PROCEEDINGS OF SPIE

Signal Processing, Sensor/Information Fusion, and Target Recognition XXV

Ivan Kadar
Editor

18–20 April 2016
Baltimore, Maryland, United States

Sponsored and Published by
SPIE

Volume 9842

Proceedings of SPIE 0277-786X, V. 9842

Signal Processing, Sensor/Information Fusion, and Target Recognition XXV, edited by Ivan Kadar, Proc. of SPIE Vol. 9842, 984201 · © 2016 SPIE · CCC code: 0277-786X/16/$18 · doi: 10.1117/12.2246519

The papers in this volume were part of the technical conference cited on the cover and title page. Papers were selected and subject to review by the editors and conference program committee. Some conference presentations may not be available for publication. Additional papers and presentation recordings may be available online in the SPIE Digital Library at SPIEDigitalLibrary.org.

The papers reflect the work and thoughts of the authors and are published herein as submitted. The publisher is not responsible for the validity of the information or for any outcomes resulting from reliance thereon.

Please use the following format to cite material from these proceedings:
Author(s), "Title of Paper," in *Signal Processing, Sensor/Information Fusion, and Target Recognition XXV*, edited by Ivan Kadar, Proceedings of SPIE Vol. 9842 (SPIE, Bellingham, WA, 2016) Six-Digit Article CID Number.

ISSN: 0277-786X
ISSN: 1996-756X (electronic)
ISBN: 9781510600836

Published by
SPIE
P.O. Box 10, Bellingham, Washington 98227-0010 USA
Telephone +1 360 676 3290 (Pacific Time) · Fax +1 360 647 1445
SPIE.org

Printed in the United States of America.

Publication of record for individual papers is online in the SPIE Digital Library.

SPIE. DIGITAL LIBRARY
SPIEDigitalLibrary.org

Paper Numbering: *Proceedings of SPIE* follow an e-First publication model. A unique citation identifier (CID) number is assigned to each article at the time of publication. Utilization of CIDs allows articles to be fully citable as soon as they are published online, and connects the same identifier to all online and print versions of the publication. SPIE uses a six-digit CID article numbering system structured as follows:

- The first four digits correspond to the SPIE volume number.
- The last two digits indicate publication order within the volume using a Base 36 numbering system employing both numerals and letters. These two-number sets start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B … 0Z, followed by 10-1Z, 20-2Z, etc. The CID Number appears on each page of the manuscript.

Contents

Authors

Numbers in the index correspond to the last two digits of the six-digit citation identifier (CID) article numbering system used in Proceedings of SPIE. The first four digits reflect the volume number. Base 36 numbering is employed for the last two digits and indicates the order of articles within the volume. Numbers start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B...0Z, followed by 10-1Z, 20-2Z, etc.

Conference Committee

Symposium Chair

David A. Logan, BAE Systems (United States)

Symposium Co-chair

Donald A. Reago Jr., U.S. Army Night Vision & Electronic Sensors Directorate(United States)

Conference Chair

Ivan Kadar, Interlink Systems Sciences, Inc. (United States)

Conference Co-chairs

Erik P. Blasch, Air Force Research Laboratory (United States)
Lynne L. Grewe, California State University, East Bay (United States)
Kenneth Hintz, George Mason University (United States)
Thia Kirubarajan, McMaster University (Canada)
Ronald P. S. Mahler, Random Sets, LLC (United States)

Conference Program Committee

Mark G. Alford, Air Force Research Laboratory (United States)
Bhashyam Balaji, Defence Research and Development Canada (Canada)
William D. Blair, Georgia Tech Research Institute (United States)
Mark J. Carlotto, General Dynamics Advanced Information Systems (United States)
Alex L. Chan, U.S. Army Research Laboratory (United States)
Kuo-Chu Chang, George Mason University (United States)
Chee-Yee Chong, Consultant (United States)
Marvin N. Cohen, Georgia Tech Research Institute (United States)
Frederick E. Daum, Raytheon Company (United States)
Jean Dezert, The French Aerospace Laboratory (France)
Mohammad Farooq, AA Scientific Consultants Inc. (Canada)
Laurie H. Fenstermacher, Air Force Research Laboratory (United States)
Charles W. Glover, Oak Ridge National Laboratory (United States)
I. R. Goodman, Consultant (United States)
Michael L. Hinman, Air Force Research Laboratory (United States)
Jon S. Jones, Air Force Research Laoratory (United States)
Georgiy M. Levchuk, Aptima, Inc. (United States)

Martin E. Liggins II, Consultant (United States)
James Llinas, University at Buffalo (United States)
Raj P. Malhotra, Air Force Research Laboratory (United States)
Alastair D. McAulay, Lehigh University (United States)
Raman K. Mehra, Scientific Systems Company, Inc. (United States)
Harley R. Myler, Lamar University (United States)
David Nicholson, BAE Systems (United Kingdom)
Les Novak, Scientific Systems Company, Inc. (United States)
John J. Salerno Jr., Harris Corporation (United States)
Andrew G. Tescher, AGT Associates (United States)
Stelios C. A. Thomopoulos, National Centre for Scientific Research Demokritos (Greece)
Wiley E. Thompson, New Mexico State University (United States)
Shanchieh Jay Yang, Rochester Institute of Technology (United States)

Session Chairs

1 Multisensor Fusion, Multitarget Tracking, and Resource Management I
Ivan Kadar, Interlink Systems Sciences, Inc. (United States)
Thia Kirubarajan, McMaster University (Canada)
Kenneth Hintz, George Mason University (United States)

2 Multisensor Fusion, Multitarget Tracking, and Resource Management II
Thia Kirubarajan, McMaster University (Canada)
Kenneth Hintz, George Mason University (United States)
Ivan Kadar, Interlink Systems Sciences, Inc. (United States)

3 Information Fusion Methodologies and Applications I
Ronald P.S. Mahler, Random Sets, LLC (United States)

4 Information Fusion Methodologies and Applications II
Michael L. Hinman, Air Force Research Laboratory (United States)
Ivan Kadar, Interlink Systems Sciences, Inc. (United States)
Kenneth Hintz, George Mason University (United States)

5 Information Fusion Methodologies and Applications III
Michael L. Hinman, Air Force Research Laboratory (United States)
Martin E. Liggins II, Consultant (United States)
Ivan Kadar, Interlink Systems Sciences, Inc. (United States)

6 Information Fusion Methodologies and Applications IV
Michael L. Hinman, Air Force Research Laboratory (United States)
Martin E. Liggins II, Consultant (United States)
Kenneth Hintz, George Mason University (United States)

7 Signal and Image Processing, and Information Fusion Applications I
Lynne L. Grewe, California State University, East Bay (United States)
Martin E. Liggins II, Consultant (United States)
Alex L. Chan, U.S. Army Research Laboratory (United States)

8 Signal and Image Processing, and Information Fusion Applications II
Alex L. Chan, U.S. Army Research Laboratory (United States)
Lynne L. Grewe, California State University, East Bay (United States)
Mark G. Alford, Air Force Research Laboratory (United States)

9 Signal and Image Processing, and Information Fusion Applications III
Lynne L. Grewe, California State University, East Bay (United States)
Martin E. Liggins II, Consultant (United States)
Alex L. Chan, U.S. Army Research Laboratory (United States)

Session Panel Members

Panel Discussion: Cyber Physical Systems Challenges with Information Fusion
Lynne L. Grewe, California State University, East Bay (United States)
Richard R. Brooks, Clemson University (United States)
Mehdi Kalantari Khandani, Resensys, LLC (United States)
Andres Kwasinski, Rochester Institute of Technology (United States)
Hairong Qi, The University of Tennessee Knoxville (United States)
Stelios C.A. Thomopoulos, National Centre for Scientific Research Demokritos (Greece)
Wei Yu, Towson University (United States)

Introduction

Cyber-Physical Systems consist of and depend on the close interaction and integration of the cyber, computational, and physical systems. Computational systems can include but are not limited to sensing and computer systems. The physical can be anything from the human to animal to plants as well as man-made systems. A key part of today's needed development in CPS involves creating new capabilities, adaptability, higher scalabilities, and usability as well as security and proficiency. Goals are to create new ways for people and the physical world to be part of and communicate with Cyber-Physical Systems.

Applications are varied including healthcare, automation, manufacturing, mobility/transportation, information fusion, active sensing, decision-making, intelligence and collaboration, challenging environments, information systems security, communications, networking, human integration and interaction with CPS, modeling human behavior, internet-of-things, smart cities, and more. For these reasons, Cyber-Physical Systems have a high possibility of transference into commercial and defense related endeavors in the near future.

The objective of this panel was to bring to the attention of the fusion community the importance of the application of Cyber Physical Systems, highlight issues, illustrate potential approaches and address challenges. A number of invited experts discussed challenges of the CPS processing and research in order to address these challenges with information fusion. The panelists illustrated parts of the above-mentioned areas over different applications and in association with information fusion. The panel highlighted impending issues and challenges using conceptual and real-world related examples associated with the applications of CPS.

Ivan Kadar
Lynne L. Grewe

Invited Panel Discussion

Cyber Physical Systems Challenges with Information Fusion

Organizers

Lynne Grewe, California State Univ., East Bay.

Ivan Kadar, Interlink Systems Sciences, Inc.

Erik Blasch, Air Force Research Lab.

Moderators

Ivan Kadar, Interlink Systems Sciences, Inc.

Lynne Grewe, California State Univ., East Bay

April 18, 2016

SPIE Conference 9842

"Signal Processing, Sensor Fusion and Target Recognition XXV"

Baltimore, MD., 18-20 April 2016

Invited Panel Discussion

Panel Participants

Prof. Richard R. Brooks, Clemson Univ., USA

Prof. Lynne Grewe, California State Univ., East Bay, U.S.A.

Prof. Andres Kwasinski, RIT, Rochester, NY, U.S.A.

Prof. Hairong Qi, Univ. of Tennessee, U.S.A.

Dr. John Salerno, Harris Corp., U.S.A.

Dr. Stelios Thomopoulos, Natl. Ctr. for Scientific Research Demokritos, Greece.

Prof. Wei Yu, Towson Univ., U.S.A.

Invited Panel Discussion
Topics

"Life and Death Decisions by Cyber-Physical Systems"
Prof. Richard R. Brooks, etal., Clemson Univ., and Prof. Chase Wu, NJ Institute of Technology.

"Information Fusion in Challenging Environments for Human-Centric Cyber Physical Systems "
Prof. Lynne Grewe, etal., California State Univ.

"Cross-Layer Framework in the Internet of Things for Cyber-Physical Systems"
Prof. Andres Kwasinski, Rochester Inst. of Technology

"Collaborative Processing in Smart Camera Networks "
Prof. Hairong Qi, Univ. of Tennessee

Invited Panel Discussion
Topics

"Panel on Cyber Physical Systems Challenges with Information Fusion: Control Systems – Examples of Cyber-Physical Systems"
Dr. John Salerno, Harris Corp.

"Cyber Physical (C-P) Systems Challenges with Information Fusion: *Modeling & Programing*"
Dr. Stelios C.A, Thomopoulos, Natl. Ctr. for Scientific Research Demokritos, Integrated Systems Lab., Greece.

"On Secure and Resilient Energy-Based Critical Infrastructure"
Prof. Wei Yu, Towson Univ.

Life and Death Decisions by Cyber-Physical Systems

Richard R. Brooks[1], Xingsi Zhong[1], Guthrie Cordone[1],
G. K. Venayagamoorthya[1], and Chase Wu[2]
[1]Holcombe Dept. of ECE, Clemson University, Clemson, SC, USA
[2]Dept. of Computer Science, New Jersey Institute of Technology,
Newark, New Jersey

March 4, 2016

Outline

- Overview
- Radiation Detection and Localization
- Distributed Vehicle Behaviors
- Smart Grid Cyber Security
- Conclusions

Overview

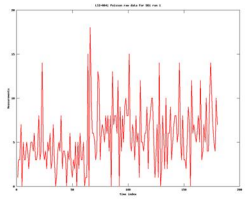
Figures from internet

The Need for Detection and Localization

- Detection and localization of radioactive sources is critical for maintaining national security
- Detonation of a dirty bomb in a populated area would be catastrophic
- Immediate health problems due to high radiation exposure
  - nausea
  - vomiting
  - death

Challenges

- There are four major reasons that detection and localization of a radioactive source is a difficult task
  - Radiation counts follow a Poisson distribution
  - Background radiation can causefalse positives
  - Radiation signal strength due to a point source follows the inverse square law
  - Obstacles between the detector and the source attenuate the radiation signal



Radiation Source Detection

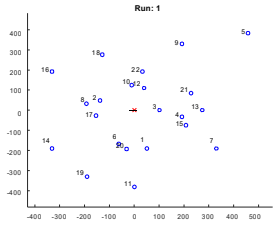
- Detection methods often based on statistical processing
- Detection with a single sensor (portals)
  - Smoothing filters (moving average, exponetial smoothing filter)
  - Sequential Probability Ratio Test (SPRT)
- Detection with multiple sensors
  - Data fusion methods
  - Decision fusion methods

Radiation Source Localization

- Estimate the location of one or more point sources within a detector field
- Geometric Localization Methods
  - Time Difference of Arrival (TDOA)
  - Ratio of Squared Distances (ROSD)
- Statistical Localization Methods
  - Particle Filter
  - Kalman Filter
  - Maximum Likelihood Estimation

Benchmark Radiation Datasets

- Datasets compiled for testing of detection and localization methods
- Test case is a field of detectors with one or more radiation sources
- Each dataset varies the source strength, source location, and number of sources
- Allow testing of may different scenarios



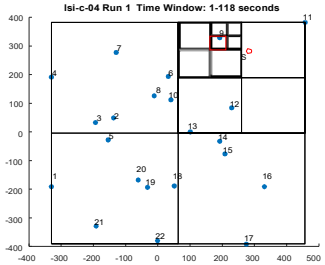
Maximum Likelihood Localization of Benchmark Datasets

- Use Maximum Likelihood Estimation (MLE) to localize source in benchmark datasets
- Divide field into grid and choose most likely grid as location of source

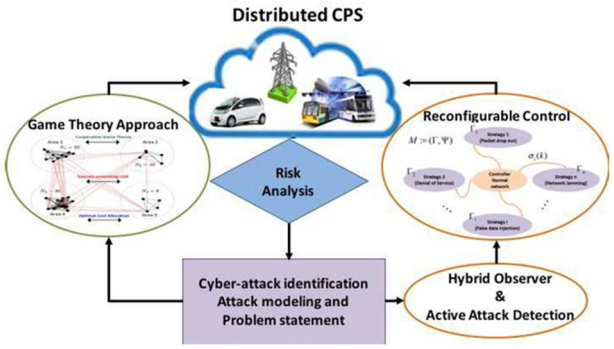
$$(\hat{A}_s, \hat{x}_s, \hat{y}_s) = \text{argmax} \sum_{i=1}^{18} \left[\left(\sum_{j=1}^{n_i} y_{i,j} \right) \ln(\lambda_i^{(m,n,p)}) - n_i(\lambda_i^{(m,n,p)}) \right] . \quad (1)$$

Maximum Likelihood Localization of Benchmark Datasets

- Multiple-layers with a small grid is much faster than a single layer with a large grid
- Issues with our MLE implementation
  - Selected grid biased to be near strongest detector
    - Need to determine optimal grid size to iteration ratio



Distributed Vehicle Behaviors



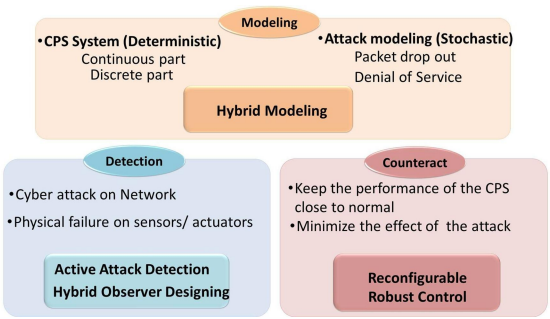
Motivation 1

- Intrusion detection systems (IDS) neither reliably detect nor distinguish cyber-attacks from normal operations.
- Some IDS product comparisons find using an IDS worse than letting hackers into your system.
- There are additional challenges for Cyber-Physical Systems.
- Damages in connected vehicle applications can include:
  - False data injection to lower system performance (ex. fuel efficiency)
  - Vehicle collisions.
- Cyber-security for connected vehicles has many interested parties: individual owners, OEMs, component suppliers, fleet operators, car dealerships, insurance companies, police, EPA, vehicle repair shops, pedestrians and effectively society as a whole.

Motivation 2

- Cyber Physical System (CPS), consists of:
  - Physical plant
    - Multi agents/ Interconnected system
    - Sensors / Actuators
  - Communication network
    - Global
    - Local
- Intentional disruption
  - Fraudulent information
  - Denial of service
  - Code/data inertion, etc.
- Physical failure
  - Sensors / Actuators

Cyber attacks on individual subsystem

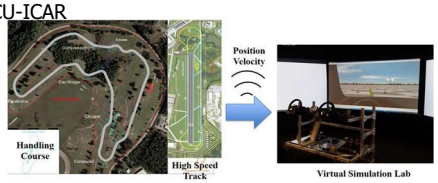


Compromised subsystem in a distributed CPS

- Game Theory : Attack Resilient Countermeasure
  - One or more than one of the subsystems in distributed networked CPS are malicious
  - Malicious components trying to maximize the global cost function
  - The rest of the group want to minimize the cost function
  - Win- lose Game theory
  - Control countermeasure is performed based on game theory

Experimental Setup

- Experimental testing and validation has 2 main components
  - CV testbed located at South Carolina Technology
    - More than 2.5-miles of straightaway test track,
    - 2.5-mile interstate-grade test track (expandable up to 17.5 miles) DSRC-based communication network for V2V and V2I
  - Aviation Center (SC-TAC); a CV virtual/simulation lab at CU-ICAR



Connected Vehicle Testbed at SC-TAC

Synchrophasor Devices in Smart Grid

- A phasor measurement unit (PMU) or synchrophasor is a device which measures the electrical waves on an electricity grid.
- Phasor Data Concentrators (PDC) are used to collect the measurements from PMUs.
- Security gateways can create VPN tunnels between secured networks. The security gateways can encrypt the packets, provide anonymity and protect the traffic. Encrypted PMU traffics are still vulnerable to side-channel attacks.

Documented security vulnerabilities

- Documented security vulnerabilities:
  - 1. Denial of Service
  - 2. Physical Attack
  - 3. Man in the Middle
  - 4. Packet Analysis
  - 5. Malicious Code Injection
  - 6. Data Spoofing

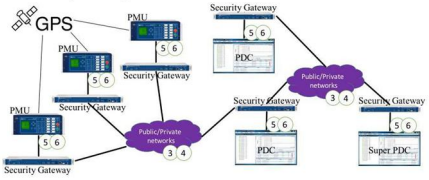
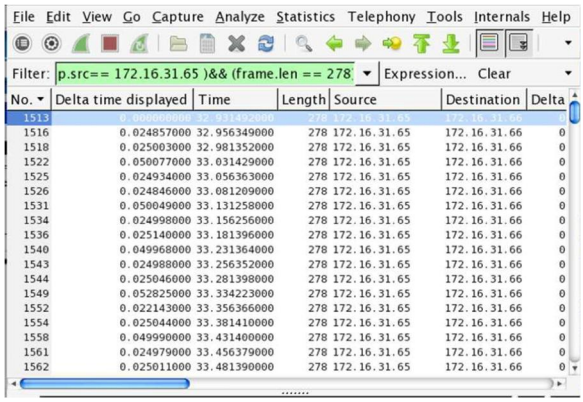


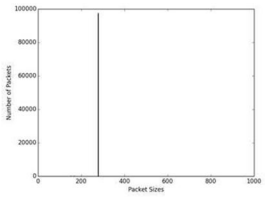
Fig. 1. An illustration of a synchrophasor network and vulnerabilities. Note that (1) (2) can affect entire network.

Side-Channels in PMU Traffic

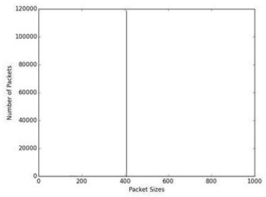


Packet Size Side-Channel

PMU model A

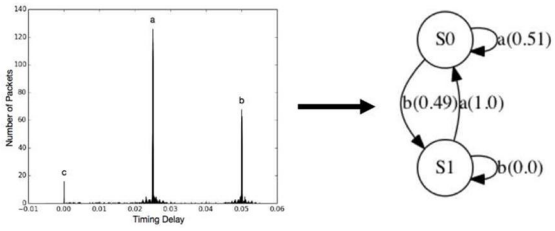


PMU model B



$$S_{cypher} = 54 + \lfloor \frac{S_{clear}}{16} + 1 \rfloor \times 16$$

Inter Packet Timing Side-Channel



Side-Channel Analysis

- Packet size and inter-packet timing side-channels can distinguish the packets generated by different PMUs sent through an encrypted VPN tunnel.
- Those side-channels can be exploited to redirect or drop a target network communication instance and remains accessibility to the remote host device within a VPN tunnel.
- It could be difficult to detect the attack since the network session is still available.

Conclusions

- Radiation detection – data from multiple inputs obscured by noise in an unstructured environment. MLE based detection and localization methods are designed;
- Automotive applications – Fault tolerance is hard to design correctly, since combinations of faults can be hard to foresee. Instead controllers should make minimal assumptions and assume the worst; and
- Smart grid – commonly used encrypted communication methods ignore many know problems. VPN tunnel established by security gateways are susceptible to side-channel attack.

Life and Death Decisions by Cyber-Physical Systems*

Richard R. Brooks[a], Xingsi Zhong[a], Guthrie Cordone[a], G. K. Venayagamoorthy[a], and Chase Wu[b]

[a]Holcombe Dept. of ECE, Clemson University, Clemson, SC, USA
[b]Dept. of Computer Science, New Jersey Institute of Technology, Newark, New Jersey

ABSTRACT

This talk considers information fusion problems embedded in national critical infrastructure. We discuss three current research problems:

1. *Detection of radiation sources* – Reliable detection is needed to stop covert smuggling of nuclear materials into the US. It is also important to keep "dirty" bombs away from attractive targets of opportunity. Detection of nuclear material is challenging. This is due both to radiation signals following a Poisson distribution and background radiation being ubiquitous. We discuss current approaches for reliable detection/localization of radiation sources within acceptable false alarm rates;
2. *Distributed vehicle behaviors* – Self-driving cars are no longer science fiction. Applications, such as collision avoidance and platooning, posit interactions between multiple vehicles that are owned and maintained by more than one entity. To avoid disaster, what assumptions can be made when designing and implementing these behaviors? To make the system robust, it is best to make no assumptions. We explain design principles for implementing a platooning system that functions well, even when interacting with poorly-maintained vehicles.
3. *The electric grid* – creating an effective feedback loop can make the electric grid more efficient and able to include renewable power sources like wind and solar. Synchrophasor sensors send real-time information to power gird control centers. These network feeds are secured using virtual private networks to prevent attackers from manipulating sensor signals. We explain how these security mechanisms are vulnerable to disruption. We also consider how these vulnerabilities are inherent to the current IP network design.

We give an overview of current challenges in the design and deployment of cyber-physical systems.

Keywords: Cyber-physical systems, smart grid, radiation detection, security, information fusion.

1. INTRODUCTION

Information technology should make the national infrastructure safe, efficient and sustainable. Feedback loops gather information, make decisions, and control the system. This paper briefly presents three representative research challenges; using them to illustrate the impact of information fusion on our cyber-physical infrastructure.

2. RADIATION DETECTION AND LOCALIZATION

Detecting and locating radiation sources is critical for maintaining national security. The detonation of a dirty bomb near a populated area would have grave personal and economic impact. Health issues caused by high amounts of radiation exposure include tissue damage, cancer, and death. Radiation detection and localization is challenging, because:

*Part of this work has been supported in part by the U.S. Department of Homeland Security, Domestic Nuclear Detection Office, under competitively awarded contract No. IAA HSHQDC-13-X-B0002; NSF under award number CPS #1544910 and NSF under award IIP #1312260. This support does not constitute an expressed or implied endorsement on the part of the Government.
Further author information: (Send correspondence to R. R. Brooks)
R. R. Brooks: E-mail: rrb@acm.org, Telephone: 1 864-656-0920

1. Radiation counts follow a Poisson distribution, where the variance of the signal is proportional to the mean (see Figure 1);
2. Non-negligible amounts of background radiation are ubiquitous;
3. Obstacles between the source and the point of measurement attenuate the signal; and
4. Radiation signals are inversely proportional to the square of the distance between the source and the sensor.

Detection of radiation signals using a single detector, without triggering a significant number of false alarms, is hard. The problem is more difficult with multiple sensors in an unstructured environment. Detection methods are often based on statistical processing. It is possible to average readings over a window and use one-sided z, F, χ^2, or SPRT tests to see if readings are from the same distribution as the background radiation. Localization uses triangulation, particle filters, or maximum likelihood estimation. One innovative tool for detection is to first attempt to localize the source(s) using random subsets of sensors. If no source is present, then the localization results will be spread across the sensing region. But if a source is present, then the results will tend to cluster. DHS is collecting data; making benchmark data-sets available to researchers; and also sponsoring research on radioactive source detection and localization. The goal is to create reliable networks of radiation sensors that have high detection and low false positive rates.

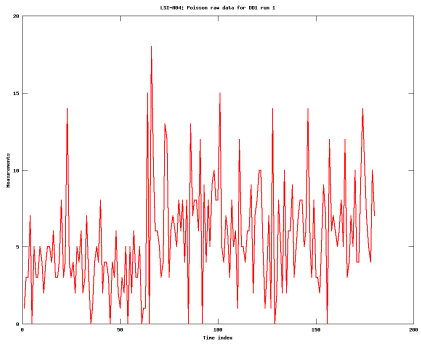


Figure 1. Time series where a radiation source is exposed after 60 seconds.

3. DISTRIBUTED VEHICLE BEHAVIORS

Automated parking, fully autonomous driving and coordination among multiple vehicles are no longer science fiction. Platooning[1] allows vehicles to follow each other in a group. Air drag is reduced; mileage increased; and total emissions reduced. Platooning requires automated control systems and frequent information exchange among vehicles to maintain the proper distance between vehicles. Poor decisions and unreliable controls can cause accidents when driving in a platoon with poorly-maintained or -behaved vehicles. Decisions based on perfect information[2] can achieve desired results. However, this information can be inaccurate due to device failures or possibly cyber-attacks. All cyber-physical components have the common challenge of operating correctly, while interacting with neighbors that may be faulty. To design reliable systems, we assume in the design stage that some components will be malicious. If the controller is able to work properly, even when intentionally deceived, it should be able to remain robust when its neighboring components fail. This is based on the well-known Byzantine Generals problem.

4. SMART GRID CYBER SECURITY

The "smart grid" uses information and communication technologies to increase the efficiency, reliability, and sustainability of the power grid.[3] This requires real-time monitoring for situational awareness. However, the use of networking technologies for situational awareness can make the electric grid susceptible to cyber-attack.[4] Phasor Measurement Units (PMUs) provide feedback of the current state of the power system in real time. PMUs communicate bus voltages, line currents, and bus frequencies in the transmission systems in real-time to

Documented security vulnerabilities:

PMU Attacks:	General Class of Attack:
1 Denial of Service	Interruption
2 Physical Attack	Interruption
3 Man in the Middle	Interception
4 Packet Analysis	Interception
5 Malicious Code Injection	Modification
6 Data Spoofing	Fabrication

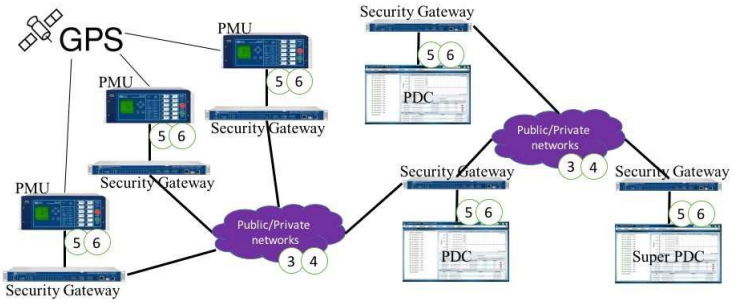


Figure 2. An illustration of a synchrophasor network and vulnerabilities. Note that 1 and 2 can affect entire network. .

the substation/control center using TCP/IP network connections. Each measurement is tagged with a global positioning system (GPS) time stamp.[5] Figure 2 shows documented security vulnerabilities in an example PMU network. Security gateways create Virtual Private Network (VPN) tunnels.[4] They connect two secured networks through an unsecured network; encrypting and decrypting packets' data.[6] Side-channel attacks extract information by observing implementation artifacts. Inter packet timing side-channel and packet size side-channel can recognize encrypted PMU traffic.[6] A Hidden Markov Model (HMM) is built using inter-packet delays, where packets are captured from encrypted PMU traffic between two security gateways. HMM inference and packet size side-channel recognize encrypted PMU traffic and can isolate packets from specific devices. This vulnerability can be exploited by an attacker to redirect or drop a target network communication instance and remain accessible to the remote host device even if all traffic is encrypted.[6]

5. CONCLUSIONS

This paper introduces cyber-physical designs that highlights information fusion challenges:

- Radiation detection – illustrates the challenge of combining multiple inputs obscured by noise;
- Automotive applications – need to make correct decisions even when working with other poorly maintained, or even deceptive, components; and
- Smart grid – designs pass data through unprotected networks, where current security tools ignore a number of known security problems.

REFERENCES

[1] Jia, D., Lu, K., Wang, J., Zhang, X., and Shen, X., "A survey on platoon-based vehicular cyber-physical systems," *Communications Surveys Tutorials, IEEE* 18, 263–284 (Firstquarter 2016).

[2] Brooks, R., Pang, J.-E., and Griffin, C., "Game and information theory analysis of electronic countermeasures in pursuit-evasion games," *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on* 38, 1281–1294 (Nov 2008).

[3] Venayagamoorthy, G., "Dynamic, stochastic, computational, and scalable technologies for smart grids," *Computational Intelligence Magazine, IEEE* 6, 22–35 (Aug 2011).

[4] Beasley, C., Zhong, X., Deng, J., Brooks, R., and Kumar Venayagamoorthy, G., "A Survey of Electric Power Synchrophasor Network Cyber Security," in [*Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2014 IEEE PES*], 1–5 (Oct 2014).

[5] Narendra, K. and Weekes, T., "Phasor measurement unit (pmu) communication experience in a utility environment," in [*Conference on Power Systems, Winnipeg, October*], 19–21 (2008).

[6] Zhong, X., Arunagirinathan, P., Ahmadi, A., Brooks, R. R., and Venayagamoorthy, G. K., "Side-channels in electric power synchrophasor network data traffic," in [*Proceedings of the 10th Annual Cyber and Information Security Research Conference*], ACM, Oak Ridge, Tennessee, USA (2015).

InformationFusion in ChallengingEnvironmentsfor Human-Centric CyberPhysicalSystems

Lynne Grewe[a], Christopher Lagali[a] and William Overell[a]
[a]Computer Science, California State University East Bay, 25800 Carlos Bee Boulevard, Hayward, CA USA, 94542

Challenges in CPS: Humans and Information Fusion

- How can humans influence Information Fusion based CPS?
- How do Humans integrate into Information Fusion based CPS?
- What kinds of modeling is present for humans-in-the loop?
- How can these models alter human'sroles?
- Can we adapt to particular users?

Explore

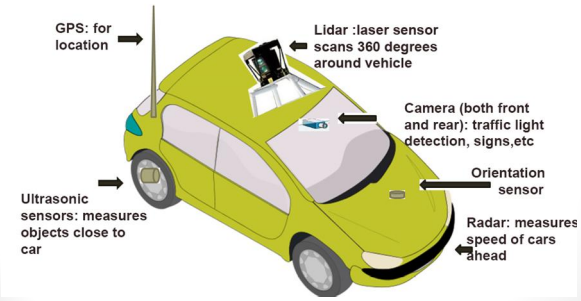
- Human oriented **applications** in Information Fusion based Cyber Physical Systems
- Human **Integration & Interaction** with Information Fusion based Cyber Physical Systems
- Human **Safety** influences on Information Fusion based Cyber Physical Systems.
- **Human Scale & Performance** in Information Fusion based Cyber Physical Systems.

Human APPLICATIONS & modeling

- Applications who's purpose is to involve or serve humans
- Many different sectors:
  - Transportation
  - Medical
  - Safety/Security
  - Lifestyle
- Can we model humans and adapt to them in general or to specific users?

Example 1: Self-driving car

- Information Fusion using range of sensors
- Application Purpose: Drive people (and things)
- Numerous companies: Uber, Google, Apple



Example 2: Blind Bike

- Information Fusion: Video, GPS, Gyroscope on Mobile Phone
- Assist Low-Vision People with task of biking:
  - Road following
  - Navigation with Intersection dectection

Model:
Model Human Actions that can take place in the operating conditions of the CPS

Intent:
Understand Human Intent*

Actions:
Understand Human Actions that can Impair System operations (see safety)*

Adapt:
Create CPSs that adapt to the human currently using the system for use in adjusting modules or even for determination of human inclusion*+

HUMANAPPLICATIONRECOMMENDATIONS

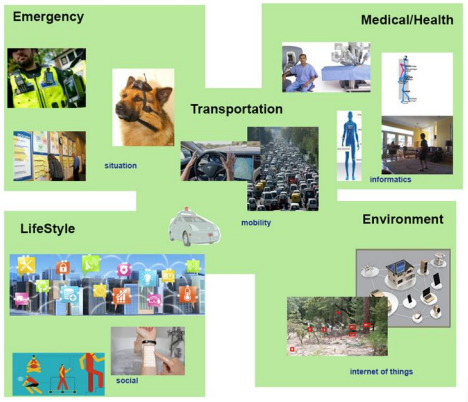
(*) impacts for Safety (+) impacts for selection of Human interaction/integration

Human INTEGRATION/INTERACTION

Consider the different stages the human can integrate into the CPS

- Human Gather Info
- Human aide Fusion
- Human Share/Social
- Human-Autonomy level
- Human Fusion presentation

Human INTEGRATION/INTERACTION Human as information collectors

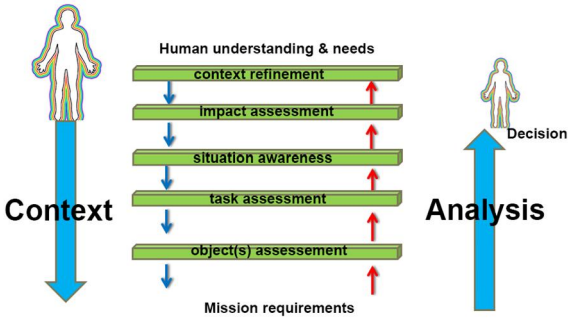


Human aided Fusion

- Example DiRecT – where user controls what data to fuse
  - user provides information for fusion including location information (for map retrieval) and intelligence reports, visual imagery and more
  - user selects which data sources for visualization
  - user controls settings for uncertainly calculations in fusion and visualizations

Human aided Fusion- context

- Humans good at context –influence fusion

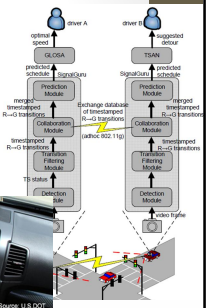


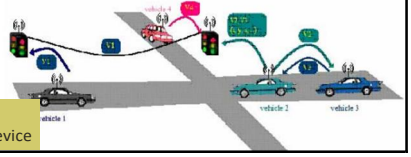
see E. Blasch, "Contextaided sensor and human-based information fusion", Aerospace and Electronics Conference, NAECON, pp. 127-134, 2014

Human Share/Social

Transportation Domain

- Traffic light sharing
- Google Traffic monitoring
- Map building
- Issues: privacy



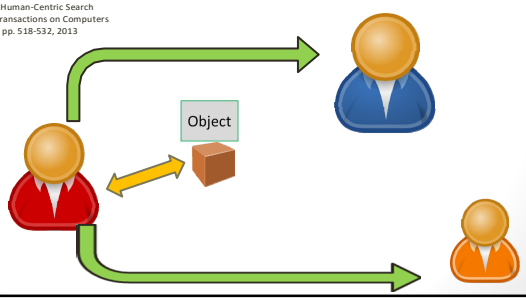


IoT
Vehicle = Mobile Device

Example: Human Social/Sharing

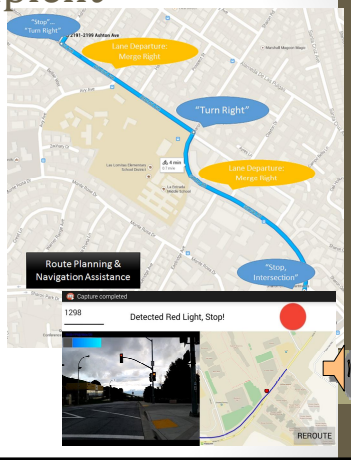
- Discovering the world of objects
- Here users share the knowledge of object existence --- for "Object Search" knowledge

See: H. Shen, J. Liu, K. Chen , J. Liu, S. Moyer, " SCPS: A Social-Aware Distributed Cyber-Physical Human-Centric Search Engine", IEEE Transactions on Computers Vol 64, Issue 2, pp. 518-532, 2013



Human as Recipient

- Simplicity, Ease of reception
- Situational constraints
- Technologies: Speech, Visualization



Information Gathering: Humans can be useful in some applications for gathering or directing system to gather data
Human Information Fusion: Humans can excel at contextual awareness and be used to help direct Information Fusion
Autonomy Level: Level can vary for each "component" of system. Naturally increase level for components that are less mission critical or only workable by machines. Decrease level when tolerance of errors increases.
Sharing/Social Data: Dissemination of data through Distributed Systems or to Centralized Systems can improve operations+
Mission Critical: Keep humans in the loop, where possible revert to human control (kill switch)*
Human Recipient: Audio, Visualization, Let Situation drive and understand of user, effect info gathered?
HUMANINTERACTION/INTEGRATIONRECOMMENDATIONS

(*) impacts for Safety (+) impacts for Privacy concerns

Fault-Tolerance:
Verification processes, model integration from multiple sources to understand fault-error-symptomcharacteristics*

Monitor:
Monitor sensors functionality, response accuracies, degradation of performance gracefully and/or leading to human intervention*

Human Modeling:
Model human's role in system, predict human behavior, monitor responses*+

Security Protocols:
Use current protocols to secure data and any transmission of data+

Invasiveness level:
minimize when possible human invasive procedures*

Communications:
Encourage communications between human and system and between multiple systems, warning systems*+

RECOMMENDATIONSFOR SAFETY/SECURITY

(*) impacts for Safety (+) impacts for Security concerns

Human Scale

- Some systems only need to respond to human based speeds like blindBike

Human Performance

- Can we model how effective a human is?
- Can we alter the level of integration of a particular user based on their performance?

Conclusions

- Humans make interesting applications
- Humans add challenges in safety and security
- Humans add opportunities in every aspect of an Information Fusion CPS.
- Consider recommendations

Information Fusion in Challenging Environments for Human-Centric Cyber Physical Systems

Lynne Grewe[a], Christopher Lagali[a] and William Overell[a]
[a]Computer Science, California State University East Bay, 25800 Carlos Bee Boulevard, Hayward, CA USA, 94542

ABSTRACT

Information Fusion is critical and faces special challenges and opportunities for Cyber Physical Systems when humans are in the loop. We will look at all aspects of humans in Information Fusion based Cyber Physical Systems such as safety and security and how this can constrain or enhance the Information Fusion task. As part of this we, explore two Cyber Physical Systems, blindBike and Senior Collapse Detection systems. blindBike is a novel system that uses cyber-physical techniques to assist in the process of bicycle driving and navigation for people with low vision, The second system, SCD, Senior Collapse Detection, uses information fusion and again a consumer sensor, the Kinect, to again achieve the goals of human safety and security in a system that assists seniors when they fall and need assistance in their homes. An overview of current information fusion challenges and recommendations in human-centric, human-in-the-loop Cyber Physical Systems conclude the discussion.

Keywords: Cyber physical systems, information fusion, human-in-the-loop, bike navigation

1. INTRODUCTION

Human involvement in Cyber Physical Systems present challenges, opportunities and new possibilities for Information Fusion. The inclusion of humans can lead us to imaginative applications and integrations in Cyber Physical Systems. We will explore how people can integrate into many different stages of a Cyber Physical Systems: from input/information gathering, aiding fusion, processing and presentation.

2. HUMAN APPLICATIONS IN INFORMATION FUSION BASED CPS

A trendy human oriented application for Information Fusion based Cyber Physical Systems is autonomous driving with companies such as Uber[1], Google[2], Apple[1] involved. In these systems, a number of sensors such as Lidar, video cameras, ultrasonic sensors and radar sensors are being used. The human is involved in two ways, in the result of their transport but, also, currently most systems have kill switch for the humans to take over driving.

Another human oriented CPS, blindBike[4,5], assists low-vision people for the task of biking. In this system, the human is integral in the system as the bike is powered and steered by the human and the CPS tracks progress prompting for road placement correction and navigaton (Figure 1). blindBike uses a camera, GPS, gyroscope, and audio sensors that are available on the relatively low cost mobile phone mounted on the bike's handlebars.

Other applications of human oriented CPSs include human monitoring. In [6,7], the Senior Collapse Detection system is described which monitors senior citizens living at home when falls occur and the senior needs medical assistance. This system fuses 3D, 2D and audio sensors. There is a wide range of human monitoring Information Fusion based CPSs that occurs for applications like disaster relief [8] and security. The list of Information Fusion based CPSs who's main application involves a human are too numerous to list and they span all the numerous areas of medicine, transportation, life-style and can be used to replace and/or assist with basic human sensors and decisions.

The best of Human-in-the loop Information Fusion based CPSs seek to understand and even model the human for

their application purposed. For example in [7], SCD, our system for detecting collapses/falls of seniors in their homes, models the mobility and movement of seniors using physical therapy data for seniors based on demographics like age and gender. Adaptation to a particular user is also possible as shown in [7,8] where SCD, our system for detecting collapses/falls adapts to the user's height to adjust its selection of a human model. Table 1 shows some general recommendations for Human-based Applications.

Figure 1: Low-vision person with blindBike mobile app: assists user with road placement, navigation.

Recommendations For Human APPLICATIONS in Information Fusion based CPSs
Model: Model Human Actions that can take place in the operating conditions of the CPS
Intent: Understand Human Intent*
Actions: Understand Human Actions that can Impair System operations (see safety)*
Adapt: Create CPSs that adapt to the human currently using the system for use in adjusting modules or even for determination of human inclusion*

Table 1: Recommendations Information Fusion based CPS APPLICATIONS (*) impacts Safety

3. HUMAN INTEGRATION & INTERACTION IN INFORMATION FUSION BASED CPS

Humans can be brought into an Information Fusion System via direct integrations and interactions in the following ways: Information Gathering, Fusion Assistance, Autonomy level, Presentation and Sharing/Social Interactions. First, humans can be used to provide information to the system. For example in [8], the DiRecT system performs information fusion on human provided data including intelligence reports. There are numerous examples of human data collection in the CPS area referred to as "Smart Cities" [9-11]. Here you see some of the future ideas of humans wearing multiple sensors and devices used to collect information for not only use by the user themselves but, for the greater good of the community. Commercial endeavors such as 3D advanced map building, shared maps and traffic monitoring are also currently active where humans are the collectors of data for fusion [12].

Humans can also be used for Fusion Assistance. For example, in [8], the system lets the user select what data is fused for visualization in a disaster relief situational awareness tool. Humans are particularly good at understanding the context of a situation and when different rules of information fusion might apply [13].

One design decision of a Human in the loop Information Fusion based CPS must make, is the level of system autonomy. We have examples of temporally limited autonomous operational modes like airplane landing, car parking and even the self-driving cars which at least for a time interval are fully autonomous. Other systems, like blindBike, simply assist the user. We see this semi-autonomous or assistive level of operation mode in domains where safety is key like medicine or in very challenging environments like blindBike where restrictions on technology or accuracy in all scenarios are not adequate (bike at tilt angle where only asphalt is visible).

Sharing/Social interactions between human based CPSs can be useful for greater collection of information for the fusion process prior to decision making. In [14] the authors describe a system whereby the CPSs automatically

share information about traffic lights for ease in intersection detection and traffic navigation. Another example is in [15], where a system for "Object Searching" is developed and objects info is provided by humans.

Humans may be the direct recipients of CPS information such as situational awareness CPSs (e.g. DiRecT for disaster relief [8]), medical applications (e.g. SCD [6,7]), information systems (e.g. navigation assistance in blindBike [4,5] see Figure 2). Understanding both physical and mental behavior as well as the situational constraints is important. Table 2 presents some general recommendations for human interaction/integration.

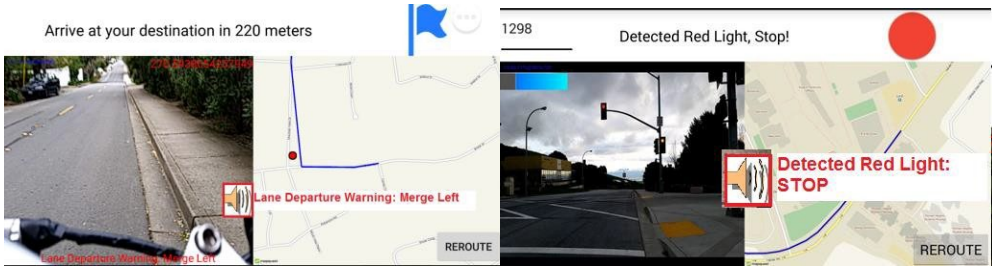


Figure 2: blindBike directs low vision person with auditory prompts for road following and intersection detection.

Recommendations For Human INTEGRATION/INTERACTION in Information Fusion Based CPSs
Information Gathering: Humans can be useful in some applications for gathering or directing system to gather data
Human Information Fusion: Humans can excel at contextual awareness and be used to help direct Information Fusion
Autonomy Level: Level can vary for each "component" of system. Naturally increase level for components that are less mission critical or only workable by machines. Decrease level when tolerance of errors increases.
Sharing/Social Data: Dissemination of data through Distributed Systems or to Centralized Systems can improve operations+
Mission Critical: Keep humans in the loop, where possible revert to human control (kill switch)*
Human Recipient: Audio, Visualization Let Situation drive and understand of user. How can this influence choice of information gathered for fusion.

Table 2: Recommendations for Human-IN-THE-LOOP Information Fusion based CPS Applications (*) impacts for Safety (+) impacts for Privacy concerns

4. HUMAN SAFTEY & SECURITY IN INFORMAITON FUSION BASED CPS

When humans are part of a system, both safety and security must be considered. Processes involving fault-tolerance and verification can be used to minimize safety risks. However, more futuristic approaches to safety could be used such as human behavior prediction and adaptation and in [16] they even suggest reading of human brain waves to accomplish this task. Safety can be increased by incorporating multi-modal sensor data as shown in blindBike [5] where knowledge of current location and navigation route information can be used to predict occurrence of upcoming intersections where special caution can be taken for user safety.

Security can mean security of data in an Information Fusion based CPS where that information reveals information about the human user. There is a lot recent concern over privacy of human location tracking in traffic monitoring systems. Other privacy/security concerns are around the collection and use of personal information. Table 3 shows a set of recommendations for the safety and security of Human-in-the loop Information Fusion based Cyber Physical Systems.

Recommendations For SAFEY & SECURITY in Information Fusion based CPSs
Fault-Tolerance: Verification processes, model integration from multiple sources to understand fault-error-symptom characteristics*

Monitor: Monitor sensors functionality, response accuracies, degradation of performance gracefully and/or leading to human intervention*
Human Modeling: Model human's role in system, predict human behavior, monitor responses*+
Security Protocols: Use current protocols to secure data and any transmission of data+
Invasiveness level: minimize when possible human invasive procedures*
Communications: Encourage communications between human and system and between multiple systems. Warning systems*+

Table 2: Recommendations for SECURITY & SAFTEY of Human-in-the Loop Information Fusion based CPS Applications (*) impacts for Safety (+) impacts for Security concerns

5. HUMAN SCALE & PERFORMANCE IN INFORMATION FUSION BASED CPSs

Human-in-the-loop Information Fusion based CPS systems can benefit in applications when humans are directly involved in that they may only need perform at a human scale speeds and not faster. Returning to our blindBike example, we have to perform fast enough to respond to the speed of human biking and related interactions. Human performance is the idea of how in a human-in-the-loop system you measure the effectiveness (accuracy, error) of the human involved. At this point most systems simply treat the human as an all-knowing, never wrong component of the system. This is dangerous and with the modeling of human behavior, metrics systems might intelligently tune the level of autonomy based on how reliable the current user is.

6. REFERENCES

[1] A. Lafrance, "The High-Stakes Race to Rid the World of Human Drivers", The Atlantic, Dec. 1, 2015.
[2] Google, "Google Self-Driving Car Testing Report", https://static.googleusercontent.com/media/www.google.com/en//selfdrivingcar/files/reports/report-annual-15.pdf,, Dec. 2015
[3] M. Harris, "Apple meets California officials to discuss self-driving car", The Gaurdian, http://www.theguardian.com/technology/2015/sep/18/apple-meets-california-officials-self-driving-car, Sep. 2015
[4] William Overell, "blindBike: Road Navigation", Thesis under development, Computer Science, California State University East Bay (2016).
[5] Christopher Lagali, "Light Detection and Intersection Crossing for blindBike", Thesis under development, Computer Science, California State University East Bay (2016).
[6] L. Grewe and S. Magana-Zook, "Occlusion, optimization, emergency response and partial falls in a senior collapse detection system",SPIE DSS, 2015.
[7] L. Grewe and S. Magana-Zook, "A cyber-physical system for senior collapse detection", SPIE DSS, 2014.
[8] L. Grewe, S. Krishnagiri, J. Cristobal, "DiRecT: A disaster recovery system", SPIE, Signal Processing, Sensor Fusion and Target Recognition XIII, 2004.
[9] "NIST Report: Smart Cities, CPS and NIST" http://www.nist.gov/public_affairs/releases/upload/smartcities_cps_budgetsheet.pdf
[10] "NSF: Cultivating Smart and Connected Communities", http://www.nsf.gov/news/news_summ.jsp?cntn_id=136253
[11] "Perspectives on CSP for Smart Cities", NSF, 2016, https://us-ignite-org.s3.amazonaws.com/resource/NSF_-_David_Corman_-_0929_Smart_Cities_Charts.pdf
[12] "OpenStreetMap", http://www.openstreetmap.org/#map=5/51.500/-0.100, 2016
[13] E. Blasch, "Context aided sensor and human-based information fusion", Aerospace and Electronics Conference, NAECON, pp. 127-134, 2014.
[14] V. Gradinescu, C. Gorgorin, R. Diaconescu, V. Cristea, L.Iftode, "Adaptive Traffic Lights Using Car-to-Car Commnications", Vehicular Technology Conference, pp. 21 – 25, 2007
[15] H. Shen, J. Liu, K. Chen , J. Liu, S. Moyer, " SCPS: A Social-Aware Distributed Cyber-Physical Human-Centric Search Engine", IEEE Transactions on Computers Vol 64, Issue 2, pp. 518-532, 2013.
[16] NSF, "Foundations for Innovation in Cyber-Physical Systems", Workshop Report, http://www.nist.gov/el/upload/CPS-WorkshopReport-1-30-13-Final.pdf, 2013

R·I·T

Cross-Layer Framework in the Internet of Things for Cyber-Physical Systems

Andres Kwasinski

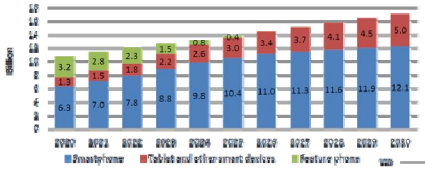
Department of Computer Engineering
Rochester Inst. of Technology

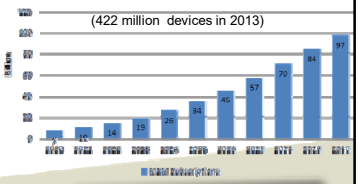
ROCHESTER INSTITUTE OF TECHNOLOGY

R·I·T

Wireless Networks Forecasts

- Dramatic growth in Internet-connected devices.
- Most of this grow will come from sensing and actuation devices that act as nodes in the Internet of Things (IoT).





Source: "IMT Traffic Estimates for the Years 2020 to 2030," International Telecommunication Union (ITU) technical report M.2370-0, July 2015.

ROCHESTER INSTITUTE OF TECHNOLOGY

What is the IoT?

- Lack of uniform agreement.
- Adopted view:
  - ➢ three distinct features for an instance of IoT application:
    1) awareness - as a result of a sensing/data collection operation,
    2) autonomy - complete operation without human intervention,
    3) actionable - using the results from the data processing for decision making and operation.
- Focused IoT application: integration with infrastructure to enable a cyber-physical system called a "smart infrastructure";
  - Example: smart grid.

ROCHESTER INSTITUTE OF TECHNOLOGY

Challenges Associated with IoT Growth

- Needs for Awareness-Autonomy-Actionable vision:
  - handling data collected from multiple and heterogeneous data sources,
  - ubiquitous and reliable connectivity,
  - IoT devices constrained in size, power consumption and data processing power.

ROCHESTER INSTITUTE OF TECHNOLOGY

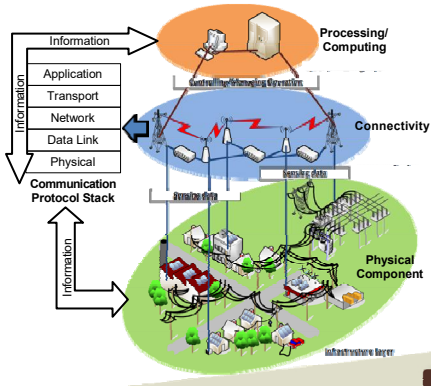
Some Notable Recent IoT Developments

- IETF standardization starts to provide "some" order in the IoT landscape:
  - RPL - IPv6 Routing Protocol for Low-Power and Lossy Networks,
  - CoAP - Constrained Application Protocol.
- Q. Wu, et al. (IEEE Internet of Things Journal, April 2014): network of *intelligent* agents that can develop self-awareness and operate autonomously.

ROCHESTER INSTITUTE OF TECHNOLOGY

Why Cross-Layer Design in IoT

- Ubiquitous communications, autonomous and self-aware device operation and handling of multiple sensed data of varying characteristics:



- IoT devices need to access information from different layers of the cyber physical system and
- can process the information in an integrated manner.
- Information needs to be integrated at a processing element for the IoT device to feature self-aware characteristics and be able to operate autonomously.

ROCHESTER INSTITUTE OF TECHNOLOGY

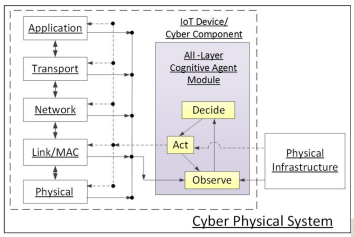
Architecture for Cross Layer IoT

- Traditionally, the modularized architecture in the protocol stack has significantly limited the exchange of information between layers.
  - Protocols at different layers may be running at different processing units.
- The challenges in propagating information extends from the protocol stack to the exchange between the physical and cybernetic domains.
- Heterogeneous nature of information also a challenge for effective integration.

ROCHESTER INSTITUTE OF TECHNOLOGY

Architecture for Cross Layer IoT

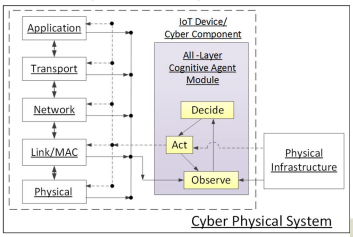
- All-layer cognitive agent module:
  - A software module that gathers information from the different layered components of an IoT device.
  - Able to develop the functions of self-awareness and autonomous operation while also bridging the separation between layers.



ROCHESTER INSTITUTE OF TECHNOLOGY

Architecture forCross Layer IoT

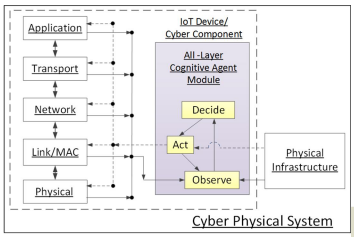
- All-layer cognitive agent module:
  - Based on the cognitive paradigm – the software implementation of an Observe-Decide-Act cognitive cycle:
    - Observe – sense the environment,
    - Decide - adapt operation based on theenvironment,
    - Act – perform adaptation.



ROCHESTER INSTITUTE OF TECHNOLOGY

Architecture forCross Layer IoT

- All-layer cognitive agent module:
  - the entities of the environment and the actions integrate variables and other data from all layers of the network,
  - Integration is for and across the cybernetic and physical components
    - physical components that are integrated are from the infrastructureand the network connectivity environment.

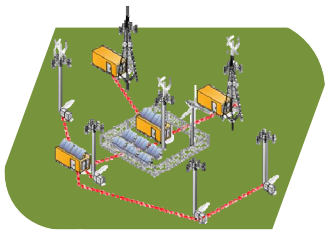


- Cognitive cycle operation allows to develop self awareness andautonomous decision making.

ROCHESTER INSTITUTE OF TECHNOLOGY

Application Case: Powering Cellular Base Stations From the Smart Grid

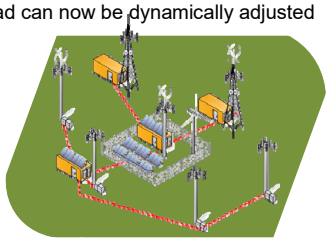
- IoT has had a key role in modernizing the electric grid – the “smart grid”.
- One development from the smart grid: microgrids.
- Microgrid: electric power grids that are confined to a local area and which can operate connected to or isolated from a main grid because loads and local energy sources (generators or energy storage devices) are integrated through a controller that operates independently of the grid.



ROCHESTER INSTITUTE OF TECHNOLOGY

Application Case: Powering Cellular Base Stations From the Smart Grid

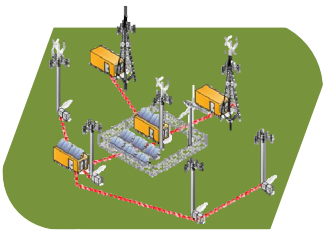
- Locality of both energy sources and loads allows for their integrated management (through the networked sensing and actuation capabilities provided by the IoT),
- operational parameters from the load can now be dynamically adjusted based on the microgrid conditions.
- ``Sustainable Wireless Area" (SWA): an architecture that integrates a group of cellular base stations in a microgrid with the goal of maximizing the use of renewable energy to power the cellular infrastructure



ROCHESTER INSTITUTE OF TECHNOLOGY

Application Case: Powering Cellular Base Stations From the Smart Grid

- Integrated management of cellular traffic and electric energy:
  - New management dimension – shape traffic based on renewable energy predicted availability and reserves.
    - Shape video and data traffic.
    - Traffic shaping is reflected on the quality of cellular service experienced by end users.
    - Resources at the base station pertaining cellular traffic and electric energy conditions are treated as a single entity.



ROCHESTER INSTITUTE OF TECHNOLOGY

Thank you!

Andres Kwasinski – axkeec@rit.edu

ROCHESTER INSTITUTE OF TECHNOLOGY

Cross-Layer Framework in the Internet of Things for Cyber-Physical Systems

Andres Kwasinski
Dept. of Computer Engineering, Rochester Institute of Technology, Rochester, NY USA 14623

ABSTRACT

The central requirement for high-performing cyber-physical system is an effective collection of sensed data and its application to act on the physical component of the system. For many cyber-physical systems, the infrastructure for sensing from and acting on the physical component is being built based on the concept and architecture of the Internet of Things. While the introduction of IETF routing and application layers protocols is helping the Internet of Things rapidly mature towards a structure that provides internetworking of sensing and actuating devices, multiple challenges still remain for an effective integration within cyber physical systems. Some of these challenges include reliable and ubiquitous communications, autonomous and self-aware operation, and handling of sensed data of varied types and characteristics. This position paper discuses the use of cross-layer techniques in the Internet of Things to address these challenges. This perspective not only encompasses the interaction between different layers of the network, but also between different cybernetic and physical components of the system. This view will be illustrated by discussing an application case that integrates the two infrastructures of the power grid and a cellular communications network. Finally, a general framework based on cognitive technology will be discussed as the elementthat enables cross-layer operation.

Keywords: Cross-layer, cyber-physical systems, Internet of Thing.

1. INTRODUCTION AND MOTIVATION

There exists a uniform agreement among studies of wireless networks forecasted growth and evolution over the next decade in foreseeing a dramatic growth in the number of devices connected to the Internet. Most of this grow will come from sensing and actuation devices that act as nodes in the Internet of Things (IoT). As a representative example of such studies, in [1] it is discussed that while in 2013 there were 422 million connections of IoT devices, this number is estimated to grow to 7 billion by 2020, 34 billion by 2025 and 97 billion by 2030. The IoT growth progresses hand-in-hand with the development of increasingly complex smart infrastructures. These infrastructures can be seen as a cyber-physical system where a computing/cybernetic layer, in effect an instance of a portion of the larger IoT, is integrated to an infrastructure (the physical component of the system) to provide more effective and efficient operation of the said infrastructure.

As much as there is agreement on the rapid growth for the IoT, there is a much more diverse view on how to characterize the IoT itself and the devices therein. We subscribe to a definition advanced by Verizon in its "State of the Market: The Internet of Things 2015" report [2], where an instance of IoT application is characterized as having all of three distinct features: awareness (as a result of a sensing/data collection operation), autonomy (in terms of complete operation without human intervention) and actionable (in terms of using the results from the data processing for decision making and operation). In order to achieve autonomous and self-aware operation, IoT devices need not only to be able to handle data collected from multiple and heterogeneous data sources, but they also need to operate within an environment of ubiquitous and reliable connectivity, all while considering that a majority of IoT devices will be constrained in size, power consumption and data processing power. It is within this combination of operational needs where multiple technological challenges still resides for the IoT.

Nevertheless, the rapid growth of the IoT has been accompanied by a steady development of new supporting technologies and solutions. At the networking and at the application layers of the networking protocol stack, the IETF has recently standardized the RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks) and the CoAP (Constrained Application Protocol). Of interest herein is the work in [3], where the idea of a cognitive IoT is proposed as a network of intelligent agents that can develop self-awareness and operate autonomously.

2. CROSS-LAYER DESIGN FOR THE INTERNET OF THINGS

2.1 Enabling Cross-Layer Operation in the Internet of Things

As previously remarked, for an effective integration and operation of IoT devices within cyber physical systems, it is necessary to develop techniques for ubiquitous communications, devices' autonomous and self-aware operation and handling of multiple sensed data of varying characteristics. The key in meeting this goals resides in ensuring that the IoT devices can access information from different layers of the cyber physical system and, more importantly, can process the information in an integrated manner. Considering a general cyber physical system with IoT integration, at the physical level, an IoT device would need to access information that characterize the physical status of the system's physical component and of the environment associated with the access and use of the medium utilized for network connectivity (be it wireless or wired). At the cybernetic (or computing) level, the device will need to access information from all the higher layers of the networking stack (the Network, Transport and Application layers). All the information from the physical and cybernetic layers, which form a very heterogeneous data set, needs to be integrated within the core processing elements of the IoT device. Integration of all the information is required for the IoT device to feature self-aware characteristics and be able to operate autonomously.

The layered architecture usually followed in network design is advantageous in simplifying the design problem into compartmentalized modules, but it also presents key difficulties, especially for information integration in the IoT-cyber physical system both between the cybernetic and physical domains and within the IoT architecture itself. This is because the exchange of information between layers has usually not been considered in the design, to the extent that layers frequently reside within different processing units in the IoT device (e.g. lower networking layers in the communications chipset and higher layers in a main processor, with some physical sensing operations residing at times in yet another integrated circuit). Consequently, we advocate that IoT devices will need to count with a software module that will be tasked with gathering information from the different layered components of an IoT device. Ideally, this software module will need to be able to not only bridge the separation between layers to integrate information but at the same time develop the functions of self-awareness and autonomous operation. All this can be accomplished by resorting to the cognitive paradigm. This paradigm, which gained popularity in networking as the core of cognitive radio technology [4], is based on the software implementation of an Observe-Decide-Act cognitive cycle [5]. As Figure 1 illustrates, we advocate for the IoT to include an "All-layer Cognitive Agent Module" that executes a cognitive cycle, repeatedly executing a sequence of "observe" (sense the environment), "decide" (adapt operation based on the environment) and "act" (perform adaptation) operations. Importantly, in the all-layer cognitive agent framework, the entities of the environment and the actions integrate variables and other data from all layers of the network in the cybernetic component as well as the physical components from the infrastructure and the network connectivity environment. The access to information and actions associated to all layers allows for the IoT device to gain awareness of the all-layer environment, decides on the all-layer adaptation actions and develops experience.

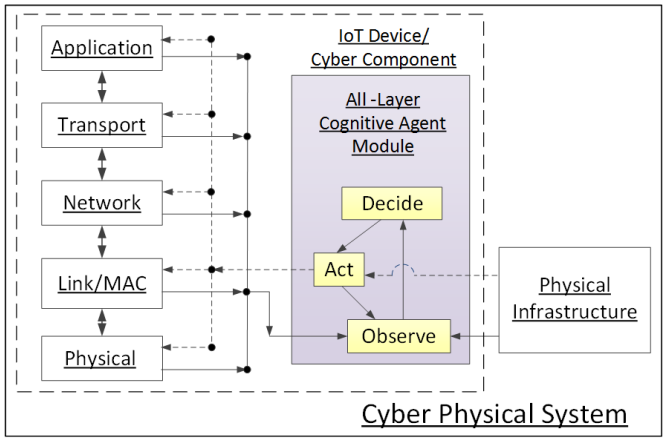


Figure 1. Block diagram of the cross-layer IoT device for cyber physical systems, where an all-layer cognitive module integrates information from the networking environment and the physical infrastructure to provide self-aware autonomous operation of the device.

2.2 Application Case: Integration of Smart Grid and Cellular Networks Infrastructure

Over the last decade, the IoT have seen an increasing important role in modernizing and expanding the capabilities of the electric power grid, in what is now frequently called the “Smart Grid”. Microgrids is a new paradigm that has arisen from the transformational development of the Smart Grid. Microgrids are electric power grids that are confined to a local area and which can operate connected to or isolated from a main grid because loads and local energy sources (generators or energy storage devices) are integrated through a controller that operates independently of the grid. The locality of both energy sources and loads allows for their integrated management (through the networked sensing and actuation capabilities provided by the IoT), to the extent that operational parameters from the load can now be dynamically adjusted based on the microgrid conditions. A realization of this approach is the idea of a ``Sustainable Wireless Area" (SWA) that integrates a group of cellular base stations in a microgrid architecture with the goal of maximizing the use of renewable energy to power the cellular infrastructure, [6]. Because for the microgrid within the SWA the generators, controllers and loads are all located in the vicinity of each other, it is possible to control the cellular traffic intensity (and the dependent Quality of Experience, QoE, of end users) based on the calculated information with the short term prediction of renewable energy availability. The control of cellular traffic based on availability of renewable energy effectively adds an extra degree of freedom to the power management system by making combined use of information from a physical component (the microgrid status) and from the cybernetic component (resource management at the base station). In [7] we presented an integrated energy at the microgrid-cellular traffic management technique that shapes the traffic serviced by an LTE base station and the number of transmit antennas based on the predicted availability of renewable energy. The management of resources at the base station is reflected by the quality experienced with real-time streaming video and the delay experienced with data traffic. This is, when it is predicted that the estimated renewable energy availability and the energy stored at the microgrid will result in a deficit of renewable energy, the traffic is shaped and the number of transmit antennas can be reduced through a controlled, smooth and transient reduction of real-time video quality and increase in data delay.

REFERENCES

[1] ITU-R, "IMT Traffic Estimates for the Years 2020 to 2030," International Telecommunication Union (ITU) technical report M.2370-0.

[2] Verizon, “State of the Market: The Internet of Things 2015”, report, http://www.verizonenterprise.com/resources/reports/rp_state-of-market-the-market-the-internet-of-things-2015_en_xg.pdf (22 March 2016).

[3] Q. Wu, et al., "Cognitive Internet of Things: A New Paradigm Beyond Connection," in IEEE Internet of Things Journal, vol. 1, no. 2, pp. 129-143, April 2014.

[4] Mitola, Joseph. "Cognitive Radio - An Integrated Agent Architecture for Software Defined Radio," Doctoral Dissertation, Royal Inst. Technol. (KTH), 2000.

[5] S. Haykin, "Cognitive Radio: Brain-Empowered Wireless Communications," in IEEE Journal on Selected Areas in Communications, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[6] A. Kwasinski, A. Kwasinski, "Operational aspects and power architecture design for a microgrid to increase the use of renewable energy in wireless communication networks," International Power Electronics Conference (IPEC), 2014.

[7] Kwasinski, A.; Kwasinski, A., "Integrating cross-layer LTE resources and energy management for increased powering of base stations from renewable energy," in 13th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt), pp.498-505, 25-29 May 2015.

AICIP RESEARCH

Systems: Evolution of Potential Solutions

Hairong Qi, Gonzalez Family Professor
Electrical Engineering and Computer Science
University of Tennessee, Knoxville
http://www.eecs.utk.edu/faculty/qi
Email: hqi@utk.edu

SPIE Panel Discussion, April 18, 2016

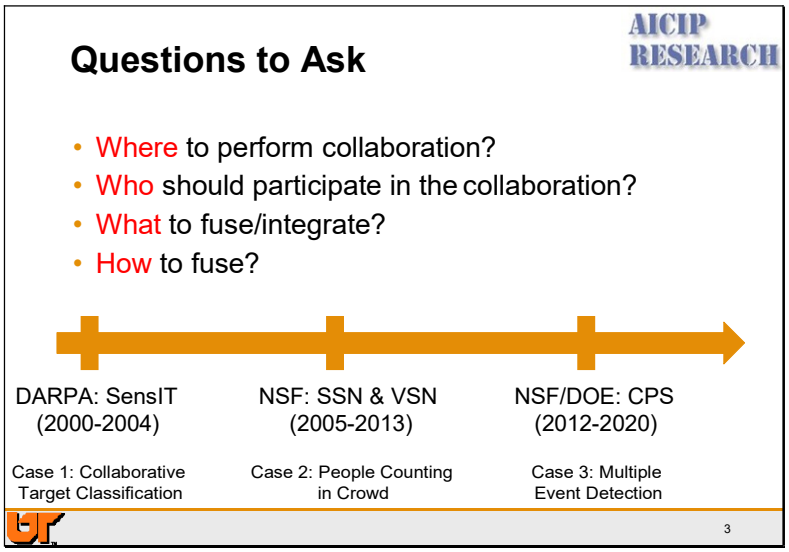
1

About AICIP Research

AICIP RESEARCH

- Advanced Imaging and Collaborative Information Processing (AICIP)
- Collaborative processing
  - In-network signal processing
  - Collaborative vs. distributed
  - DARPA, NSF, ONR
- Webpages
  - http://aicip.eecs.utk.edu
- Advanced Imaging
  - Automatic target recognition and subpixel recognition using multi/ hyper-spectral imaging
  - Medical imaging using infrared
  - US Army, ONR, ORNL

2



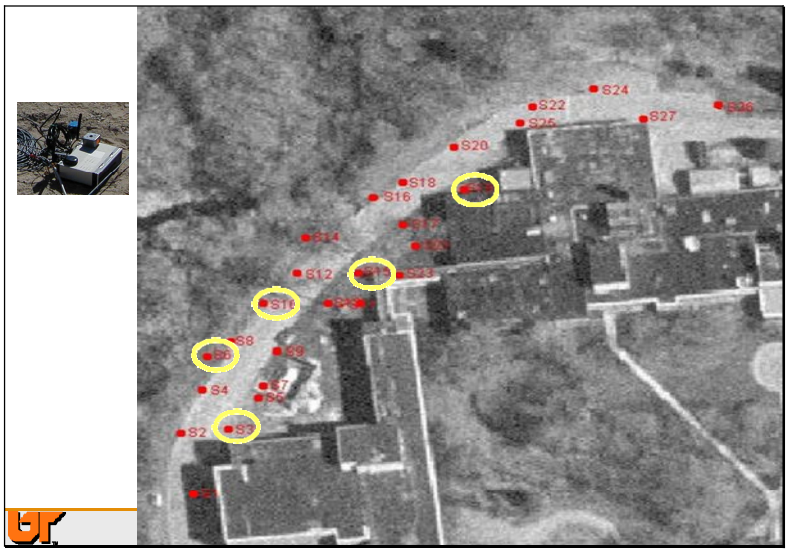
The research focus of collaborative processing is essentially to solve a pair of conflict goals for sensor networks, that is, the collaborative processing should provide fault tolerance, while at the same time save energy. However, in order to save energy, the fundamental principle is to eliminate redundancy. And in order to provide fault tolerance, the fundamental principle is to use redundancy. A balanced collaborative processing algorithm is desired.

This tutorial focuses on issues related to collaborative processing in sensor networks. We divide our tutorial into three sections with each section answers a unique question related to collaboration, that is, how to collaborate, who to collaborate, and where to collaborate. In the first section, we discuss the computing models that support collaborative processing. In the second section, we investigate the problem on who to collaborate. We differentiate "distributed processing" and "collaborative processing" in the sense that collaborative processing is conducted only among neighbors. Therefore, it's important to decide a cluster among which the sensor would collaborate. On the other hand, since the density of the sensor network is high and not all of them need to be on the same time, we need to design sensor selection protocols to see which sensors need to be on or idle. The third section is about where to collaborate. This concerns in-network processing and self-deployment

AICIP RESEARCH

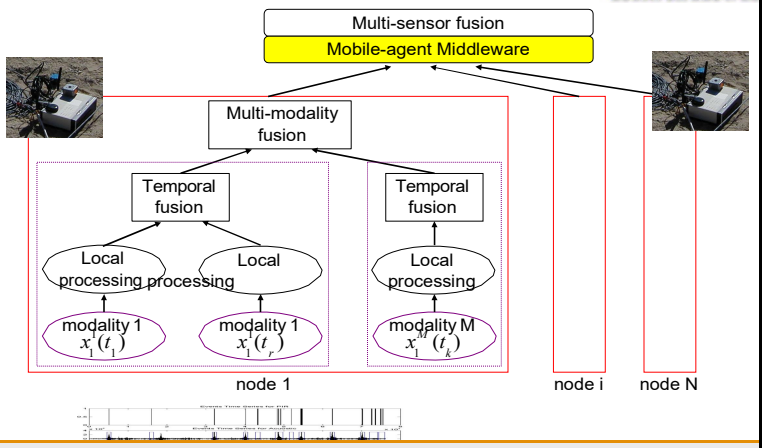
Case Study 1: Collaborative Target Classification in Ground Sensor Networks

4



Collaborative Target Classification

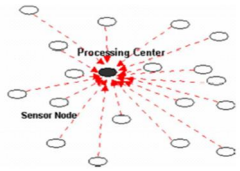
AICIP RESEARCH



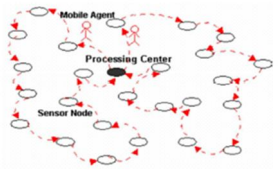
6

Distributed Computing Paradigms

AICIP RESEARCH



- Energy and network bandwidth requirement
- Scalability
- Reliability
- Progressive accuracy
- Task adaptivity
- Fault tolerance



Client/Server Computing

Mobile-agent-based Computing

	Transfer Unit	Computing
Client/Server Computing	Data	Centralized, occurs at the servers
Mobile agent Computing	Mobile agent	Distributed evenly among sensor nodes

7

SITEX02 Scenario Setup

AICIP RESEARCH

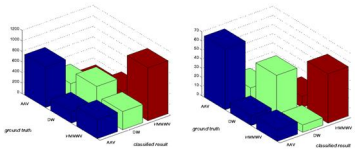
- Acoustic sampling rate: 1024Hz
  Seismic sampling rate: 512 Hz
- Target types: AAV, DW, and HMMWV
- Collaborated work with two other universities (Penn State, Wisconsin)



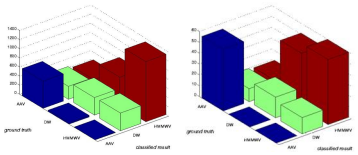
8

Confusion Matrices of Classification on SITEX02

AICIP RESEARCH

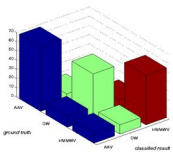


Acoustic (75.47%, 81.78%)

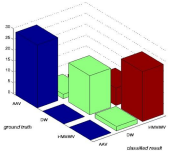


Seismic (85.37%, 89.44%)

	AAV	DW	HMV
AAV	29	2	1
DW	0	18	8
HMV	0	2	23

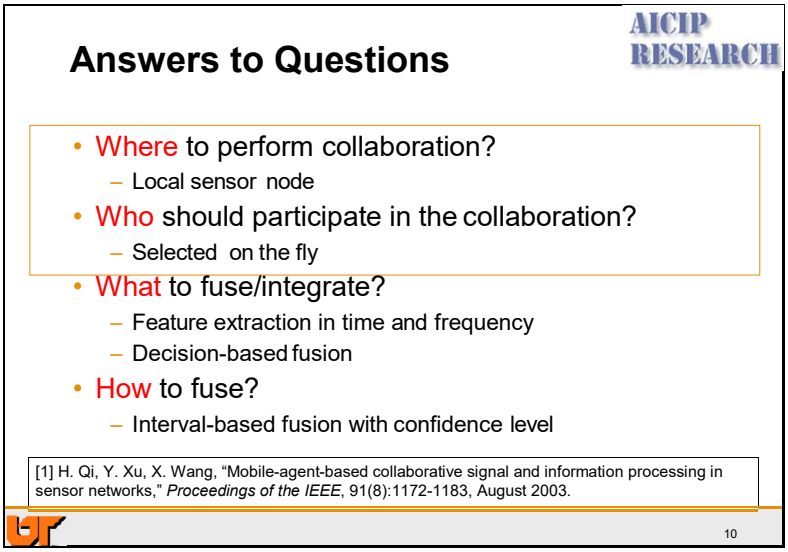


Multi-modality fusion (84.34%)



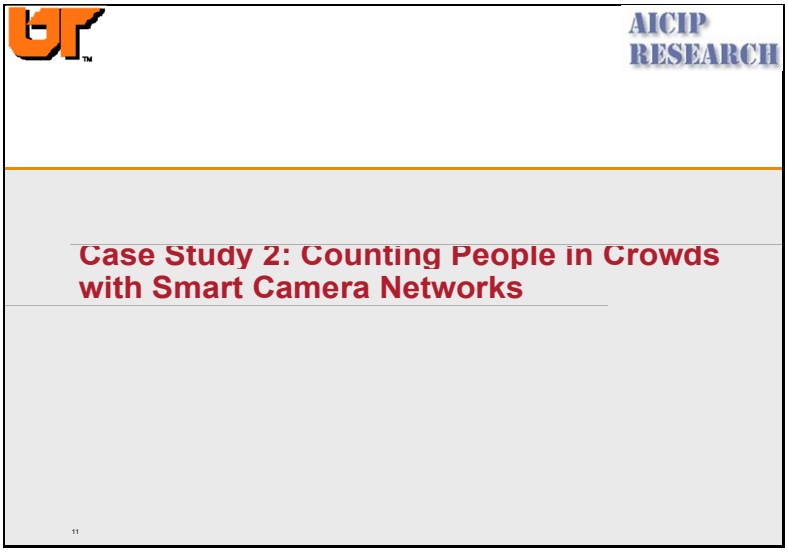
Multi-sensor fusion (96.44%)

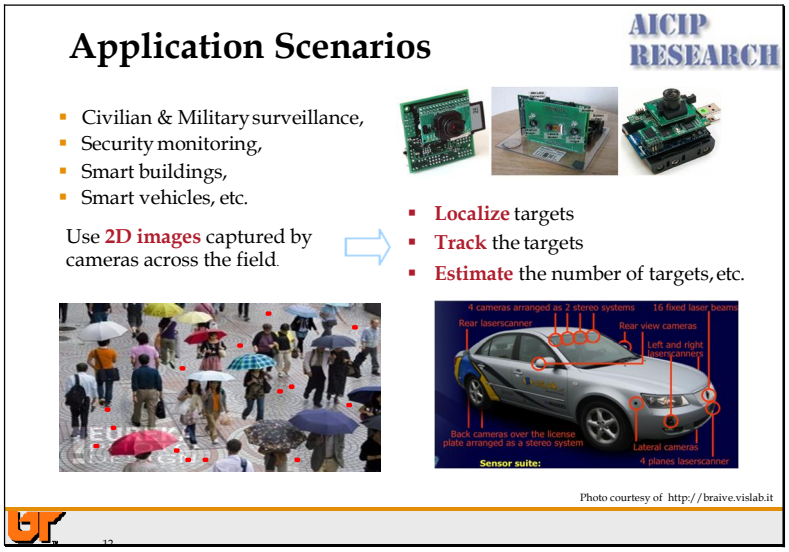
9



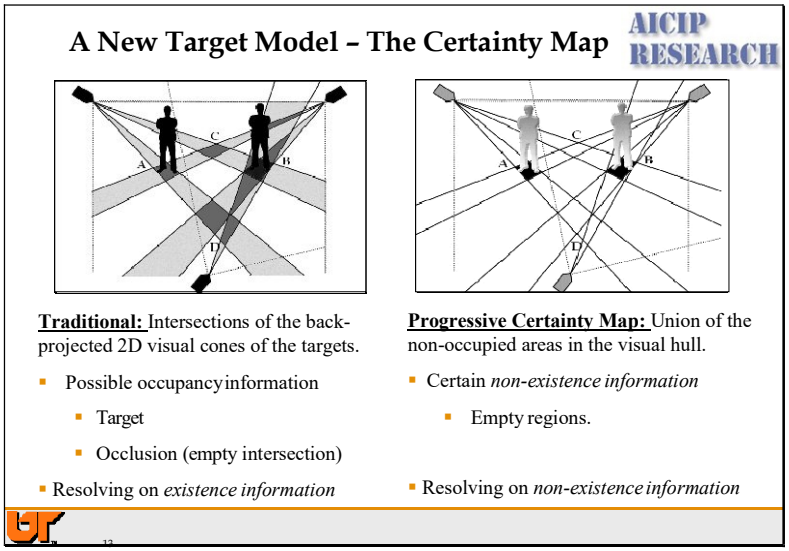
The research focus of collaborative processing is essentially to solve a pair of conflict goals for sensor networks, that is, the collaborative processing should provide fault tolerance, while at the same time save energy. However, in order to save energy, the fundamental principle is to eliminate redundancy. And in order to provide fault tolerance, the fundamental principle is to use redundancy. A balanced collaborative processing algorithm is desired.

This tutorial focuses on issues related to collaborative processing in sensor networks. We divide our tutorial into three sections with each section answers a unique question related to collaboration, that is, how to collaborate, who to collaborate, and where to collaborate. In the first section, we discuss the computing models that support collaborative processing. In the second section, we investigate the problem on who to collaborate. We differentiate "distributed processing" and "collaborative processing" in the sense that collaborative processing is conducted only among neighbors. Therefore, it's important to decide a cluster among which the sensor would collaborate. On the other hand, since the density of the sensor network is high and not all of them need to be on the same time, we need to design sensor selection protocols to see which sensors need to be on or idle. The third section is about where to collaborate. This concerns in-network processing and self deployment

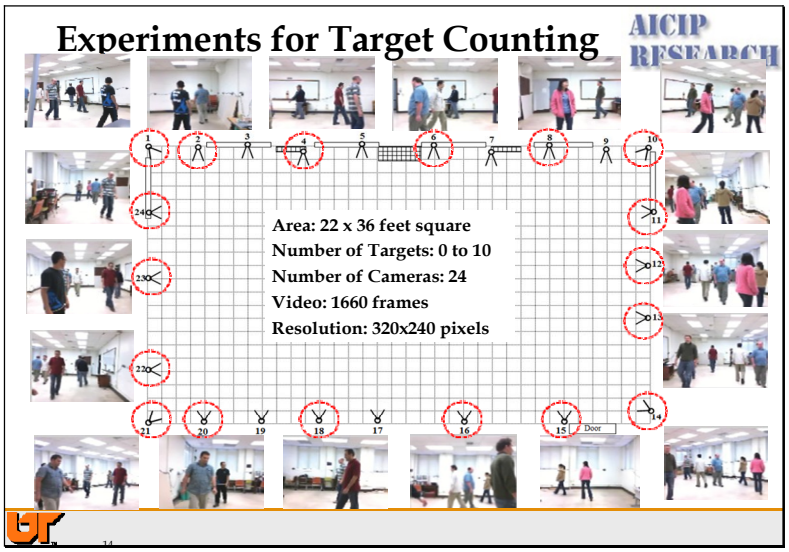




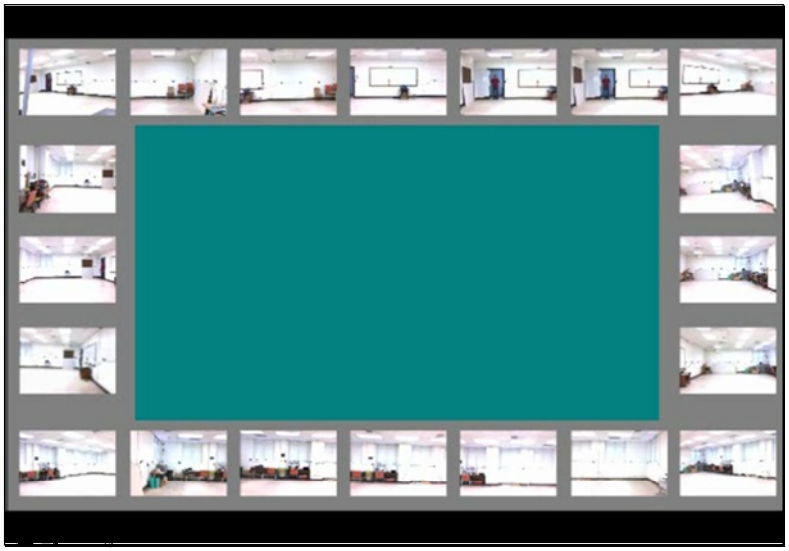
- Based on their advantages and capabilities, many researchers called the visual sensor network as the fundamental of the next generation of smart surveillance Systems.
- Visual sensor networks are facilitated in many different multi-camera applications in diverse environments.
- Surveillance and security are the most obvious applications of the visual sensor networks to cover the large environments.
- In addition to this, visual sensor networks have different application areas including smart buildings, medicine and entertainment.
- The methodology of the VSN is by using 2D images captured by cameras across the field to Localize and Track the targets, or Estimate the number of targets, etc.



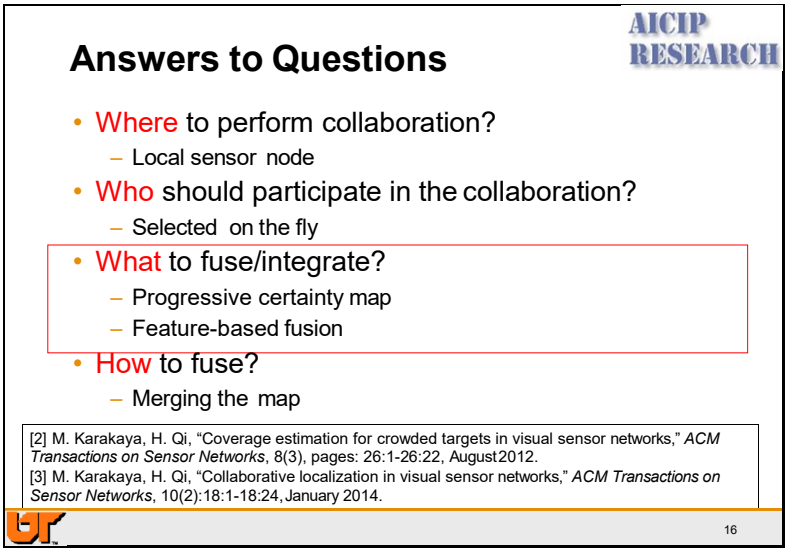
- For example, there are two targets standing at A and B.
- To detect these targets, the traditional target localization algorithms use the intersections of the back-projected 2D cones of the targets.
- These 2D cones correspond to the possible occupancy information in the visual hulls, also referred to as the existence information.
- However, there is an uncertainty about the object existence in occupied areas which can appear to be the real object or made by occlusion.
- In crowded environments, many “empty” intersections that are not actually occupied by any targets are created because of occlusion, as shown in Fig.
- Although our proposed technique, progressive CM, shares the same visual cone idea but it differs in that we identify the non-occupied areas where the non-existence of target is certain. And we progressively combine these non-occupied areas to localize the objects in a distributed fashion.



* Real data is tested for different types of itineraries and voting thresholds.
* In simulation, different node and target density is chosen.
* Captured images and local CM is shown for real data.



* Real data is tested for different types of itineraries and voting thresholds.
* In simulation, different node and target density is chosen.
* Captured images and local CM is shown for real data.



The research focus of collaborative processing is essentially to solve a pair of conflict goals for sensor networks, that is, the collaborative processing should provide fault tolerance, while at the same time save energy. However, in order to save energy, the fundamental principle is to eliminate redundancy. And in order to provide fault tolerance, the fundamental principle is to use redundancy. A balanced collaborative processing algorithm is desired.

This tutorial focuses on issues related to collaborative processing in sensor networks. We divide our tutorial into three sections with each section answers a unique question related to collaboration, that is, how to collaborate, who to collaborate, and where to collaborate. In the first section, we discuss the computing models that support collaborative processing. In the second section, we investigate the problem on who to collaborate. We differentiate "distributed processing" and "collaborative processing" in the sense that collaborative processing is conducted only among neighbors. Therefore, it's important to decide a cluster among which the sensor would collaborate. On the other hand, since the density of the sensor network is high and not all of them need to be on the same time, we need to design sensor selection protocols to see which sensors need to be on or idle. The third section is about where to collaborate. This concerns in-network processing and self deployment

AICIP RESEARCH

Case Study 3: Event Unmixing in Smart Grid

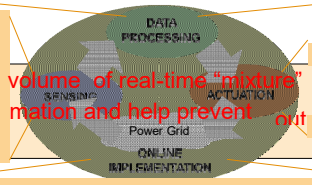
17

AICIP RESEARCH

Event Unmixing
Multiple event detection, recognition, spatial and temporal localization vs. single event analysis

Sensing towards the Edge
Distribution level vs. Transmission level
Cost: $1,000 vs. $80,000
Challenge: accurate freq. est.

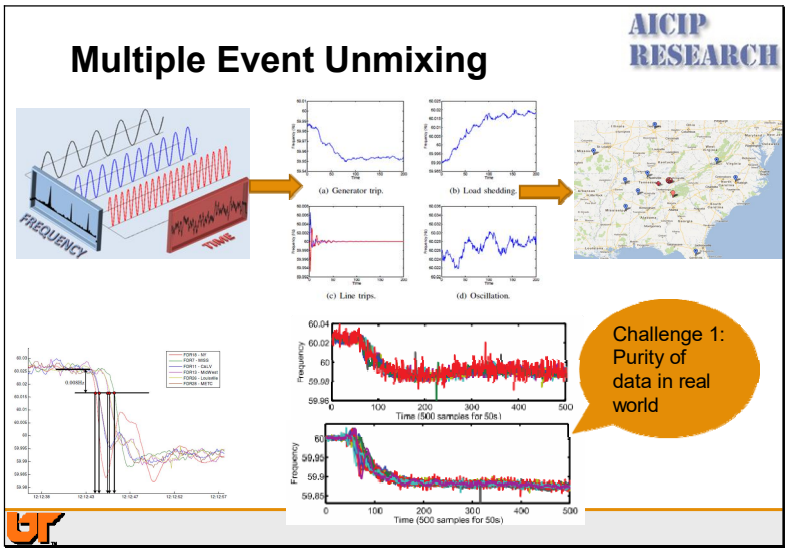
FDR

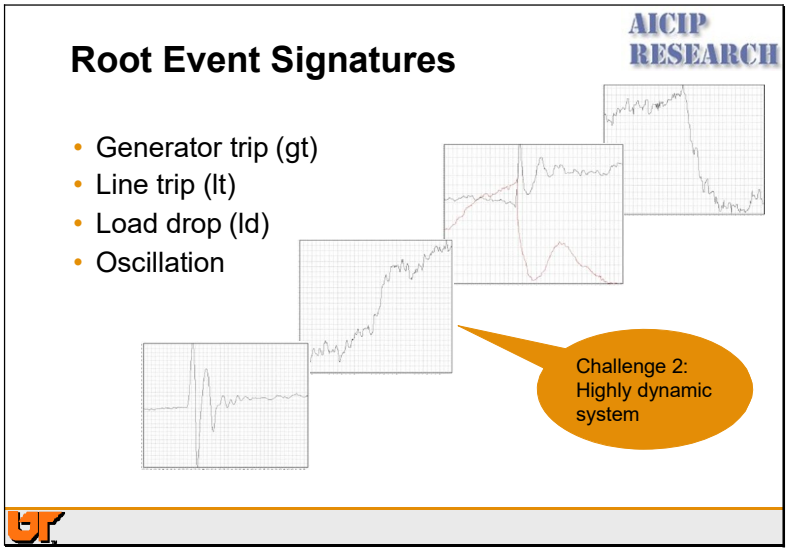


volume of real-time "mixture" mation and help prevent out

Local Load Participation
Residential and small commercial partici pation
Huge economic impact

Fast online data processing by Approximation
With probabilistic guarantee


Multiple Event Unmixing
AICIP RESEARCH
FREQUENCY
TIME
(a) Generator trip.
(b) Load shedding.
(c) Line trips.
(d) Oscillation.
Challenge 1: Purity of data in real world
Frequency
Time (500 samples for 50s)

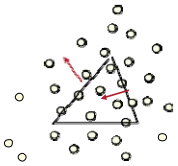

Root Event Signatures
AICIP RESEARCH
Generator trip (gt)
Line trip (lt)
Load drop (ld)
Oscillation
Challenge 2: Highly dynamic system

Initial Trial

AICIP RESEARCH

- x=As+n
- Unsupervised unmixing using minimum volume constraints, J(A)

$$\begin{aligned} &\text{minimize} \quad f(\mathbf{A},\mathbf{S}) = \frac{1}{2}\|\mathbf{X}-\mathbf{AS}\|_F^2 + \lambda J(\mathbf{A}) \\ &\text{subject to} \quad \mathbf{A} \geq \mathbf{0},\ \mathbf{S} \geq \mathbf{0},\ \mathbf{1}^T\mathbf{S} = \mathbf{1}^T \end{aligned}$$



- Failed!
- What is a good constraint?
  - The sparsity constraint
  - Signature training and learning

1-21

Algorithm - Sparsity-constrained Unmixing

AICIP RESEARCH

- x=As+n
- Abundance estimation via sparse coding
  - The sparse coding formulation (an NP-hard problem): minimize the number of non-zero elements in s while s is subject to the least-square constraint

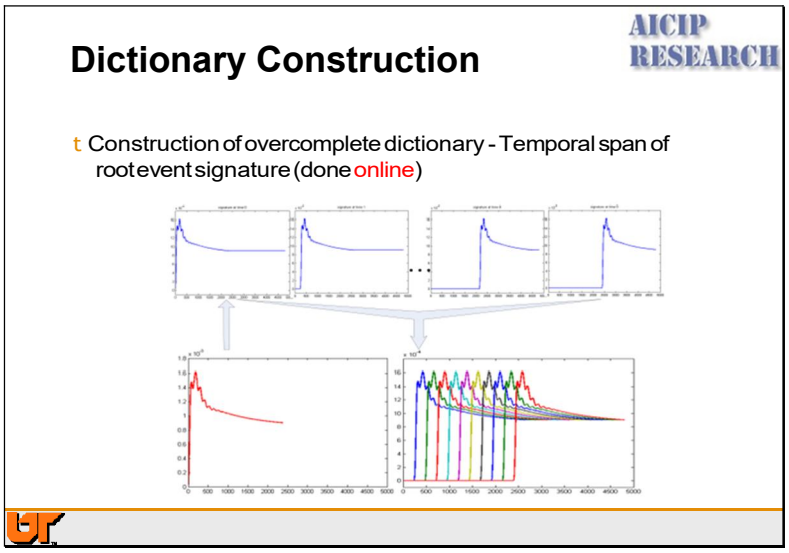
$$\min \|s\|_0 \quad \text{s.t.} \quad \|As - X\|_2^2 \leq \varepsilon$$

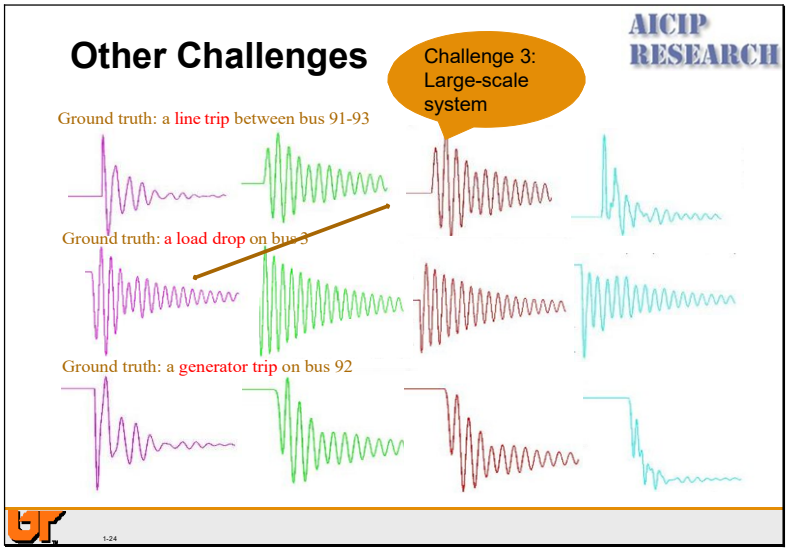
  - If s is sufficiently sparse, we can solve for s by instead minimizing the l_1-norm

$$\min \|s\|_1 \quad \text{s.t.} \quad \|As - X\|_2^2 \leq \varepsilon$$

  - "Feature sign search" is used to solve the optimization problem

$$s = \underset{s}{\operatorname{argmin}} \|X - As\|_2^2 + \lambda\|s\|_1$$

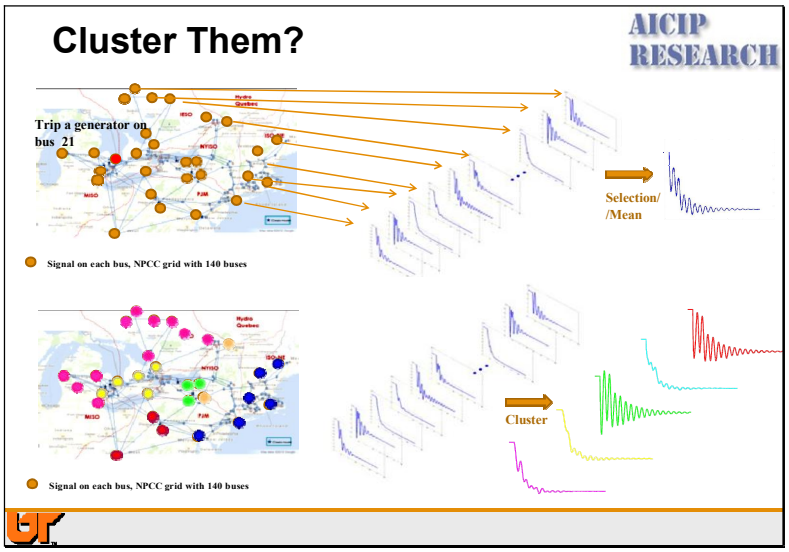




The network is complex connected with each other. The device(generator, load are various, means with different power) in the system is various, So the reaction when they are attacked is more complex and diversity.

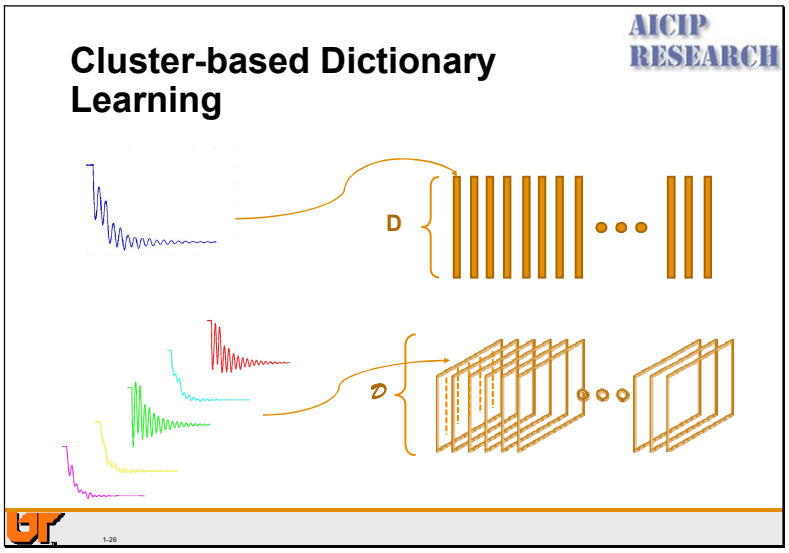
If we do unmixing based on a single signal, it will bring a lot error.

But there is a phenomenon that the same buses always have their own pattern or their own characteristic

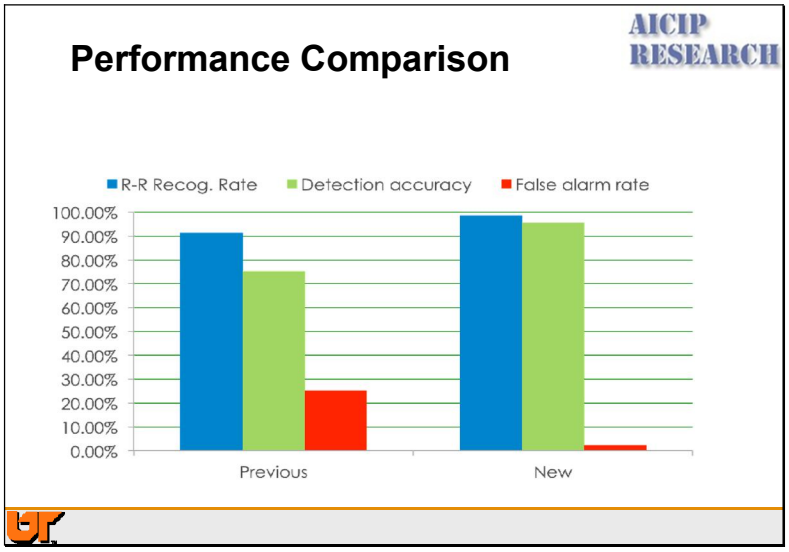


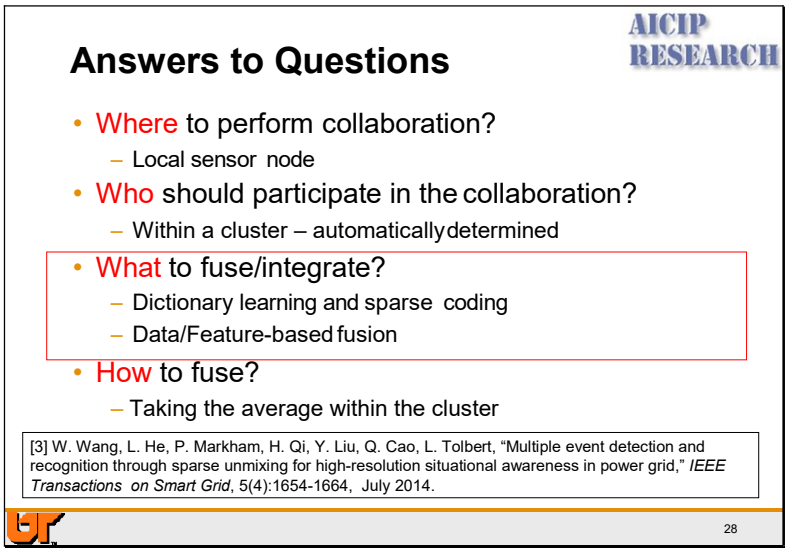
What is the benefit?
Is it reasonable?
Questions: for all kind of attacks/events/test data, whether all reaction have the same group clustering. Answer: yes.
since the power system is a network. So a group of feature maybe can better present the whole system

This new idea is more reasonable since they reveal the truth of large power system. For this case, since power system can be seen as a Network, if a generator trip at one bus, other buses which have strong relation or connection may have a big reaction, but this may just bring a little disturbance for some buses which is far away from where it happened. For those far away buses, it just looks like a line been tripped. Away in electrical distance may have it is a generator trip.



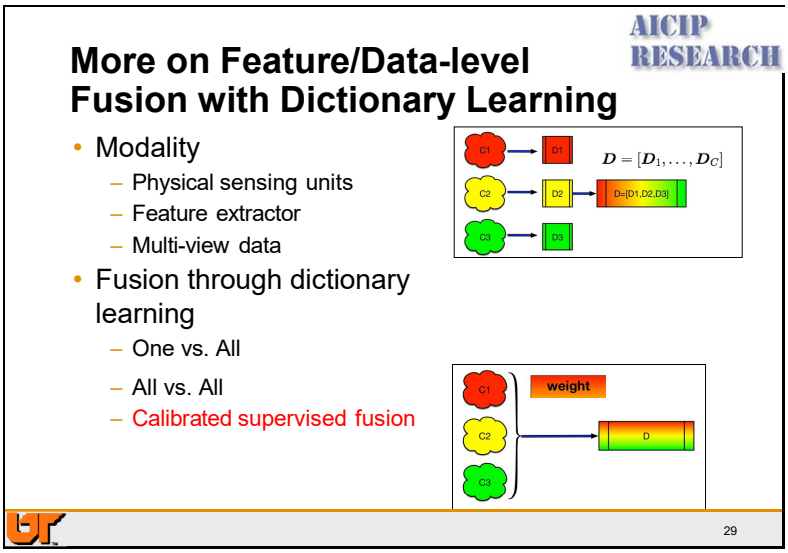
The reaction on certain buses always follow their own pattern. So it is reasonable to

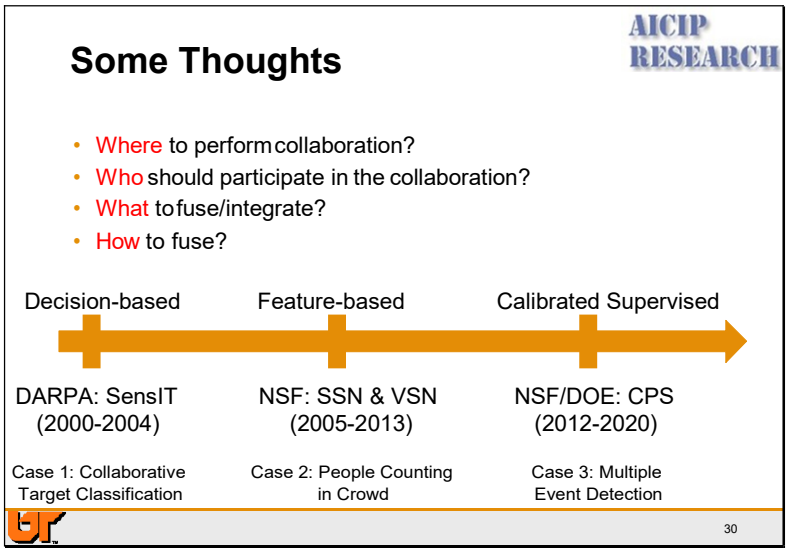




The research focus of collaborative processing is essentially to solve a pair of conflict goals for sensor networks, that is, the collaborative processing should provide fault tolerance, while at the same time save energy. However, in order to save energy, the fundamental principle is to eliminate redundancy. And in order to provide fault tolerance, the fundamental principle is to use redundancy. A balanced collaborative processing algorithm is desired.

This tutorial focuses on issues related to collaborative processing in sensor networks. We divide our tutorial into three sections with each section answers a unique question related to collaboration, that is, how to collaborate, who to collaborate, and where to collaborate. In the first section, we discuss the computing models that support collaborative processing. In the second section, we investigate the problem on who to collaborate. We differentiate "distributed processing" and "collaborative processing" in the sense that collaborative processing is conducted only among neighbors. Therefore, it's important to decide a cluster among which the sensor would collaborate. On the other hand, since the density of the sensor network is high and not all of them need to be on the same time, we need to design sensor selection protocols to see which sensors need to be on or idle. The third section is about where to collaborate. This concerns in-network processing and self-deployment





The research focus of collaborative processing is essentially to solve a pair of conflict goals for sensor networks, that is, the collaborative processing should provide fault tolerance, while at the same time save energy. However, in order to save energy, the fundamental principle is to eliminate redundancy. And in order to provide fault tolerance, the fundamental principle is to use redundancy. A balanced collaborative processing algorithm is desired.

This tutorial focuses on issues related to collaborative processing in sensor networks. We divide our tutorial into three sections with each section answers a unique question related to collaboration, that is, how to collaborate, who to collaborate, and where to collaborate. In the first section, we discuss the computing models that support collaborative processing. In the second section, we investigate the problem on who to collaborate. We differentiate "distributed processing" and "collaborative processing" in the sense that collaborative processing is conducted only among neighbors. Therefore, it's important to decide a cluster among which the sensor would collaborate. On the other hand, since the density of the sensor network is high and not all of them need to be on the same time, we need to design sensor selection protocols to see which sensors need to be on or idle. The third section is about where to collaborate. This concerns in-network processing and self-deployment.

Acknowledgement

AICIP RESEARCH

- DARPA, NSF, DOE
- S. S. Iyengar (FIU), Chakrabarty (Duke), Yu Hen Hu (UW), P. K. Biswas, Yilu Liu, Charles Cao, Leon Tolbert (UTK)
- Graduate students: Xiaoling Wang, Yingyue Xu, Teja Kuruganti, Yang Bai, Mahmut Karakaya, Wei Wang, Yang Song

Panel on Cyber Physical Systems Challenges with Information Fusion: Control Systems - Examples of Cyber-Physical Systems

J. Salerno, PhD
Harris Corp, 474 Phoenix Drive, Rome NY USA 13441

ABSTRACT

Control Systems have been around for decades and much longer than the computer, but with the advent of the computer they have become much more powerful and prolific. Today's controllers provide the decision maker with the ability to access multiple sensors from a single point and fuse them to make more intelligent recommendations and allow for increased overall system efficiency. In this paper we will present a number of systems that use control systems that aid in their operations. These include industrial/commercial environments to control systems that run national level critical infrastructures. We conclude this paper with a few challenges.

Keywords: Controllers, System Monitoring, Vulnerabilities, Situation Awareness, Situation Understanding, Building Management Systems, Supervisory Control and Data Acquisition

1. INTRODUCTION

Computers have become embedded in just about everything we have and do. Control systems are no different. Control systems can provide supervision, control (both passive and active), monitoring, and data acquisition. There are many ways to categorize the various systems. In this paper we present two categories or tiers of control systems: Building Management Systems (BMSs) and Supervisory Control Data and Acquisition (SCADA) systems. BMSs (or Tier 1 systems) are used to monitor and control industrial/commercial environments (e.g., malls, industrial plants, and office buildings, etc.) while SCADAs (or Tier 2 systems) are used to interconnect two or more Tier 1 systems (a complex, university or where there are multiple buildings) or national infrastructures such as electrical power, oil, etc. Regardless what they are called, majority of today's controllers have the same basic architecture (See Figure 1).

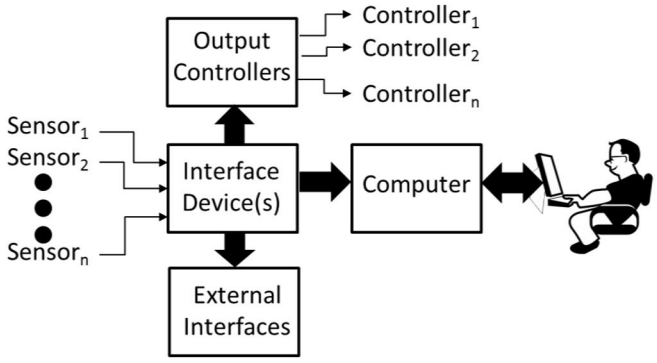


Figure 1: Overall Controller Architecture

Whether the controller is used as a BMS or SCADA, they receive sensory information from the system(s) being monitored, process these inputs and based on any changes provide some type of

output/control. These systems are not just supervisory. Most basic systems have some type of active control, e.g., maintaining the temperature in a room. In majority of the cases the output will be an alert to a user or decision maker. Hopes are, at some time in the future, more automation will be added to provide some degree of autonomous feedback and control and have the potential to forecast potential failures. In the sections that follow we will investigate where and how such controllers exist.

1.1 Building Management Systems (Tier 1)

BMSs are used to monitor various systems used by industrial/commercial facilities. Such facilities can include manufacturing plants, office buildings and malls. These systems include: Energy Management; Heating, Ventilating and Air Conditioning (HVAC); Security (access control, intrusion detection, close circuit television, etc.); Transportation/traffic (elevator, escalator and parking); pollution control (interior and exterior air quality); Electric and Life Safety. Figure 2 provides a sample of the various types of systems that could exist within a plant or commercial facility. For more details see [1].

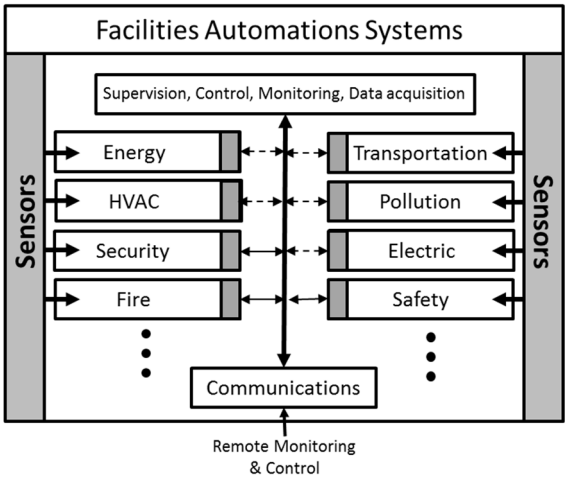


Figure 2: Examples of Industrial/Commercial Controllers

1.2 Supervisory, Control and Data Acquisition (Tier 2)

A university (consisting of multiple buildings) or a complex can have multiple BMSs (one in each building) interconnected to a higher level Tier 2, controller. This controller is referred to as a SCADA system. SCADA systems are also used as part of a number of critical infrastructures; electricity, oil, natural gas, etc. For example, within the electrical grid, SCADA systems control the balancing of generating and consumption of electricity and display the status to the system operators. Many of these SCADA systems have interconnections to the internet and are connected to sensors such as Phasor Measurement Units (PMUs) and Remote Terminal Units (RTUs). PMUs measure voltages and currents at principal intersecting locations (critical substations) on a power grid and can output accurately time-stamped voltage and current phasors. According to [3] RTUs connect to sensors in the process and convert sensor signals to digital data. They have telemetry hardware capable of sending digital data to the supervisory system, as well as receiving digital commands from the supervisory system. Figure 3 provides a sample layout of a power network, its control network and interdependency on the communications network.

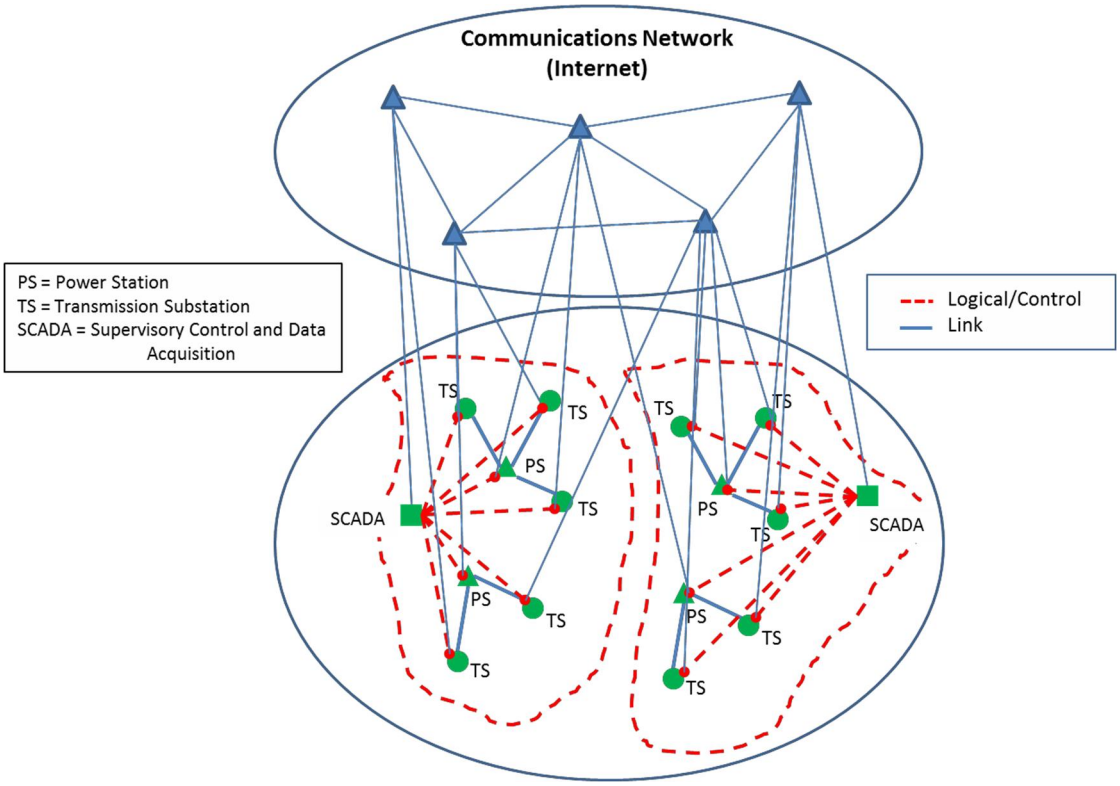


Figure 3: Electrical Power Grid

2. SUMMARY

In this paper we provide examples of a number of controllers. Control systems provide an excellent example of a cyber-physical system. They take in various inputs from sensors, process them (fuse) and provide the operator current situational awareness (alerts). They provide greater efficiency in the operations of the system, but there is still much work to be done. Control systems can collect a significant amount of data. Tools currently identify abnormalities to human operators to take action(s) if needed and simple active control (changing temperatures). Additional intelligence can be introduced such as machine learning/clustering techniques to provide increased autonomous monitoring and control and forecasting of potential failures. A second problem that is more important than automation is the cyber vulnerabilities (due to interconnections to the communication network, i.e., the internet) they introduce. These vulnerabilities create major wholes that can be exploited by criminals, terrorists and adversaries and need to be taken seriously.

REFERENCES

[1] IEEE Draft Recommend Practice for Application of Controllers and Automation to Industrial and Commercial Power Systems, P3001.11/D8, October 2015.
[2] Draft Guide for the Interoperability of Energy Storage Systems Integrated with the Electric Power Infrastructure, P2030.2/D8.0, October 2, 2014.
[3] Wikipedia, https://en.wikipedia.org/wiki/SCADA.

Panel Discussion

Cyber Physical (C-P) Systems Challenges with Information Fusion: Modeling - Programming - Ethics & Privacy

Ste l ios C.A. Th omopoulos (scat@iit.demokritos.gr)

April 18, 2016

National Ctr. for Scientific Research «Demokritos»
Institute of Informatics& Telecommunications
Integrated Systems Laboratory

Everyday examples of Cyber Physical (C-P) Systems

In-car GPS Navigation (e.g. Google Maps)

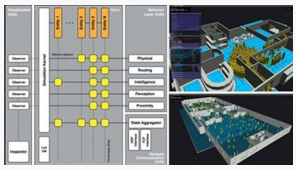
Cyber System

Centralized computation server, scheduling and routing all connected clients (cars)

Physical System

People driving cars equipped with smartphones running in-car navigation software

Advnaced Human Behavior Simulators



Used for, e.g., evacuation planning in conjunction with real-time human actions and feedback from sensors and humans

1

More advanced examples of Cyber Physical (C-P) Systems

Situational awareness enhancemnent using a swarm of UAVs *and* *Humans* Cyber System - Example: Fire detection & warning systems

Centralized computation server, responsible for the flight data and sensory focus of all UAVs, making decisions based on fused information from UAVs

Physical System

UAVsequipped with sensors needed to enhance the situational awareness over a large area

Humans with Mobile Apps

Humans as "sensors" reporting on events - *crowd-sourcing*

Cyber-Physical System Issues

- Data Integrity
- Latency (Time Delays)
- Humans as a "sensor": *Ethics - Privacy - Models*?
- Cyber Threats - Spoofing
- Priors - Fusion Models

2

Issues

- Physical world is unpredictable; C-P systems need higher reliability and robustness standards
- Especially when people are involved, it is difficult to account for their statistical behaviour (*even higher unpredictability*):
  - Priors of CPS? ⇒ *Appripriatestatistics*? *Generalized Evidence Theory**?
  - Big Data Analytics for crowd-sourced data statistics - Ethics - Privacy
- Temporal dimension is not intrinsic toprogramming (e.g. C, C++, Java) but must be accounted for
  - On the fly model changes?
- Physical dynamics and Computation must be dealt in a unified manner
  - How?
- Network Latency will play a major role*

- *S. C. A. Thomopoulos, "Sensor Integration andData Fusion," Invitedpaperin special issue on Sensor Integration andData Fusionfor Robotic Systems, Journal of Robotic Systems, 1990, Volume 7, No. 3, pp. 337-372, 1990.
- **S. C. A. Thomopoulos, an d L. Zhang, "Distributed Decision Fusion with Networking Delays and Channel Errors." SPIE Proceedings. Sensor Fusion. (1988). Volume 931. pp. 154-160. 1988.
- **S. C. A. Thomopoulos and L. Zhang, " Distributed Decision Fusion with Networking Delays and Channel Errors," "Information Sciences: An International Journal, nos. 1 & 2, December1, 1992, Volume 66, pp. 117-131, 1994.

3

Cyber Physical Systems Challenges with Information Fusion

PANEL DISCUSSION[1]

Stelios C. A. Thomopoulos

Integrated Systems Laboratory, Institute of Informatics and Telecommunications
National Center for Scientific Research "Demokritos"

P. Gregoriou 1 & Neapoleos, Ag. Paraskevi, Athens 15310, Greece
email: scat@iit.demokritos.gr - telephone: +30 210 650 3154 - fax: +30 210 653 2175

INTERVENTION

Cyber-Physical Systems (CPS) are systems that integrate computation, networking, and physical processes. In a typical CPS, embedded computers and networks monitor and control physical processes, which (physical processes) in turn affect computations that affect the processes themselves. CPS technology builds on the use of embedded systems, computers and software in devices whose initial intent was not computation, such as cars, toys, medical devices, appliances, and scientific instruments. CPS integrates the dynamics of the physical processes with those of the software and networking, providing abstractions and modeling, design, and analysis techniques for the integrated whole.

In summary, embedded computation, networking, feedback and control, all integrated into a common physical process, is what constitutes a CPS. However, with the wide spreading of ubiquitous communications and inexpensive computational capacities, the CPS concept was further extended to include embedded micro-computers with rudimentary processing capabilities, capable of executing elementary data processing, interconnected in distributed networks and using IP for data exchange. To differentiate these systems from the traditional CPS, the later were called IoT (Internet of Things). In essence though, IoT may differ from CPS in that they address primarily consumer orientated systems and services, as compared to CPS that address primarily industrial systems, processes and applications. Another difference between CPS and IoT is that the later may be more open to human intervention and crowd sourced information, thus probably making data fusion models a more challenging proposition for IoT systems.

In the sequel, when we mention CPS we make no differentiation between CPS and IoT with the understanding that some differences may still exist that may require additional consideration of data fusion models for IoT. To that extent, we will use only the term CPS in what follows to be compliant with the theme of the panel discussioin as well.

The key issue with CPS is weather new data fusion models are required to co-op with the "dual nature" of CPS: cyber and physical. Before attempting to answer the question, we should look into the systemic aspects and the data structures of CPS and weather indeed they result into new data structure and data models that have not been accounted for in data fusion theories in the past or new data fusion models are required. It is true that since the late 90's, computer and data communication networks, and more specifically IP networks, have begun emerging allowing the interconnectivity of devices with each other and with humans thus creating a more open environment with more dynamic data format and not known a priori

statistical distributions, non-stationarity and difficult to estimate and model, in particular at the signal and raw data level.

The pervasive use of IP networks in cyberphysical systems have made affordable and popularized the extensive use of sensors and actuators, while replacing the term CPS with IoT (Internet of Things). In essence CPS and IoT represent the same reality with may be the only difference that IoT has a stronger sense of IP over CPS that represents a previous generation of networking with RS232/485 networks. Furthermore, IoT may involve more heavily the human in the loop that CPS. In this expose we consider CPS and IoT as two sides of the same coin. So, whatever is said here about CPS it applies to IoT as well.

These difficulties have led in context-based data modeling using linguistic approaches and semantics in an attempt to overcome the lack of statistical knowledge at the level of raw data and handle the fusion problem at a higher level, be it decision or inference, by embedding a priori contextual knowledge into the processing model and performing data understanding and fusion using AI and linguistics techniques. This approach has been proven to be successful, in particular in cases of CPS where the human is involved in the data generation process as either a probe or decision factor affecting the data collection process and sensory sources. In as much as successful these techniques have been in addressing the lack of a priori statistical knowledge about the raw data, they are hard to generalize as they heavily depend on the context they are used an require a fair amount of preprocessing in order to encapsulate the contextual knowledge into the process, which, at any rate, differs from case to case.

However, the question remains: are new data fusion models required for CPS ? To further understand the issue, we provide a number of examples to identify the issues that that may play affect data fusion when dealing with CPS.

Case 1 In-car GPS Navigation (e.g. Google Maps)

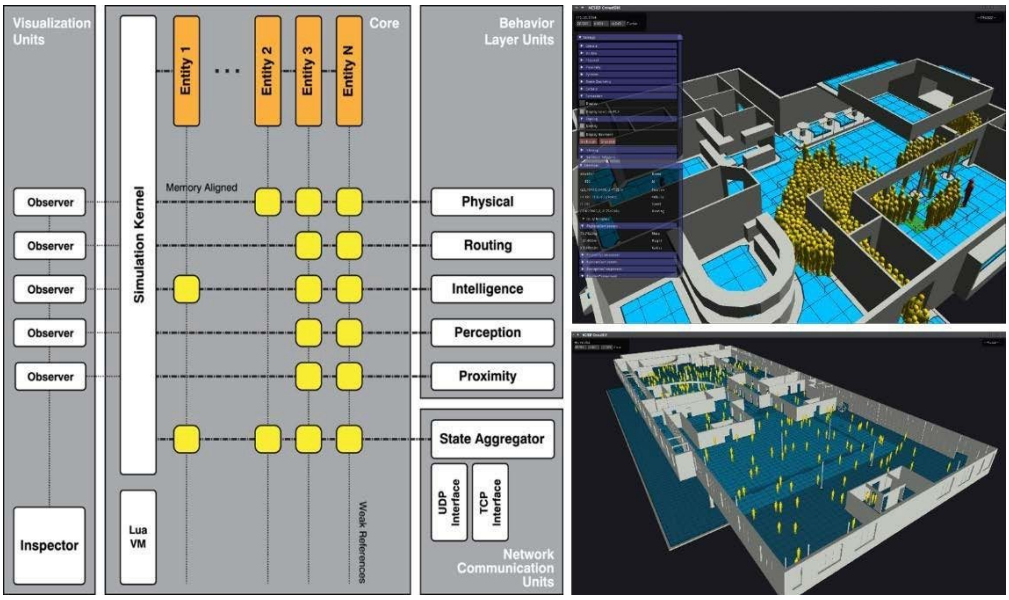
- Cyber System
- Centralized computation server, scheduling and routing all connected clients (cars)
- Physical System
- People driving cars equipped with smartphones running in-car navigation software

Data fusion use case: The vehicles with the navigation system are used to provide location information whereas the human driver reports information about traffic, incidents, etc. If we assume that the data fusion system that uses this information is designed to provide tips to drivers to avoid traffic jams, it is then a tantamount importance that the system is reliable and trusted. Reliability comes from the information provided by the drivers about traffic conditions, road incidents, etc. Trust is required both by drivers about the instructions given to them about avoiding traffic as well as by the system trusting that the drivers will follow its recommendations in order to build reliable predictive traffic models to improve congestion avoidance and navigation instructions. Thus it is very important from the system mission point of view that an accurate statistical model of the data provided by the drivers is available in order to properly fuse the information according to the appropriate confidence levels. The key issues, from the data fusion point of view are:

- Data Integrity
- Latency (Time Delays)
- Cyber Threats - Spoofing
- Priors - Fusion Models

- Humans as a “sensor”: Ethics - Privacy - Models?

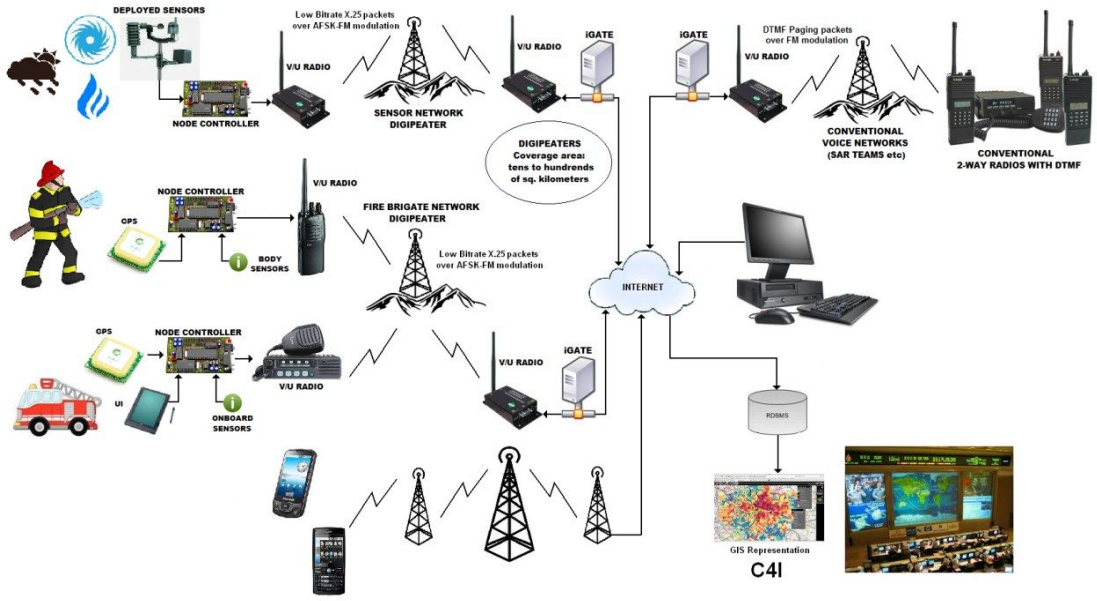
Case 2 Advanced Human Behavior Simulators (AHBS)

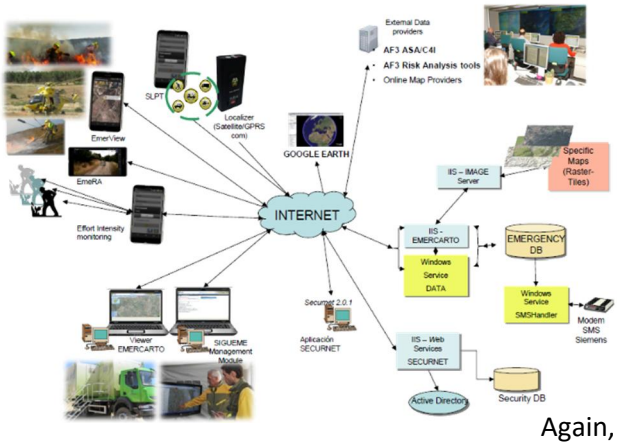


AHBS can be considered as CPS of high complexity, in particular when the cyber aspect of the simulator is interfaced with actual physical sensors and actuators, possibly even involving a human in the loop, for hybrid cyber-physical simulation, training and operations. Used for, e.g., evacuation planning in conjunction with real-time human actions and feedback from sensors and humans, such a system provides new challenges in data fusion models, in particular because of the limited a priori knowledge of the human in the loop, but, and even more fundamentally, the agents used in the simulation. Of course, the advantage of an AHBS lies in the ability to run a large number of simulation and collect statistics that can be, in turn, used to enhance the data fusion modelling. However, the difficulty remains with the validation of the results from an AHBS as data collection from the application field may be extremely difficult and thus juxtaposition with the simulated results and validation of the simulated (say via Monte Carlo) data statistics even more difficult.

Case 3 Situational awareness enhancement using a swarm of UAVs and Humans Cyber System - Example: Fire detection & warning systems

- Centralized computation server, responsible for the flight data and sensory focus of all UAVs, making decisions based on fused information from UAVs
- Physical System
- UAVs equipped with sensors needed to enhance the situational awareness over a large area
- Humans with Mobile Apps
- Humans as “sensors” reporting on events - crowd-sourcing
- Cyber-Physical System Issues





Again, the case is very similar to the AHBS case. The issues ar the same:

- Data Integrity
- Latency (Time Delays)
- Cyber Threats - Spoofing
- Priors - Fusion Models
- Humans as a “sensor”: Ethics - Privacy - Models?

From the brief analysis of the four use cases it follows that the issues that relate with CPS and data fusion refer pretty much to same fundamental issues that exist with any data fusion system, namely statistical data models, data integrity, data latency [2], communication errors [3], and thee fundamental questions: in which of the three levels of the canonical data fusion architecture [1], fusion is done best in a given scenario. In CPS, however, that include a feedback control loop and, possibly, a human in the loop and data crowd sourcing, additional issues in data fusion models may arise from: (a) non-stationarities; (b) cyber threats and human behavior that may not be easy to model statistically and predict (in a statistical sense) their behavior; (c) data integrity that relates to the trust in crowd sourced data; and (d) ethics and privacy issues as human personal data enter in the picture.

Do the above issues require new data fusion models? It is our belief that new models may not be required. However, there is a definite need of expanding and adapting existing models to account for the peculiarities introduced by CPS and IoT, in particular the human in the loop, date crowd sourcing, but also the extensive use of hybrid and large scale simulators in analyzing and predicting the behavior of complex CPS in virtual and augmented reality environments. Furthermore, new, and more powerful, pre-processing tools from the fields of knowledge engineering, linguistics and AI (artificial intelligence), as well as quantum physics, may be required for better data conditioning taking into account the context in which data fusion takes place. Moreover, Big Data Analytics may be required to derive reliable statistical models for integrating crowd-sourced data (and their statistics) into the data fusion model.

In conclusion, the physical world is unpredictable and thus CPS exhibit more unpredictable behavior, calling for data fusion model need higher reliability and robustness standards. Especially when people are involved, it is difficult to account for their statistical behavior, leading to even higher unpredictability in the data fusion model. Some of he questions that need to be address are:

1. Knowledge of a priori probability distribution (priors) in CPS and what are the appropriate statistics to use. Do Bayesian models still apply, or one should look into non-measure theory based methods, such as Dempster-Schafer, Fuzzy logic, or Generalized Evidence Processing (GEP) theories [1]?
2. Big Data Analytics for crowd-sourced data statistics and how questions and methodologies related to ethics and privacy are integrated into the model to make the results compliant with related legislation?
3. Temporal dimension is not intrinsic to programming (e.g. C, C++, Java) but must be accounted for when in comes to AHBS.
4. How on- the-fly model changes in CPS are accounted for in the data fusion model design?
5. How physical dynamics and computations are dealt in a unified manner?
6. How is network latency and communication errors taken into account t in the design of data fusion models in order to end up with a robust and resilient data fusion design? And
7. How cyber threats accounted for in the design of the data fusion model?

References

[1] S. C. A. Thomopoulos, "Sensor Integration and Data Fusion," Invited paper in special issue on Sensor Integration and Data Fusion for Robotic Systems, Journal of Robotic Systems, 1990, Volume 7, No. 3, pp. 337-372, 1990.

[2] S. C. A. Thomopoulos, and L. Zhang, "Distributed Decision Fusion with Networking Delays and Channel Errors," SPIE Proceedings, Sensor Fusion, (1988), Volume 931, pp. 154-160, 1988.

[3] S. C. A. Thomopoulos and L. Zhang, “Distributed Decision Fusion with Networking Delays and Channel Errors,” Information Sciences: An International Journal, nos. 1 & 2, December 1, 1992, Volume 66, pp. 117-131, 1994.

On Secure and Resilient Energy-Based Critical Infrastructure

Dr. Wei Yu
Associate Professor
Director of Cyber-Physical Networked System & Security Laboratory
Department of Computer & Information Sciences
Towson University
http://wp.www.towson.edu/wyu
Email: wyu@towson.edu

Outline

- Part I. Overview
- Part II. An Integrated Modeling Framework for Efficient Energy Resource Management
- Part III. Threats on System Operation

Smart Grid Overview

- **Smart grid will be our future energy critical infrastructure**
  - Integrating modern computing and communication technologies
  - Being more efficient, reliable, secure, and resilient
  - Providing better energy service to users

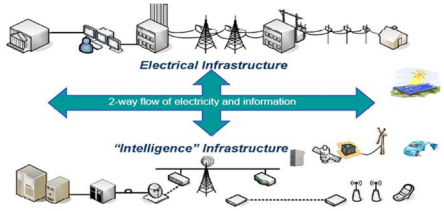


Fig. 1: Smart Grid (Source: NIST)

Goal and Contributions

- **The goal**
  - Establishing a theoretical and empirical foundation for designing efficient and securing smart grid
- **Contributions**
  - Designing modeling and simulation techniques for efficient resource management
  - Developing a framework to systematically explore attacks against system operation and end users
  - Understanding the impact of these attacks and developing mitigating schemes

Challenges

- **Smart grid is a highly distributed and complicated system**
  - Consists of numerous function components
  - Operates under the presence of various uncertainties
    - Different types of failures and attacks
    - Failures and attacks can come from cyber and physical grid components

Fig. 2: Smart Grid Domain Model (Source: NIST)

Framework

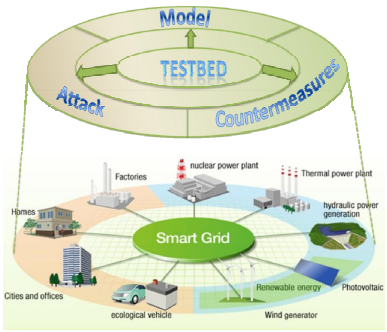


Fig. 3: Framework

Research Focus

- **Integrated Modeling Framework for Smart Grid Energy Management**
  - Develop modeling and simulation techniques to quantify different uncertainties from cyber components and physical grids
- **Attacks Impacts on System Operation and End users in Smart Grid**
  - Explore the space of attacks against system operation, understand them, and develop mitigating schemes to prevent, detect and attribute to attacks
  - Develop electricity price models and investigate attack impacts on users, as well as privacy-preserving techniques

Outline

- Part I. Overview
- Part II. An Integrated Modeling Framework for Efficient Energy Resource Management
- Part III. Threats on System Operation

Integrated Modeling Framework for Energy Management

- **Problems**
  - Quantify different types of uncertainties
  - Reduce impact from those uncertainties

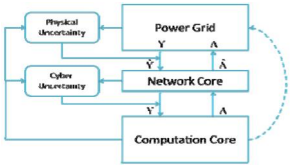


Fig. 4: Coordinating Cyber & Physical Components

- **Our Ideas**
  - Develop modeling techniques to quantify the risk of those uncertainties
  - Develop techniques to effectively manage energy resources and to adapt uncertainties and make system resilient

SPIE 2016 Towson University Wei Yu

Integrated Modeling Framework for Energy Management (cont.)

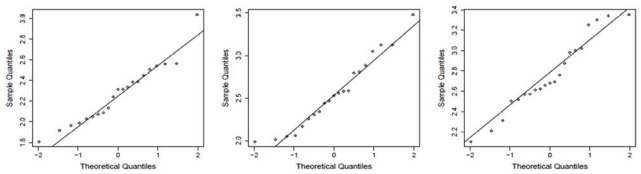
- **Different types of uncertainties**
  - Differentiating and quantifying the risk of different uncertainties
    - <cyber component, failure> & <cyber component, attack>
    - <physical component, failure> & <physical component, attack>
  - Investigating the impacts of different uncertainties
    - Random or non-random
    - Physical grid or cyber components
- **Mechanisms to tackle uncertainties**
  - Managing energy resources (e.g., transmission, distribution and storage)
  - Modeling and predicting energy generation and demands from users, as well as critical components

SPIE 2016 Towson University Wei Yu

Results: Statistical Modeling and Forecasting of Energy Usage

- **Deriving a statistical model for energy usage**
  - The real-world meter reading data set from Stanford university
    - Nearly 300 houses over 200 days between February 2010 and October 2010
  - Using non-parametric tests
    - Shapiro-Wilk test & Quantile-Quantile (Q-Q) plot normality test
- **Developing machine learning based approaches to perform accurate forecasting of energy usage**
  - Standard Radial Basis Function (RBF) based SVM
  - Least Squares (LS) based SVM
  - Backward Propagation Neural Network (BPNN)

Results: Statistical Modeling and Forecasting of Energy Usage (cont.)



(a) Morning data (b) Noon data (c) Evening data

Fig. 5: Q-Q Plot of Energy Consumption Data

Method	Statistics	MAPE	γ^2	MSE
SVM	Mean	7.1261%	0.7593	0.0037
	Variance	0.0004	0.0144	0.0009
LS-SVM	Mean	14.5649%	0.6219	0.0321
	Variance	0.002	0.0128	0.0014
BPNN	Mean	16.8356%	0.4338	0.0732
	Variance	0.007	0.0130	0.0571

Table 1: Prediction of Energy Consumption

Outline

- Part I. Overview
- Part II. An Integrated Modeling Framework for Efficient Energy Resource Management
- Part III. Threats on System Operation

Cyber Attacks on Power Grid

- **Real World Examples**
  - In 2003, computers infected by *Slammer* worm shut down safety display systems at power plant in Ohio
  - In 2008, *computer intrusions* in European power utilities
  - In 2010, *Stuxnet* worm provides a blueprint for aggressive attacks on control systems
  - In 2011, malware *BlackEnergy* disrupts processes controlled HMIs products from vendors, e.g., General Electric, Siemens, Advantech
  - Between April 2013 and 2014, hackers managed to break into **37%** of energy companies, according to a survey by ThreatTrack Security
  - In 2014, a remote access Trojan program called *Havex* was used to hack into the websites of industrial control system and SCADA manufacturers and poisoning legitimate software downloads
  - In 2013 and 2014, there were **224** hacking incidents at energy companies investigated by the Computer Emergency Readiness Team, a division of the Department of Homeland Security (DHS)
  - In March 2014, TrustedSec discovered *Spy malware* in the software that a major U.S. energy provider uses to operate dozens of turbines, controllers and other industrial equipment
  - **...**

xc

Problems and Out Ideas

- **Problems**
  - Smart meters and sensors can be compromised
  - System operation can be disrupted through compromised components
- **Our Ideas**
  - Exploring the space of attacks against the system operation from key function modules
    - Static & dynamic state estimation
    - Energy price
    - Integration of distributed energy resources
    - Power flow control
    - ...
  - Understand their risk to system operation in smart grid and develop countermeasures

Framework for Exploring Attack Space

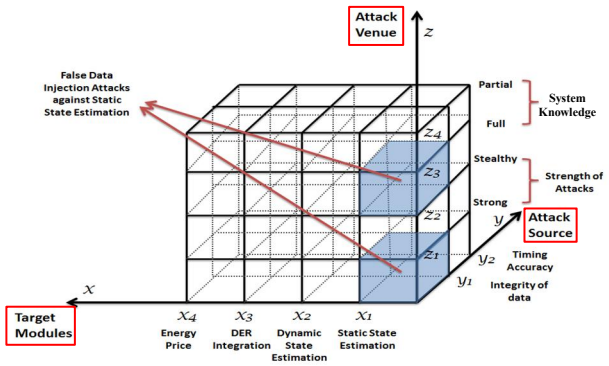


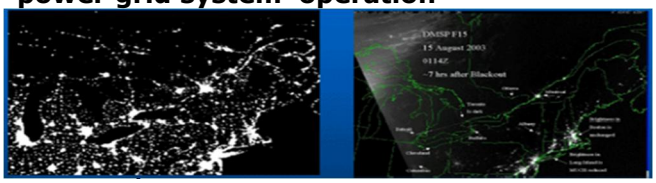
Fig. 6: A 3D Threat Space

False Data Injection Attacks

- Smart grid may operate in hostile environments
  - Meters and sensors lacking tamper-resistance hardware increases the possibility to be compromised
- The adversary may inject false measurement reports to disrupt the smart grid operation through compromised meters and sensors
- Those attacks denoted as **data integrity attacks**
  - State estimation
  - Energy price
  - Others: Distributed energy resources integration, microgrid, power control, time synchronization, etc.

Data Integrity Attacks on State Estimation

- **State estimation is a key component in power grid system operation**



- **Objectives of this research**
  - Modeling data integrity attacks against power system state estimation
  - Developing countermeasures against such attacks

Data Integrity Attacks on State Estimation

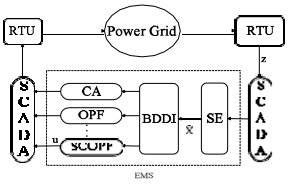


Fig. 7: State Estimation

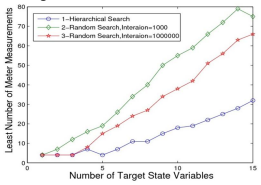


Fig. 8: Results for Finding Minimum Set of Meters

- **How can an adversary choose the meters to compromise in order to cause the most significant deviation of the system state estimation?**
  - Formalizing the problem and mapping it to minimum subadditive joint problem
  - Developing heuristic algorithms
- **How can a system operator defend against such attacks?**
  - Protection based approach
  - Both spatial and temporal correlation based detection

Big Data in Smart Grid

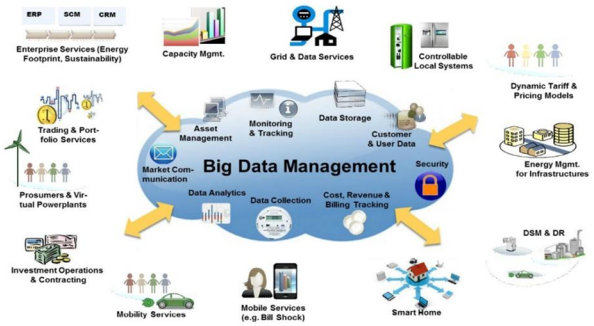


Fig. 9: Big Data Management for Smart Grid

Challenges

- Smart grid must be dependable, cost-effective, secure, and efficient, which can operate in real-time
- High volume data streams associated with smart grid operations need to be quickly processed and analyzed
  - Collected massive streaming data will be generated from power grid to energy management system (EMS) to enable efficient system operation

System Architecture

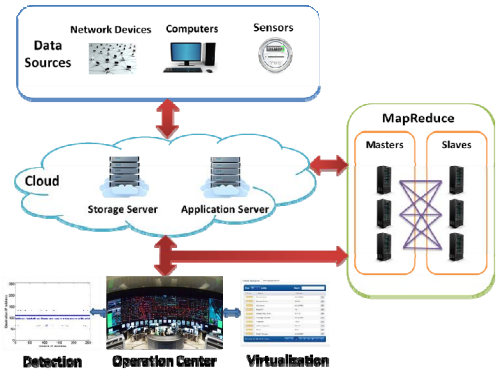


Fig. 10: System Architecture

Position Paper
On Secure and Resilient Energy-Based Critical Infrastructure

Wei Yu
Associate Professor, Department of Computer and Information Sciences
Towson University, Towson, MD 21252
Email: wyu@towson.edu

ABSTRACT

The smart grid, as a typical energy-based cyber-physical system and critical infrastructure, uses modern computing, communication, and control technologies to make the power grid more efficient, reliable, secure, and resilient. As a highly distributed and complex system, the smart grid consists of numerous functional components and could operate under the presence of various uncertainties raised by diverse types of failures and attacks from both cyber and physical components. To address these issues, we shall systematically identify cyber threats in the smart grid, utilizing modeling and simulation techniques to understand their impacts on both system operations and end users, while simultaneously developing effective mitigation schemes to defend against these attacks.

Keywords: Smart Grid, Energy-Based Cyber-Physical System, Modeling and Simulation, Cyber Threats and Mitigation.

OVERVIEW

The modernization of the electrical power grid is paramount to efforts for increasing energy efficiency, transitioning to clean and cost-effective renewable energy resources, securing critical infrastructures, etc. The development of smart grid, which is denoted as a typical energy-based cyber-physical/ critical infrastructure system, has received renewed attention. While major research efforts have been conducted in the area of improving the operational efficiency and reliability of power grids through the use of advanced information communication technologies, the risks of failures and cyberspace breaches on power grid systems need to be seriously investigated before a massive deployment of smart grid technologies can be realized.

Concerns about security and resilience in the smart grid are growing. The operation and control of the smart grid depends on a complex cyberspace of computers, software, and communication technologies. Component failures could trigger cascading failures, leading to power outages. An adversary has the potential to cause great damage to the grid through extended power outages, destruction of electrical equipment, and increased energy cost and price, but only if they are able to compromise the system. Because the measurement components supported by smart equipment (smart meters and sensors) play a vital role in smart grid operation, they are likely targets for cyber-attacks and hold significant potential for subverting the system. It is worth noting that those measuring devices connected through open network interfaces further increase the possibility of being compromised by the adversary.

Developing secure and resilient smart grid remains challenging due to three significant reasons. First, the smart grid is a highly distributed and complicated system, and inherently operates under the presence of various uncertainties in both energy supply and demand. Uncertainties can be malicious attacks or unforeseen failures raised by information communication components and physical grid components. Second, the smart grid consists of many distinct and varied functional components. Systematic investigation of the impact of attacks on the performance of the smart grid, and the development of effective countermeasures to mitigate such attacks, becomes more challenging as component diversity increases. Third, it is commonly known that the deployment of the smart grid for research and education is exceedingly expensive, and unattainable for many institutions. The development of an evaluation platform to validate the effectiveness of the modeling theory, attacks/failures, and countermeasures is likewise limited by cost and feasibility.

Addressing these challenging issues calls for the development of a modeling and simulation framework to investigate the interaction between communication networks and the physical power grid. The modeling and simulation framework has

the potential to not only advance the understanding of failures and cyber-attacks on the smart grid system operation and end users, but also to help the development of innovative responses to protect the smart grid. We have thus carried out our research to this end. We have derived a statistical model for energy use based on a real-world smart meter dataset, and have developed machine-learning-based approaches (e.g., support vector machine, neural networks) to perform an accurate forecasting of energy usage [1]. To understand the interaction and the reciprocal effects between the communication network and power grid applications in the smart grid, we investigated the performance of demand/response and dynamic market pricing under various states of communication networks (e.g., normal operation, degraded performance, and security threats) based on a co-simulation platform [2]. We have also investigated vulnerabilities of key function modules of the smart grid, including data integrity attacks against static/dynamic state estimation [3, 4], distributed energy transmission [5], energy price [6], and cascading failures [7].

In addition to the modeling and understanding of the impact of failures and security vulnerabilities on the performance of the smart grid, we shall develop effective mitigation techniques to handle failures and attacks. To be specific, we intend to develop mechanisms with respect to prevention, detection, and attribution. For prevention, we will investigate protection mechanisms to increase the cost of launching attacks. For example, to deal with cascading failures, we could investigate mechanisms to identify the most critical locations for launching attacks and deploy defensive devices (threat monitoring sensors, energy storage components, etc.). One related problem is to determine the optimal location of energy storage components and storage capacity to maximize protection effects against cascading failures with the lowest deployment cost. To make the power grid resilient to cyber-attacks, we will develop cost-effective protection schemes by optimally deploying smart sensors. For detection and attribution of failures and threats, we will develop diverse and effective anomaly detection techniques [8]. For example, we will consider schemes such as hypothesis tests that leverage the fact that, statistically, to cause the most damage to a system, manipulated measurements in the smart grid must deviate more from the mean than regular measurements with random noise. For slow and stealthy failures or attacks (e.g., marginally manipulating meter readings over time to cause damage slowly while avoiding detection), we will leverage nonparametric cumulative sum schemes, amongst others, that accumulate small deviations of the observed measurement until the value approaches a given threshold. We also intend to study efficient detection techniques to detect compromised meters by correlating software behavior, network traffic, and characteristics in power flows. We shall likewise develop schemes to identify and isolate compromised and failing devices. In addition, given the massive data required for monitoring and controlling the smart grid, we will leverage the cloud computing environment and parallel computing algorithms to improve the efficiency of data analysis in the smart grid.

REFERENCES

[1] Wei Yu, Dou An, David Griffith, Qingyu Yang, and Guobin Xu, "On Statistical Modeling and Forecasting of Energy Usage in Smart Grid," in Proc. of ACM International Conference on Reliable & Convergent Systems (RACS), October 2014.

[2] Paul Moulema, Wei Yu, David Griffith, and Nada Golmie, "Performance Evaluation of Smart Grid Applications using Co-simulation," in Proc. of IEEE International Conference on Computer Communication and Networks (ICCCN), August 2015.

[3] Qingyu Yang, Jie Yang, Wei Yu, Dou An, Nan Zhang, and Wei Zhao, "On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures," IEEE Transactions on Parallel and Distributed System (TPDS), 25(3): 717-729, 2014.

[4] Qinyu Yang, Liguo Chang, and Wei Yu, "On False Data Injection Attacks against Kalman Filtering in Power System Dynamic State Estimation," to appear in the International Journal of Security and Communication Networks (SCN) – John Wiley & Sons (Accepted in June 2013).

[5] Jie Lin, Wei Yu, Xinyu Yang, Guobin Xu, and Wei Zhao, "On False Data Injection Attacks against Distributed Energy Routing in Smart Grid," in Proc. of the 3rd ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS), April 2012.

[6] Jie Lin, Wei Yu, and Xinyu Yang, "On False Data Injection Attack against Multistep Electricity Price in Electricity Market in Smart Grid," IEEE Transactions on Parallel and Distributed Systems (TPDS), 27(1): 286-302, 2016.

[7] Xin Chen, Wei Yu, David Griffith, Nada Golmie, and Guobin Xu, "On Effectiveness of Energy Storage System against Smart Grid Cascading Failure," in Proc. of ACM International Conference on Reliable & Convergent Systems (RACS), October 2014.

[8] Wei Yu, David Griffith, Linqiang Ge, Sulabh Bhattarai, and Nada Golmie, "An Integrated Detection System against False Data Injection Attacks in the Smart Grid," International Journal of Security and Communication Networks (SCN) – John Wiley & Sons, 8(2): 91-109, 2015.