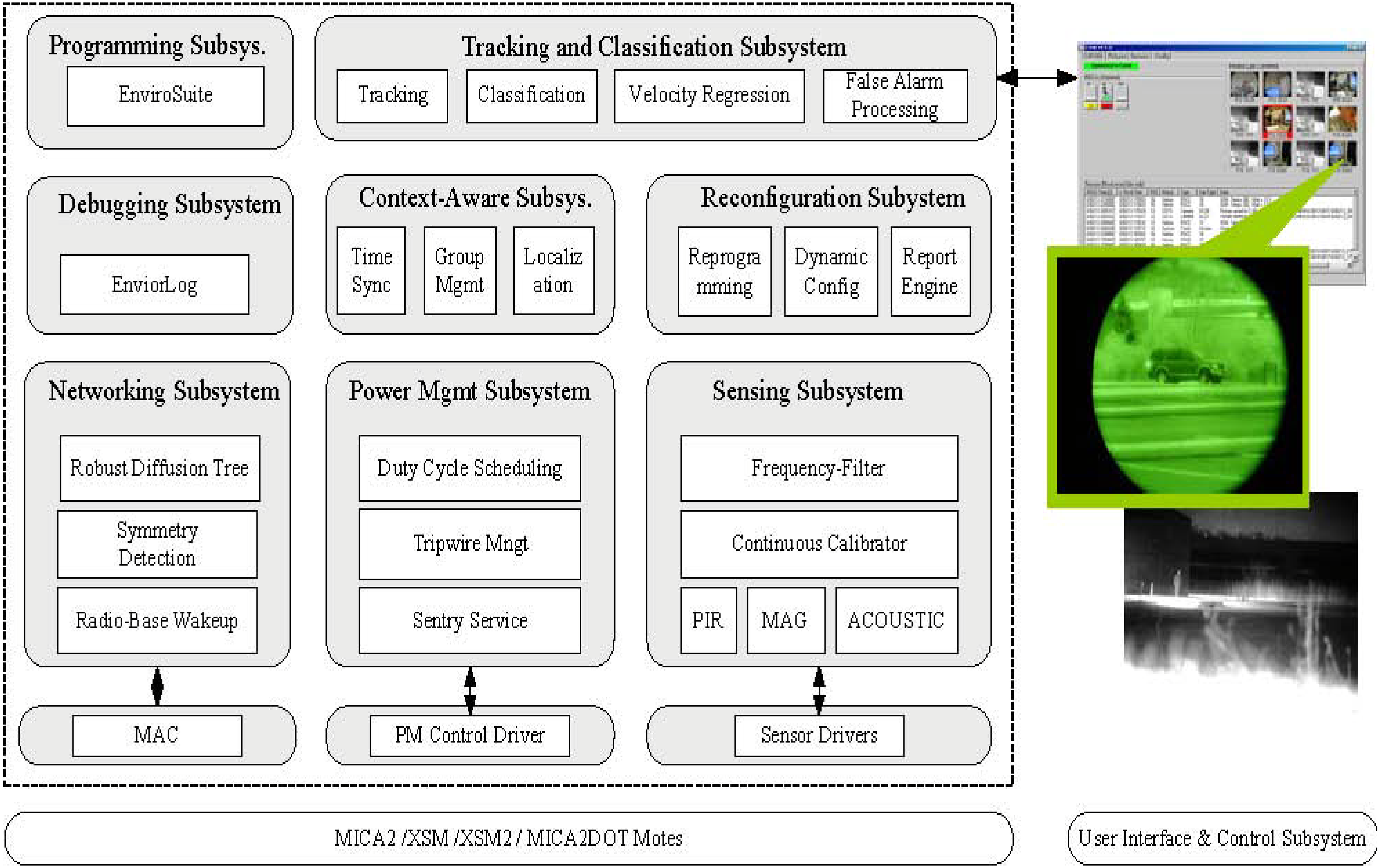


1. An unmanned plane (UAV) deploys motes

2. Motes establish a sensor network with power management

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

VigilNet Architecture



Programming Subsys.

EnviroSuite

Tracking and Classification Subsystem

Tracking | Classification | Velocity Regression | False Alarm Processing

Debugging Subsystem

EnviorLog

Context-Aware Subsys.

Time Sync | Group Mgmt | Localiz ation

Reconfiguration Subystem

Reprogra mming | Dynamic Config | Report Engine

Networking Subsystem

Robust Diffusion Tree

Symmetry Detection

Radio-Base Wakeup

Power Mgmt Subsystem

Duty Cycle Scheduling

Tripwire Mngt

Sentry Service

Sensing Subsystem

Frequency-Filter

Continuous Calibrator

PIR | MAG | ACOUSTIC

MAC

PM Control Driver

Sensor Drivers

MICA2 /XSM /XSM2 / MICA2DOT Motes

User Interface & Control Subsystem

University of Virginia

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:

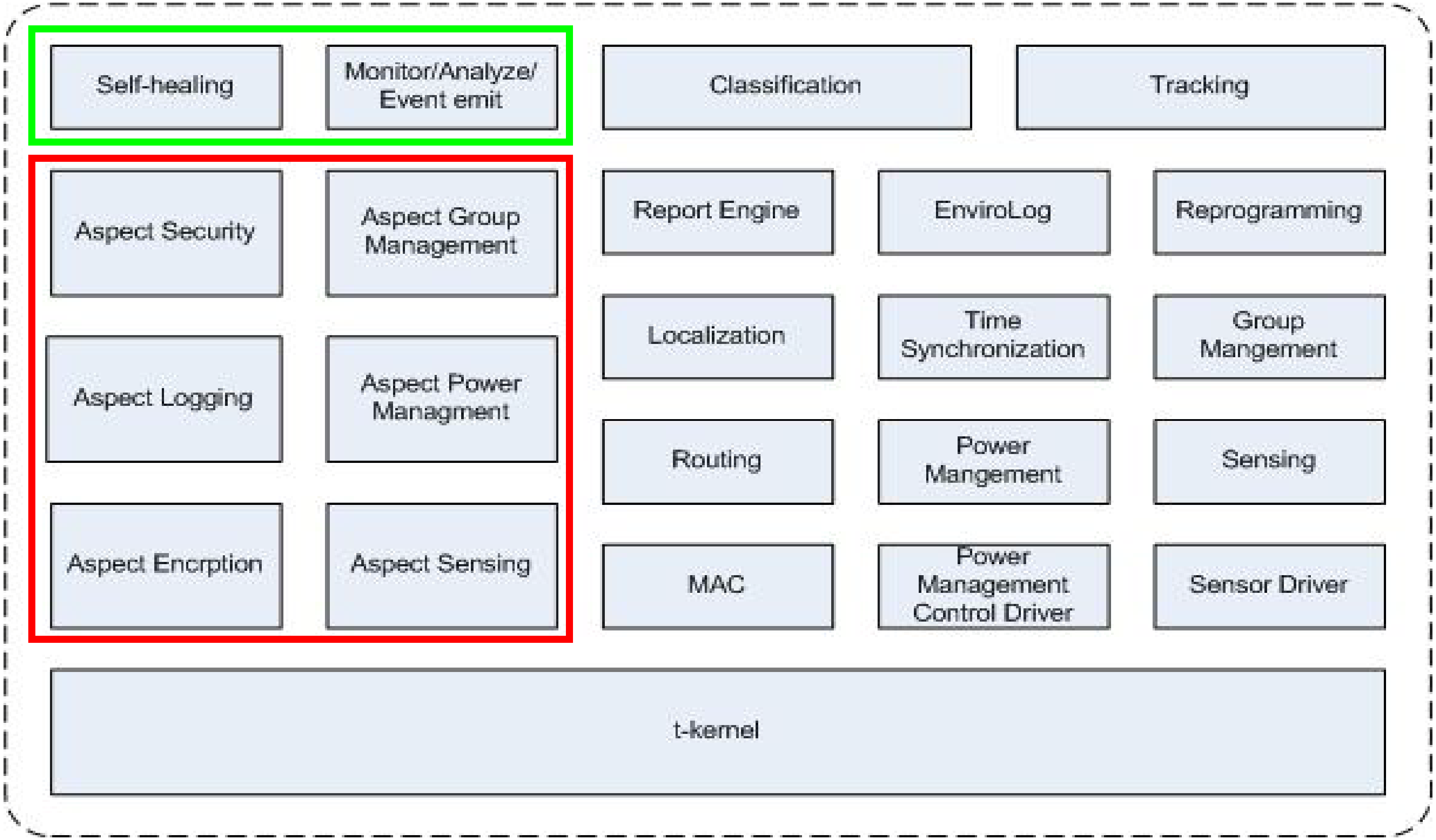
8 MHz 8-bit uP
128 MB code
4 KB data mem
250 Kbps radio

Security Approach

- Operate in the presence of security attacks
  - Robust decentralized protocols
  - Runtime control of security vs. performance tradeoffs

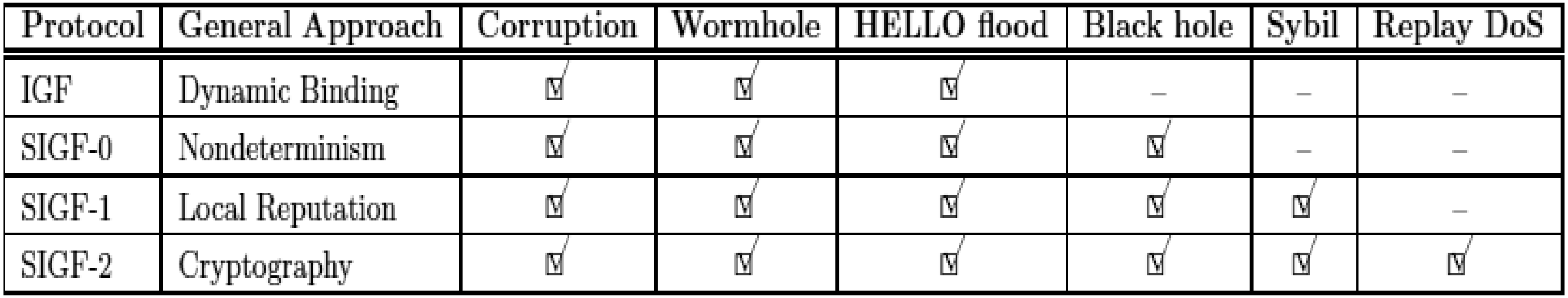
- Self-healing architecture
- Evolve to new, unanticipated attacks
- Lightweight solutions required due to severe constraints

Self-Healing Architecture



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.

University of Virginia

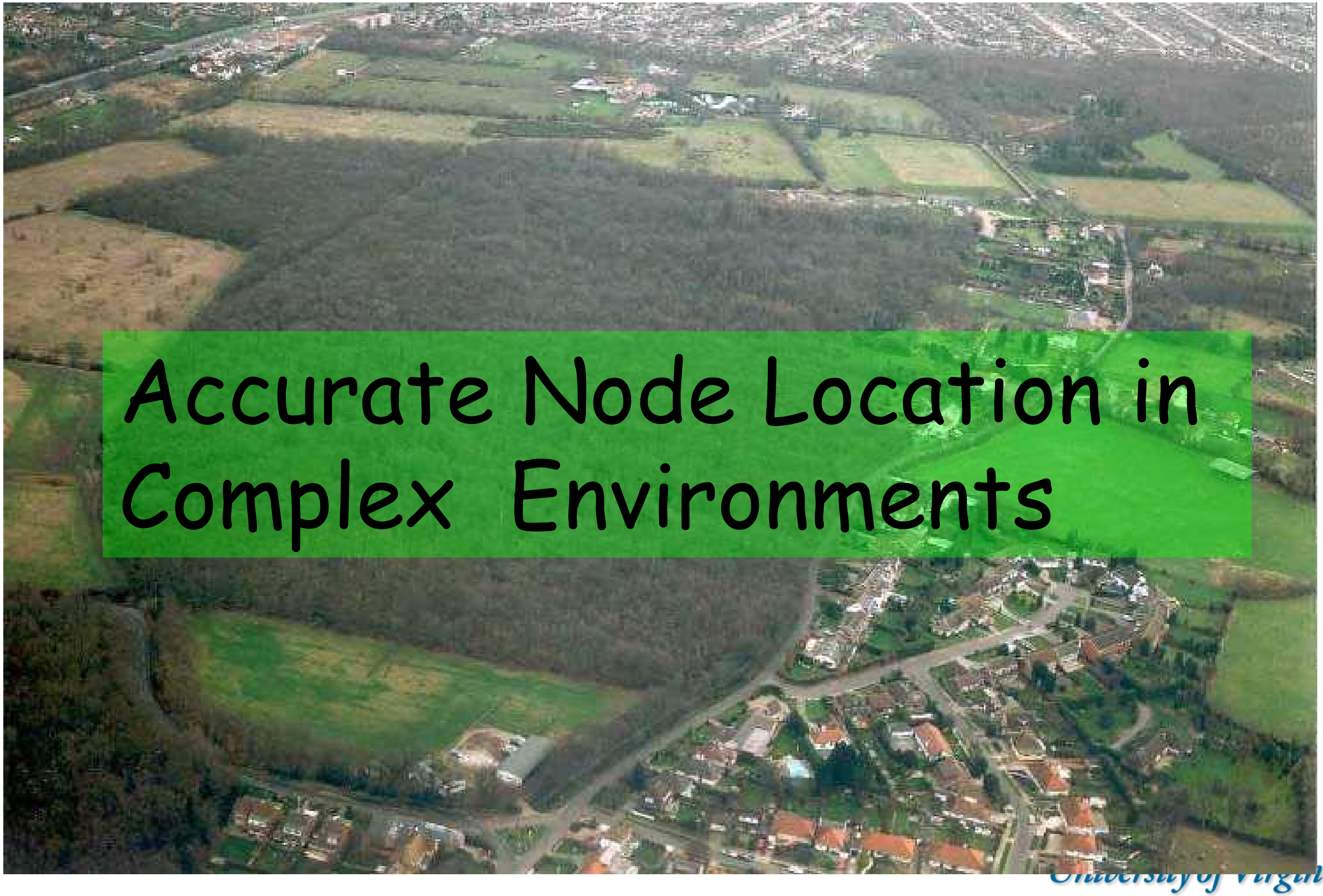
Dynamic Aspects

- Mechanism for implementing the “right defense at the right time” strategy
  - Switch consistently
  - Choose the correct keys

Other Security Issues

- Encrypt all control messages when attack suspected
  - Time sync, localization, power management
- Across nodes: Double the key lengths and increase message size

Robust Localization



Accurate Node Location in Complex Environments

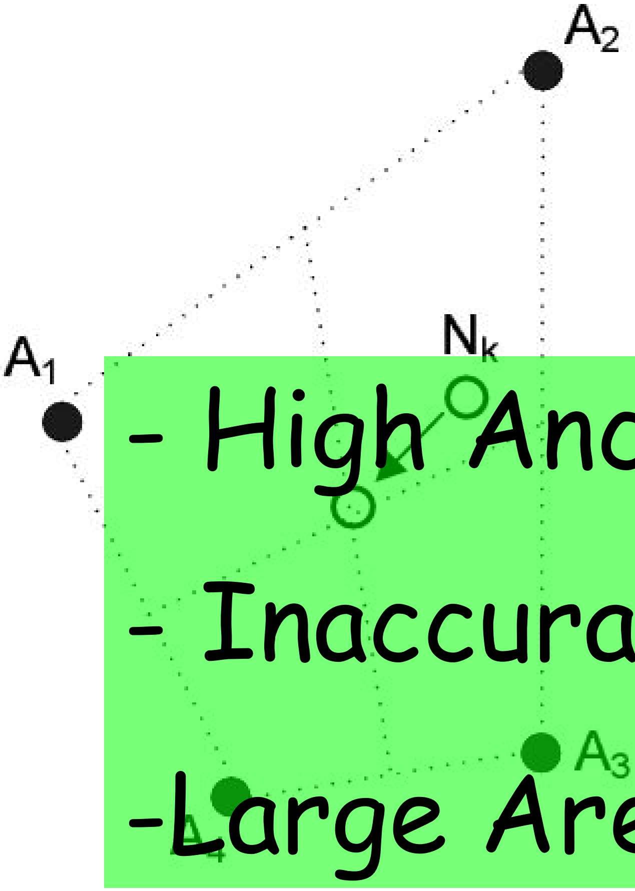
GPS

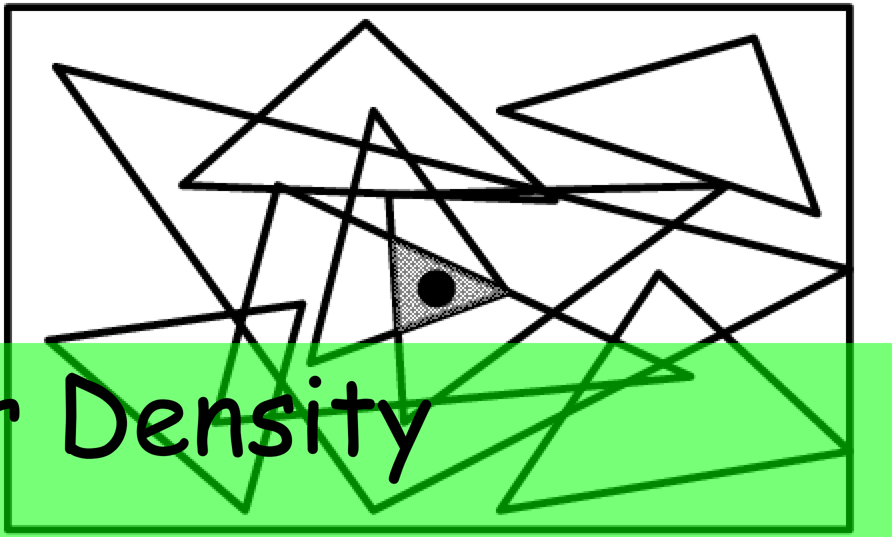
- Not Cost Effective
- Line of Sight

Range Free

Centroid

APIT





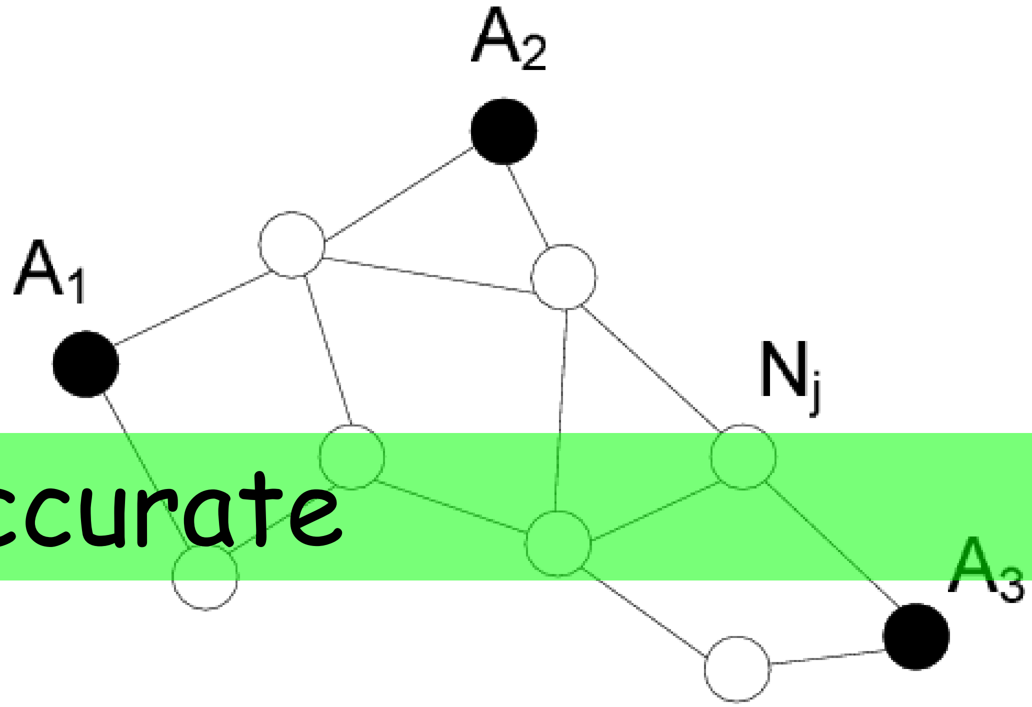
- High Anchor Density

- Inaccurate

-Large Areas without anchors

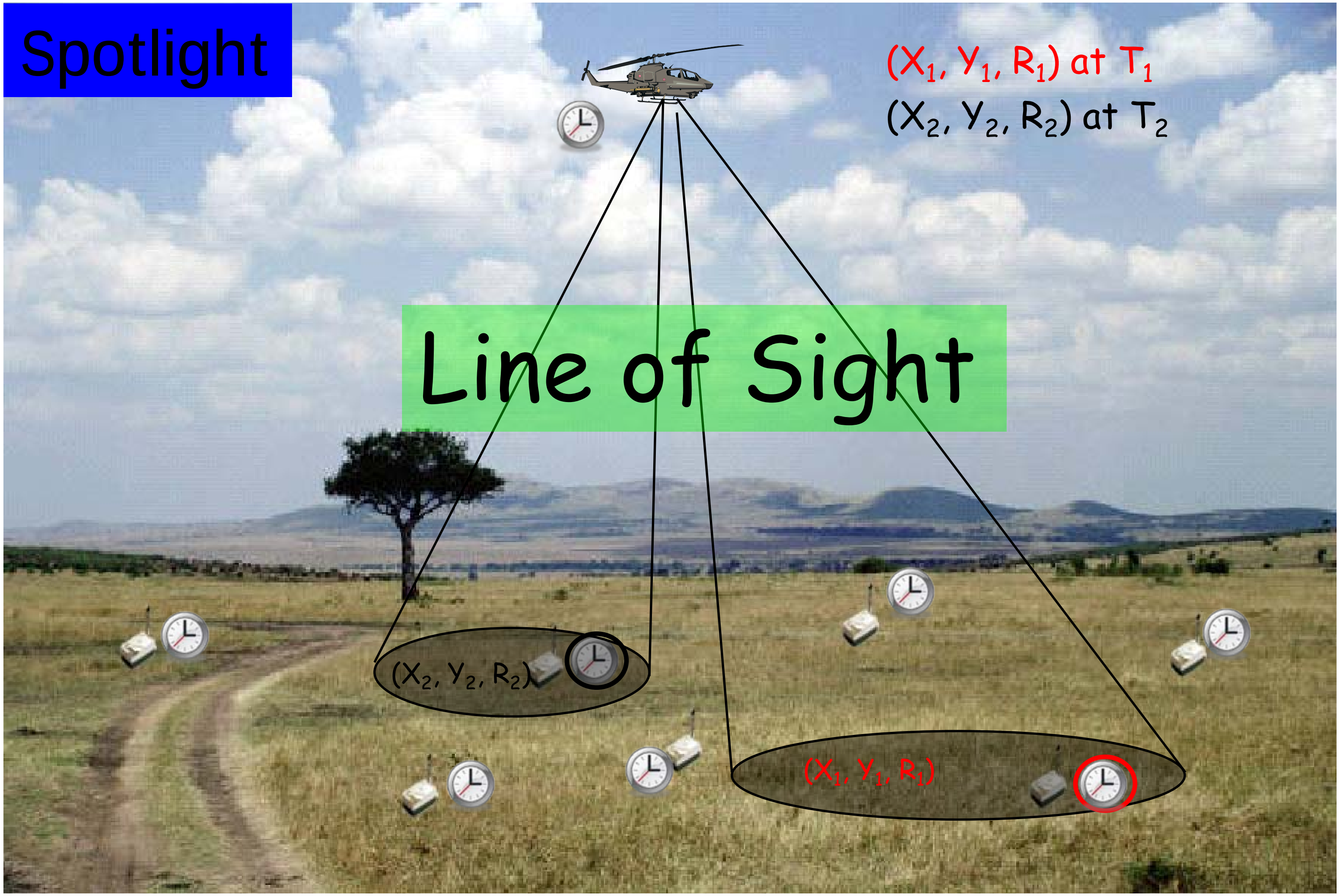
Range Free

DV-Hop



Inaccurate

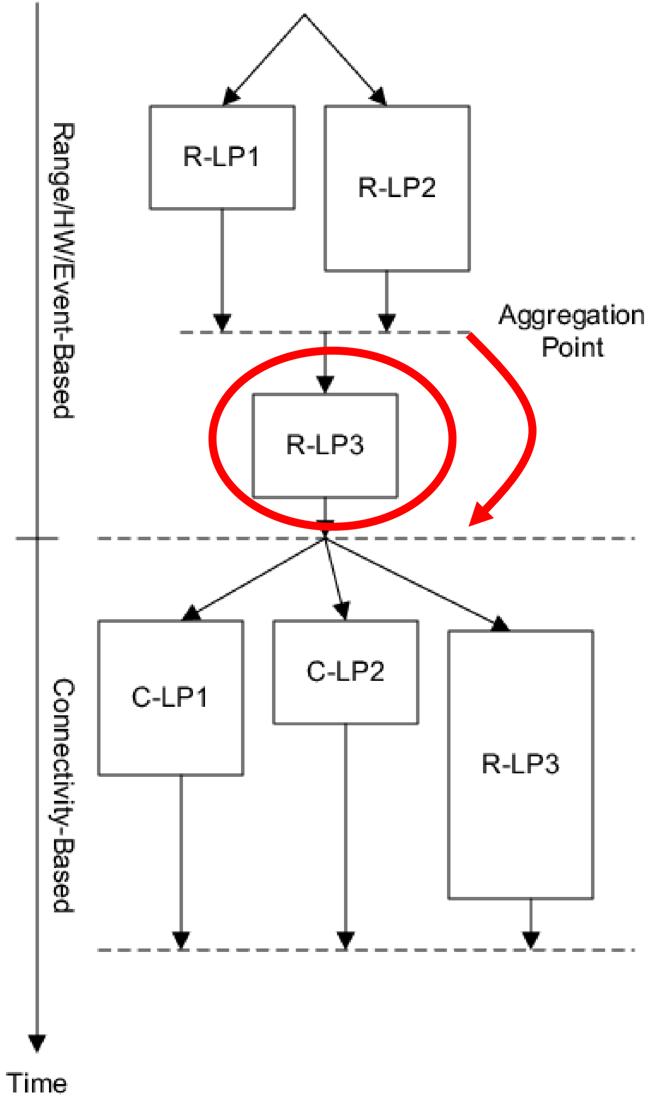
Low Cost - Accurate



CPS

- Complex physical properties of environments render “individual” solutions brittle

Hierarchical Framework

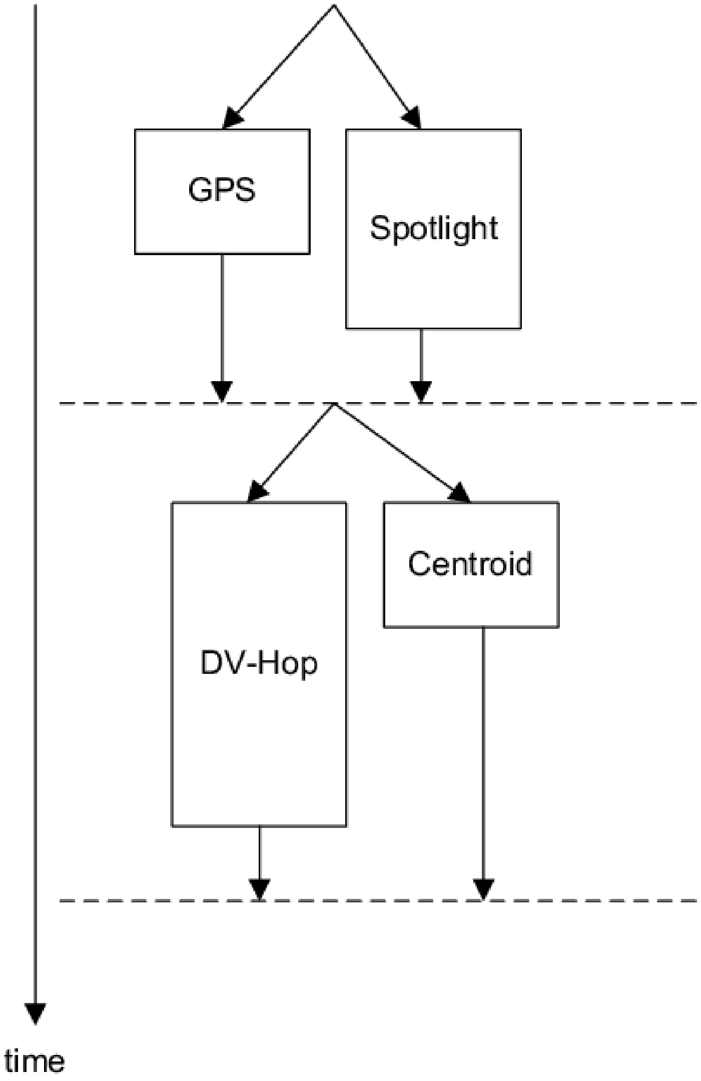


- Choose best / Weighted average
- If not localized – try another algorithm
- All nodes have a location at this point.

Evaluation

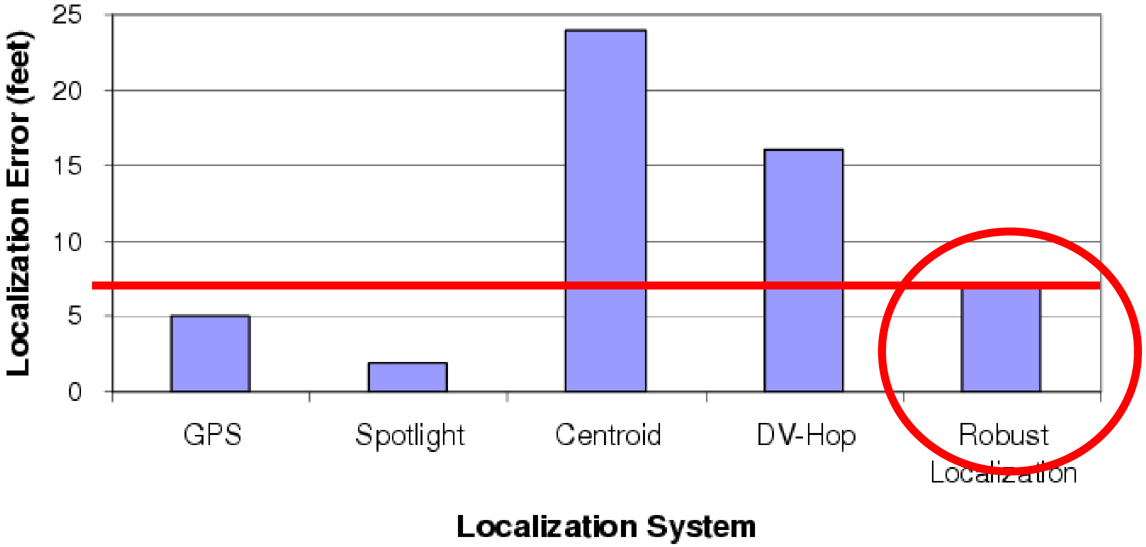
- TOSSIM
  - 400 nodes in 300x300ft2
  - 200x200ft^2 obstructed area
  - 50ft radio range
  - 10% nodes have GPS
  - 15% nodes in open area can't be localized

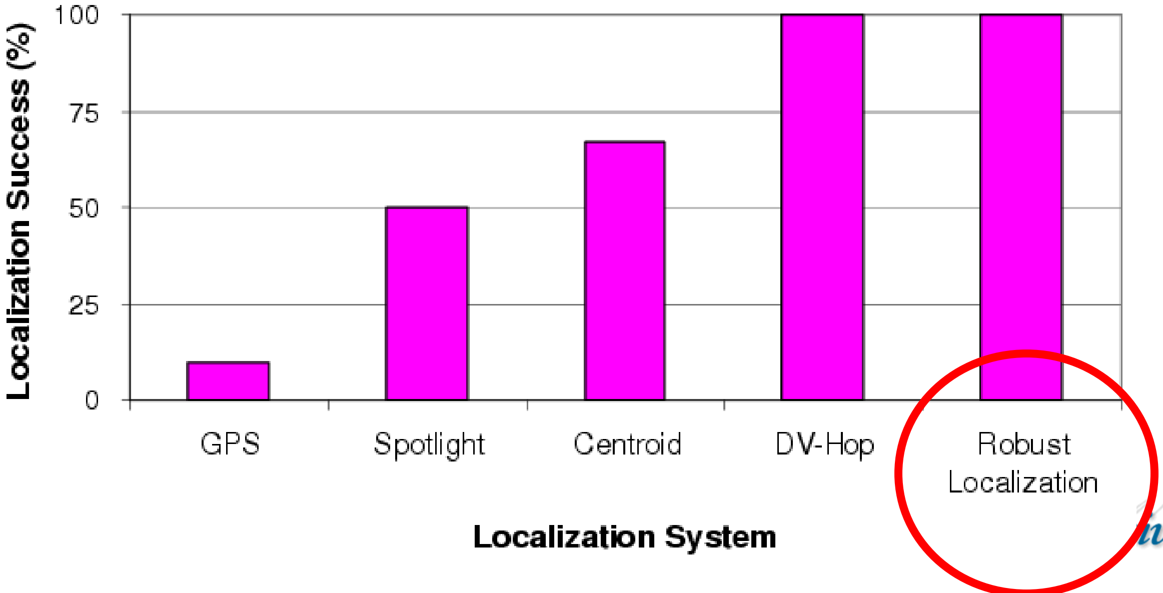
Evaluation



University of Virginia

Evaluation





All nodes are localized

Dynamic Aspects

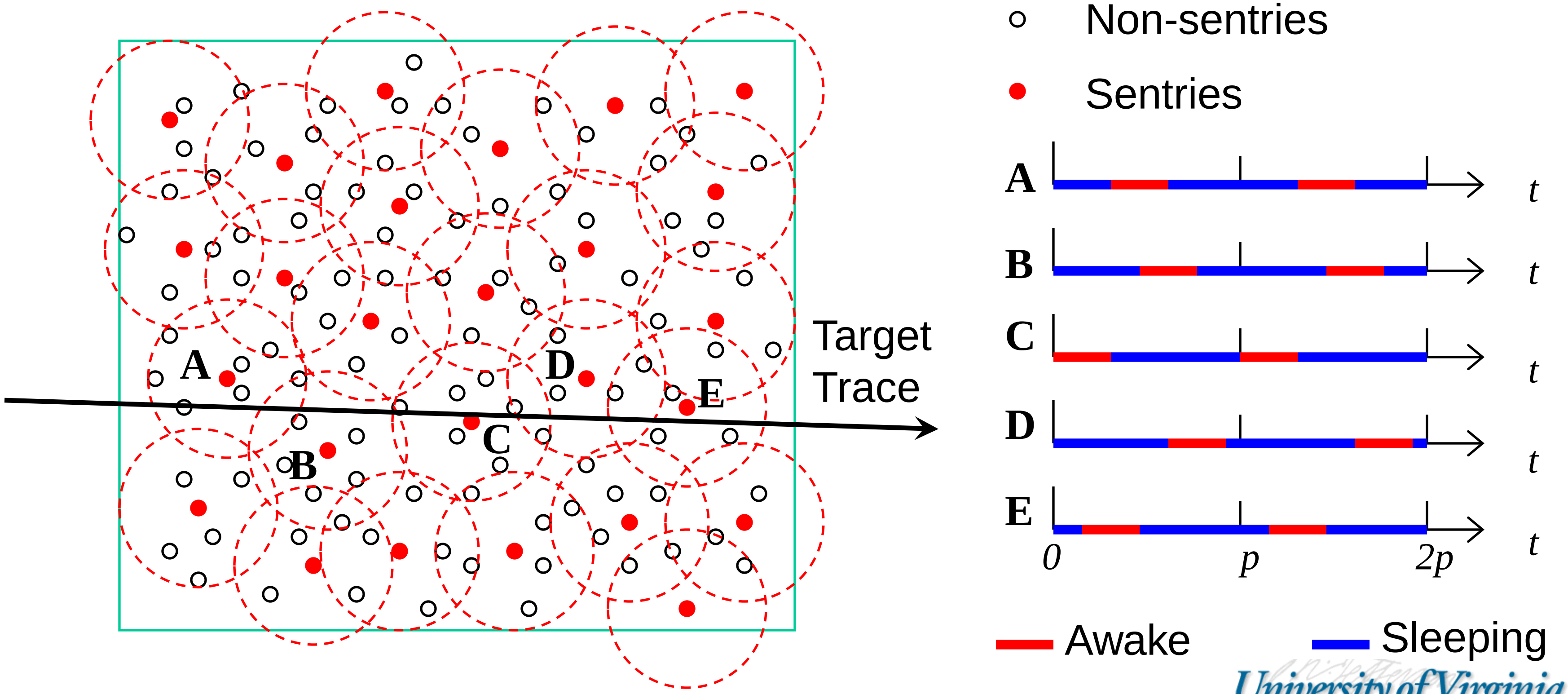
- Weave in new localization protocols as required

Power Management

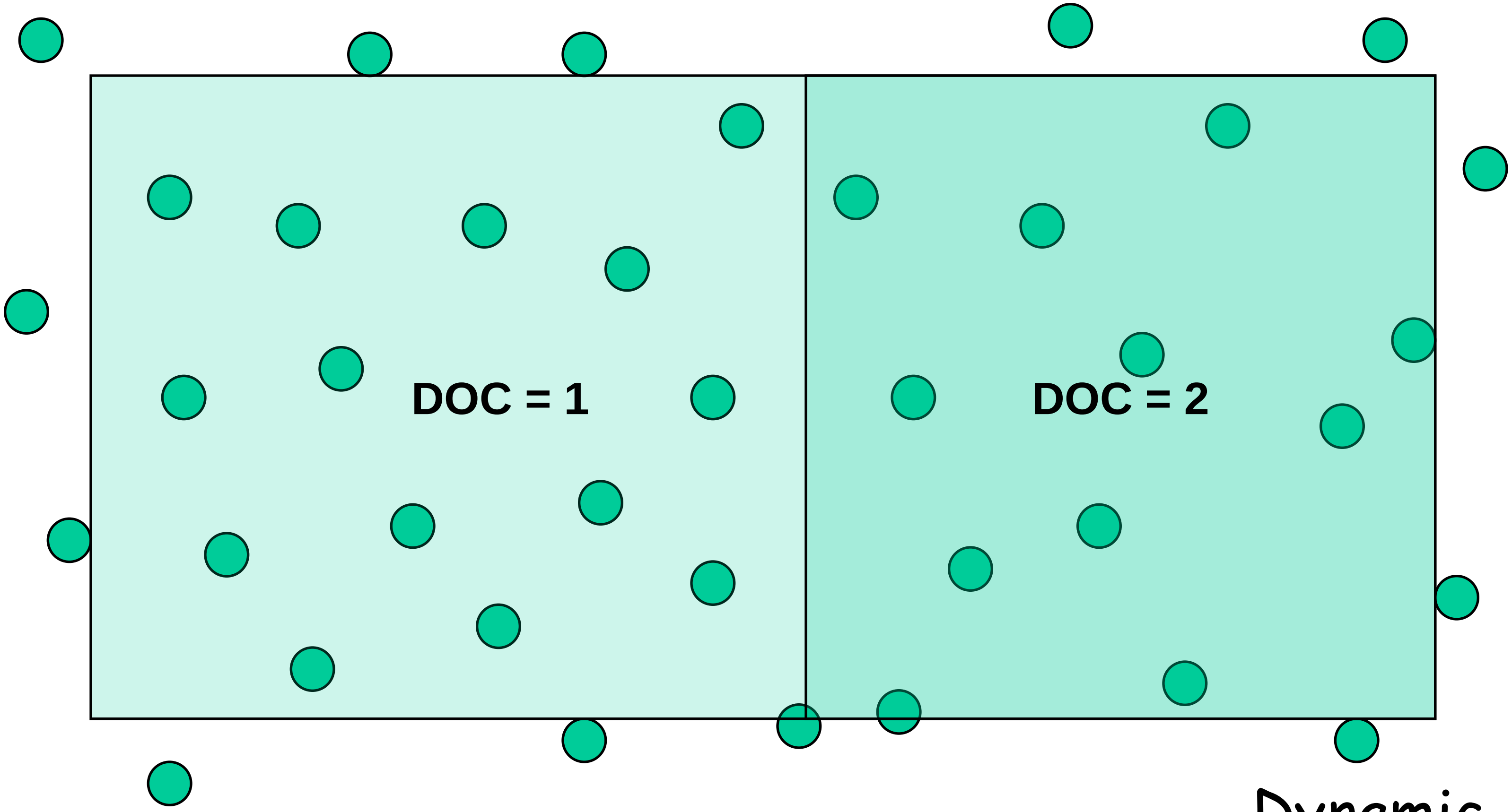
- Power Management in the Small
  - Individual protocols: MAC, Routing, Clock Sync, Localization
- Power Management in the Large
  - Overarching protocols for additional power savings
    - Sentry Service
    - Tripwire Management Service
    - Duty Cycle
    - Differential Surveillance

Sentry Duty-Cycle Scheduling

- A common period *p* and duty-cycle *β* is chosen for all sentries, while starting times T_{start} are randomly selected



Differentiated Surveillance Solution



Dynamic

DOC = Degree of Coverage

Aspects

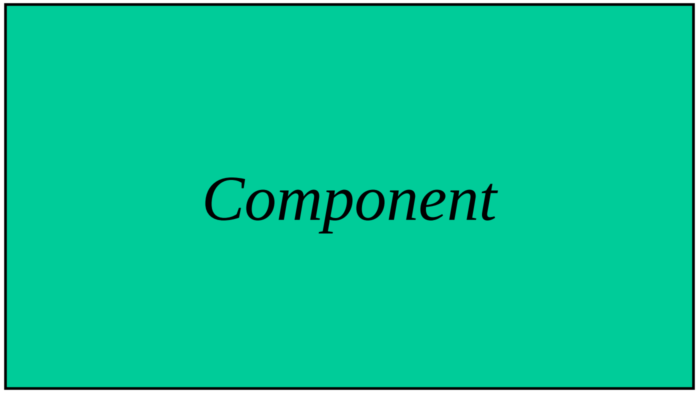
- Sets of coordinated changes (pointcuts in)
  - In MAC
  - In Routing
  - In Clock Sync
  - For duty cycle
  - Turn off/on tripwire section

Feedback Control

- Node Level
- Neighborhood Level
- System Level
- Systems of Systems Level

- Explicit and Implicit Interactions Across FC loops

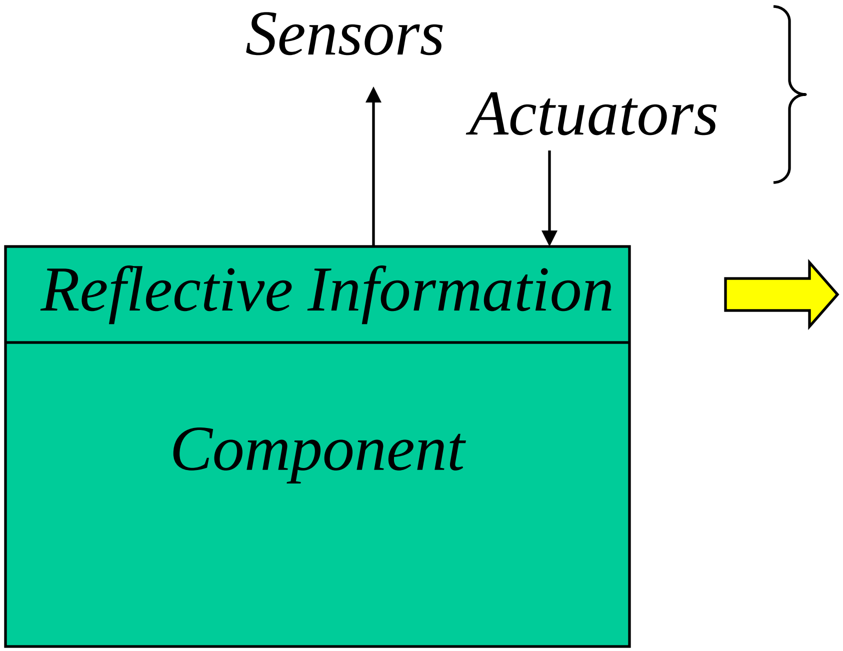
Component-Based (today - mostly)



Reuse
Modularity
Portability
Reconfigure

Beginning to consider performance

Component-Based (Tomorrow)



Support for control; reflect the physical

Support for

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

Interaction Among FC Loops

- "n" controllers increase/decrease control parameter in same direction
  - overshooting

- "n" controllers fight each other
  - Change parameters in opposite directions

Examples

- Real-Time: monitor E2E delay
  - Change sleep cycle (PM), backoff times (MAC), congestion thresholds (Routing), packet aggregation amounts (Middleware), sensing rates (SP), …

- Power Control: monitor voltage
  - Change duty cycle, coverage, sector policy, message rates

Final Thoughts (1)

- 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
  - (Mostly) Wireless Airplanes
  - Next Generation Internet

Final Thoughts (2)

- Connection to the physical world will be so pervasive that systems will be *open* even if you think they are not
- Degree of uncertainty is high
- Flexibility offered by (Dynamic) AOP has great potential