PANEL
Trends in Networking and Services

ICNS 2009

Cancun

March 7-12, 2010

Guests

Moderator:

Petre Dini, IARIA, USA // Concordia University, Canada

Guest Panelists:

Miklós Molnár, IRISA, INSA Rennes, France
Juan Flores, Universidad Michoacana, Mexico
Jaime Lloret, Polytechnic University of Valencia, Spain
Srikant Akella Vardhana, Infosys Technologies Ltd., India

Facts and Questions

Facts

- there are adaptive components and adaptive systems
- some of them might have 'brain', some not, yet still adaptive
- there are agent-based mechanisms, self-learning mechanisms, leading to certain autonomy

Questions:

? what is the core feature set towards evolving systems?
? what is the distance between utopia and realism, in dreaming/designing self-evolving systems?
? are there any methodology/guidelines for building such systems?

?

Panel: Robustness and Trust in Autonomic System

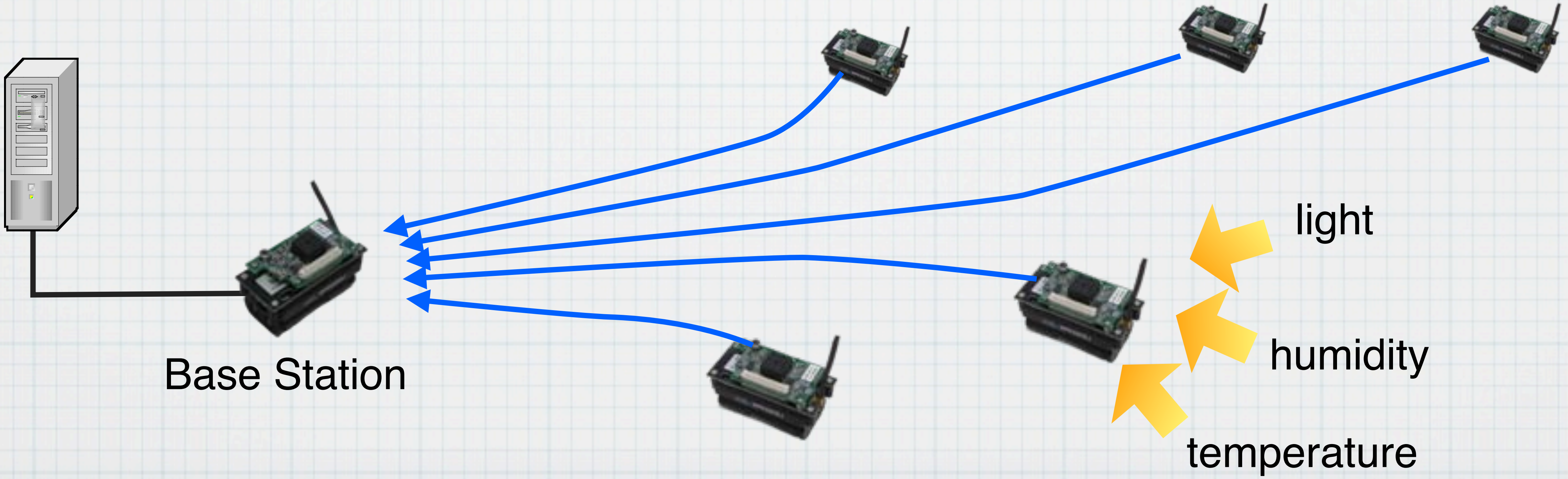
Robustness and Trust in Autonomous Power Saving on the Sensor Networks

Toshio Hirotsu (Hosei Univ., Japan)

Mar. 9th, 2010

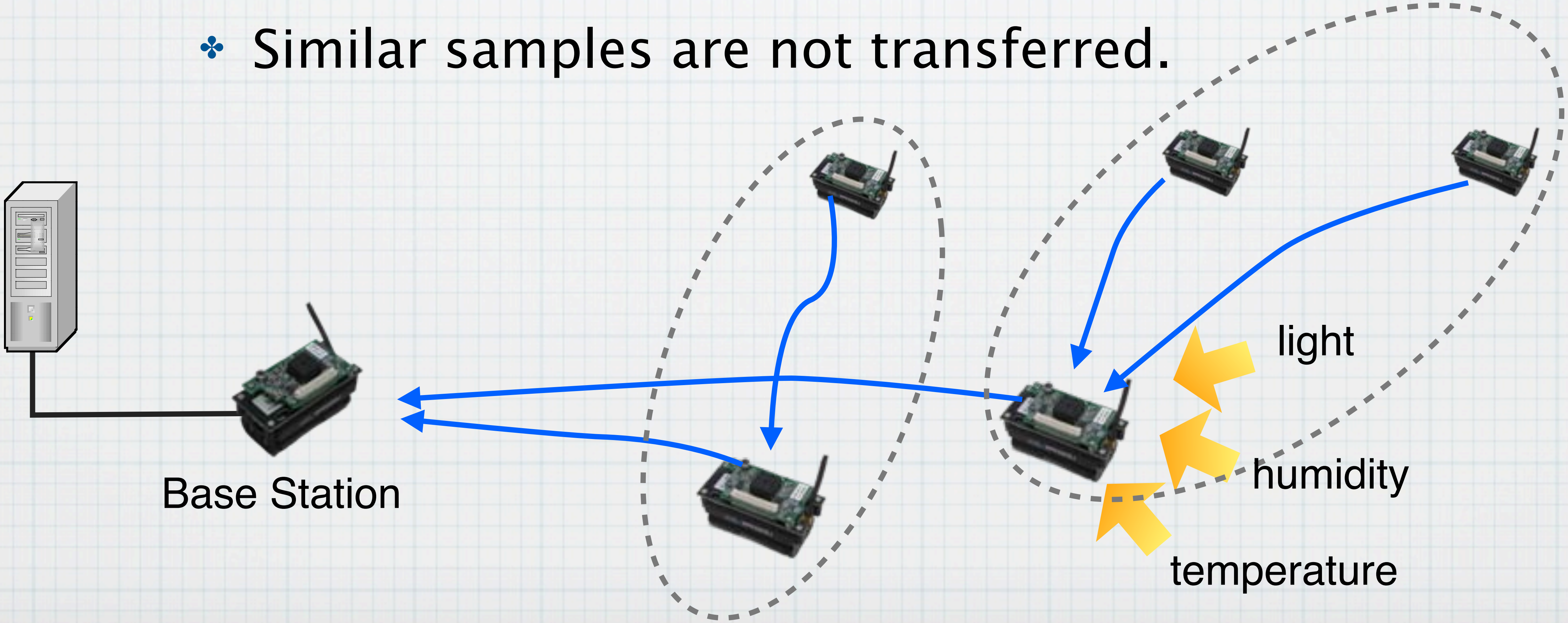
Wireless Sensor Networks (WSN)

- Gathering the sensed environmental information
  - temperature, humidity, light, acoustic, ...
- Wireless communication to the base station
  - Nodes can be located arbitrary position.
- Battery powered
  - Control of the power consumption is important.



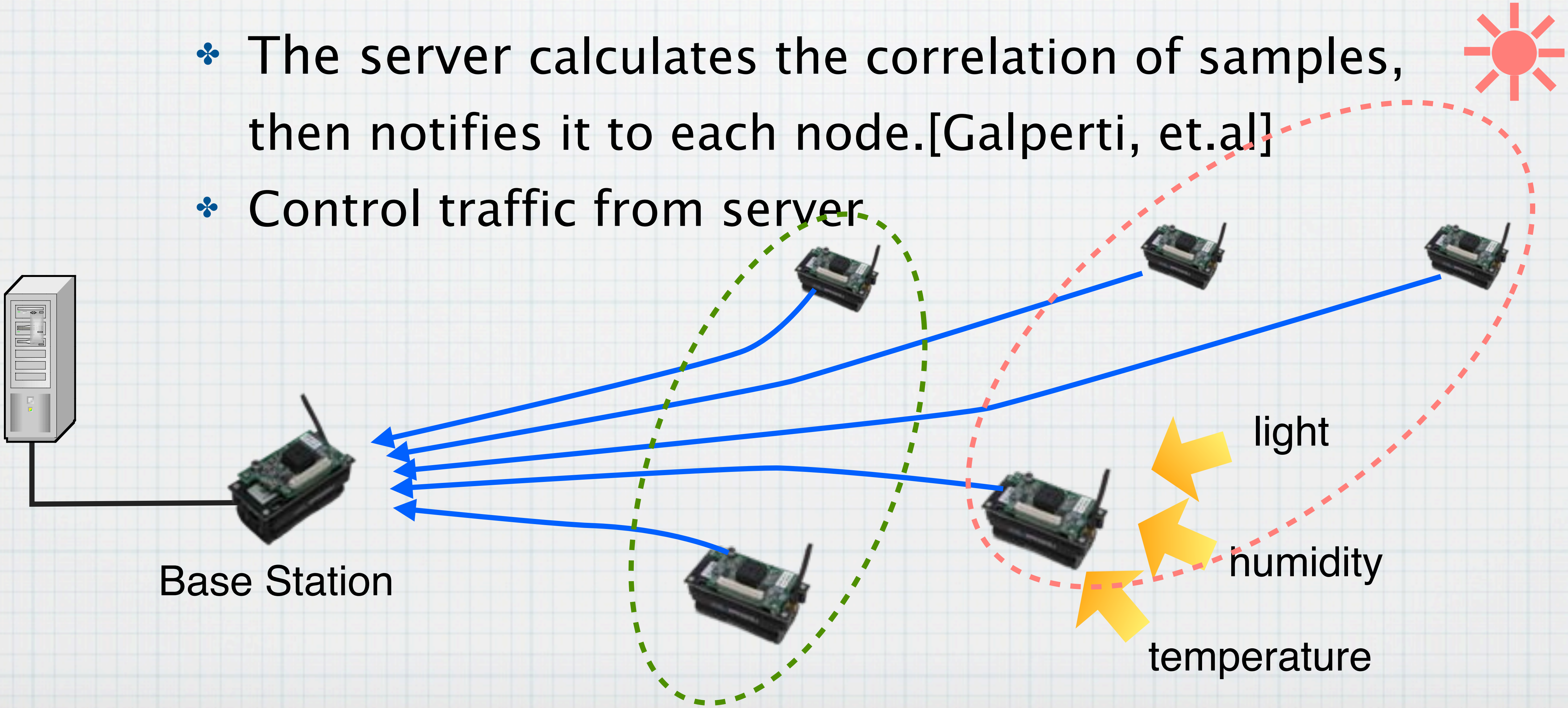
Power Saving on WSN

- Controlling power on the radio communication
  - Reduction of the total distance ... clustering
  - Reduction of data size
    - Nodes sensing similar results construct a cluster.
  - Reduction of communication frequency
    - Similar samples are not transferred.



Power Saving on WSN

- Controlling power on sensing (sampling)
  - Reduction of sampling frequency
    - This may suffer the quality of the sampled data.
  - Centralized control
    - The server calculates the correlation of samples, then notifies it to each node.[Galperti, et.al]
    - Control traffic from server



Autonomous Power Saving Control

- To keep the battery lifetime longer...
  - Power on communication module
    - Reduction of the distance between node
    - Reduction of the volume of data
    - Reduction of the frequency of data transfer
  - Power on sensing device
    - Reduction of the frequency of sampling
- Large number of nodes work together.
  - It is hard to manage/calibrate per-node basis.

Autonomous and self-optimized control is desirable.

Robustness in Autonomous Power Saving

- Centralized Control
  - Efficient and precise control can be achieved with enough computation power and data.
  - Lack of some special nodes may degrade the control.
- Decentralized Control
  - Good control scheme is required.
    - It need to work under low computation power with small amount of data.
  - Lack of any nodes suffer the control of the power consumption of the whole network.

Trust in Autonomous Power Saving

- Quality of gathered data
  - Schemes related to the radio communication
    - Fixed interval (in usual)
    - The interval is decided by each application’s request.
  - Schemes changing the sampling rate
    - Variable interval: it depends on the fluctuation of sampled results.
    - This scheme may drop the data when the interval becomes large.

ROBUSTNESS AND TRUST IN AUTONOMIC SYSTEMS

Panel @ ICAS 2010

Marc Zeller, Fraunhofer Institute for Communication Systems ESK

Robustness and Trust in Autonomic Systems

- ”Robustness is the invariance of [a property] of [a system] to [a set of perturbations]” (Alderson et al. 2007)

- Self-managing / autonomic artificial (engineered) systems provide a “natural” robustness to changes and failures
  - Systems with self-healing properties contain intrinsic recovery capabilities
  - Robustness also realized in many “traditional” systems

- Important is the **degree of robustness** the autonomic system exposes
  - Which failures can be “repaired” by the system itself?
  - The degree of robustness is an essential part of **Trust**

Robustness and Trust in Autonomic Systems

Trust in autonomic systems is an umbrella term for:

- Functional Correctness
  - Does the system actually do what it should do?
- Safety
  - Will there be any undesired effects?
- Security
  - Does the system prevent any unauthorized access?
- Robustness / Reliability
  - What is the probability that a service is available when it is needed?

system –oriented facets

- Credibility
  - Does the system fulfill legal requirements? (e.g. in the automotive or aviation domain)
- Usability

user-oriented facets

Robustness and Trust in Autonomic Systems

- Autonomic systems are highly dynamic, composed of a vast number of changeable components and are located in an ever changing environment
  - Important: Users must learn to trust such systems

- Main focus must be to develop **trustworthy** autonomic / self-managing systems
  - Systems which exhibit the desired behavior and prevent unwanted behavior (“Controlled Self-Organization”)
  - Systems which are trusted by the end-user
  - Systems which can be certified (e.g. fulfill certain regulations)
  - Systems which provide their services even under various disturbances (e.g. failures)

Robustness and Trust in Autonomic Systems – Future Research Directions

Yiming Ji and Lei Chen

Emails: yimingji@uscb.edu and chen@shsu.edu

University of South Carolina Beaufort

Sam Houston State University

Sam Houston
STATE UNIVERSITY
A Member of The Texas State University System

Future Research Directions (I)

- More effective radio propagation models
  - Provides dynamic radio estimation for 3-D environments
  - Consider representative indoor objects (desks, chairs, doors, windows, different partitions,….)
  - Consider impacts from weather / temperature / pressure or others

Future Research Directions (II)

- Impact of Radio Dynamics or Perturbations on the performance of indoor systems
  - Radio attacks, or non-cryptographic attacks that modify radio signals at reference landmarks
  - Impacts and solutions
  - This affects not only indoor location determination systems, but it is also an interesting direction for general sensor networks

Future Research Directions (III)

- Mobility modeling – these are the common factors considered
  - velocity
  - direction
  - Vehicles, pedestrians, others
- Security in mobile networks
  - Lightweight
  - Limited power
  - Range
  - etc.