High Confidence Swarms for Cyber Physical Systems

Swarm Visions
December 6, 2011

Shankar Sastry
Swarm Applications- Taxonomy

◆ **Understanding phenomena:**
  – Data collection for offline analysis
    ◆ Environmental monitoring, habitat monitoring
    ◆ Structural monitoring
◆ **Detecting changes in the environment:**
  – Phase transitions, anomaly detection
    ◆ Security systems, traffic surveillance
    ◆ Wildfire detection
    ◆ Fault detection, threat detection
◆ **Real-time estimation and control:**
  – Traffic control, building control, environmental control
  – Manufacturing and plant automation, power grids, SCADA networks
Case Study: Industrial Automation

- **Motivation: Cost reduction**
  - More than 85% reduction in cost compared to wired systems (case study by Emerson)
  - SCADA (Supervisory Control And Data Acquisition)

- **Reliability is the number one issue**
  - Robust estimation: Estimation of parameters of interest from noisy measurements with high fidelity in the presence of unreliable communication
  - Real-time control: A must for mission-critical systems
Substantive Cost Reduction

A Shift In Total Data Acquisition Cost Will Drive A New Asset Management Paradigm

Field Device ~$1,500\textsuperscript{a}
Conduit / Wiring / Dwgs ~$9,500\textsuperscript{a}
Field JBox
I/O / Loop Check / Config ~$500\textsuperscript{a}

Integrate into:
DeltaV
AMS
ROC/RTU
Historian
Standard PC
3rd Party Hosts

* Budgetary estimates per point

Total Cost per Point
Host Scalability Requirement

7-10x $5 Reduction
Greater Reliability

Therefore, Self Org Nets Are Proving to be More Reliable, Easier to Use, & Cost Effective

Wireless HART (Self Organizing Networks)

\[
\text{Measurement} \quad \times \quad \text{Communication} \quad \times \quad \text{Data Management} = 99.99\%
\]

\[
\text{Traditional Point-to-Point Wireless (Proprietary)}
\]

\[
\text{Measurement} \quad \approx 90\% \quad \times \quad \text{Communication} \quad \approx 70\% \quad \times \quad \text{Data Management} \quad \approx 99\% = \approx 64\%
\]

The overall system can only be as strong as the weakest link
Attacks now reported on wireless SCADA swarms:

1. Sewage treatment systems, Maroochy Shire, Australia, 2000
4. LA traffic system, 2008
5. Polish Subway, 2008

Attackers: Cyber Criminals, Hacktivists, Rogue Hackers, Corporate Spies, Cyberwarriors
High Confidence Swarms

- Robust Estimation and Correctness by Construction
  - Unreliable communications
  - Mobility
- Fault Tolerance
  - Limits on scalability, safety and optimality
- Security and Resilience
  - Confidentiality
  - Integrity
  - Availability
  - Graceful Degradation
Three Open Problems for Cybersecurity of Swarms

- **Threat Assessment**
  - How to model an attacker and strategies
  - Consequences of successful attack

- **Attack Diagnosis**
  - How to detect corruption of data (integrity attacks)
  - False alarm versus missed diagnosis of stealthy attacks

- **Resilient Control and Defenses**
  - Design of resilient controls for integrity and availability attacks
  - Economic incentives for investing in cybersecurity