Missouri University of Science and Technology
Formerly University of Missouri-Rolla

Computer Science Department

Securing CPS and IoT in Smart Living

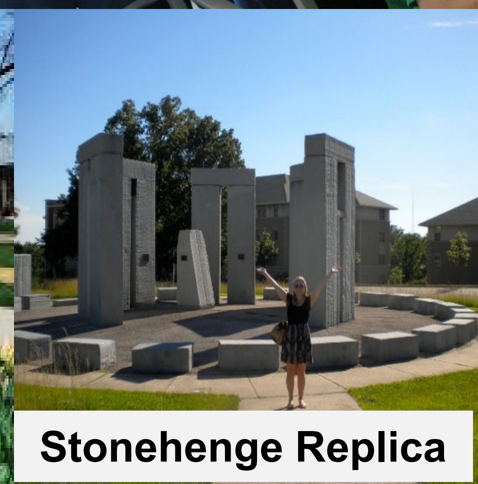
Sajal K. Das

(sdas@mst.edu)

Missouri S&T, Rolla

Miners Dig Deeper

Founded in 1870



Stonehenge Replica

Solar Car

Solar Village

Warm Up

Who is the founder of Facebook?

Who is the Co-founder and CEO of Twitter?

Jack Dorsey

… was a student in our department

He’s also CEO and Co-founder of Square!

Career Evolution

Parallel Computing (1985 -) →	Mobile Computing (1995 -) →	Pervasive / Smart Computing (2001 -)
• HPC	• Cellular (3G/4G) Networks	• Sensor Networks, IoTs
• Parallel Algorithms	• Ad hoc Networks, WLANs	• Pervasive Computing
• Distributed Systems	• Opportunistic Networking	• Situation-awareness
• Petri Nets	• Cognitive Radios	• Middleware Services
• Interconnection Networks	• Wireless Mesh Networks	• Security, Privacy, Trust
• Task Scheduling	• Mobility Management	• Smart Environments
• Load Balancing	• Resource Management	• Cyber-Physical Systems
• Cluster Computing	• Wireless Internet Multimedia	• Smart Health Care
• P2P Networking	• Wireless QoS and QoE	• Smart Grid / Energy
• Grid / Cloud Computing	• Mobile Cloud	• Smart City
• Green Computing	• Edge and Fog Computing	• Mobile Crowd Sensing

- Computational Systems Biology (2005 -); Social Networks (2007 -)
- Smart and Connected Communities (2016 -)

Smart Sensing → CPH → Smart Computing

Efficient Architectures, Algorithms and Protocols, Modeling, Analysis, Optimization, Performance Evaluation, Prototype

Security, Privacy, Trust, Reliability, Vulnerability

Smart Systems and Applications
Smart City, Cyber-Physical-Human Systems (CPH), Mobile Crowd Sensing, Internet of Things (IoT)

Distributed/Mobile/Cloud/Pervasive Computing
Middleware Services and Virtualization

3G/4G/5G Cellular, Mobile Ad hoc, WLANs, Cognitive Radios	Wireless Sensors, Wearables, IoT, RFID	Broadband, P2P, Optical, Internet, Home/Enterprise Networks

Economics, Auction, Policy, Human Behavior, Game Models, Social Networks

See Google Scholar …

My Collaborations with Australia

- UNSW, Sydney

  Prof. Boualem Benatallah
  A/P Dr. Wen Hu
  Prof. Salil Kanhere
  Prof. Mahbub Hassan
  Prof. Sanjay Jha
  Prof. Aruna Seneviratne

- Univ. of Sydney
  Prof. Albert Zomaya

  UTS, Sydney
  Prof. Guoqiang Mao

- ANU, Canberra
  Prof. Weifa Liang

  RMIT, Melbourne
  A/P Dr. Tao Gu
  A/P Dr. Flora Salim

- Data61
  Dr. Sara Khalifa

  Univ. of Queensland
  Prof. Jaga Indulska

- Central Queensland Univ.
  Dr. Jahan Hassan

  Curtin Univ.
  Prof. Sweta Venkatesh

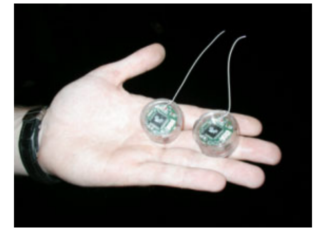
Outline

- Sensor Networks and IoT Security
  - NSF Project: *Pervasively Secure Infrastructures (PSI)*
- Smart City and Cyber-Physical-Human Convergence
  - NSF Project: *Smart Grid Security*
- Mobile Crowdsensing
  - *Trustworthy Vehicular Crowd Sensing*
- Future Directions

Era of Observation: Sensing the Physical World

Wireless Sensors

(A miniature Cyber-Physical System)



Computation

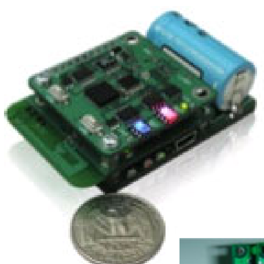
In-network Processing:

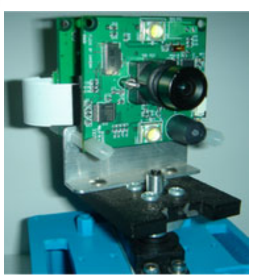
Fusion, Estimation,
Filtering, Aggregation

Communication
(Wireless)

Transmission/Reception:

Broadcasting, Routing,
Dissemination

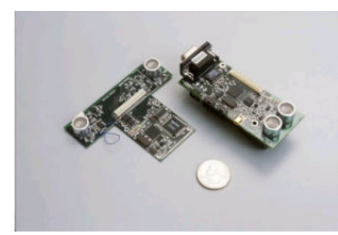




Control
(Sensing / Actuation)

Data Sensing & Collection:

temperature, humidity,
pressure, light, velocity,
sound, image



M. Di Francesco, S. K. Das, and G. Anastasi, “Data Collection in Wireless Sensor Networks with Mobile Elements: A Survey,” *ACM Transactions on Sensor Networks*, 8(1), Aug 2011.

Smartphone: A Rich Sensing Platform

- By 2020, number of smartphones is expected to be > 8 billion

- Plethora of Sensors
  - temperature, light, humidity, motion, acceleration, GPS, …
- Multiple Wireless Interfaces
  - WiFi, Bluetooth, long range cellular radio to connect to external sensors
- Internet Access
  - high-speed 3G/4G connection
- Multimedia Sensing
  - Audio, video, image, text

R. Fakoor, M. Raj, A. Nazi, M. Francesco, S. K. Das, "An Integrated Cloud-based Framework for Mobile Phone Sensing," *Proc. ACM SIGCOMM Workshop on Mobile Cloud Computing*, Aug 2012.

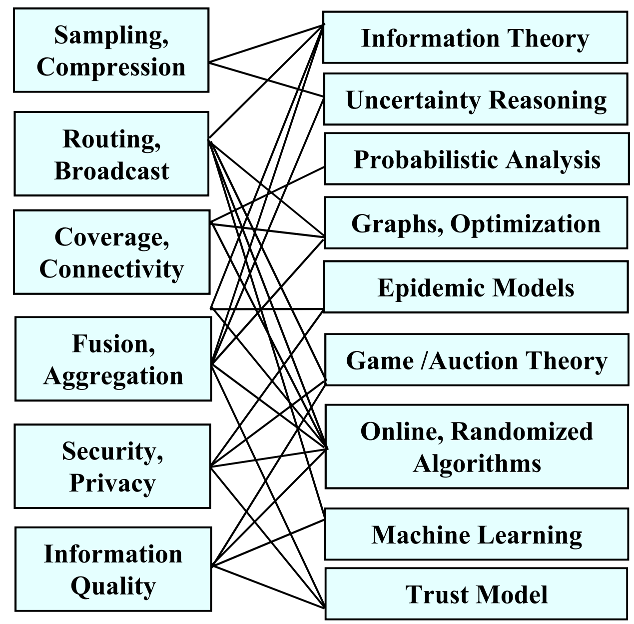
Sensor and IoT Challenges

➢ Reliability, Security, Privacy and Trust

- ❖ How to *secure* against adversarial, selfish, and malicious attacks? Prevent cascade failures?
- ❖ How to *trust* reported data (crowdsensing) for robust decisions? IoT data quality and QoI?
- ❖ How to incentivize for reliable information?

➢ Interdependence and Data Analytics

- ❖ How to model interdependence and information loss across overlapped smart spaces?
- ❖ How to analyze (multi-modal) data and design machine learning and prediction models?
- ❖ What are the impacts of social dynamics and human behavior on Smart Living?



- J.-W. Ho, M. Wright, S. K. Das, "Zone Trust: Fast Node Compromise Detection and Revocation in Sensor Networks," *IEEE Transactions Dependable and Secure Computing* (special issue on Learning and Games, Security), 9(4): 494-511, 2012.
- P. De, Y. Liu, and S. K. Das, "An Epidemic Theoretic Framework for Vulnerability Analysis of Broadcast Protocols in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, 8(3): 413-425, Mar 2009.
- N. Marchang, R. Dutta, and S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, 66(2): 1684-1695, Feb 2017.
- S. Bhattacharjee, N. Ghosh, V. K. Shah and S. K. Das, "QnQ: Quality and Quantity based Unified Approach for Secure and Trustworthy Mobile Crowdsensing," *IEEE Transactions on Mobile Computing*, 19(1): 200-216, Jan 2020.

NSF Project (completed)

Pervasively Secure Infrastructures (PSI): Integrating Smart Sensing, Data Mining, Pervasive Networking and Community Computing

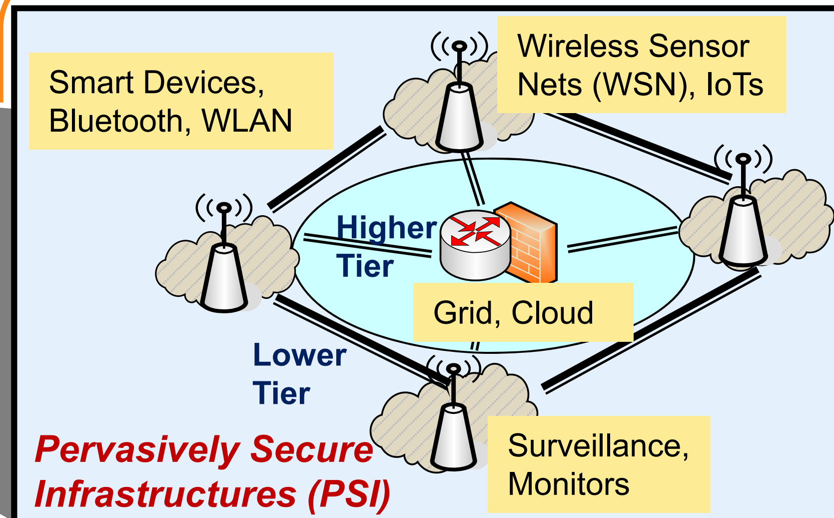
Securing Sensor Networks and IoT

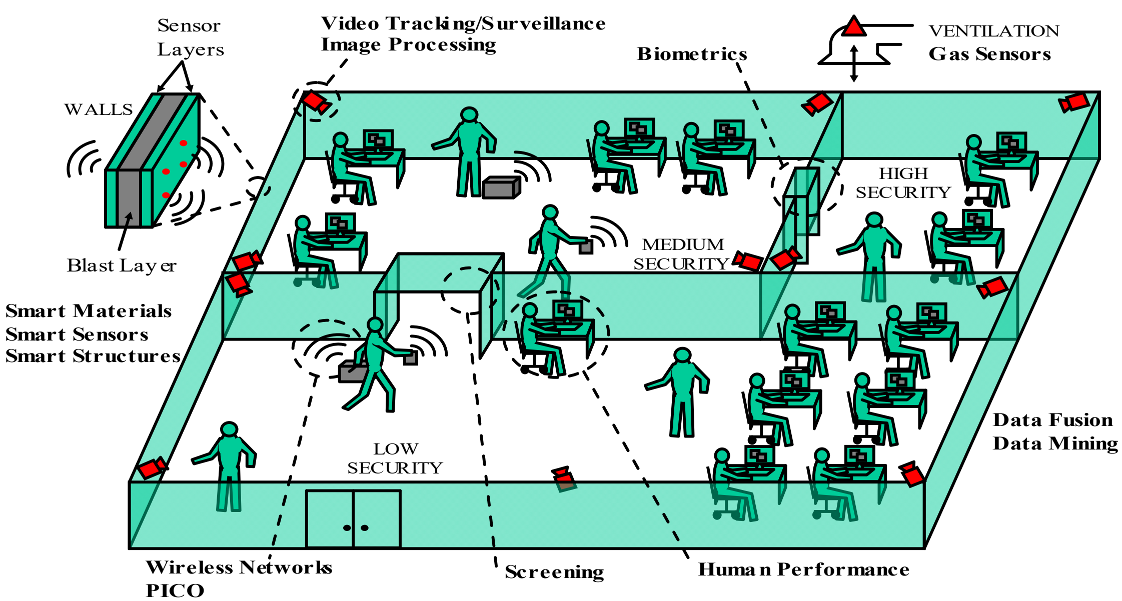
Goal: ***A multi-level security framework for IoT and Sensor Networks to monitor, detect, prevent (recover from) natural and man-made disasters.***

Methodology: Sensor Fusion; Situation-awareness; Information Theory; Game Theory; Epidemic Theory; Trust and Belief Models; Machine Learning; Data Analytics.

Publications: TDSC'17, TMC'11, ToSN'18, TDSC'12, TVT'17, AdHoc'15, AdHoc'13, TMC'09, Infocom'19, ComsNets'19, SmartCity'18, BuildSys'17

Resi-lience





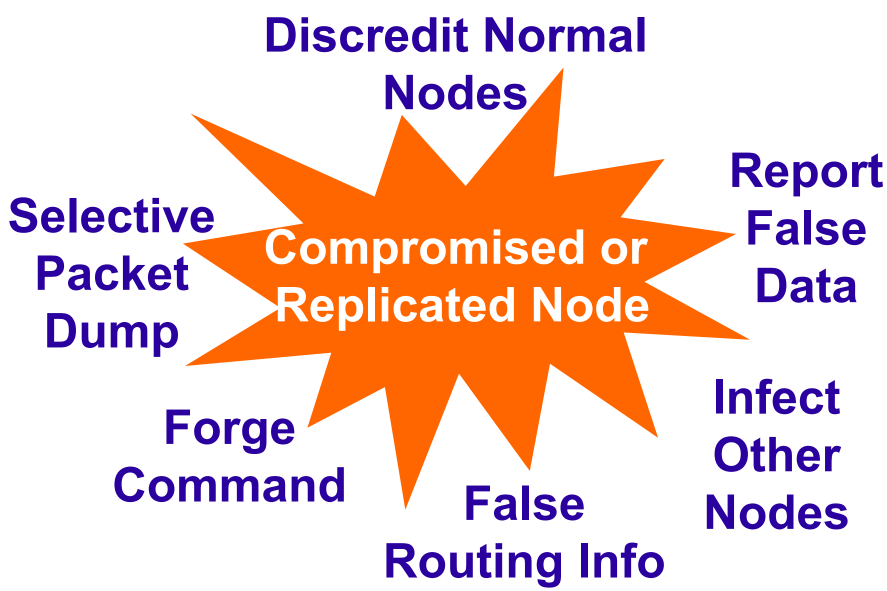
Broader Impacts:

- Critical infrastructure protection and border security
- Transportation (air, rail)
- Utility plants
- Public / private places (airport, train stations, shopping malls, parks)

Threats to WSNs and IoT

- Attack Types
  - Node Compromise
  - False Data Injection
  - Route Disruption
  - Denial of Service (DoS)

- Node Compromise
  - Physically capture sensor / IoT node
  - Generate replicas
  - Spread self-propagating worm
- Revealed Secrets
  - Cryptographic keys, code, commands
- Enemy's Puppeteers
  - Trojans in network with full trust



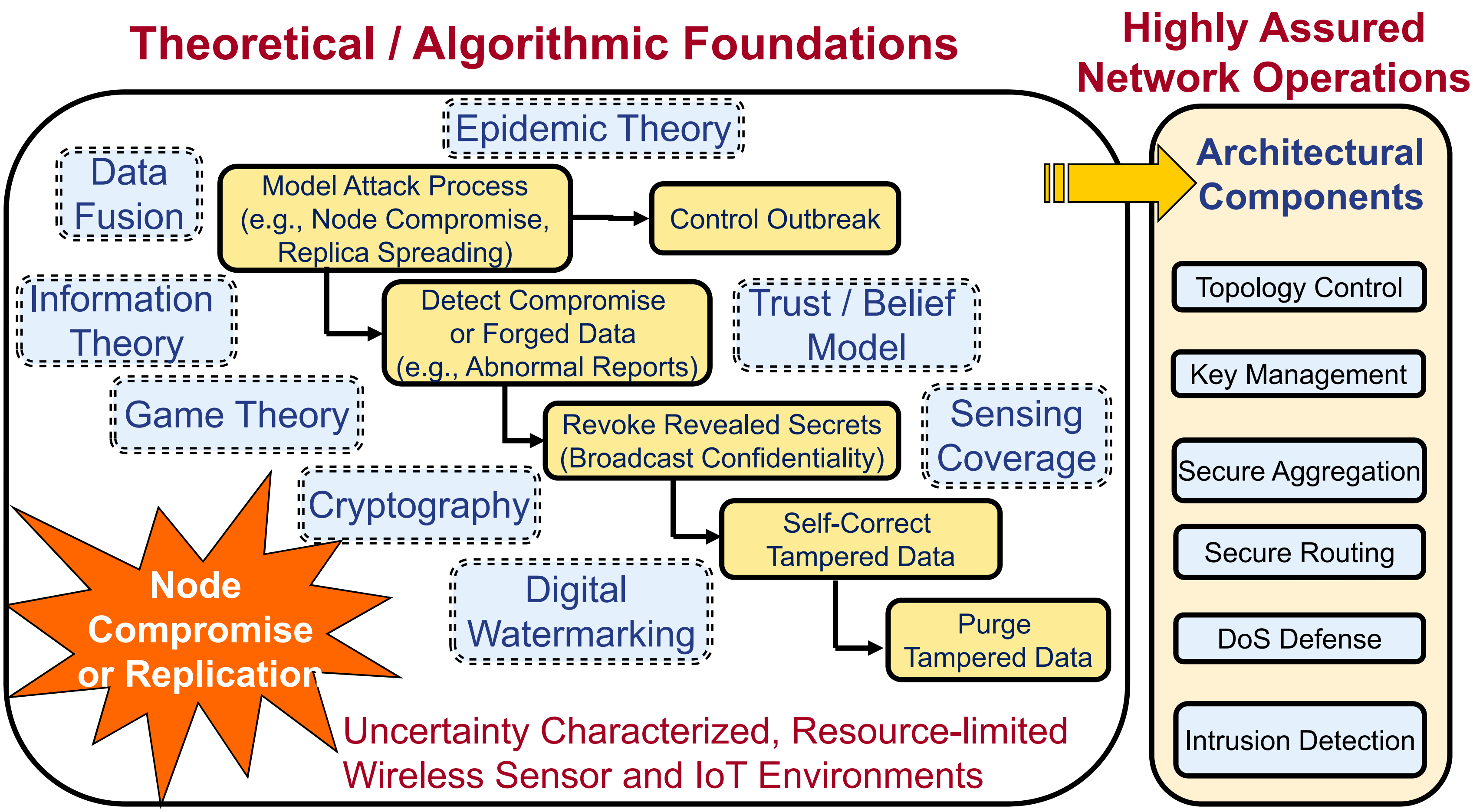
Worm Propagation Detection

Static /Mobile Node Replica Detection

Static / Mobile Node Compromise Detection

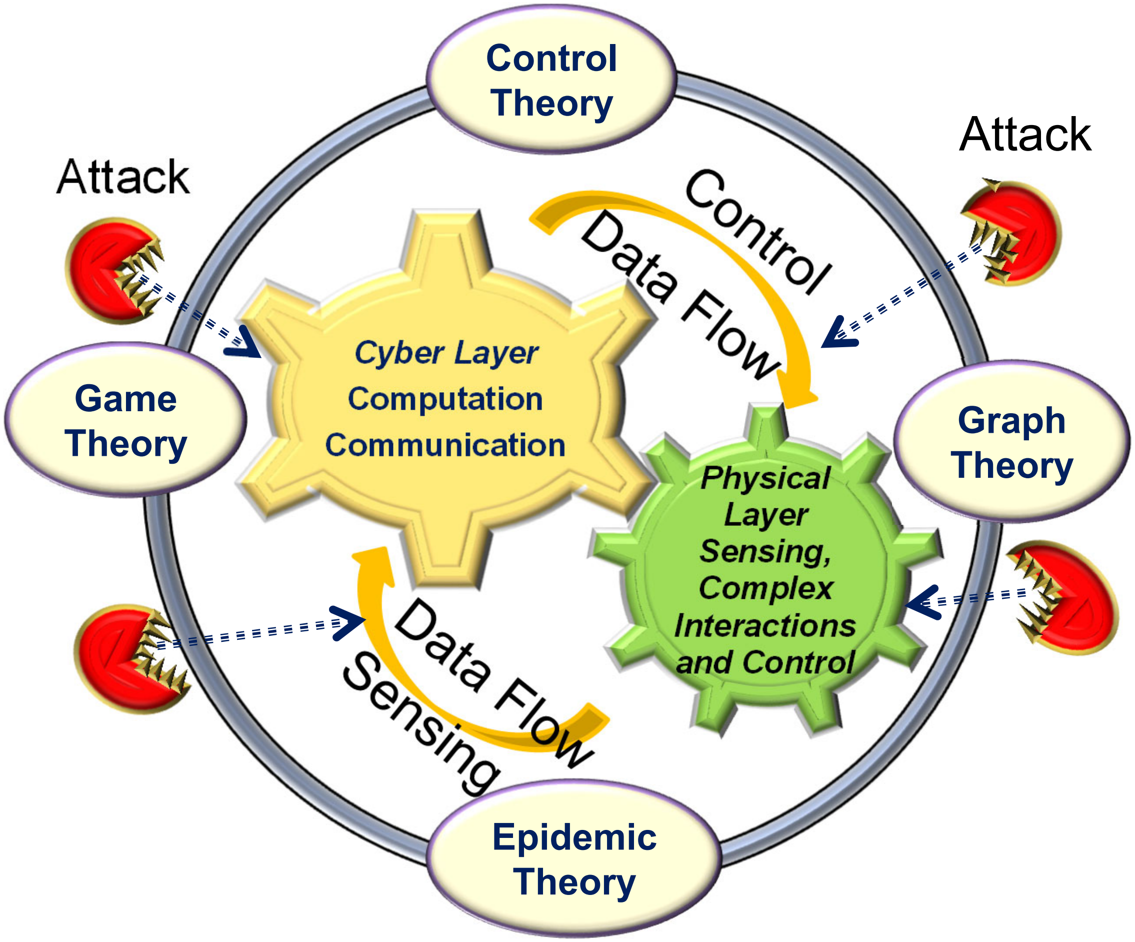
Modeling → Detection → Revocation → Self-correction → Purge

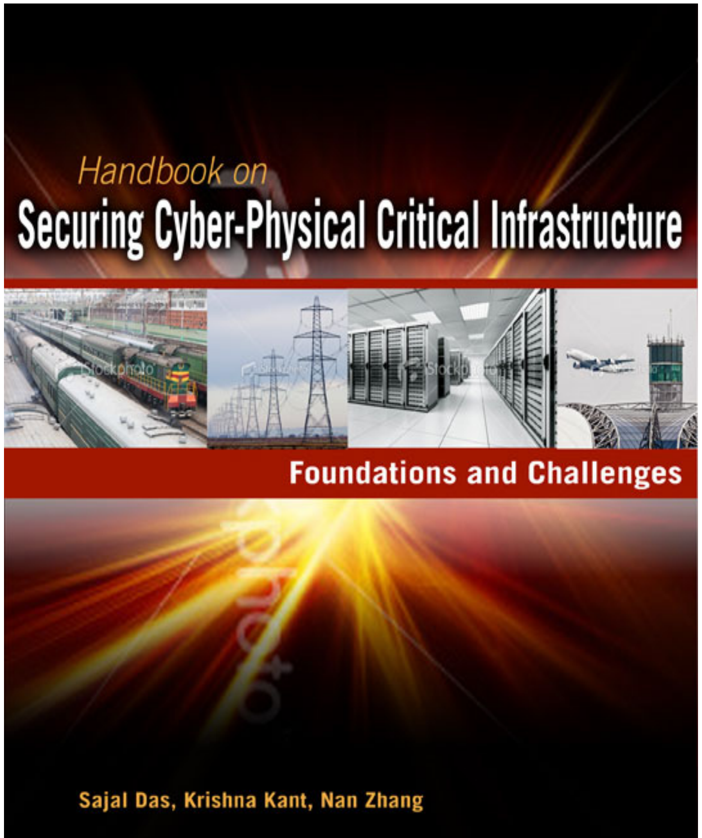
Multi-Level Security Framework



- J.-W. Ho, M. Wright, and S. K. Das, "Fast Detection of Mobile Replica Node Attacks in Sensor Networks Using Sequential Hypothesis Testing," *IEEE Transactions Mobile Computing,* 10(6): 767-782, June 2011.
- J.-W. Ho, M. Wright, S. K. Das, "Zone Trust: Fast Node Compromise Detection and Revocation in Sensor Networks," *IEEE Transactions Dependable and Secure Computing* (special issue on Learning and Games, Security), 9(4): 494-511, 2012.
- P. De, Y. Liu, and S. K. Das, "An Epidemic Theoretic Framework for Vulnerability Analysis of Broadcast Protocols in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, 8(3): 413-425, Mar 2009.
- N. Marchang, R. Dutta, and S. K. Das, "A Novel Approach for Efficient Usage of Intrusion Detection System in Mobile Ad Hoc Networks," *IEEE Transactions on Vehicular Technology*, 66(2): 1684-1695, Feb 2017.

Foundations of CPS Security





Das, Kant and Zhang
Morgan Kauffman, 2012

- S. Roy, M. Xue, S. K. Das, “Security and Discoverability of Spread Dynamics in Cyber-Physical Networks,” *IEEE Trans. on Parallel and Distributed Systems* (special issue CPS), 23(9): 2012.
- A. Sturaro, S. Silvestri, M. Conti, and S. K. Das, “A Realistic Model for Failure Propagation in Interdependent Cyber-Physical Systems,” *IEEE Transactions on Network Science and Engineering* (Special Issue on Network Science for High-Confidence Cyber-Physical Systems), 7(2): 817-831, 2020.

Outline

- Sensor Networks and IoT Security
  - NSF Project: *Pervasively Secure Infrastructures (PSI)*
- Smart City and Cyber-Physical-Human Convergence
  - NSF Project: *Smart Grid Security*
- Mobile Crowdsensing
  - *Trustworthy Vehicular Crowd Sensing*
- Future Directions

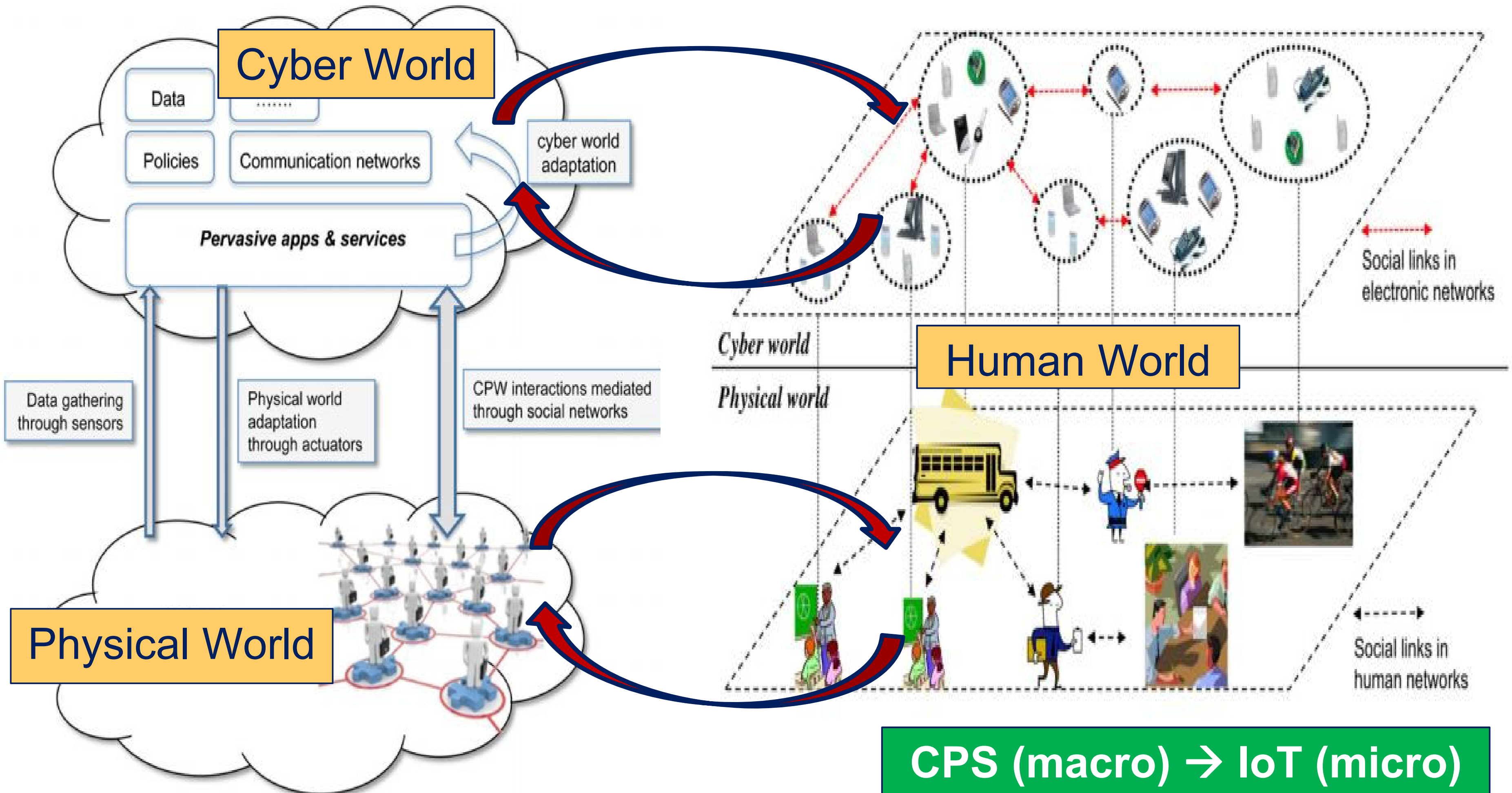
Cyber-Physical-Human (CPH) Convergence

CPH are natural / engineered systems that integrate sensing, communication, computing, control and human in the loop

M. Conti, S. K. Das, et al. "Looking Ahead in Pervasive Computing: Challenges and Opportunities in the Era of Cyber-Physical Convergence. *Pervasive and Mobile Computing*, *8*(1): 2-21, 2012.

Cyber-Physical-Human (CPH) Convergence

CPH are natural / engineered systems that integrate sensing, communication, computing, control and human in the loop



CPS (macro) → IoT (micro)

M. Conti, S. K. Das, et al. "Looking Ahead in Pervasive Computing: Challenges and Opportunities in the Era of Cyber-Physical Convergence. *Pervasive and Mobile Computing*, *8*(1): 2-21, 2012.

What is a Smart Environment?

A Smart Environment is one that is able to autonomously *acquire* and *apply* knowledge about inhabitants and their environment, and *adapt* to improve experience *without explicit awareness*

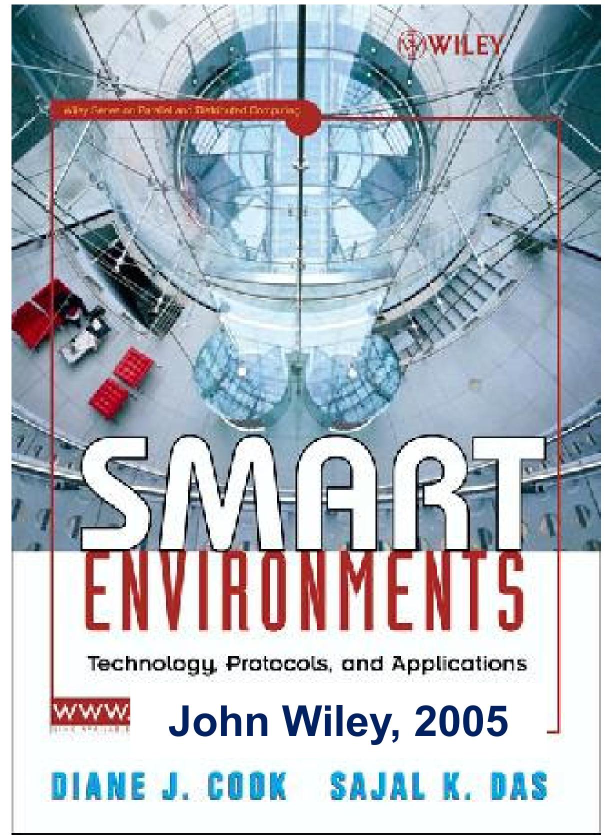
Corollary: makes *intelligent decisions* in *automated, context-aware* manner

→ pervasive or ubiquitous computing

Context /Situation-awareness is the key

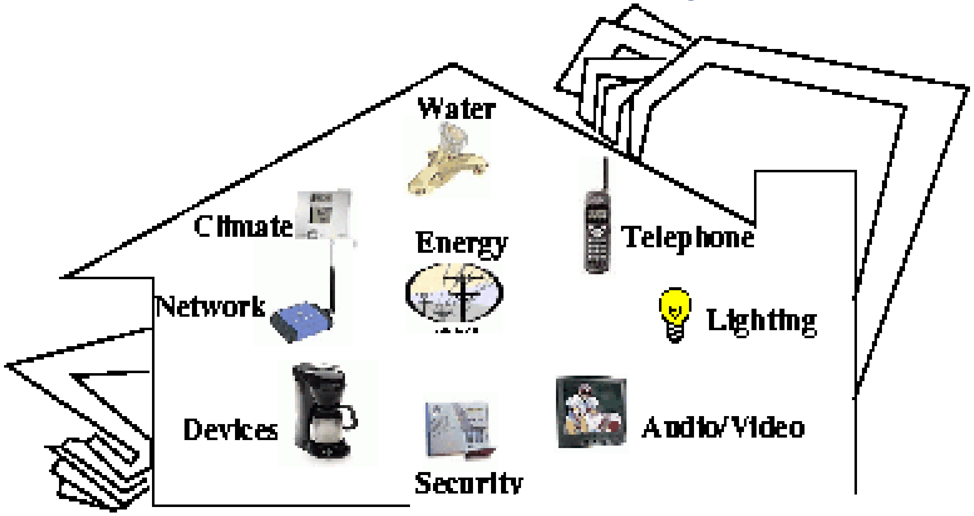
Example Contexts:

- Mobility, Activity, Occupancy, Preferences, …
- Desire, Behavior, Mood, Emotions, …

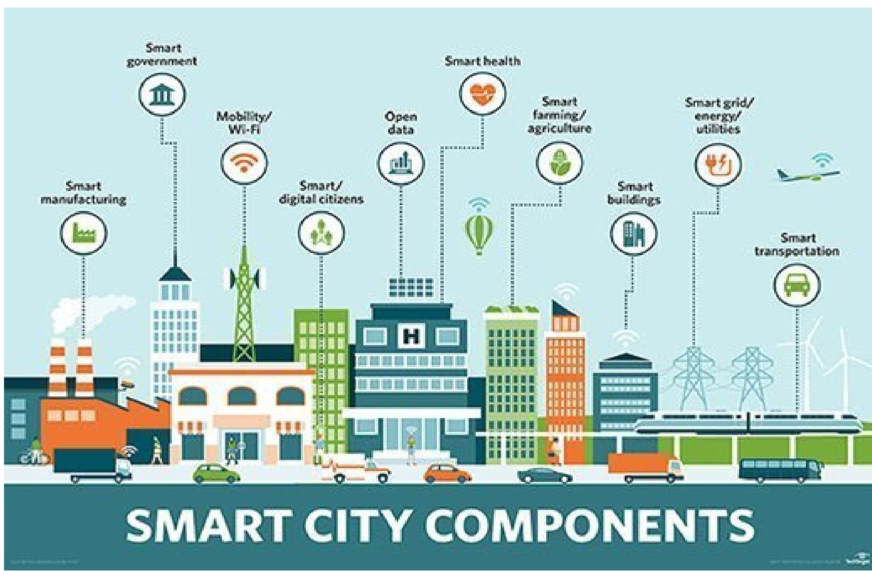


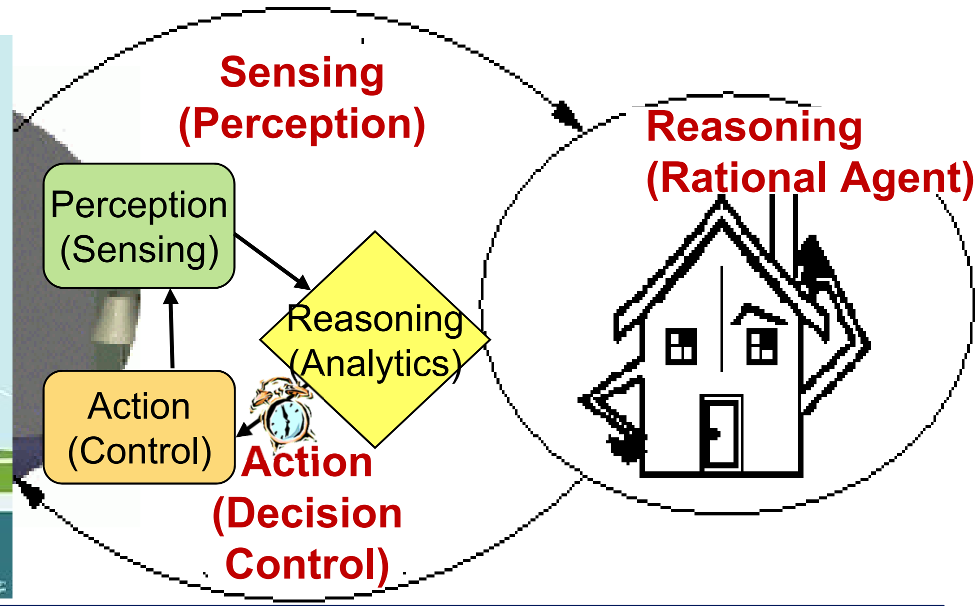
- D. J. Cook and S. K. Das, "How Smart Are Our Environments? An Updated Look at State of the Art," *Pervasive and Mobile Computing*, 3(2). 2007.
- A. Roy, S. K. Das, and K. Basu, "A Predictive Framework for Context-aware Resource Management in Smart Homes," *IEEE Transactions on Mobile Computing*, 6(11): 1270-1283, 2007.

Smart City as a Rational Agent



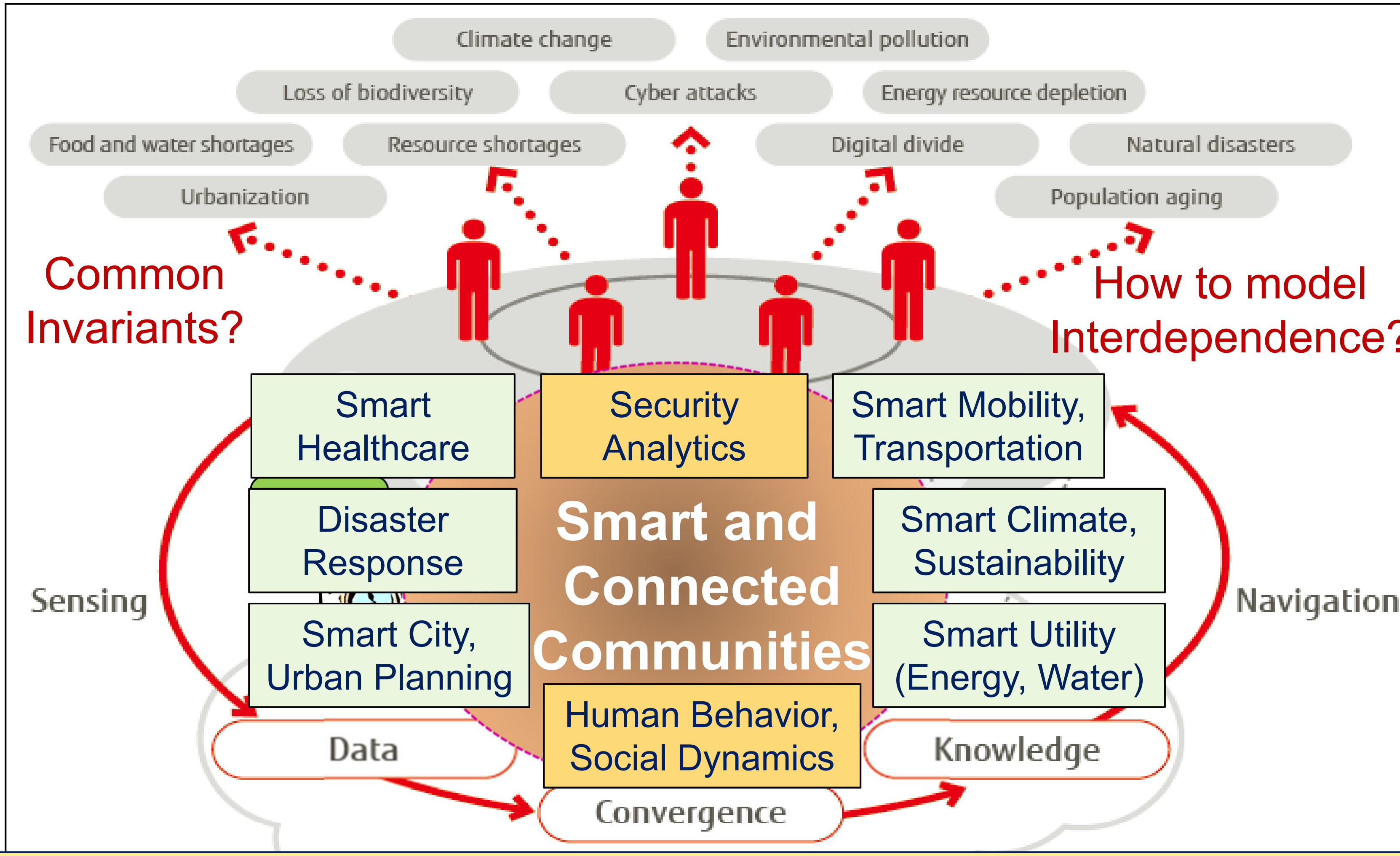
- *Perceives* the state of an environment via *sensors* and *acts* on it via *actuators.*
- *Reasons* about and adapts to inhabitants, predicts context and makes *intelligent decisions.*





- D. J. Cook and S. K. Das, "How Smart Are Our Environments? An Updated Look at State of the Art," *PMC*, 3(2): 2007.
- S. Roy, N. Ghosh, S. K. Das, "A Bio-inspired Data Collection Framework for QoI-aware Smart City Applications," *IEEE PerCom*, Mar 2019.
- V. K. Shah, S. Bhattacharjee, S. Silvestri, and S. K. Das, "An Effective Dynamic Spectrum Access based Network Architecture for Smart Cities," *IEEE Annual International Smart Cities Conference*, Sept 2018.
- V. Shah, B. Luciano, S. Silvestri, S. Bhattacharjee, and S. K. Das, "A Diverse Band-aware DSA Network Architecture for Delay-Tolerant Smart City Applications," *IEEE Transactions on Network and Service Management*, 17(2): 1125-1139, June 2020.

Smart Living: The Next Frontier



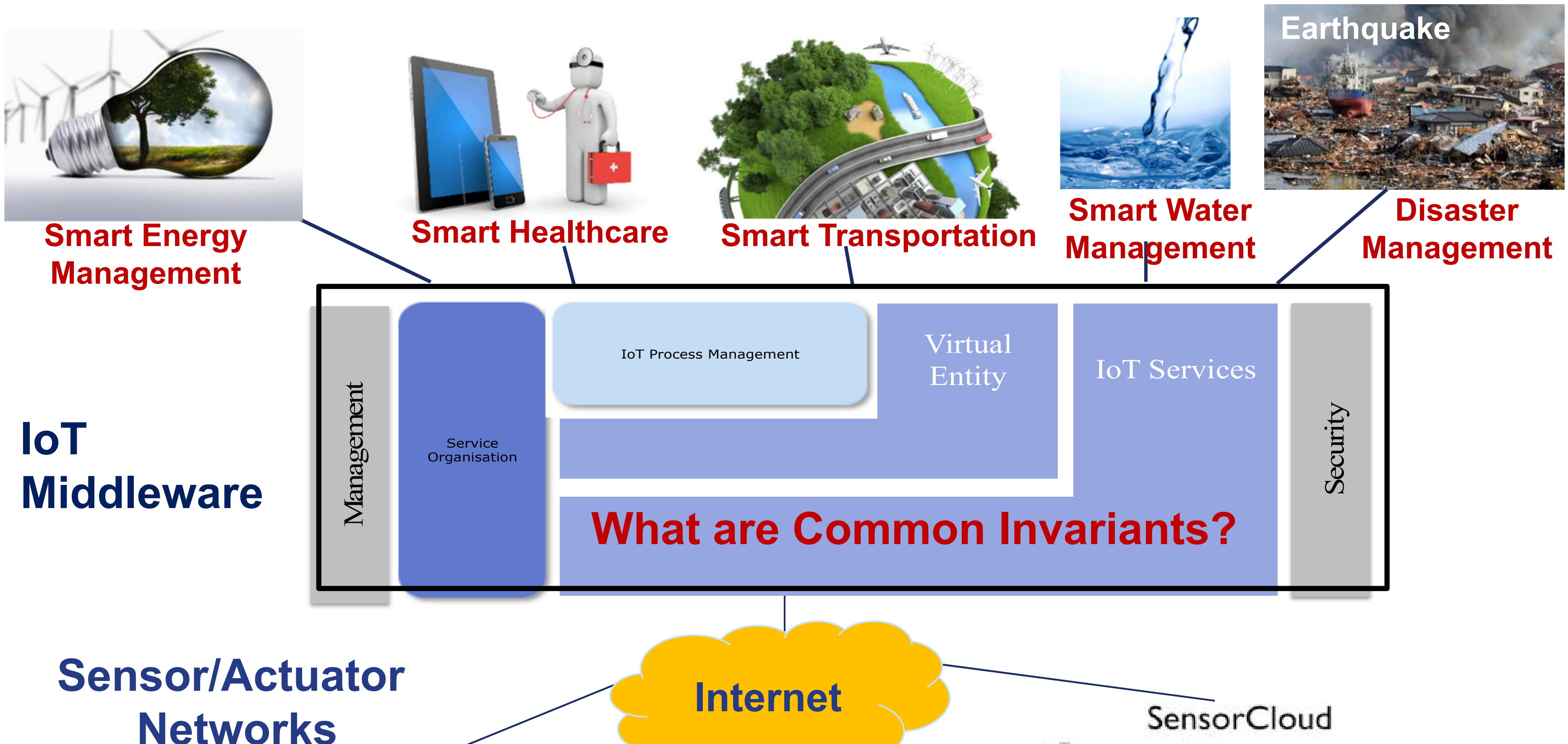
Characteristics: Complex Systems, Heterogeneous, Large-scale, CPH, Big Data, IoT

Challenges: Interdependence, Robustness, Reliability, Resiliency, Security, Privacy

Conti, Passarella, and Das, "The Internet of People (IoP): A New Wave in Pervasive Computing," *PMC*, 41, 2017.

Shah, Bhattacharjee, Silvestri, Das, "Designing Sustainable Smart Connected Communities," ACM BuildSys, 2017

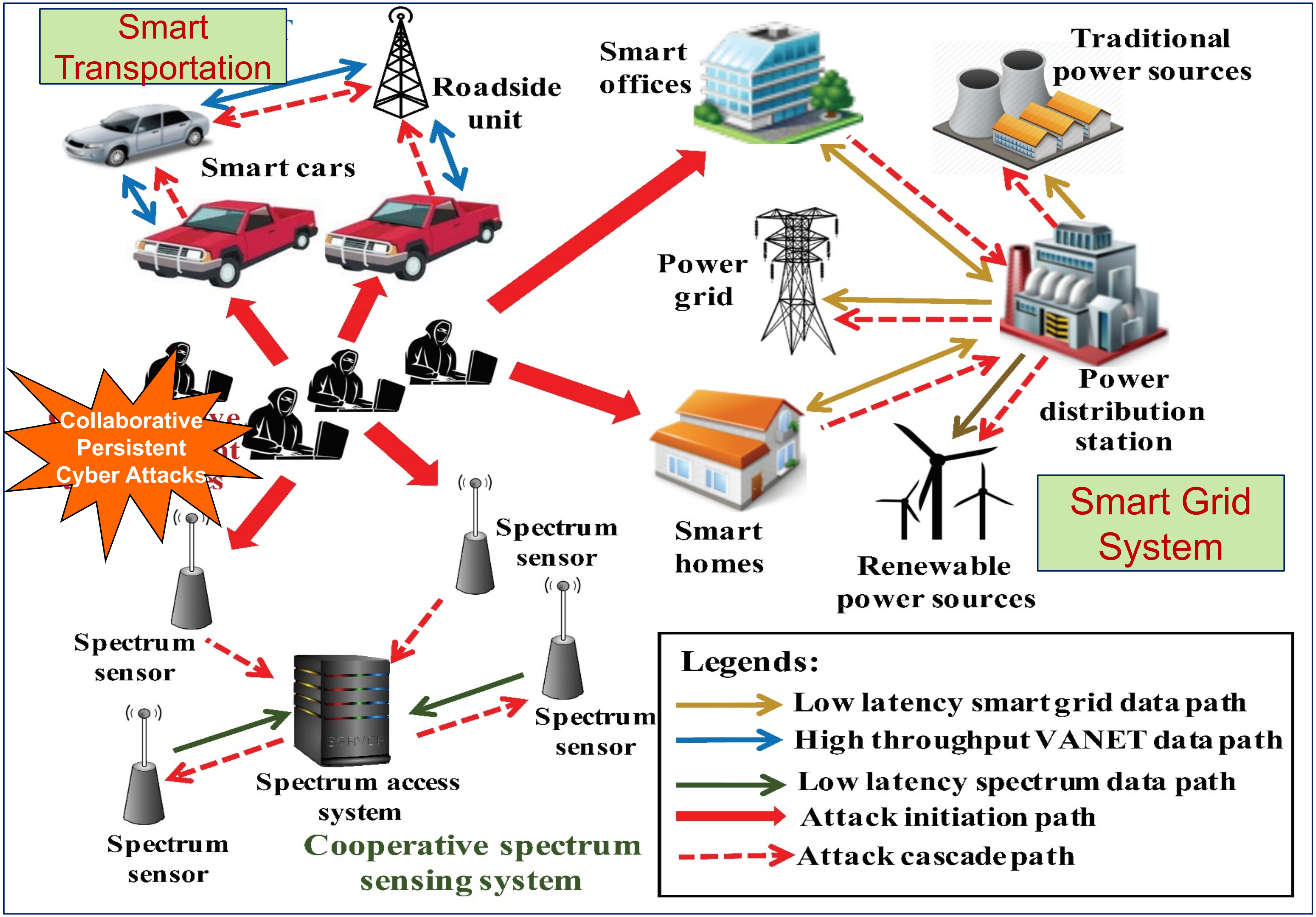
IoT Enables Societal-Scale CPH



Security Related Grand Challenges:

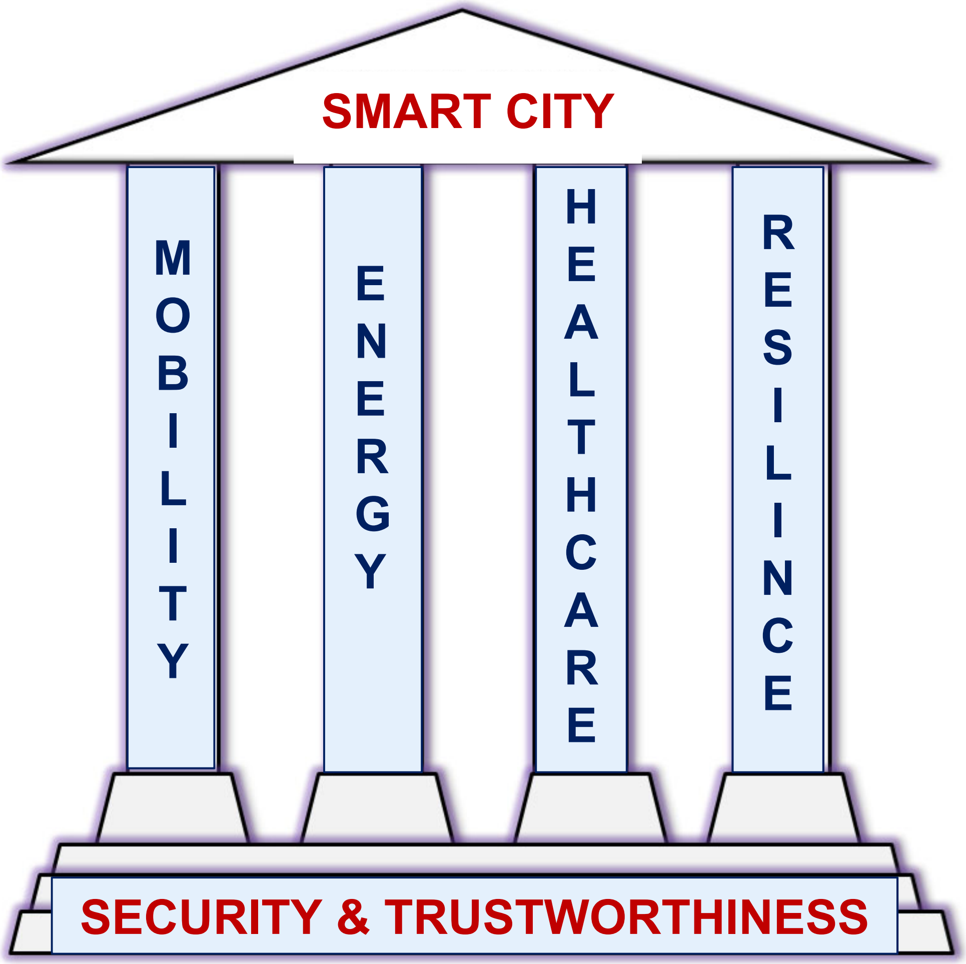
- Security and Safety of People, Infrastructures, information, Assets
- Extreme Events Management (before, during, after disasters)
- Healthcare (health risks, wellbeing)
- Sustainability (air pollution & hazard monitoring, detection and mitigation)

Vulnerability in Smart City Scenario



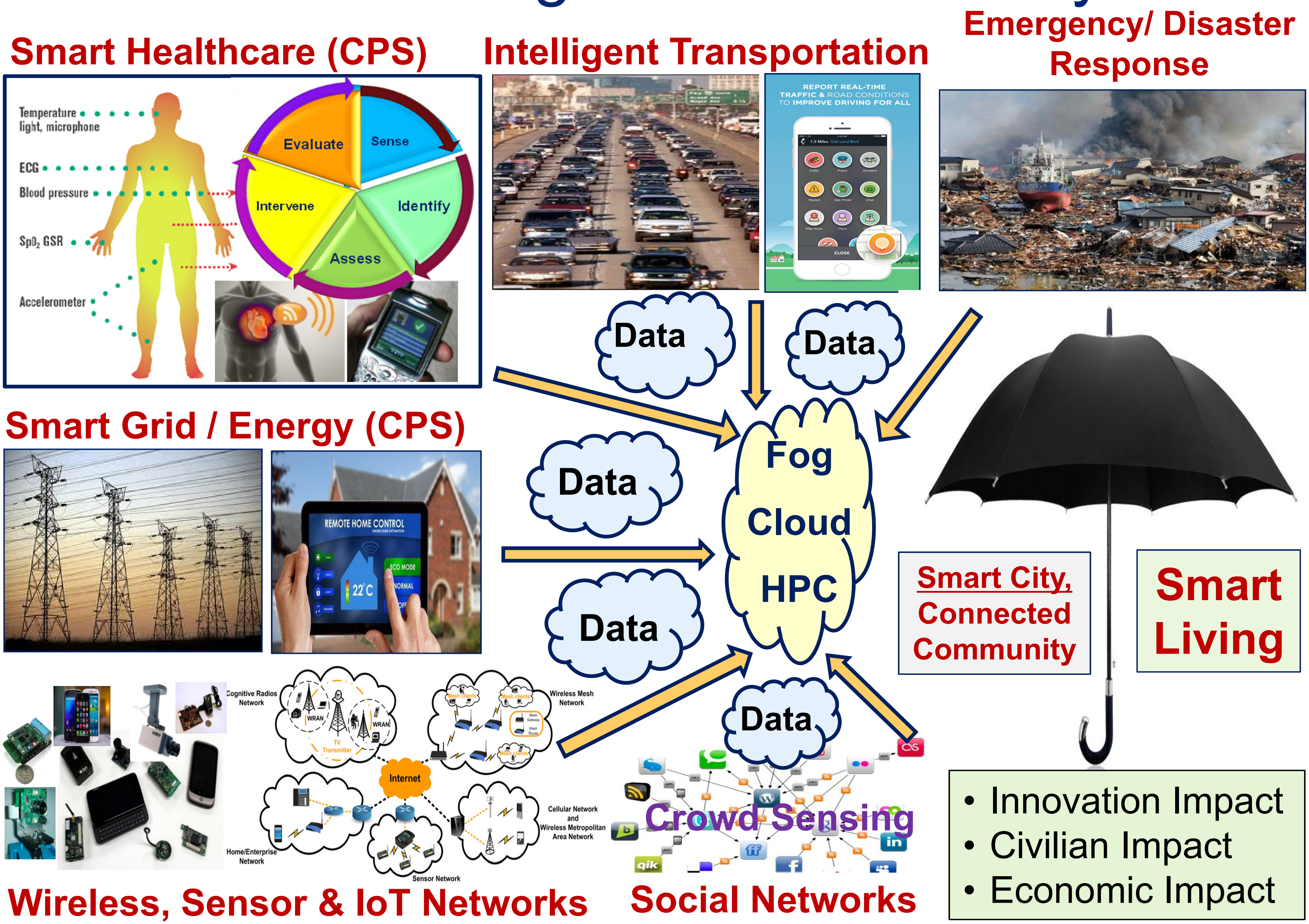
Smart City Security: Data-driven Approach

Convergent Research: ***Unified Frameworks*** **and** ***Invariants*** for secure and trustworthy decisions in interdependent CPSs (Smart City, Smart Mobility, Smart Grid / Energy, Smart Healthcare, Sustainability, Resilience).



S. Tan, D. De, W. Song and S. K. Das, "Security Advances in Smart Grid: A Data Driven Approach," *IEEE Communications Surveys and Tutorials*, 18(1): 397-422, 2017.

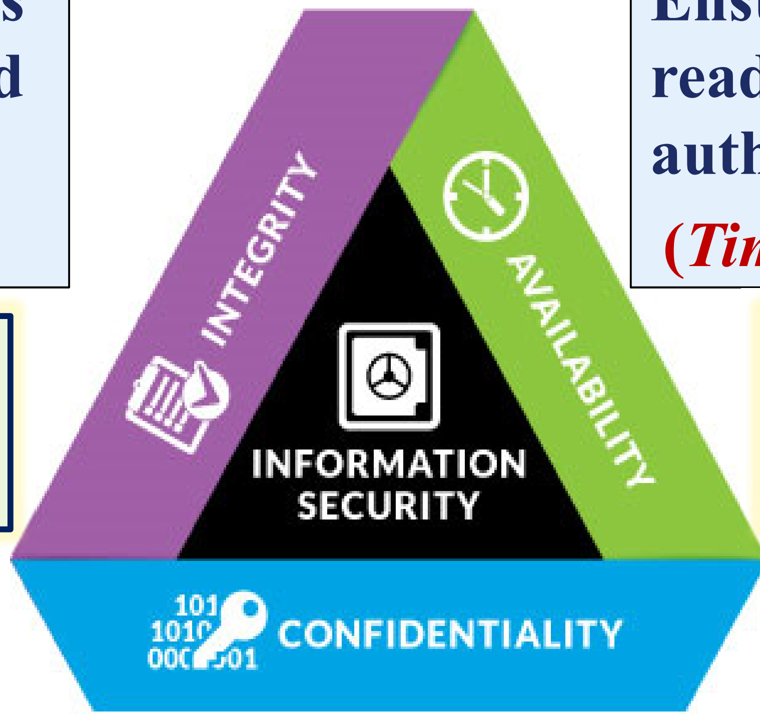
Smart Living CPS/IoT Security



Security: The CIA Triad

Integrity
Ensure information is not modified, falsified nor manipulated.
(Accuracy of Data)

False Data Injection, Data Falsification, Byzantine and Spoofing Attacks



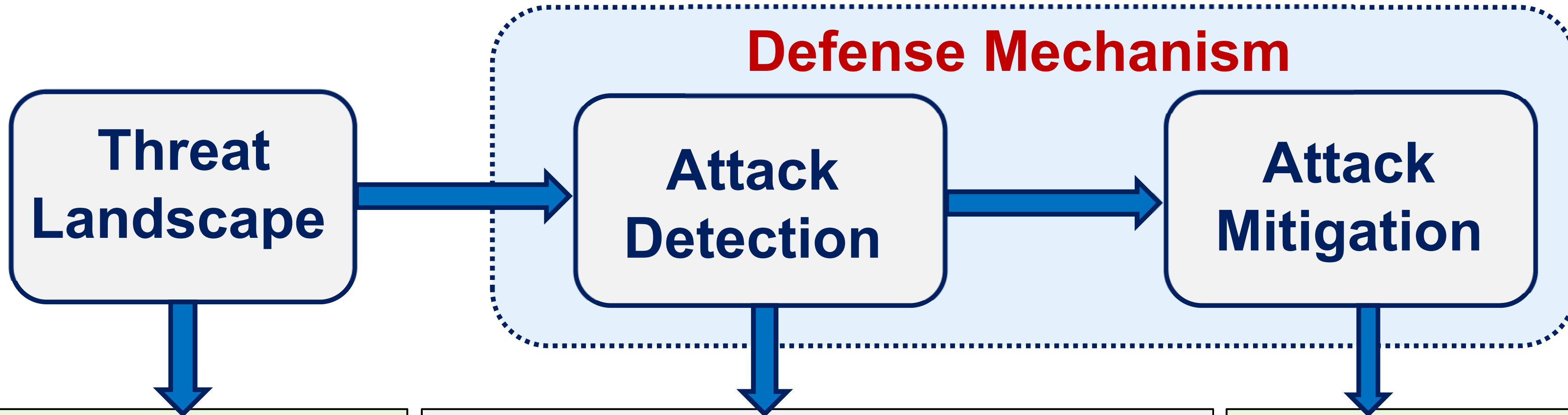
Availability
Ensure information is readily available to authorized entities.
(Timely Access & Use)

Denial of Service (DoS), Data Omission Jamming Attacks

Confidentiality
Ensure information is not disclosed to unauthorized entities.
(Restricted Visibility)

Phishing, Keylogging, Wiretapping, Sniffing

Security and Trustworthiness



- Attack Types
- Attacker Strategies
- Adversarial Objectives and Capabilities
- Extent of Prior Knowledge
- Attacker Utilities

Anomaly / Intrusion Detection

- Presence of Attack
- Gather Evidence (Labels / Scores)
- Consensus Correction

Trust based Models

- Translate Labels into Trust Scores
- Classification, Kernel Tricks

- Isolation
- Robust Fusion
- Dependable Decision
- Reduction of Undetectable Strategy space

Smart Grid: Data (Smart Meter) → False Data Injection → Mitigate via Isolation

Crowd Sensing: Data (Human Reports) → Malicious Intent → Mitigate via Dependable Decision

NSF CPS Breakthrough Project (2015-2020)

Securing Smart Grid by Understanding Communications Infrastructure Dependencies

Securing IoTs in Smart Grid

Goal: ***Create a technology-enabled, multi-level security framework to monitor, detect, prevent (recover from) natural and man-made disasters.***

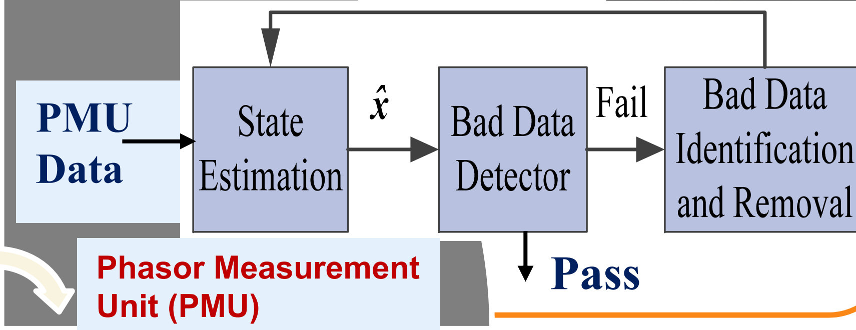
Methodology: Sensor Fusion; Situation-awareness; Information Theory; Game Theory; Epidemic Theory; Trust and Belief Models; Machine Learning; Data Mining.

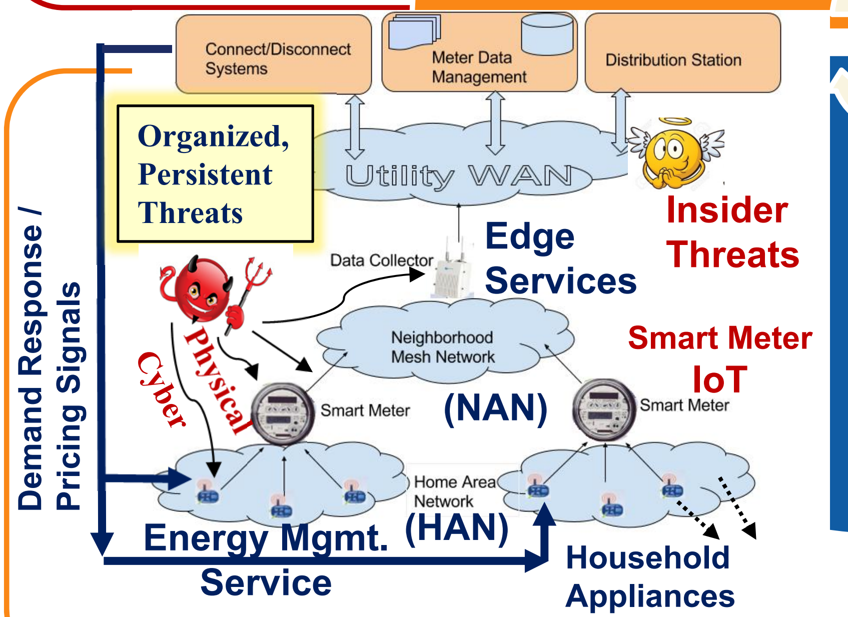
Publications: TDSC'17, TMC'11, ToSN'18, TDSC'12, TVT'17, AdHoc'15, AdHoc'13, TMC'09, Infocom'19, ComsNets'19, SmartCity'18, BuildSys'17,

Resi-lience

Integrity of AMI Data

- Billing, Safety
- Demand Response (DR)
- Load Forecast, Planned Generation/Distribution





Advanced Metering Infrastructure (AMI)

Smart Energy

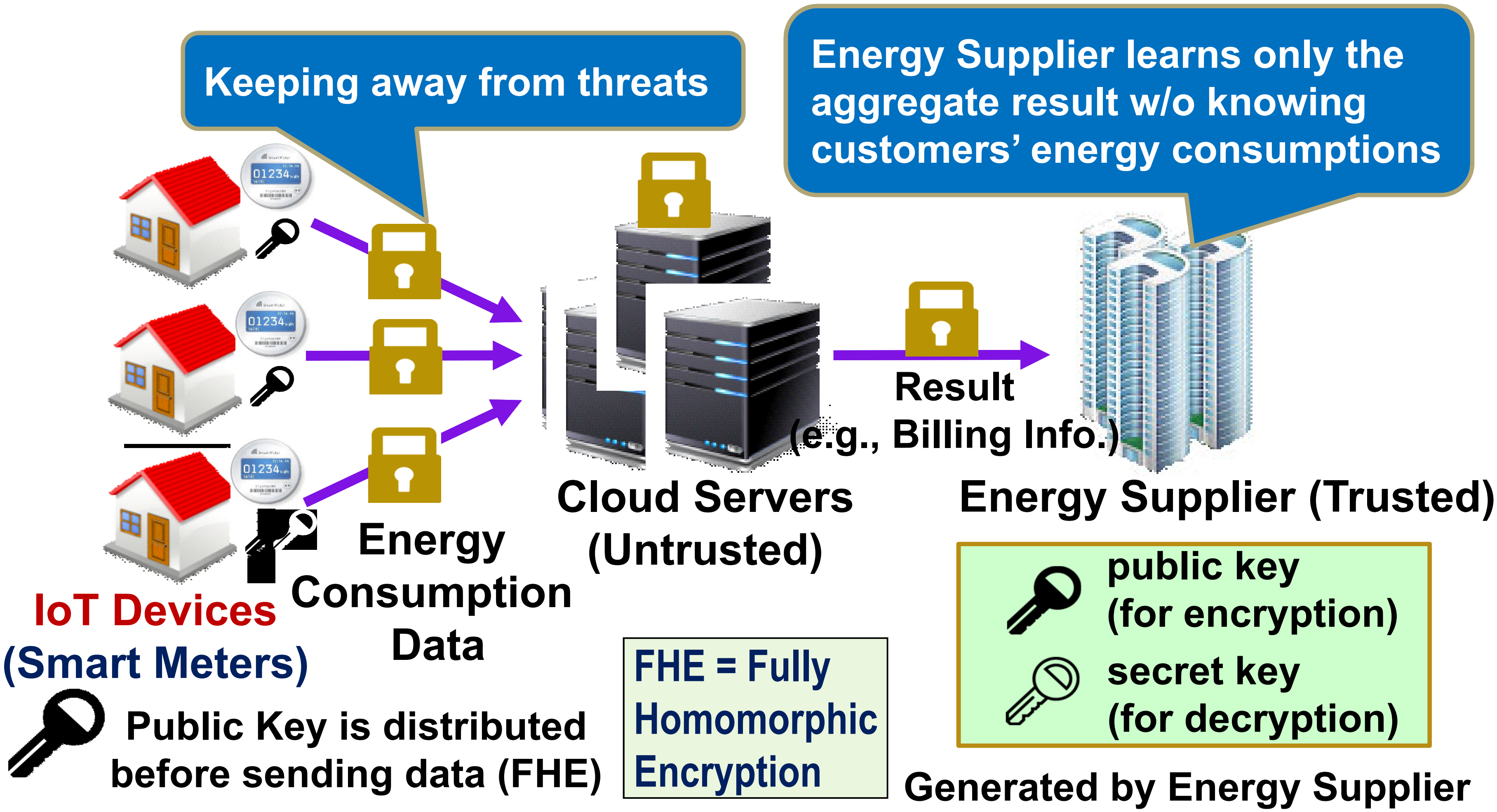
Publications: TMC'20, TDSC'20, TNSE'20, TOPS, TSG'15, CST17, SUR14, CCS'18, CODASPY'17, CNS'17, SmartGrid'12

Methodology: Time Series Data Analytics; State Estimation; ML; Anomaly Detection; Trust and Reputation Model; Utility & Prospect Theory; Incentives.

Goal: ***Detect anomalies in energy consumption (false data injection attacks); mitigate cascade failure; secure and trustworthy decisions***

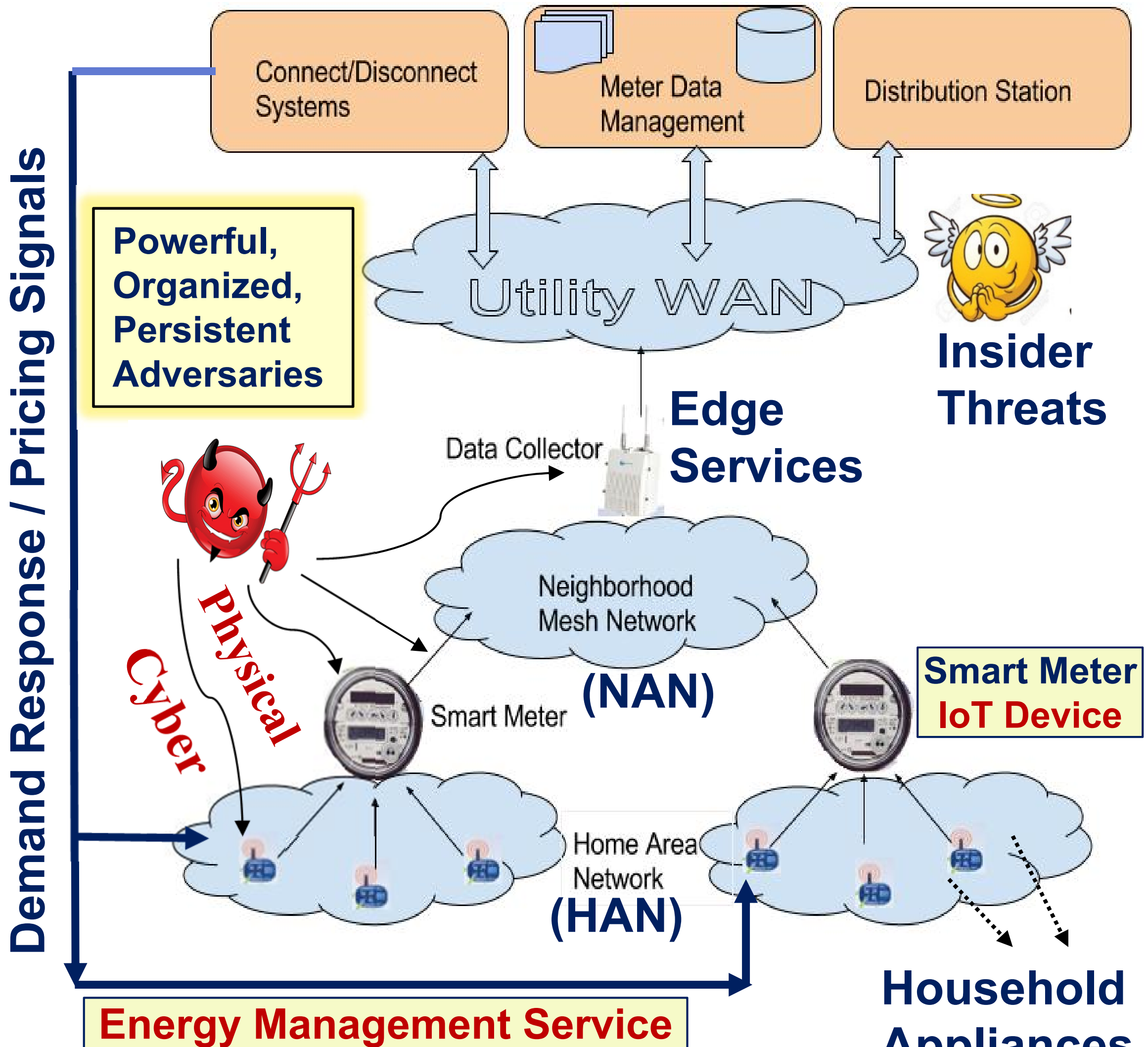
Securing a Smart Grid

(Secure Computation between IoT Devices and Energy Utility)



S. Tan, D. De, W. Song and S. K. Das, "Survey of Security Advances in Smart Grid: A Data Driven Approach," *IEEE Communications Surveys and Tutorials*, 18(1): 397-422, 2017.

Advanced Metering Infrastructure (AMI)



Use of AMI Data

- Automated Billing
- Automated Demand Response (DR)
- Load Forecast and Planned Generation/ Distribution

Securing a Smart Grid

- **Integrity of AMI data**
- Protection against **false data injection**
- AMI attack detection and mitigation
- Attack and trust models
- Billing system vulnerability

S. Bhattacharjee, A. Thakur, S. Silvestri, and S. K. Das, "Statistical Security Incident Forensics against Data Falsification in Smart Grid Advanced Metering Infrastructure," *ACM Conference on Data and Applications Security and Privacy* (CODASPY), Scottsdale, Arizona, pp. 35-45, Mar 2017. [*IEEE Trans. Dependable and Secure Computing*, to appear, 2020]

Data Falsification Attacks in AMI

Actual recorded power consumption for smart meter i at time t : $P^i{}_t(act)$

Time series of power consumption data of N smart meters $p_t = [p_t^1, \cdots, p_t^N]$

Data Falsification Attack Types:

- **Additive** → $P^i{}_t = P^i{}_t\,(act) + \delta_t$
- **Deductive** → $P^i{}_t = P^i{}_t\,(act) - \delta_t$
- **Camouflage**: Balanced additive and deductive attacks from different meters.
- **Conflict**: Uncoordinated additive and deductive attacks.

Strength of the Attack:

$\delta_t \in \{\delta_{min}, \delta_{max}\}$ is a false random bias value chosen according to some strategic distribution.

δ_{avg} (***Margin of False Data***) is the average value of δ_t

Margin of False Data (δ_{avg})

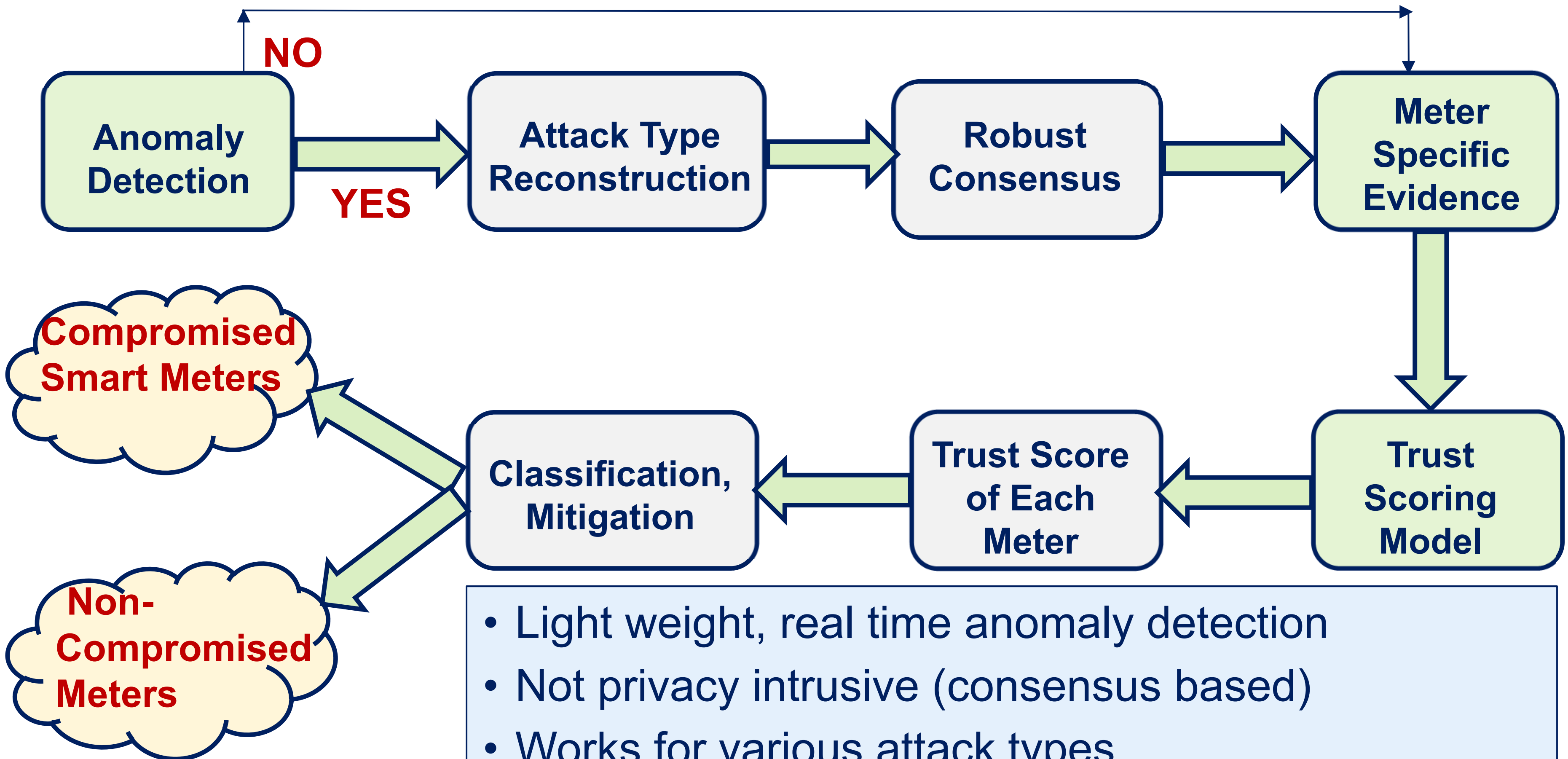
- Short-term Greedy → 900W +
- Medium-term → 400 - 900W
- Long-term Stealthy → 50 - 400W

Fraction of Compromised Nodes

$$(\rho_{mal} = M/N)$$

- M = Number of Compromised Meters injecting false data
- Isolated Adversary → 1% - 5%
- Organized Adversary → 5%-50%
- Advanced Adversary → 50% +

Novel Security Forensic Framework

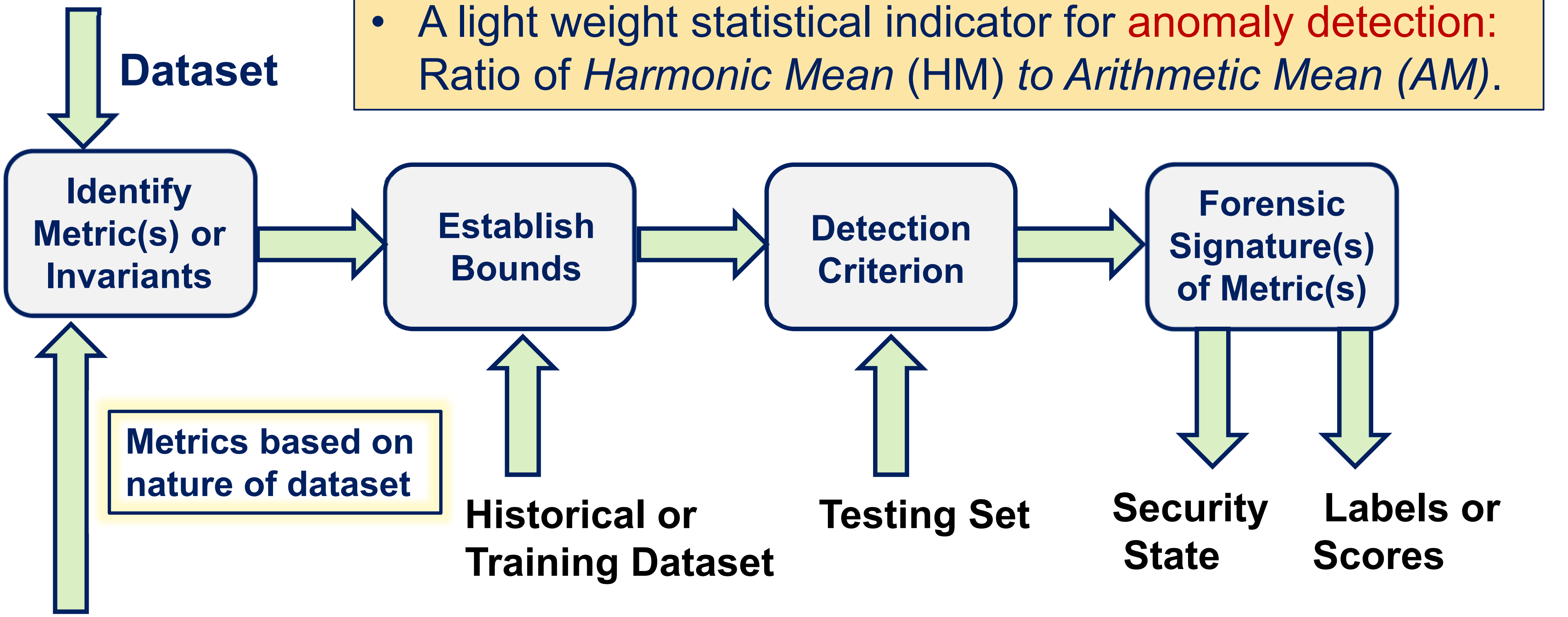


- Light weight, real time anomaly detection
- Not privacy intrusive (consensus based)
- Works for various attack types
- Distinguishes legitimate vs. malicious changes
- Suitable for both isolated and organized attacks

- S. Bhattacharjee and S. K. Das, “Detection and Forensics against Stealthy Data Falsification in Smart Metering Infrastructure,” *IEEE Transactions on Dependable and Secure Computing*, to appear, 2020.
- S. Bhattacharjee, A. Thakur, and S. K. Das, “Towards Fast and Semi-supervised Identification of Smart Meters Launching Data Falsification Attacks,” *13th ACM Asia Conference on Computer and Communications Security* (ASIACCS), pp. 173-185, 2018.

Anomaly Detection: A Data Driven Approach

- Transform the observed data into a Gaussian mixture.
- A light weight statistical indicator for anomaly detection: Ratio of *Harmonic Mean* (HM) *to Arithmetic Mean (AM)*.

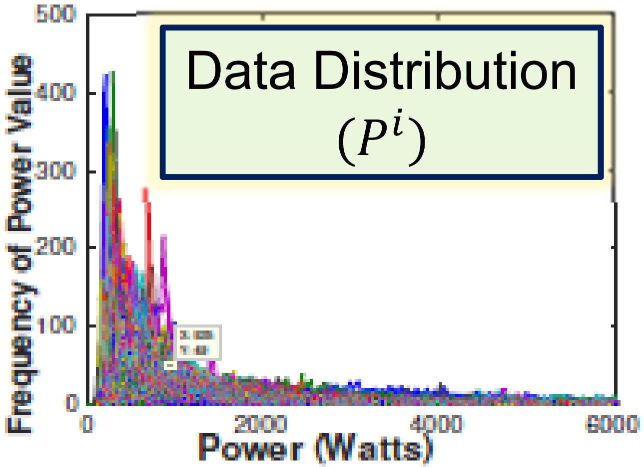


Point Anomaly: Individual data instances of detection metric is anomalous.

Collective Anomaly: Cumulative subsequence of individually non-anomalous data instances are collectively anomalous.

Context Anomaly: Data instances violates a known attribute or law.

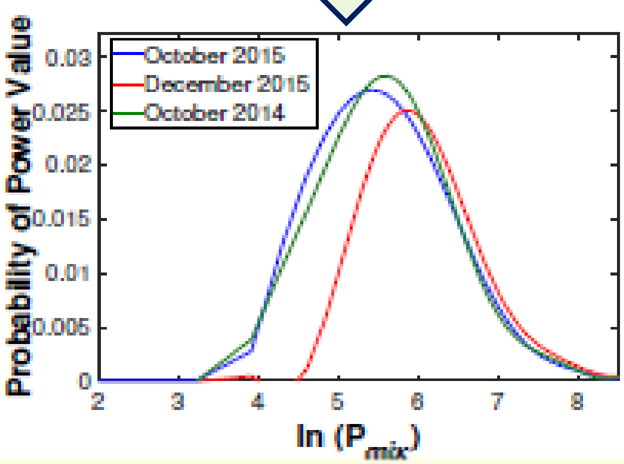
Nature of Data and Challenges

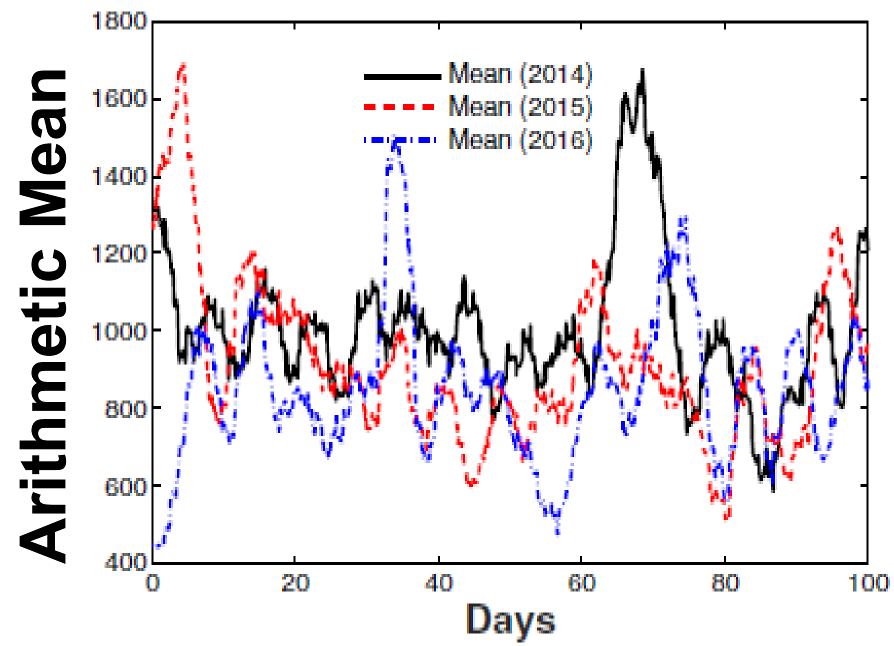


Data Distribution
(P^i)

Hourly Power Consumption Data from Austin, Texas Micro-Grid Dataset of 800 houses

Box-Cox Transformation





- Approximate Gaussian P^i
- More Data on left of the mean

Auto-Regressive Moving Average (ARMA), Cumulative Sum of *Arithmetic Mean*

- Exhibits high fluctuations
- Large Standard Deviation

Proposed Point Anomaly Detection Metric

HM / AM Ratio is a Highly Stable Invariant across Datasets

Daily HM to AM Ratio (Q)

$$Q^r(T) = \frac{\sum_{t=1}^{24} HM_t(T)}{\sum_{t=1}^{24} AM_t(T)}$$

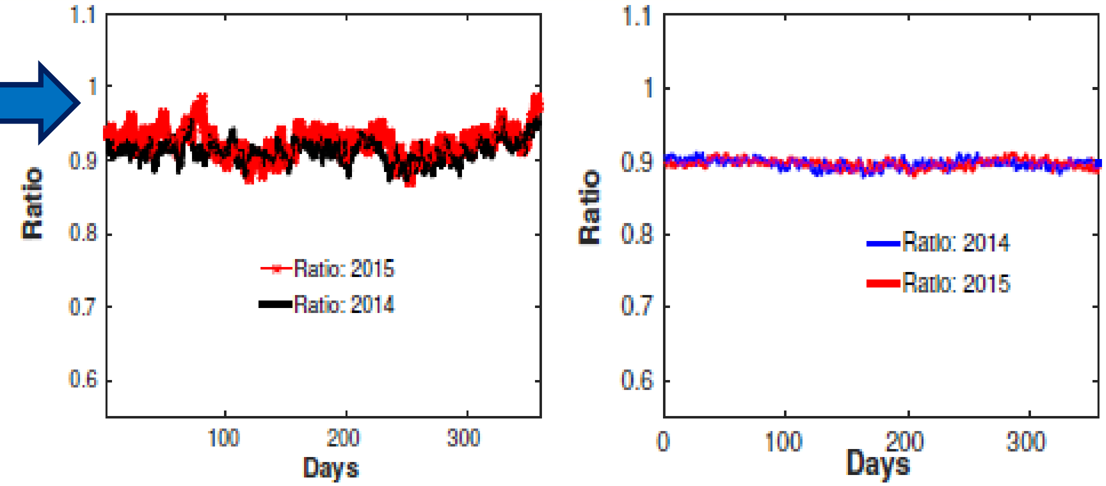
$$\forall \quad T \in \{1, \cdots, 365\}$$

Arithmetic Mean (AM)

$$AM_t = \frac{\sum_{i=1}^{N} p_t^i}{N}$$

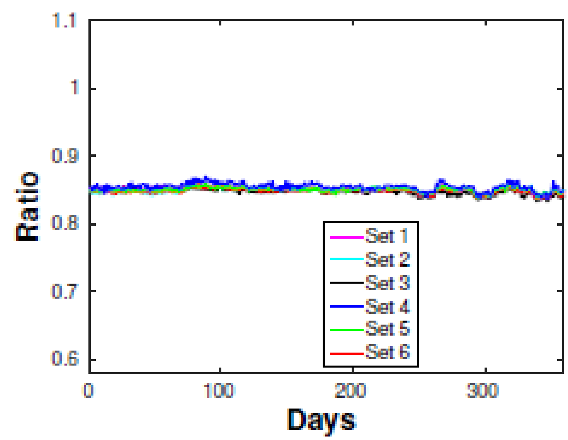
Harmonic Mean (HM)

$$HM_t = \frac{N}{\sum_{i=1}^{N} \frac{1}{p_t^i}}$$



(a) 200 meters (b) 800 meters

Texas Dataset: Years 2014 and 2015



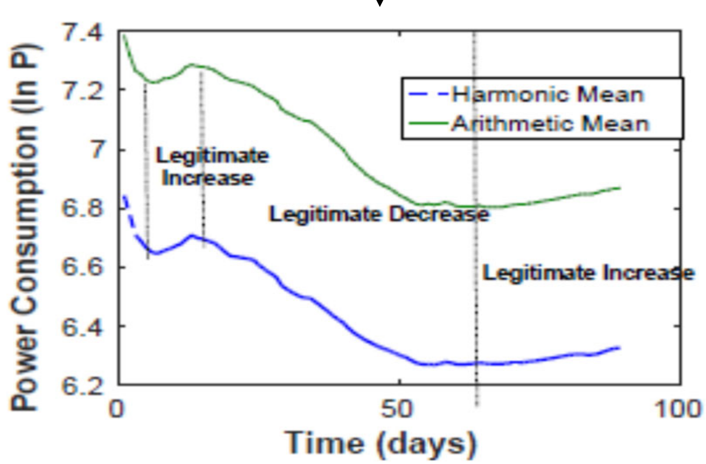
Irish Dataset: 5,000 smart meters from 6 Regions in Dublin 2010

Legitimate and Malicious Changes

- Transform the observed data into a Gaussian mixture
- A light weight statistical indicator for anomaly detection: Ratio of Harmonic Mean (HM) to Arithmetic Mean (AM) of Gaussian mixture

HM and AM of mixture data may change due to legitimate weather and other contextual factors

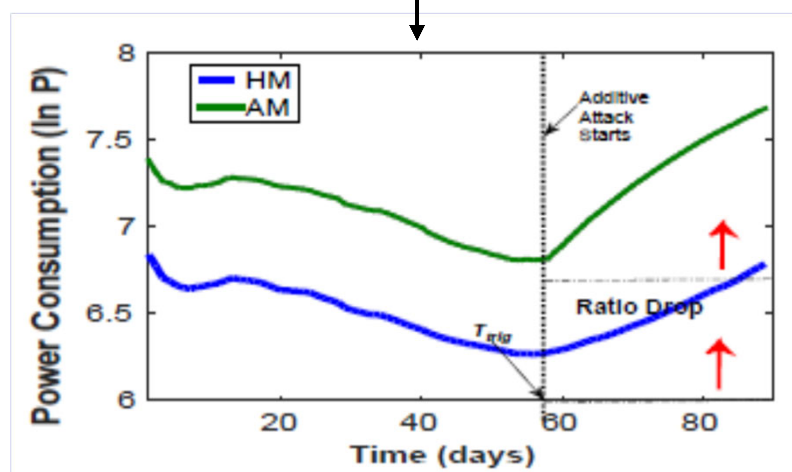
Symmetric Change in HM and AM under legitimate change



HM vs. AM: Legitimate Data

HM and AM may change due to data falsification too

Asymmetric Change in HM and AM under attacks



HM vs. AM: Under Attacks

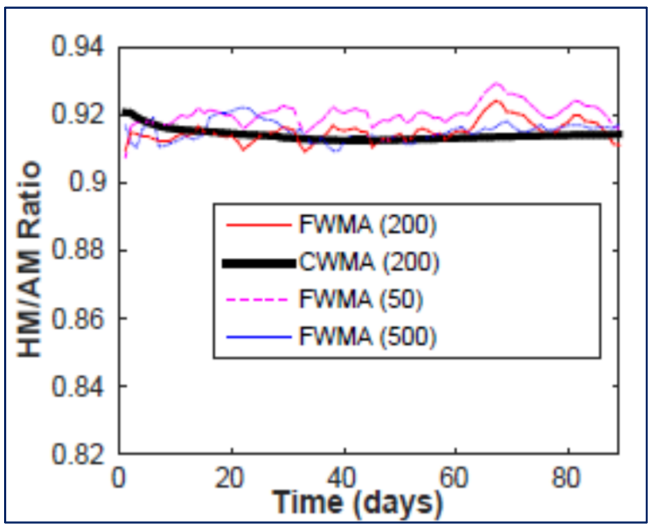
Intuition:

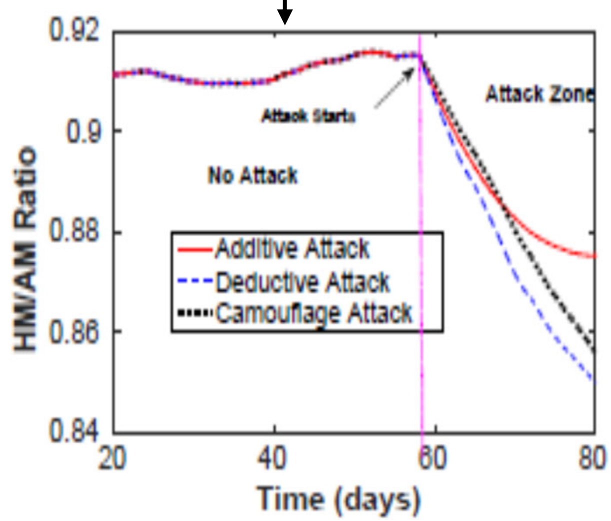
Track HM / AM Ratio

Anomaly Detection

HM/AM ratio
highly stable against
Legitimate Changes

HM/AM ratio
drops for all types
of Data Falsification





- Drop in HM / AM ratio indicates organized falsification
- Maintain ratio as forgetting and cumulative weighted moving averages
- Property holds for all attack types and higher fraction of compromised nodes

Evidence for Meter Diagnostics

Three Approaches:

1. Entropy based Trust Model with binary evidence space (Supervised) (ACM CODASPY 2017, IEEE TDSC'20)
2. Folded Gaussian Trust with multinomial evidence space (Semi-Supervised) (ACM ASIACCS 2018, ACM TOPS)
3. Information Theoretic Diversity Index based Approach(Unsupervised) (Under Review)

Folded Gaussian Trust Semi-Supervised Method

Input:

- Attack Status = Y or N
- Attack Type = if "Y"
- Robust Mean = μ_{MR}
- Robust Standard Deviation = σ_{MR}

→ Folded Gaussian Trust Model →

Output:
Compromised and Non-Compromised Meters

- Scales well for large micro grids.
- Accuracy depends on training.
- More fine-grained approach to evidential modeling improves accuracy.

KL-Distance based Trust Scoring and Classification

True (Historical) Proximity Distribution

$$X_i(t) = \begin{cases} 1 \longrightarrow & p^i(t) \in \{\mu(t) \mp \sigma(t)\} \\ 0 \longrightarrow & \text{Otherwise} \end{cases}$$

$\boxed{X_i(t) = 1 \rightarrow \text{probability } (r)}$

Observed (Current) Proximity Distribution

$$Y_i(t) = \begin{cases} 1 \longrightarrow & p^i(t) \in \{\mu_{MR}(t) \mp \sigma_{MR}(t)\} \\ 0 \longrightarrow & \text{Otherwise} \end{cases}$$

$\boxed{Y_i(t) = 1 \rightarrow \text{probability } (q)}$

Kullback-Leibler (KL) Divergence

$$D_i(X_i || Y_i) = (1-r)\, ln\left(\frac{1-r}{1-q}\right) + r\, ln\left(\frac{r}{q}\right)$$

Inverse Square Root

$$Q_i = \frac{1}{1+\sqrt{D_i(X||Y)}} \qquad 0 \le Q_i \le 1$$

Generalized Linear Model

$$W^i = log_2\left(\frac{Q^i}{1-Q^i}\right)$$

Trust Score

$$KT^i = \begin{cases} 1-e^{-|W^i|} & \text{if } W^i > 0; \\ -(1-e^{-|W^i|}) & \text{if } W^i < 0; \\ 0 & \text{if } W^i = 0 \end{cases}$$

Comparison with Existing Works

Parameter	Proposed Method	Neural Network [1]	ARMA Model [2]	Relative Entropy [3]
False Alarm	13%	29%	33%	11%
Missed Detection	9%	24%	28%	8%
δ_{avg}	400W	400W	N/A	800W
ρ_{mal}	> 40%	N/A	N/A	< 40%
Micro-grid size	5000	5000	200	200
Learning Type	Semi-Supervised	Supervised	Supervised	Supervised
Detection Time	< 10 days	1 year	1 month	1 month

[1] Neural Network, Jokar et. al, IEEE Transactions on Smart Grid, 2016.

[2] ARMA (Auto Regressive Moving Average), Mashima et. Al, RAID 2012.

[3] Entropy: Bhattacharjee, Das, et. al, ACM CODASPY 2017; IEEE TMC 2020.

Proposed Methord: Folded Gaussian Trust model

Emulation of Attacks

- Fed real smart meter data into a virtual simulated AMI micro-grid since real malicious data are not available.
- Chose a subset (*M*) of meters as compromised (ρ_{mal}) and launched data falsification with some false data margin (δ_{avg}).
- For each ρ_{mal} , experimented with varying subsets *M* and different starting points.
- Repeated for all ρ_{mal} and δ_{avg} that got manifested according to various attack distributions.

Attack Distributions:

- **Non-Data Order Aware**: δ_t is distributed uniformly random. (***No prior knowledge***)
- **Data Order Aware**: Bias vector elements are intelligently matched with $\boldsymbol{P^{i}}_{\boldsymbol{t}}(\boldsymbol{act})$. (***Partial knowledge***)
- **Incremental**: Increase $\boldsymbol{\delta_{avg}}$ slightly in each time slot
- **Omission**: Drop the data.
- **On-Off:** Attack on specific time.
- **Persistent:** Strategies that ensure evasion. (***Complete knowledge***)

Performance of Intrusion Detection

Average Time to Detect (TTD):

Difference in time between attack launched and eventual detection

Detection

Expected Time between False Alarms:

$$E(T_{fa}) = \frac{\sum_{1}^{\eta_{FA}} T_{BFA}}{\eta_{FA}}$$

Number of False Alarms: η_{FA}

Time between pair of False Alarms: T_{BFA}

Impact of Undetected Attack per Hour:

$$I = (\delta_{avg} * M * C) / 24$$

C = electricity cost/KWH

Mitigation

Break Even Time:

Mitigation

Time taken for impact revenue to equal the initial attack cost.

Why not ROC curves?

- For persistent attacks that are undetected, there is no way to quantify mitigation benefit.

Solution: Plot $E(T_{fa})$ vs. I

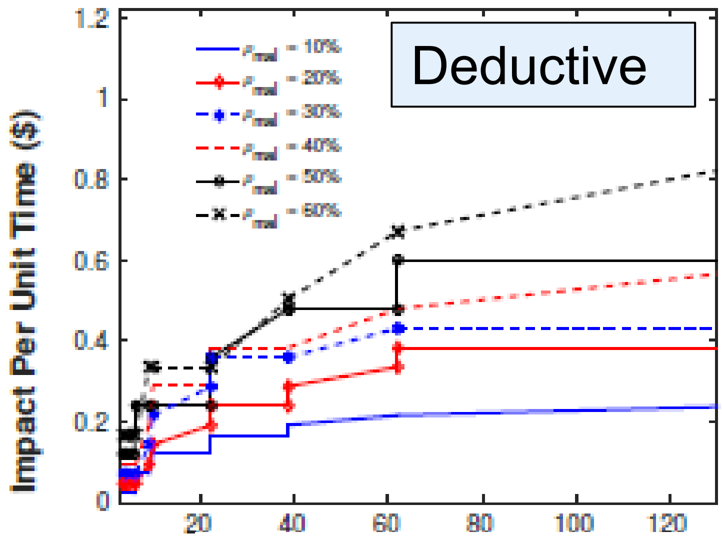
[Urbina et. al, CCS 2016]

- Free from biases such as *base rate fallacy.*

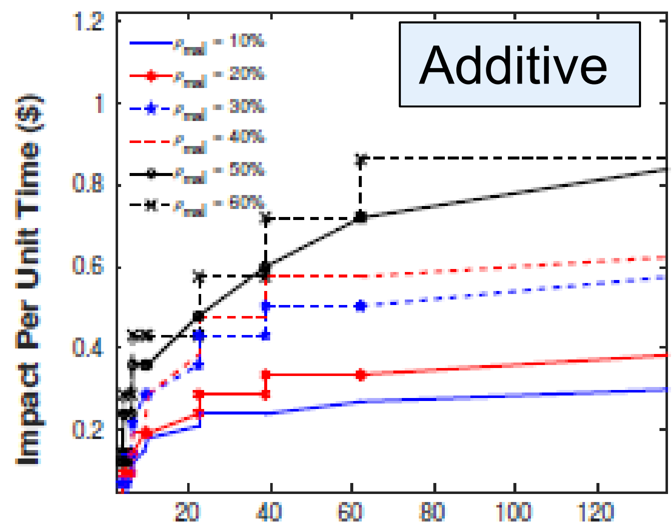
Break Even Time indicates attractiveness of low margins of attack.

[ACM CODASPY'17, IEEE TDSC'20]

Mitigation Performance against Persistent Attacks



Exp. time btw. False Alarms



Exp. time btw. False Alarms

Y axis = impact ($) of attacks that escapes detection for a given $\boldsymbol{\kappa}$

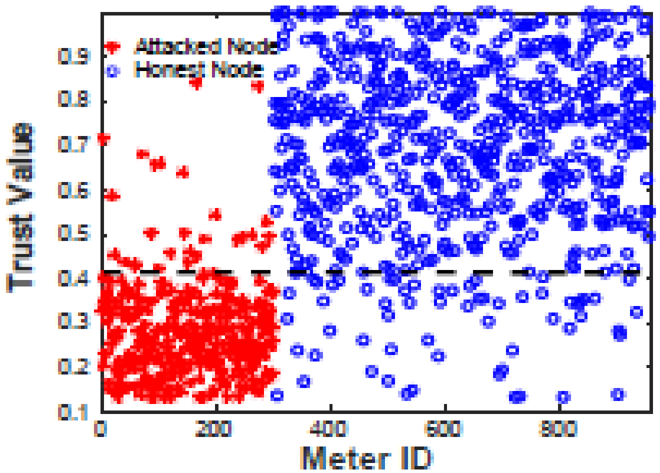
X axis = Expected time between False Alarms for same $\boldsymbol{\kappa}$ in days

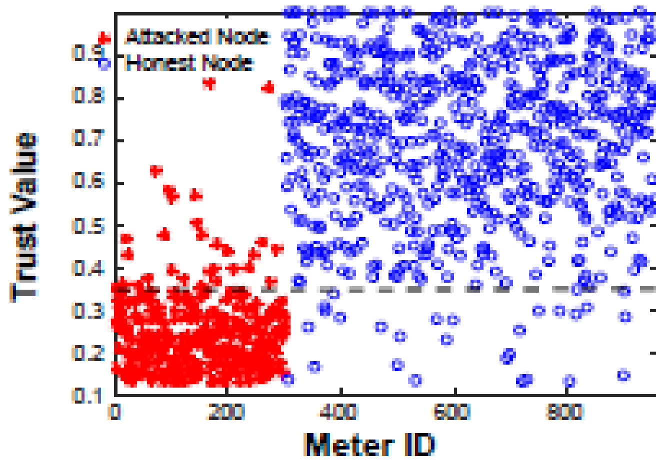
- As $\mathrm{E}(T_{fa})$ increases, the frequency of false alarms decreases.
- The increase in attack's Impact per unit time does not arbitrarily increase.
- Also true for higher $\boldsymbol{\rho_{mal}}$.

Illustrative Example:

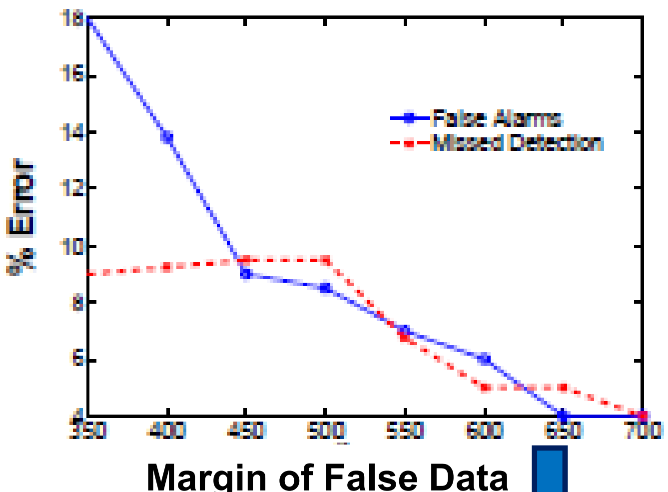
- $\boldsymbol{\kappa} = 2s_r$, $\boldsymbol{\rho_{mal}}$ = 30%, $\delta_{avg} \leq$ 80W escapes detection
- The adversary requires **5.5 yrs** to recover total cost
- Attack cost is $400/meter for **Puerto Rico Attack on Grid**

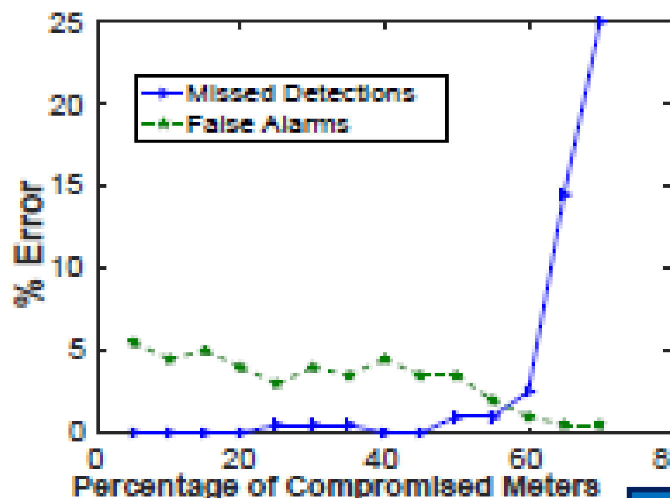
Compromised Meter Detection Results





Classification scales for 5,000 houses





Below 350W classification degrades

Resilience at high ρ_{mal}

Outline

- Sensor Networks and IoT Security
  - NSF Project: *Pervasively Secure Infrastructures (PSI)*
- Smart City and Cyber-Physical-Human Convergence
  - NSF Project: *Smart Grid Security*
- Mobile Crowdsensing
  - *Trustworthy Vehicular Crowd Sensing*
- Future Directions

NSF JUNO2 Project (2018-2021)

STEAM: Secure and Trustworthy Framework for Integrated Energy and Mobility in Smart Connected Communities

Missouri S&T (PI: Das)

Jointly with
Vanderbilt University, USA
Osaka University, Waseda University, Nara Institute of Technology, Japan

Securing CPS and IoTs

Goal: ***Create a technology-enabled, multi-level security framework to monitor, detect, prevent (recover from) natural and man-made disasters.***

Methodology: Sensor Fusion; Situation-awareness; Information Theory; Game Theory; Epidemic Theory; Trust and Belief Models; Machine Learning; Data Mining.

Publications: TDSc'17, TMC'11, ToSN'18, TDSC'12, TVT'17, AdHoc'15, AdHoc'13, TMC'09, Infocom'19, ComsNets'19, SmartCity'18, BuildSys'17,

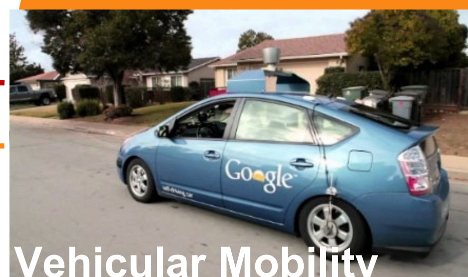
Resi-
lience

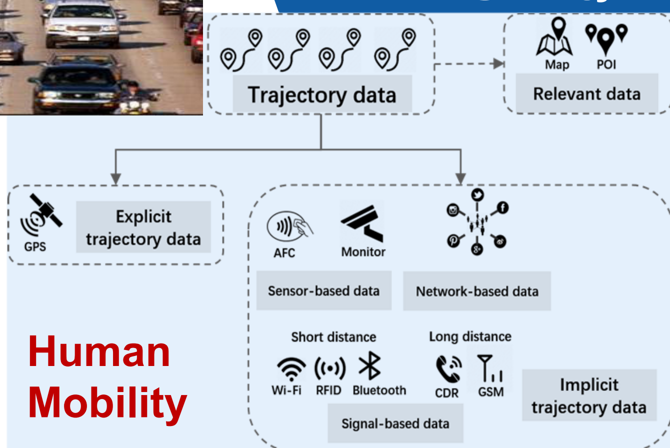
Smart
Mobility

Goal: ***Detect false event reporting in vehicular and human mobility; transport planning; air quality; congestion; disease spread.***

Methodology: Information Theory; ML; Stochastic Games; Dictionary Compression; Crowdsensing; Utility Theory; Behavior Models; Privacy-Preserving Data Mining.

Publications: TCPS'19, TII'17, ToN'08, TMC'12, PMC'18, Entropy'15, WiNet'02, PerCom'15, SDM'18, PerCom'06, InfoCom'04, MobiCom'99





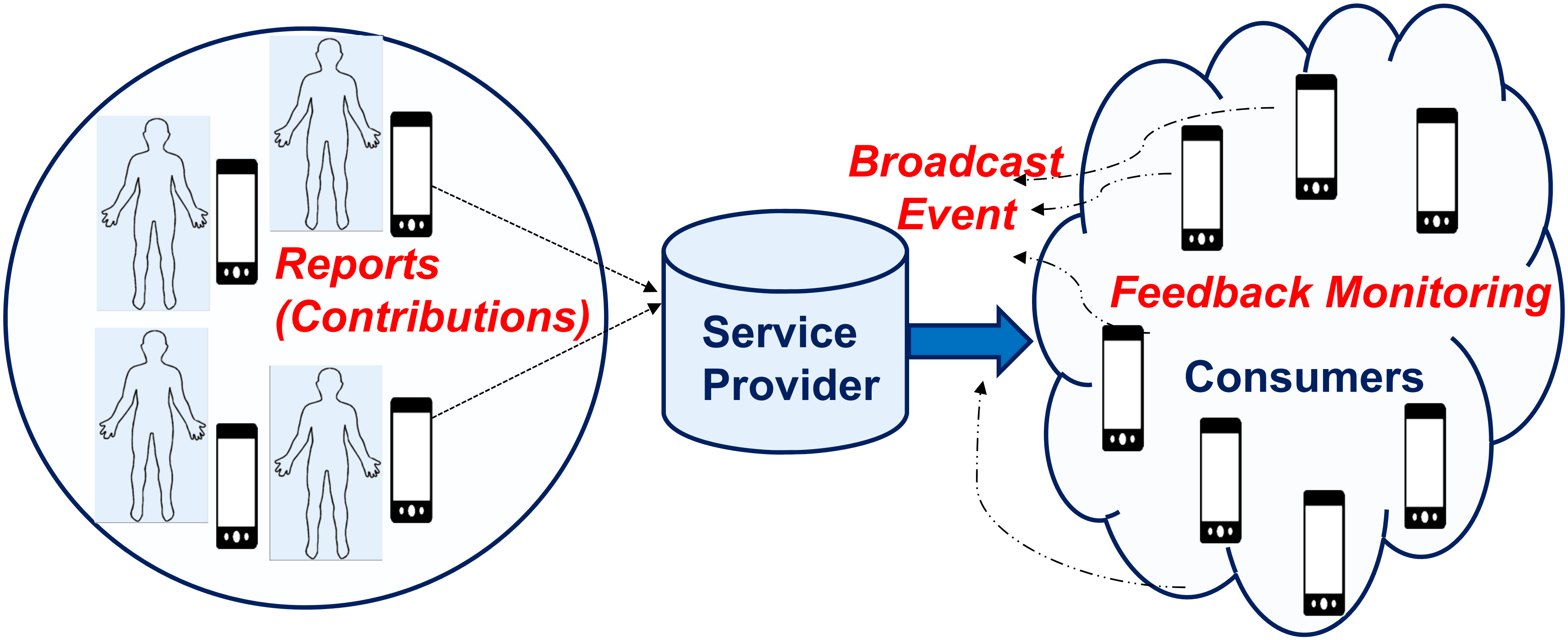
Smart
Energy

Publications: TMC'20, TDSC'20, TNSE'19, TOPS, TSG'15, CST17, SUR14, CCS'18, CODASPY'17, CNS'17, SmartGrid'12

Methodology: Time Series Analysis; State Estimation; ML; Anomaly Detection; Trust and Reputation Model; Epidemic & Prospect Theory; Incentives.

Goal: ***Detect anomalies in energy consumption (false data injection attacks); mitigate cascade failure; secure and trustworthy decisions***

Crowd Sensing (CS) Architecture

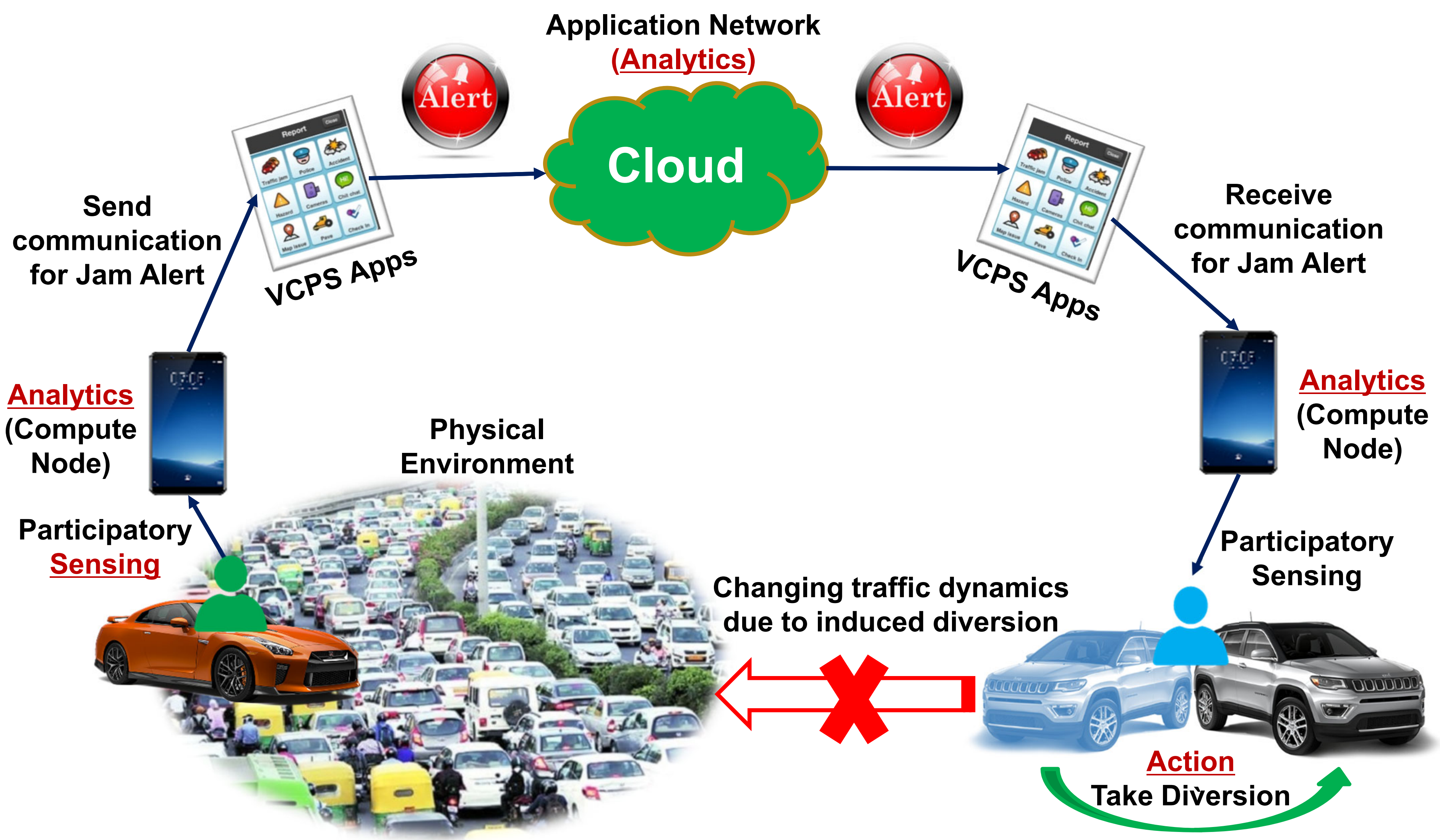


Report: Citizens contribute to data, alerts, notifications, etc.

(Published) Event: A summary statistic inferred from the reports (e.g. traffic jam, accident, road closure, weather hazard).

Feedback Monitoring: Endorsement on the published event or Ratings (*e.g., Useful, Not useful, Not sure, 5 star ratings*)

Vehicular CPS



R. P Barnwal, N. Ghosh, S. K. Ghosh, S. K. Das, "Publish or Drop Traffic Event Alerts? Quality-aware Decision Making in Participatory Sensing Vehicular CPS," *ACM Transactions Cyber-Physical Systems,* 4(1): Jan 2020.

Vehicular Crowd Sensing: Threats Landscape

Why Selfish Intent?

- Credit-based reward mechanism to motivate constant reports.
- Incentivizes degree of contribution (**quantity**) rather than **quality** of contributions.

(Huge # of *false reports* in Waze traffic Dataset, *IEEE* SMARTCOMP 2016)

Why Malicious Intent ?

- Create congestion (civilian impact)
- Drain company's revenue (economic impact)
- Strategic blockage (internal security impact)

Problems with Existing Models

- Cannot embed variations in quantity of ratings on final trust
- Not Null Invariant
- **Sacrifice Quality for Quantity or vice-versa.**

(IEEE PerCom Workshop 2017, IEEE TMC 2020)

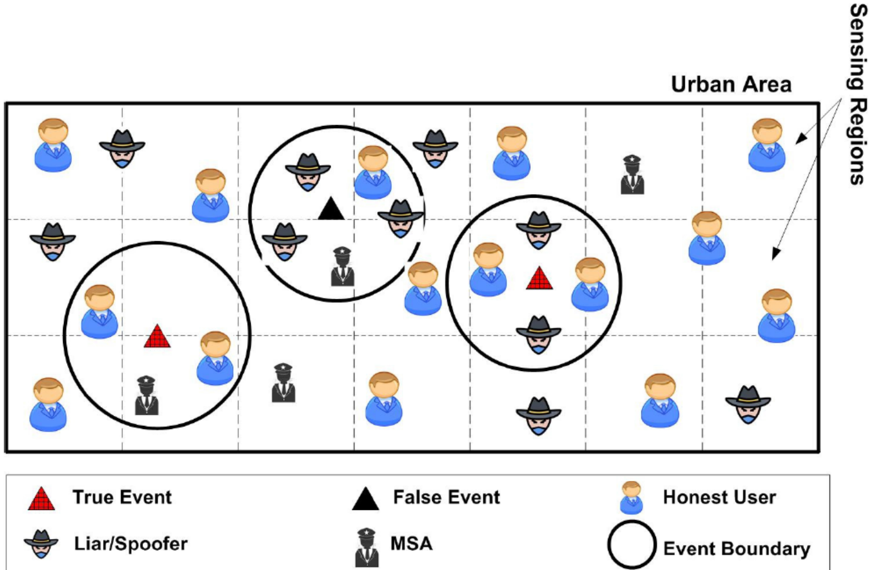
Reporting Behaviors:

- **Honest:** mostly reports true events.
- **Selfish:** intermittently generate true and false reports with certain probabilities.
- **Malicious:** collude on reporting the same false event type in a vicinity.

Rating Behaviors:

- **Ballot stuffing:** Rogue raters give positive ratings to false events.
- **Bad mouthing:** Rogue raters give false ratings to true events.
- **Obfuscation stuffing:** Rogue raters give uncertain ratings to false events.

Vehicular CPS

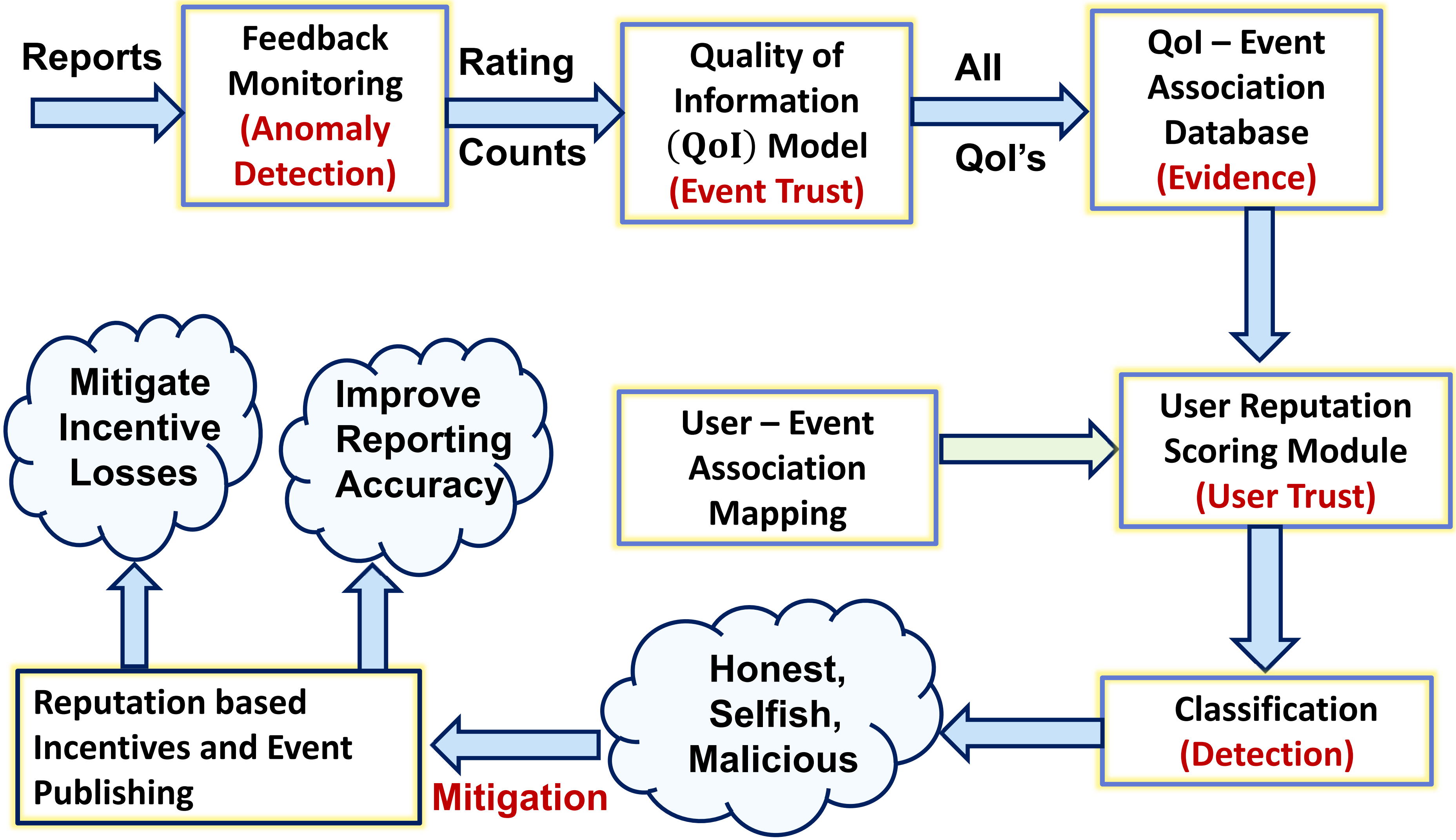


- System Model
  - Vehicles/ Apps (called nodes) are networked acting as communication units
  - VCPS nodes (cyber agent of human) sense events and share alerts with peers for informed decision making
  - Based on sensing information, vehicles take decision resulting into change of traffic dynamics

- **Vehicular sensing node / Adversary**
  - Spoofs location to report random event alerts to earn undue rewards: Side channel participation (Spoofing Attack)
  - Raises false event alerts to decrease system reliability or gain resources: False Participation (Spamming Attack)

- **Objectives**
  - Devise a framework to identify location spoofing, spamming nodes
  - Define Quality of Contribution (QoC) metric for nodes' contributions based on reputation history; classify as Honest, Liars, or Spoofers
  - Expected Utility Theory (EUT) based decision model to filter false events

Quality and Quantity (QnQ) Framework



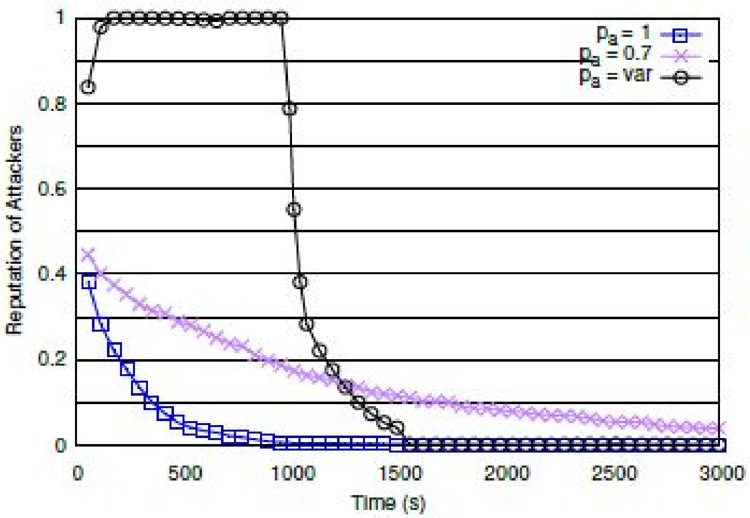
S. Bhattacharjee, N. Ghosh, V. K. Shah, S. K. Das, "QnQ: A Reputation Model to Secure Mobile Crowdsourcing Applications from Incentive Losses," *IEEE Conf. on Communications and Network Security* (CNS), 2017. [Extended version, *IEEE Transactions on Mobile Computing*, 19(1): 200-216, Jan 2020.]

Trust and Belief Model

- How to build trust to guarantee reliable operations?

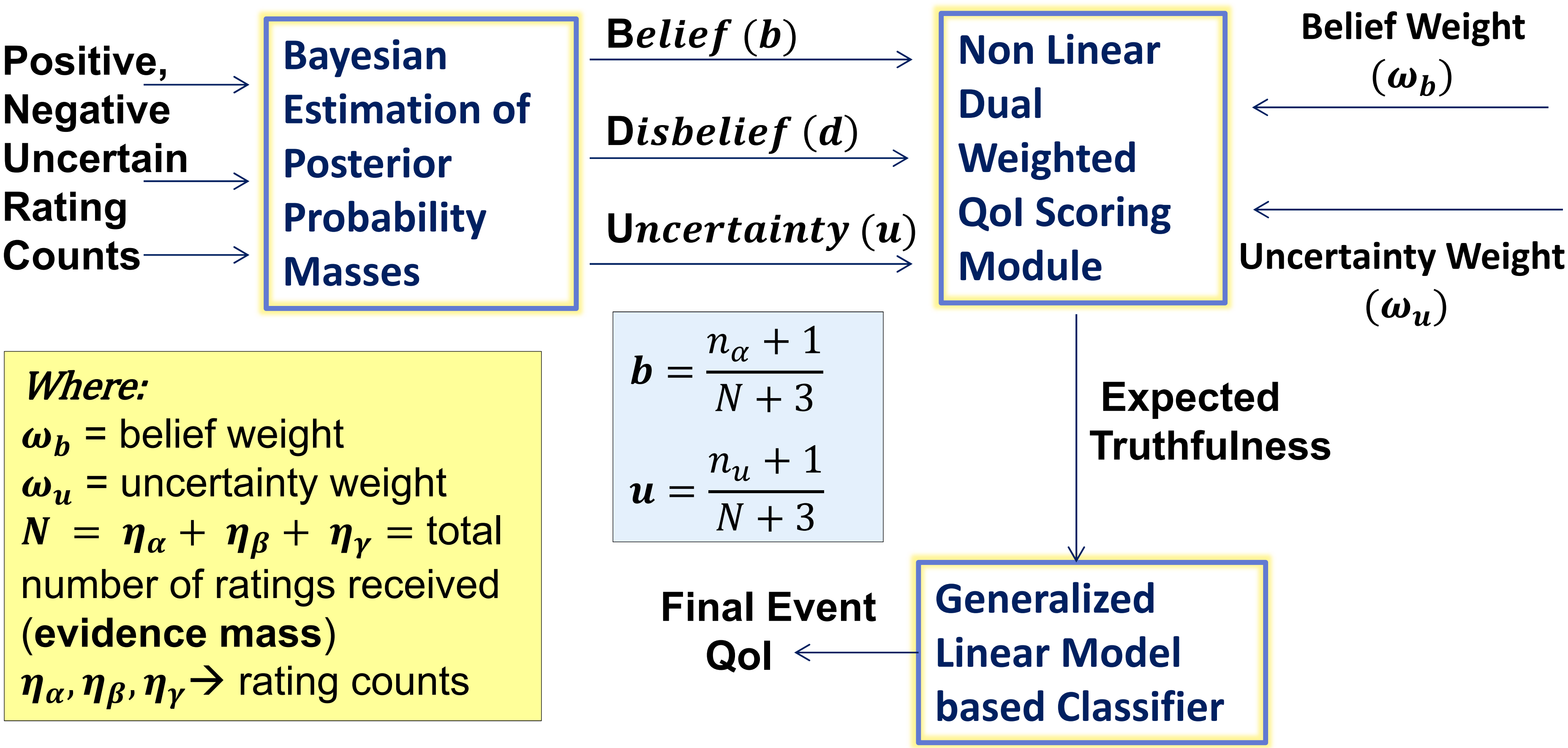
- Trust is extremely complex:
  - ✓ How to model and quantify trust?
  - ✓ How to propagate trust?
  - ✓ How to reach trust consensus?

- Build a Reputation System
  - ✓ Reliable users are rewarded and hence have high reputation
  - ✓ Reputation evolves dynamically with time – may also go down



- F. Restuccia and S. K. Das, "FIDES: A Trust-based Framework for Secure User Incentivization in Participatory Sensing," *IEEE Symposium on a World of Mobile Multimedia Networks* (WoWMoM), June 2014.
- T. Luo, S. S. Kanhere, J. Huang, S. K. Das, and F. Wu, "Sustainable Incentives for Mobile Crowdsensing: Auctions, Lotteries, Trust and Reputation Systems," *IEEE Communications Magazine* (special issue on Sustainable Incentive Mechanisms for Mobile Crowdsensing), 55(3): 68-74, Mar 2017.

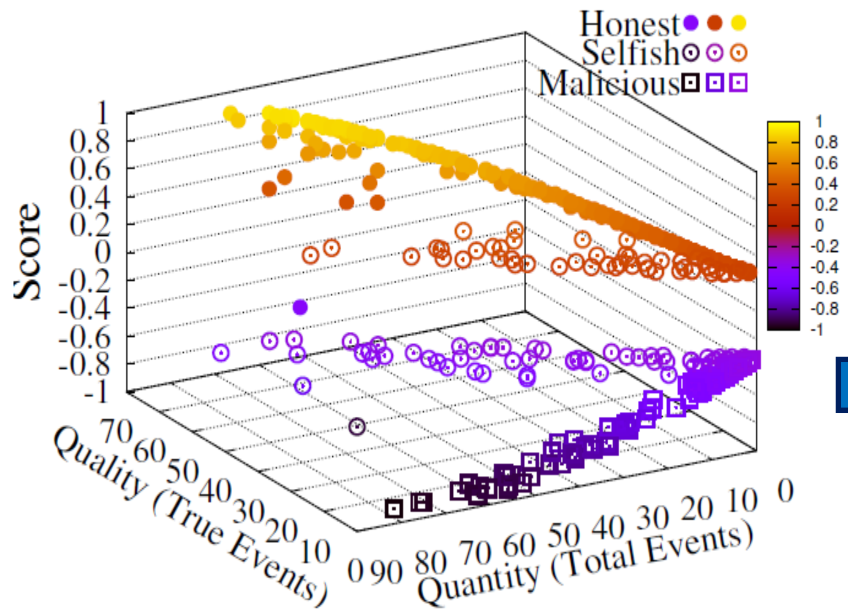
Quality of Information (QoI) Model

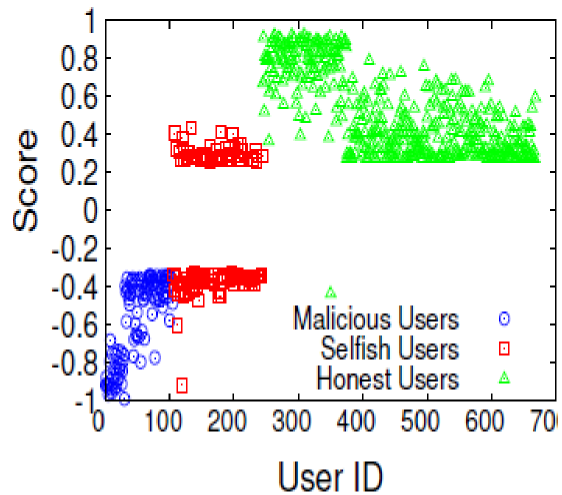


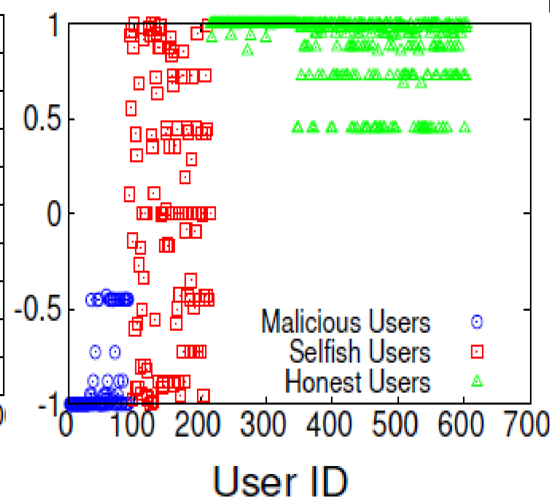
- T. T. Luo, J. Huang, S. S. Kanhere, J. Zhang, and S. K. Das, "Improving IoT Data Quality in Mobile Crowdsensing: A Cross Validation Approach," *IEEE Internet of Things Journal*, 6(3): 5651-5664, June 2019.
- F. Restuccia, N. Ghosh, S. Bhattacharjee, S. K. Das, and T. Melodia, "Quality of Information in Mobile Crowdsensing: Survey and Research Challenges" *ACM Transactions on Sensor Networks*, 13(4): 34:1-34:43, 2017.
- F. Restuccia, S. K. Das, and J. Payton, "Incentive Mechanisms for Participatory Sensing: Survey and Research Challenges" *ACM Transactions on Sensor Networks*, 12(2): Apr 2016.

Results: Attack Detection

Classification Performance







Classification: Proposed Approach (Left); D-S Reputation (Right)

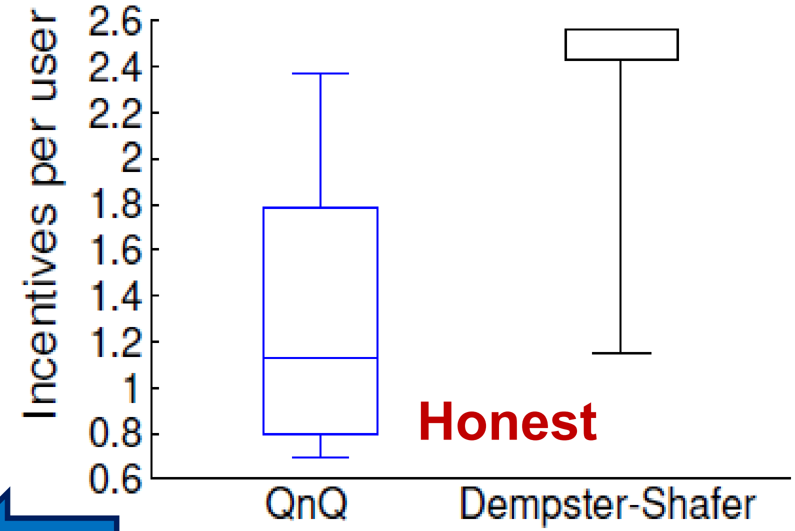
- Three user groups classified
  - Lowest group: **Malicious**
  - Middle group: **Selfish**
  - Top group: **Honest**
- Reputation unifies both quality and quantity
- Selfish and malicious groups cannot increase reputation with only higher participation

- Selfish users have two groups:
  - Higher true event contributions
  - Higher false event contributions
  - Success in Fairness as well
  - Can be used for incentives
- Better than Dempster-Shafer

Results: Attack Mitigation

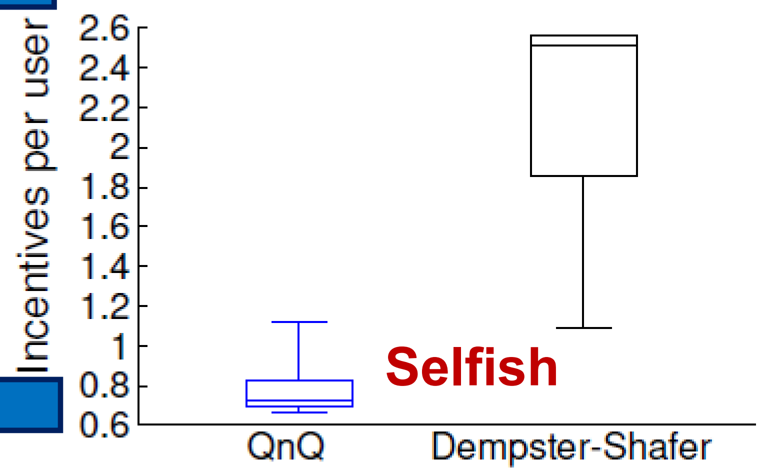
Incentive Mechanism:

- Implemented incentive mechanism [Restuccia and Das, IEEE WoWMoM'14] with QnQ framework.
- Computed rewards for honest and selfish users using QnQ and Dempster-Shafer (D-S) reputation models.



Key Observations:

- Rewards for honest users comparable
- For selfish users: mean incentive is more than 50% less than D-S
- Prevents loss of revenue due to rogue reporting.
- Improves reliability

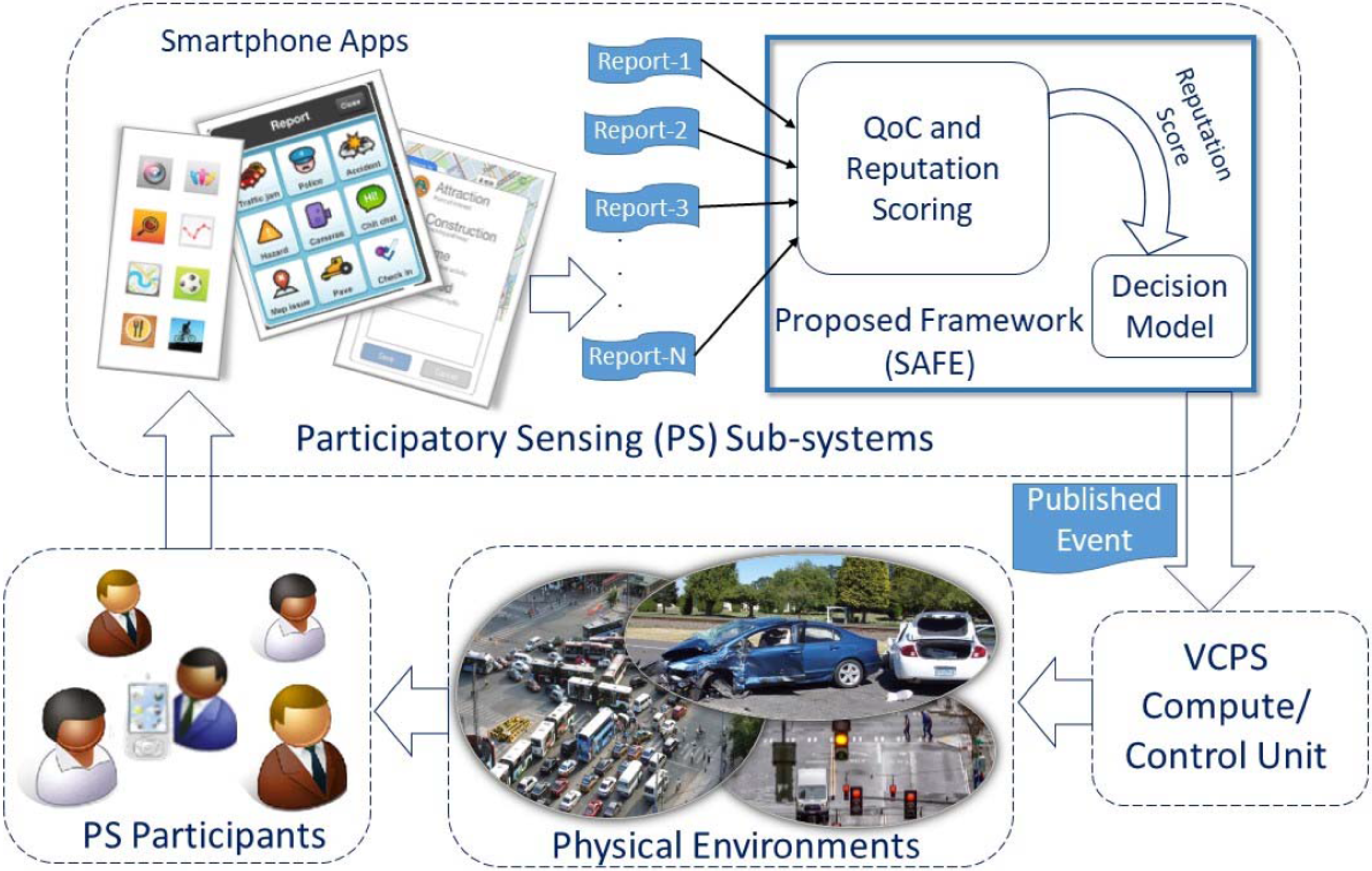


T. Luo, S. S. Kanhere, S. K. Das, and H.-P. Tan, "Incentive Mechanism Design for Heterogeneous Crowdsourcing Using All-Pay Contests," *IEEE Transactions on Mobile Computing*, 15(9): 2234-2246, 2016.

T. Luo, S. K. Das, H.-P. Tan, and L. Xia, "Incentive Mechanism Design for Crowdsourcing: An All-Pay Auction Approach," *ACM Transactions on Intelligent Systems and Technology*, 7(3): 1-26, 2016.

Vehicular CPS: The SAFE Framework

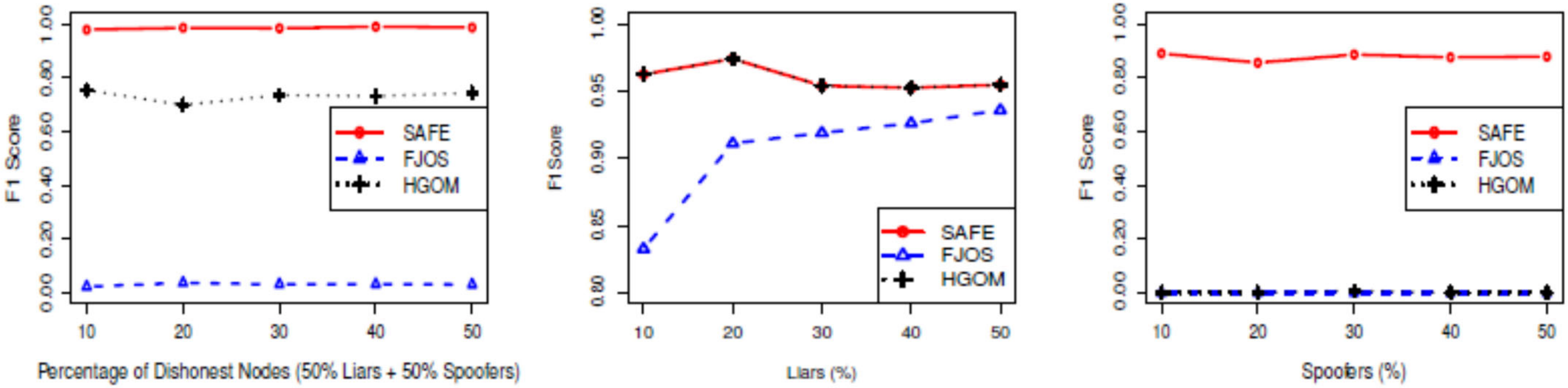
SAFE = Spoofed and False Report Eradicator



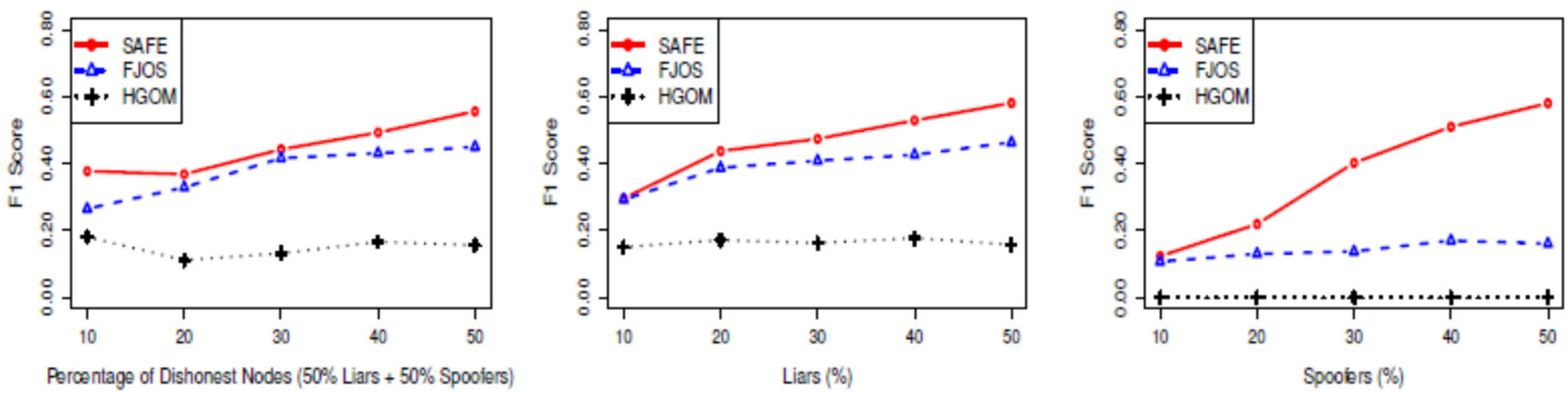
Experimental Evaluation

- Experimental evaluation of the SAFE framework is based on
  - **Synthetic Data:** Vehicular node mobility traces, event generation and report contribution simulated using R tools
  - **Real Data:** Real taxi-mounted smartphone app-generated GPS traces of 289 taxicabs across different regions of Rome (from CRAWDAD)
- Performance metrics:
  - **F1 score (F measure):** Harmonic average of precision and recall for classification of rogue or genuine reporting nodes
  - **Success/ Error rate:** Decision making accuracy to publish the true event reports and drop the false event reports
- Comparison with state-of-the-art methods: FJOS (FIDES trust model) and HGOM (Gompertz function based model).

Experimental Results

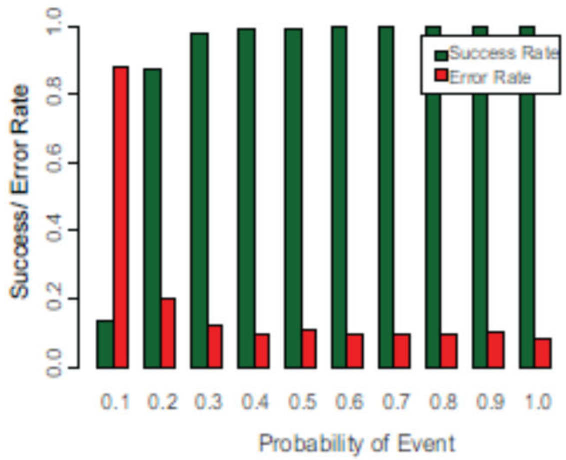


Relative performance of SAFE using Synthetic dataset

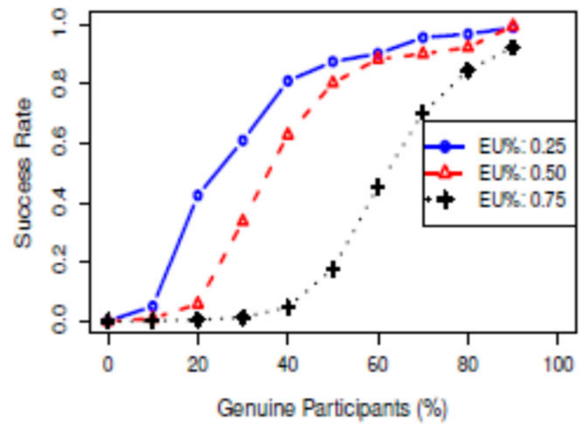


Relative performance of SAFE using Real dataset

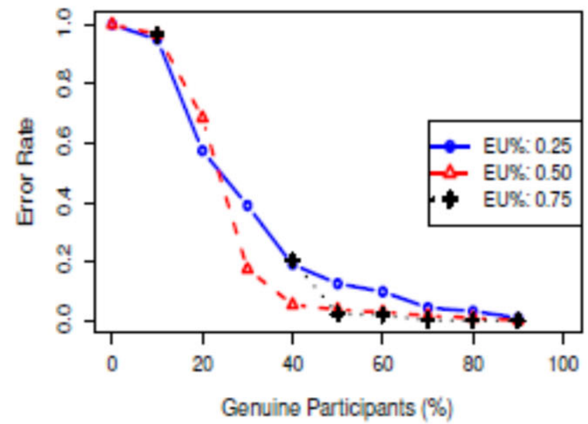
Results



(a) Success/Error Rates vs p_z



(b) Succ. Rate vs % Genuine Participation



(c) Error Rate vs % Genuine Participation

Performance of Expected Utility Theory (EUT) based decision model

- Spoofing and False reporting are genuine problems in VCPS and can be measured using the concept of Quality of Contributions (QoC).
- SAFE framework is more effective for classification of rogue and genuine reporting nodes in VCPS (with false and spoofing report generators).
- Two-level EUT-based decision making model gives high success rate and low error rates even when genuine nodes are in minority (40 - 45%)

Securing CPS and IoTs

Goal: ***Create a technology-enabled, multi-level security framework to monitor, detect, prevent (recover from) natural and man-made disasters.***

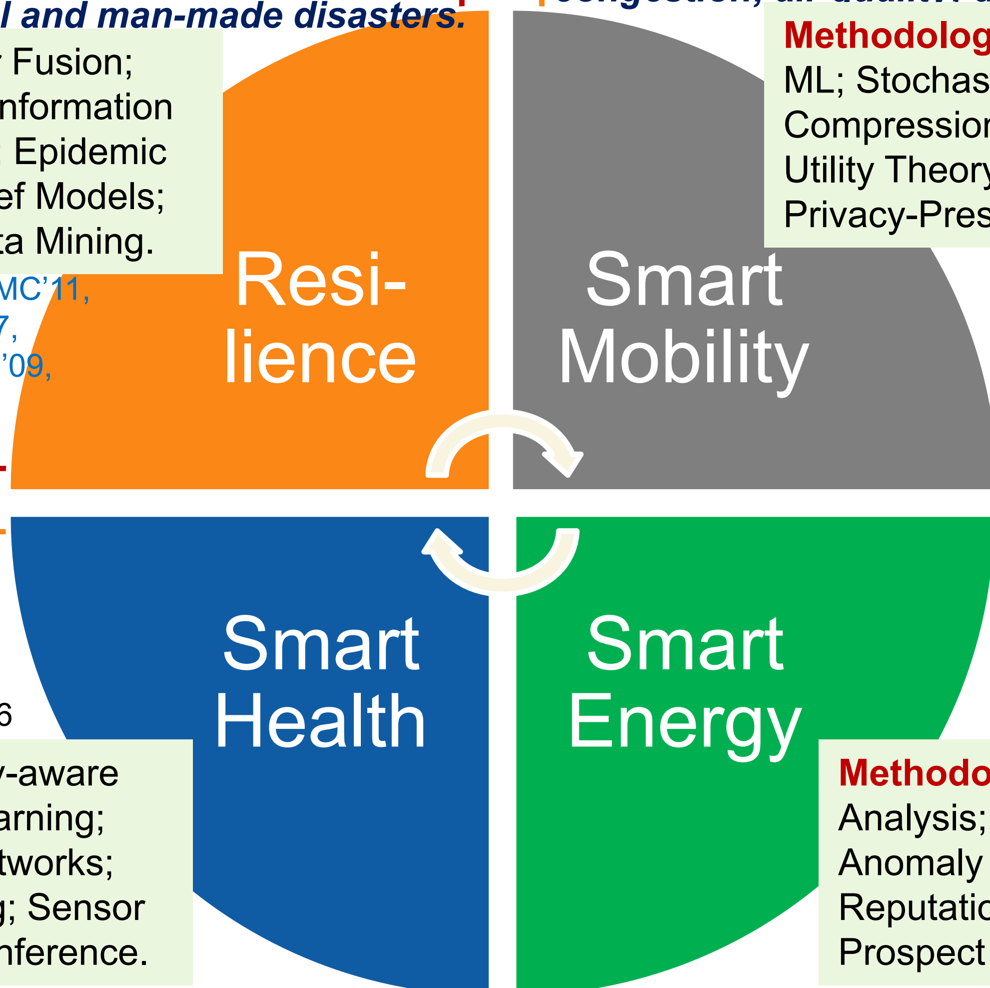
Methodology: Sensor Fusion; Situation-awareness; Information Theory; Game Theory; Epidemic Theory; Trust and Belief Models; Machine Learning; Data Mining.

Publications: TDSc'17, TMC'11, ToSN'18, TDSC'12, TVT'17, AdHoc'15, AdHoc'13, TMC'09, Infocom'19, ComsNets'19, SmartCity'18, BuildSys'17,

Goal: ***Predict human and vehicular mobility; detect false event reporting; transport planning; congestion; air quality; disease spread.***

Methodology: Information Theory; ML; Stochastic Games; Dictionary Compression; Crowdsensing; Utility Theory; Behavior Models; Privacy-Preserving Data Mining.

Publications: TCPS'20, TII'17, ToN'08, TMC'12, PMC'18, Entropy'15, WiNet'02, PerCom'15, SDM'18, PerCom'06, InfoCom'04, MobiCom'99



Publications: TMC'19, TMC'18, TSC'18, PMC'17, ToN'16, SMC'16, TMC'12, Computer'18, BSN15, PerCom'19, SmartComp'16

Methodology: Privacy-aware Data Fusion; Deep Learning; Dynamic Bayesian Networks; Uncertainty Reasoning; Sensor Analytics; QoI-aware Inference.

Goal: ***Cognitive / physical health monitoring; wellness management; dementia detection; fine-grain activity recognition under uncertainty.***

Publications: TMC'20, TDSC'20, TNSE'19, TOPS, TSG'15, CST17, SUR14, CCS'18, CODASPY'17, CNS'17, SmartGrid'12

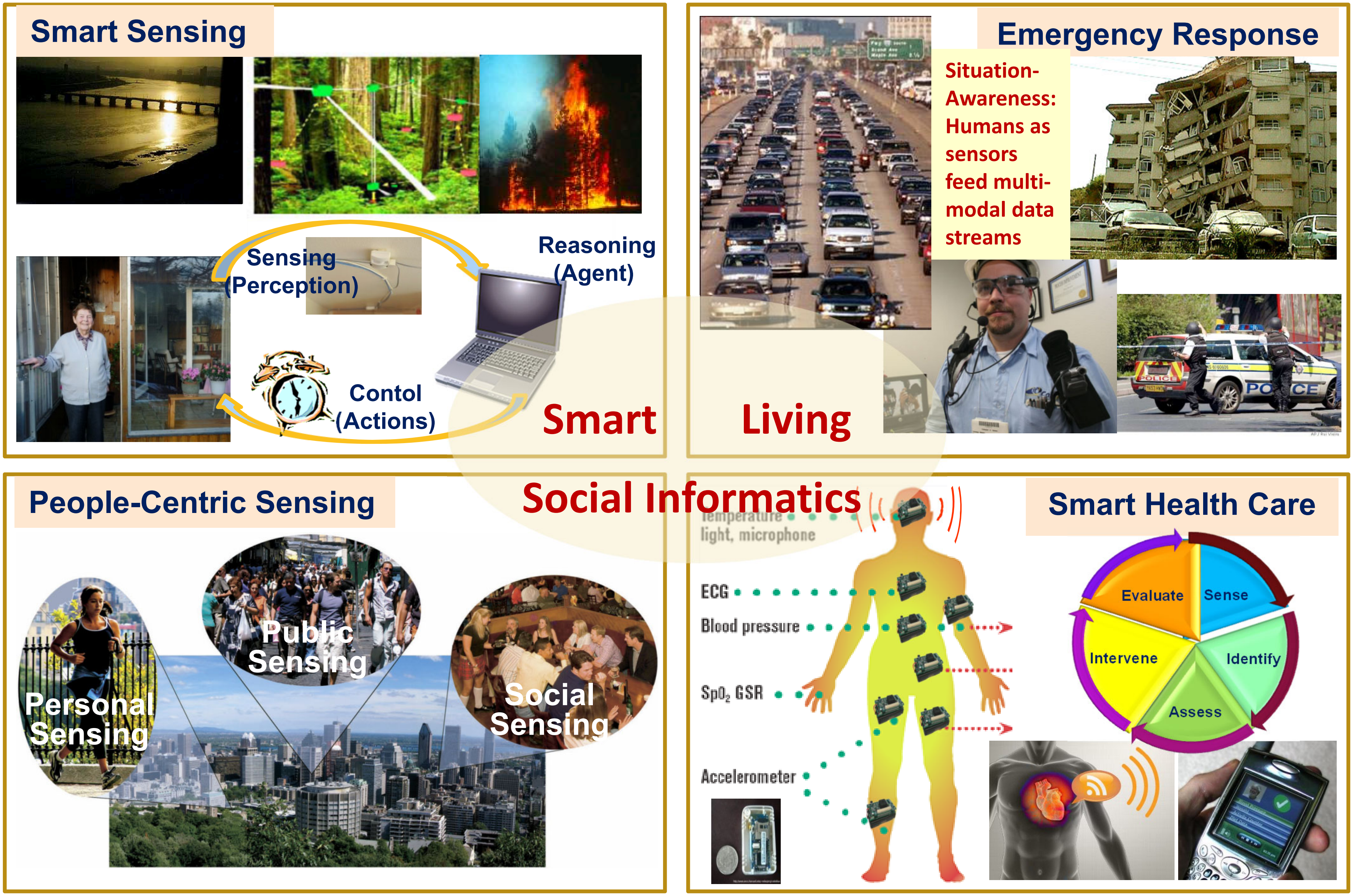
Methodology: Time Series Analysis; State Estimation; ML; Anomaly Detection; Trust and Reputation Model; Epidemic & Prospect Theory; Incentives.

Goal: ***Detect anomalies in energy consumption (false data injection attacks); mitigate cascade failure; secure and trustworthy decisions***

Outline

- Sensor Networks and IoT Security
  - NSF Project: *Pervasively Secure Infrastructures (PSI)*
- Smart City and Cyber-Physical-Human Convergence
  - NSF Project: *Smart Grid Security*
- Mobile Crowdsensing
  - *Trustworthy Vehicular Crowd Sensing*
- Future Directions

Sensing, Reasoning and Control



Securing a Smart City

Interdependence and Uncertainty related to:

- Complexity and Scale
- Security & Privacy in Multiple Smart Spaces
- Human Behavior and Social Dynamics
- Mobility-Energy-Health
- AI, ML, Data Analytics
- Decision Making
- Full System Modeling

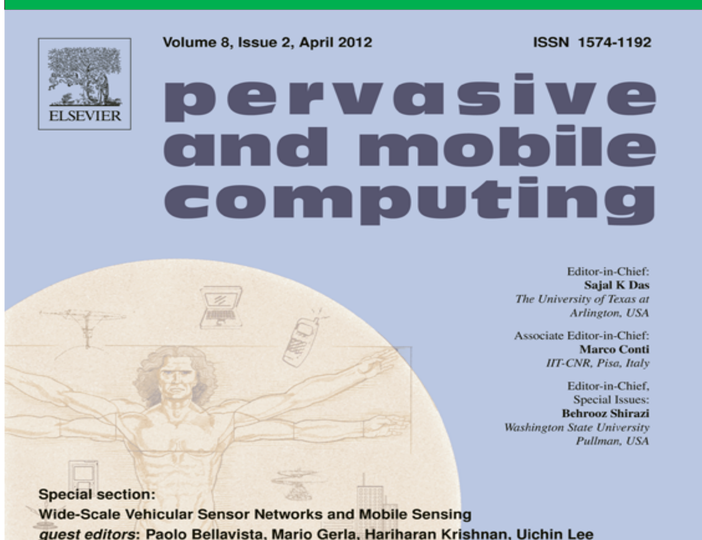
Uncertainty Reasoning	Stochastic Optimization	Dynamic Control	Game Theory	Information Theory	Impact Spread Dynamics

IEEE SMARTCOMP 2020

Big Data IoT Security Workshop

www.smart-comp.org

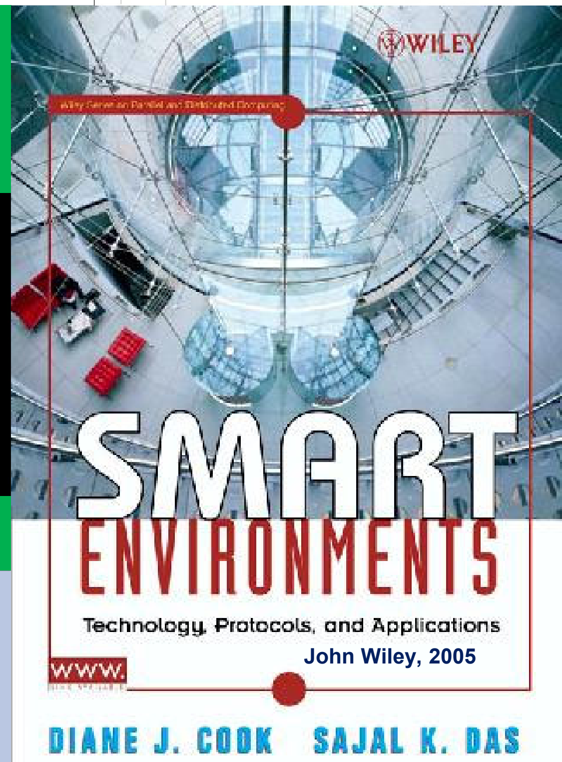
Bologna, Italy, Sep 14-17, 2020

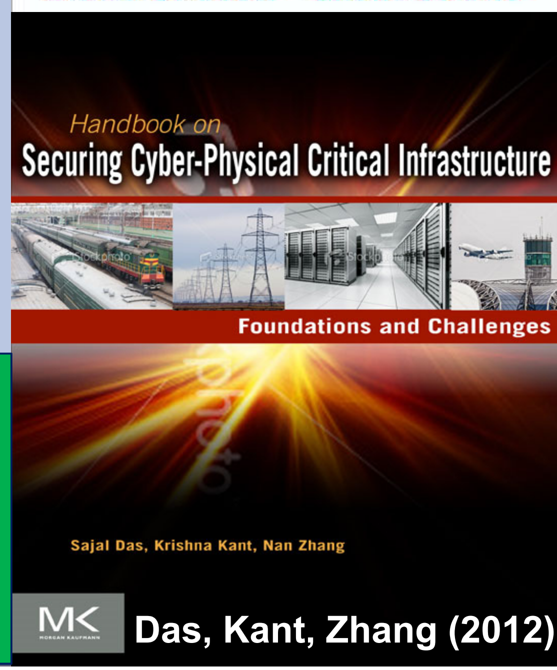


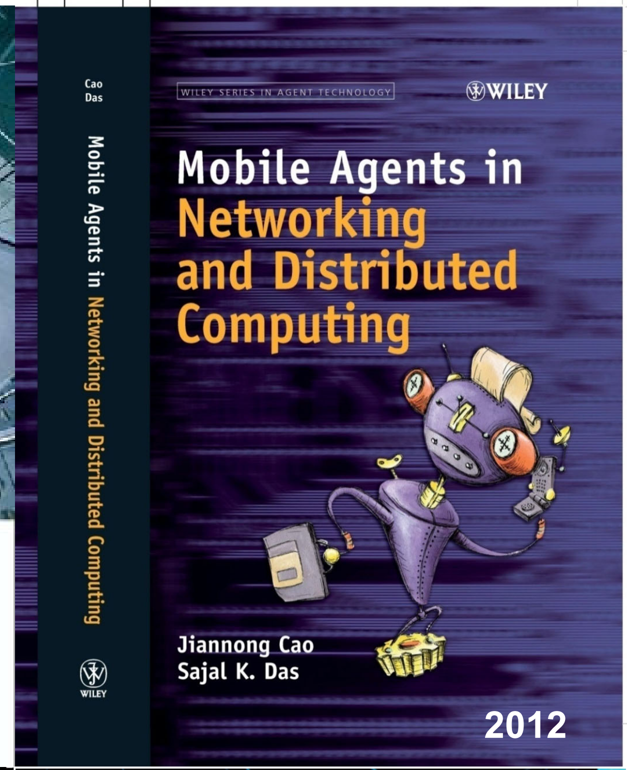
22nd International Conference on Distributed Computing and Networking (ICDCN 2021)

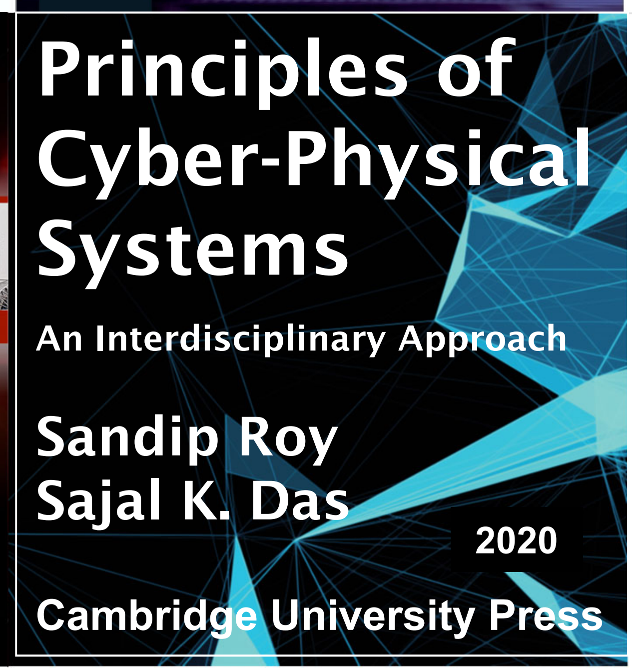
Jan 5-8, 2021 (www.icdcn.org)

Nara, Japan (Deadline July 17)





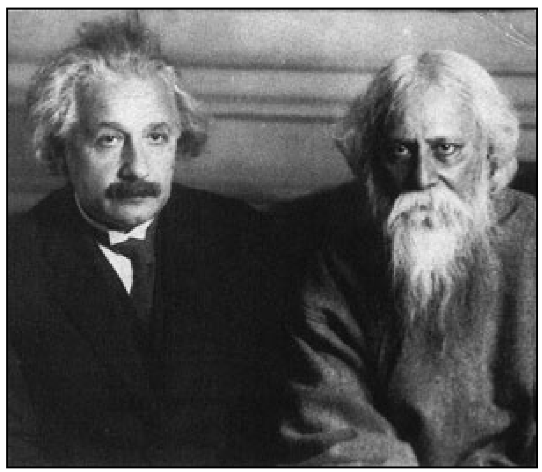




Epilogue

"A *teacher* can never truly teach unless he is still learning himself. A lamp can never light another lamp unless it continues to burn its own flame. The teacher who has come to the end of his subject, who has no living traffic with his knowledge but merely repeats his lesson to his students, can only load their minds, he cannot quicken them".

Rabindranath Tagore (1861-1941)
Indian Poet, Nobel Laureate (1913)



"Imagination is more important than knowledge." – Albert Einstein (1879-1955)

Thank You

sdas@mst.edu	www.cs.mst.edu	h-index: 86
DBLP Sajal K. Das	Erdős Number: 3	Citations: 33,000+