Security and Protection of SCADA: A Bigdata Algorithmic Approach

RK Shyamasundar
Tata Institute of Fundamental Research
Mumbai, India
shyam@tifr.res.in

ACM SIN 2013, Aksaray, Turkey, Plenary Invited Talk

Agenda

- Scada- Overview
  - Attacks, Characteristics
- Learning from STUXNET
- Challenges of SCADA Security
- Existing Approaches
- Big Data Approach
  - Algorithmic Methodology
  - Scalability
- Conclusions

Scada (Supervisory Control And Data Acquisition): Risks

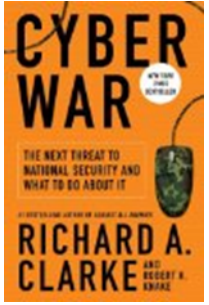
- Control Systems
  - Now at a higher risks to computer attacks because their vulnerabilities are increasingly becoming exposed and available to an ever-growing set of motivated and highly-skilled attacker
- Miscreants tailor their attacks with the aim of damaging the physical systems under control
- Essentially a **Cyberwar**

Some SCADA Attacks

- March 1997: Worcester Air Traffic Communications Attack
- January 2000: Maroochy Shire Sewage Spill
- 2000 and 1982: Gas Pipelines in Russia (and the former Soviet Union)

Leading to Cyber Wars

Cyber War



- Cyber warfare has been defined by government security expert Richard A. Clarke, in his book Cyber War (May 2010), as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption
- All “big” nations are currently preparing for Cyber War
  - Cyber Defense Centers established in all these nations within their military structure & NATO
  - Cyber Defense Centre of Excellence in Estonia
  - Cyber Defense part of new NATO Strategy (Article 5 excluded)
  - Military and government networks are currently being hardened against attacks
  - All nations and, to and unbelievable large scale, China are training offensive cyber war personnel and are preparing for offensive an defensive cyber war
- **Information Superiority:** the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (US Army Vision 2010)

Some Cyber Wars

- **Titan Rain** was the U.S. government's designation given to a series of coordinated attacks on American computer systems since 2003
- **Estonia 2007** Cyberattacks on Estonia refers to a series of cyber attacks that began April 27, 2007 and swamped websites of Estonian organizations, including Estonian parliament, banks, ministries, newspapers and broadcasters
- **Israel attack on Syria** During the night, an Israeli transport helicopter entered Syrian airspace and dropped a team of Shaldag Unit commandos into the area. The commandos took up positions close to the nuclear site. Israeli Air Force F-15I Ra'am fighter jets armed with laser-guided bombs, escorted by F-16I Sufa fighter jets and an ELINT aircraft, took off from Hatzerim Airbase. The ELINT aircraft successfully obscured the attacking aircraft from detection by Syrian radars.

Cyber Terrorism vs Cyber Crime vs Cyber war

STUXNET

- Stuxnet is a Windows computer worm discovered in July 2010 that targets industrial software and equipment
- it is the first discovered malware that spies on and subverts industrial systems
- Kaspersky Labs concluded that the sophisticated attack could only have been conducted "with nation-state support"
- Stuxnet attacked Windows systems using an unprecedented four zero-day attacks (plus the CPLINK vulnerability and a vulnerability used by the Conficker worm)

Stuxnet

- Astonished by the complexity of the program and the quantity of zero day exploits used in this worm.
  - Zero day exploits are those that have no work around or patch.
- Another unique aspect of Stuxnet is that it contained components that were digitally signed with stolen certificates.
- a root kit was found for the programmable logic controller (PLC) which allows the manipulation of sensitive equipment.
- Expected to have been created by a team of as many as 30 individuals. – STATE SUPPORT
- indicates a level of organization and funding that probably has not been seen before
- What was Stuxnet designed to do?
  - While there is no direct evidence, the code suggests that Stuxnet looks for a setup that is used in processing facilities that handle uranium used in nuclear devices
  - Thus the ultimate goal is to sabotage that facility by reprogramming to controllers to operate

What should be the strategy to deal with these kinds of attacks?

- Should it go along the lines of IT security?
- How about Defense-in-depth mechanisms analogous to anomaly detection?
- What about false-alarms in anomaly detection?
- Should the focus be on Physical systems rather than software/network models?

Control Systems Security

- Control systems are not suitable for patching and frequent updates
- While current tools from Information security can give necessary mechanisms for securing control systems, these alone are not sufficient for defense-in-depth of control systems
- **When attackers bypass even basic defenses they may succeed in damaging the physical world**

Security Issues(1)
IT Systems Vs Control Systems (SCADA)

Security Feature	IT Systems	SCADA
Antivirus and Mobile Code	Very common; deployed and updated easily	By Design not open for software updates.
Patch Management	Automated remote patch management possible. However, one needs care from malware perspective	Not designed for it. May impact Performance and also security
Cyber Security Testing & Audit Methods	Standard methods like *Metasploit framework* can be used	Testing has to be tuned for an online system. May impact plant operation.
Change Management (CM)	Classical approach feasible	Strategic scheduling; non trivial process, Impact Analysis is important

Security Issues(2)
IT Systems Vs Control Systems (SCADA)

Security Feature	IT Systems	SCADA
Incidence Response & Forensics	Well established procedure	Difficult to capture as event logs pose problems due to constraints like memory etc.
Physical Security	Normally poor	Normally excellent
Secure System Development	Normal Practice for security sensitive IT applications	Need of the hour for in-house and outsourced development
Security Compliance	Lifetime 2-3 years	Lifetime 5-20 years

Consequences of an Attack

Risk Assessment

- While studies exist on cyber security of SCADA there are very few studies to identify attack strategy of an adversary once it gains access (existing studies pertain to data injection for power grids, electricity markets etc.)
- Need to understand threat model to design appropriate defenses and take measures to secure the most critical sensors and actuators

New Attack detection Patterns

- Dynamic system models for specifying Intrusion detection Systems
  - Current studies pertain false data injection attacks in control systems

New Attack detection Patterns

- Dynamic system models for specifying Intrusion detection Systems
  - Current studies pertain false data injection attacks in control systems
- Replay and Stealth Attacks

Attack Resilient Algorithms and Architectures

- Design to withstand cyber assault

- Reconfigure and adapt control systems when under attack

Control Systems Security: Summary

- Understand the consequences of attacks
  - Do a thorough risk analysis
- Find Attack patterns
  - Design detections
- Design new attack-resilient algorithms and architectures
- Automatic response measures

Multi Disciplinary: Control Engineers + CS + Domain of Application …

Risk Management

- Process of shifting the odds in your favor by finding among all possible alternatives, the one that minimizes the impact of uncertain events

- Process Control Systems usually will have a network of sensors
  - Examples of impact of attack on sensor network on the process control system

Vulnerabilities Due to Embedded IT Systems

- Need to keep in mind the economic constraints on the cost of SCADA (for instance, in smartgrids it is important keep the cost of the meters viable for the society).
- The knowledge of the underlying systems is almost freely available.
- As analyzing Bigdata has become manageable privacy intrusions have become common which in turn has led to several security problems.

SCADA Domain Vulnerabilities

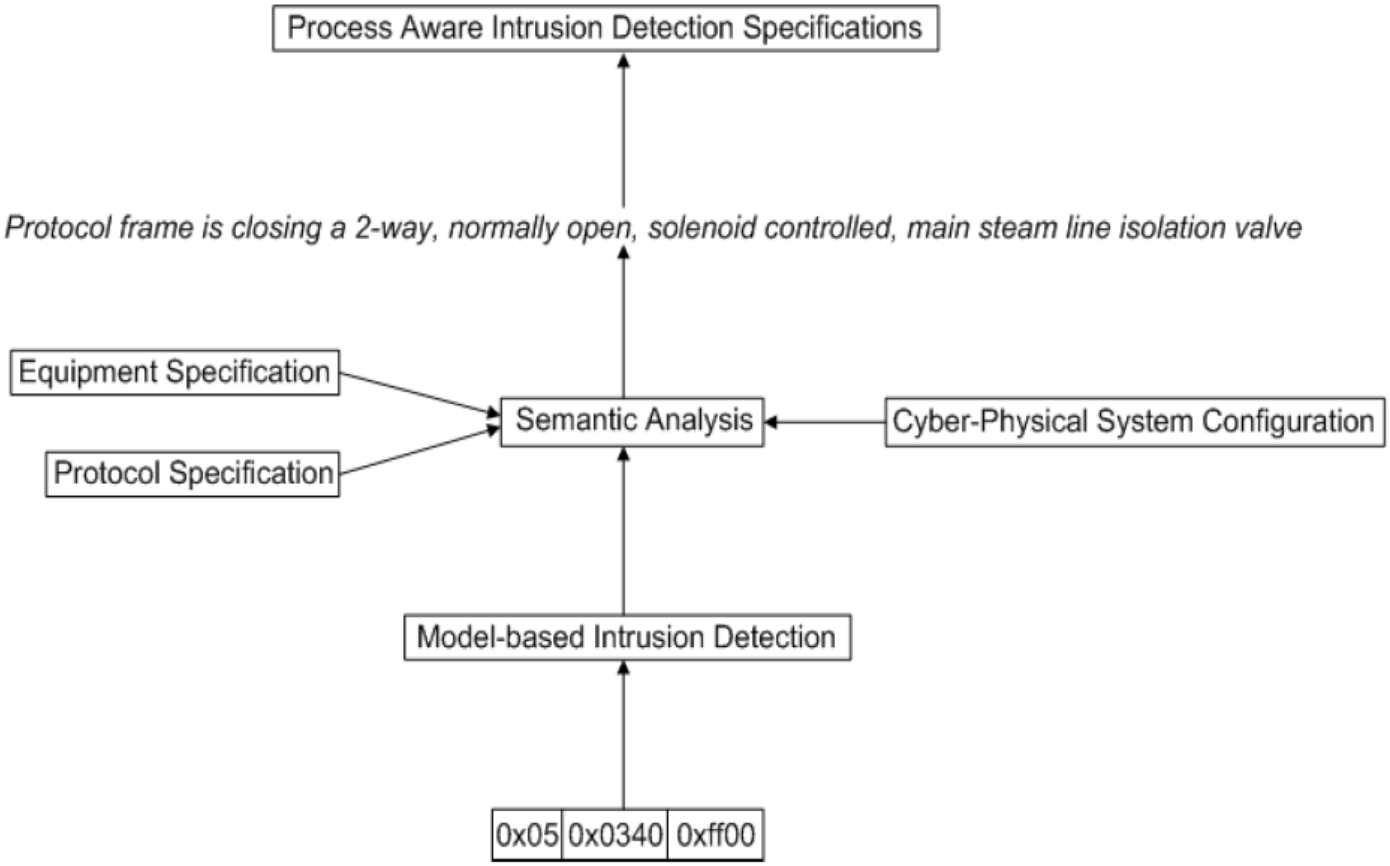
- SCADA Design:
  - stability, safety of plant & env., + performance
  - Not designed for intruders/attackers
  - In the context of Internet intruders can induce attacks that would not have been considered by the designer
  - Thus, the major challenge for SCADA security lies in arriving at methods of control of the plant that shall overcome such plausible attacks and maintain the stability and the trustworthiness of the system – thus, making the system robust.

Approaches for securing SCADA

Intrusion Detection

- Misuse detection
  - Based on signatures of known attacks
- Anomaly detection
  - Based on learning profiles of normal behaviour
    - Could detect unknown attacks but suffers from high false alarm rates
- Specification-based Detection
  - Manually developing specification of legitimate behaviour and hence has less false alarm rates
  - But ability to detect new attacks is also less.

Process Aware Intrusion



Mirage Theory for Deception-Based Detection

- Military Deception (MILDEC): those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions or inactions that will contribute to the accomplishment of the friendly mission.
- Relies on DISPLAYs: simulation, disguising, and/or portrayal of friendly objects, units, or capabilities that may not exist but are made to appear so.
- Eg. (physical means): dummy and decoy equipment and devices, tactical actions, movement of military forces, etc.
- Eg (technical means) include emission of chemical or biological odors, emission of radiation, reflection of energy, computers, etc.,
- Eg (administrative means) techniques to convey or deny physical evidence.

Mirage Theory Applications: Ideas

- **Basis:** leverage of the boundary between continuous and discrete spaces, leverage of how the presence of a continuous space is redirected on a corresponding discrete space, and simulation or emulation of physical processes and physical equipment.
- A computer network attack provides an adversary with access that may extend to a whole discrete space.
- Nevertheless, due to physical limits there are no feasible ways for an adversary to gain visibility over a continuous space through a computer network attack.
- In other words, a computer network attack won't enable an adversary to virtually move beyond the analog-to-digital and digital-to-analog conversion integrated circuits.
- Consequently an adversary cannot verify whether input electrical signals are indeed applied by existing sensing devices, nor can he/she verify whether output electrical signals indeed reach an existing actuating device.

Securing SCADA

- Make the system secure with respect to IT. This could be done through the classical hardening approaches developed for IT security along with appropriate authentication and encryption as required.
- Ensure that the system also works in the safe zone as projected by the control system/plant designers.

Monitoring Control Systems

- Most of the approaches may be classified under:
  - Developing models from first principles using the laws of physics,
  - Empirical behavior using simulation tools, and
  - A hybrid of the above
- While safety critical systems demand accurate models, it is not always feasible due to the underlying complexity and economics.
- Usually, the behavioural model is constructed in the industry using several tools like identification packages that enable the development of physical systems using training data.

Fault Detection and Diagnosis

Problems

- Generation of residuals that are close to zero under no-fault condition, minimally sensitive to noises and disturbances, and maximally sensitive to faults
- Evaluation of residuals corresponds to decision rules with respect to the handling of residuals.

Deriving Statistics in Data

- Assess level of significance of discrepancies with respect to uncertainties & reflect as to whether the parameter perturbation is significant or not.
- Parameter estimation provides us with relative sizes of estimation errors with respect to noises on the system measurements.

Solving Detection Problems

- Model validation: Given a reference point of the parameter and a new data sample, the problem is to decide whether the new data are still well described by this parameter value or not and could be done by a sliding window of fixed size.
- On-line Change detection: Given a data sample and an instant t, the problem is to decide whether the parameter has deviated from the given reference point and if so classify into the required categories.
- Off-line Change detection: Given a data sample consisting of N samples, the problem is to decide whether at some instant, t, the given parameter has drifted to some other value that needs attention.

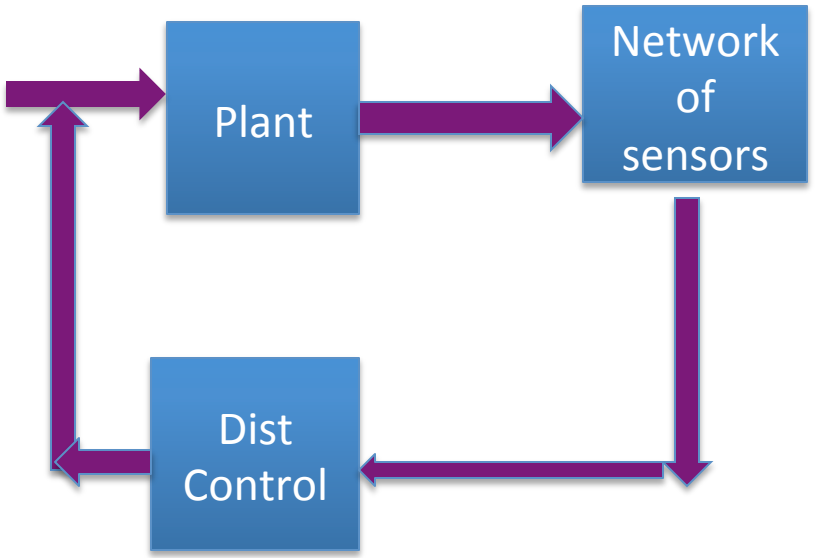
Some Tools used

- **Instance Control Charts:** Control charts essentially present a graphic display of process stability or instability over time.
- A control chart is a statistical tool: to distinguish between variation in a process resulting from common causes & variation due to special causes.
- The control chart differentiates between two types of variation:
  - Special Cause Variation: variations due to causes which are not normally present
  - Common Cause Variation: are the result of numerous ever-present differences in the process.

Monitoring and Protecting SCADA

a. Malware attacks of the computing elements
   - to be handled primarily from the IT defense perspective.

b. New possible attacks on the plant arising from the malware attack on its control system.
   - Is it possible to handle so that SCADA will always be in the SAFETY Zone and also be indicative of a possible attack



Challenge: New Scenario of Attacks

- Sensor Measurement: Y (k) ={y1(k), . . . , yp(k)},
  - yi(k) denotes measures by sensor i at time k.
  - ∀k, yi(k) ∈ [ymin, ymax] in the DOM (Y)
- Each sensor has a unique Crypto identity key
- Zi(k)s signals recd. by process controller (Val in domain – else gets det.).
  - Zi(k)= aik if in attack slot

    = yik other wise

- **Integrity Check:**

If attackers have compromised a sensor they can inject any value aik – an arbitrary value in the domain

- Replay and Stealth Attacks
- **DOS Attack**
  - Notices lack of measurements
  - A solution is to use the last value

SCADA Design : Change Detection Basis for Safety

- Hypothesis:
  - We have the statistics of its good performance recorded over time to classify as normal operation and possible abnormal behavior.
  - Note that it must be kept in mind that the control system is a continuous system rather than a discrete one.
- Under abnormal operations, assume
  - plant will be operated under safe parameters
  - declaring it as an alarming zone for further action.
- In other words, in the data of the d-dimensional space, with respect to a reference point of operation,
  - we have a set of vectors that reflects possible variations that would still keep the system in a stable/safe state; falling outside would mean possible unsafe operation

Question

- Assuming we have captured the behaviour of the system, is it possible to design a control system such that:
- It follows the control law design and
- Detect Black Swan events – large impact, hard to predict, rare events – difficult to predict lying beyond the realm of normal expectations, and
- Guarantees that it will always operate in a safe domain, sounding alarm whenever it finds the behaviour is not as expected around the reference anchor points

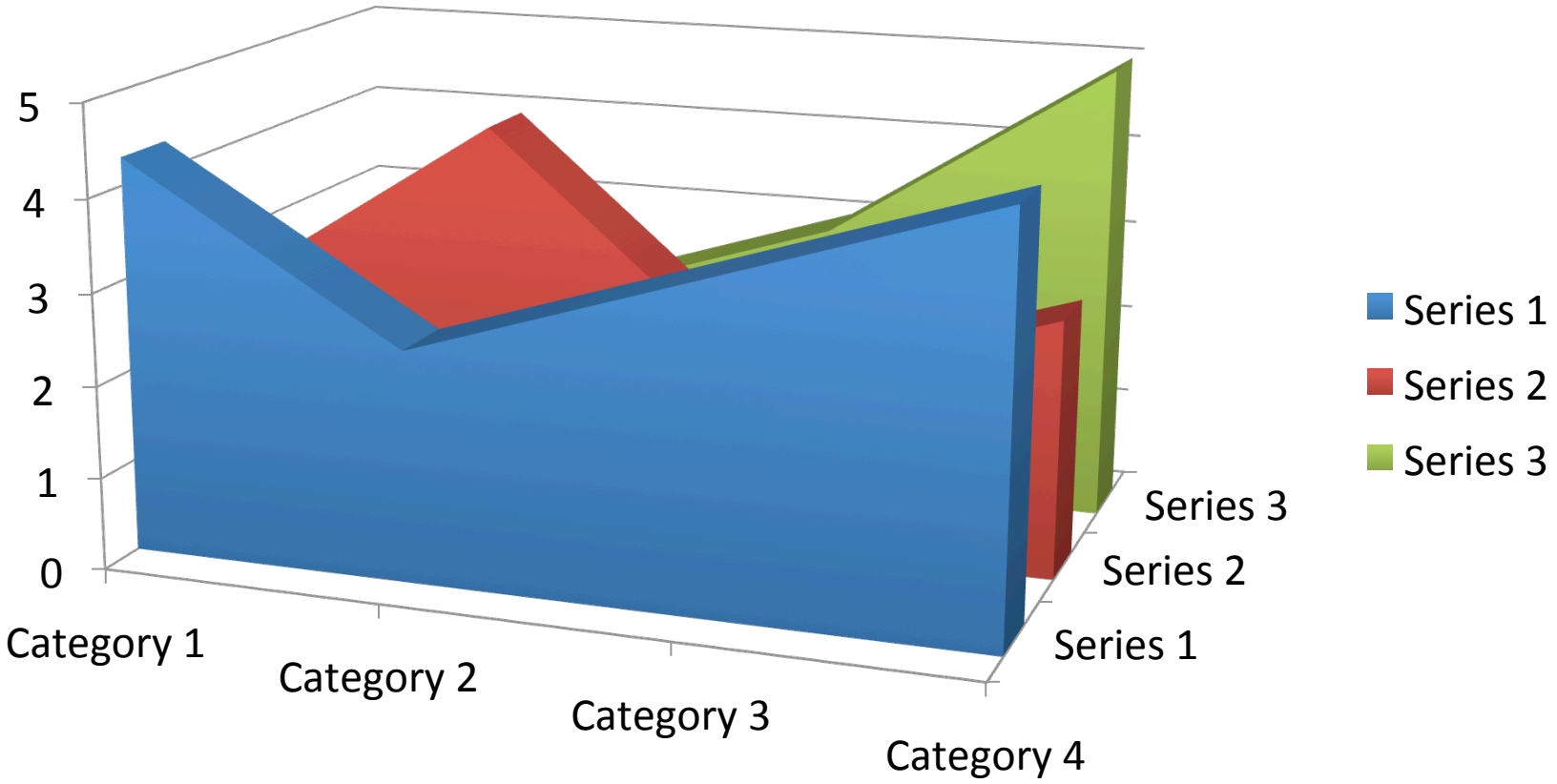
Challenge and Solution

- Lies in providing a scalable solution

- Solution Basis:
  - Reducing the problem to problem of monitoring a distributed set of streams through queries

An Algorithmic BigData Approach

What is the intuition?



Anomaly Detecting Controller

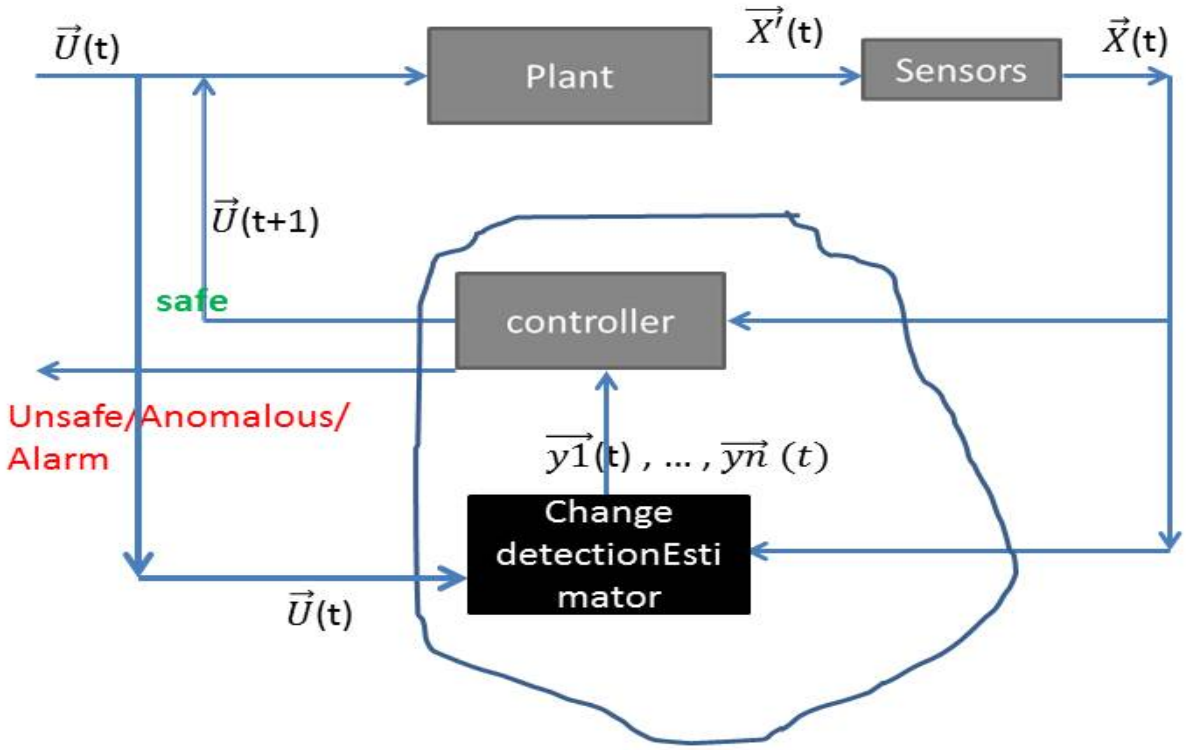


Figure 1. Anomaly Detecting Controller

Safety of the System

- *U(t)* : plant input at t & *X'(t)*: output of plant & *X*(t): denote the same measured through the sensors at time t.
- **Now, the input *U*(t+1) at time t+1, is determined by the controller which finds whether there is anomaly at this point using the possible perturbations assuming a stable operation at time t, with input *U (t)* through the Change-Detect-Estimator (CDE) .**
- if {*Y1 , …, Ym* } is the set of vectors taking into account the possible perturbations corresponding to input *U (t),* output *X'(t*) as detected by the sensors.
  - Note that *Y1, …, Ym* essentially denote possible perturbations with respect to input and output of the plant as reflected in its' behaviour.
- **Then *X (t*)will be said to be safe if *X(t)* is in the convex hull of { *Y1, … , Yn* }.**

Question

- **Can we compute convex hull in a scalable manner?**
- **Yes**
- Izchak Sharman and Assaf Schuster, A Geometric Approach to Monitoring Threshold Functions over Distributed Streams, ACM TODS, Vol 32, Nov. 2007, pp. 23:1-23:29.

Distributed Computation of the Convex Hull [3]: Let $\vec{X}(t)$, $\overrightarrow{Y1}$, … , $\overrightarrow{Yn}$ be vectors in d-dimensions over the reals (i.e., $\mathbb{R}^d$). Let Convex-hull ($\vec{X}(t)$, $\overrightarrow{Y1}$, … , $\overrightarrow{Yn}$) denote their convex hull. Let Bi($\vec{X}, \overrightarrow{Yk}$) denote a ball centered at $(\vec{X} + \overrightarrow{yk})/2$ with a radius of $\|(\vec{X} - \overrightarrow{yk})/2\|$, for each k. Then,

$$\text{convex-hull}(\vec{X}, \overrightarrow{Y1}, \ldots, \overrightarrow{Yn}) \subset \cup_{k=1}^{k=n} \mathrm{B}(\vec{X}, \overrightarrow{Yk}).$$

Geometric Method

(SKS MOD 2006 as presented in Minos Garofalakis –BDA 2013)

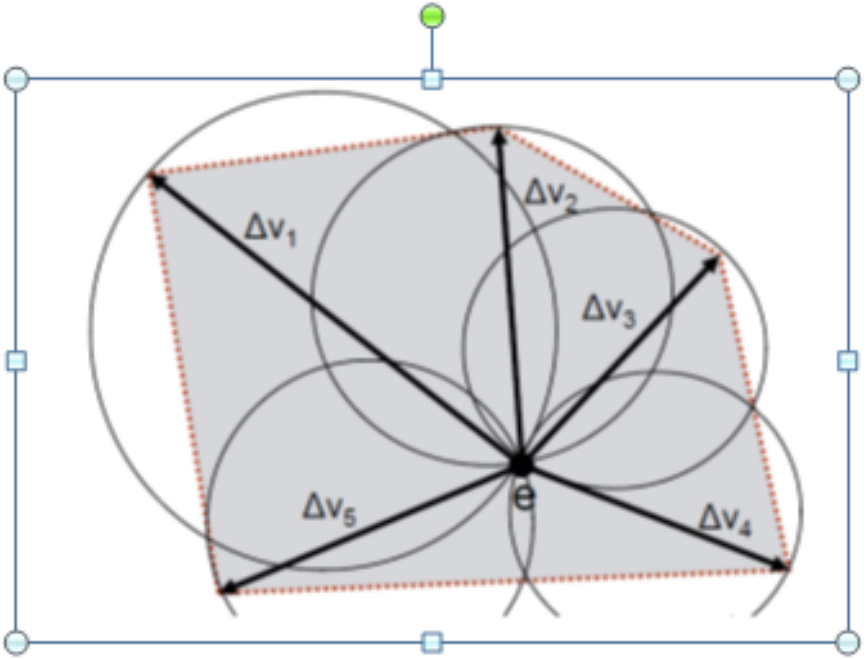
- Monitor **function domain** rather than range of values!
- Tracks local statistics vector Vi (data distribution)

- Global condition is $f(v) > \tau$, $v = \Sigma_i \lambda i vi$ $(\Sigma_i \lambda i = 1)$
  - v = convex combination of local statistics vectors
- All sites share estimate $e = \Sigma_i \lambda i vi'$ of v based on latest update vi′ from site i
- Each site i tracks its drift from its most recent update $\Delta vi = vi - vi'$

Cover of Convex Hull

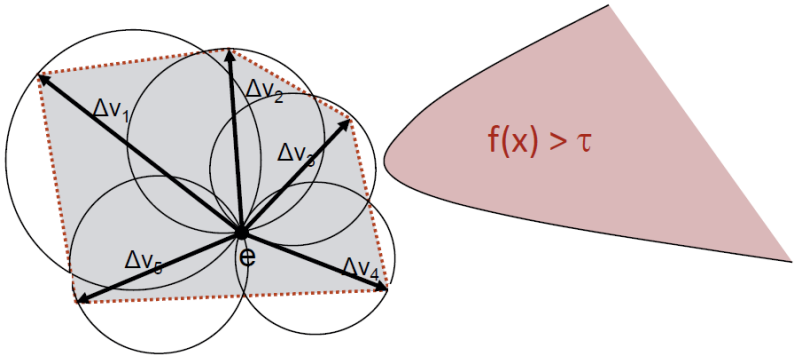
Main Idea:

- $v = \Sigma_i \lambda_i \cdot (e+\Delta v_i)$
  - a convex combination of local drifts
  - v lies in the convex hull of $(e+\Delta v_i)$ vectors
  - Convex hull -- covered by spheres with radii $||\Delta v_i/2||$ centered at $(e+\Delta v_i)/2$
  - Each such sphere can be constructed independently

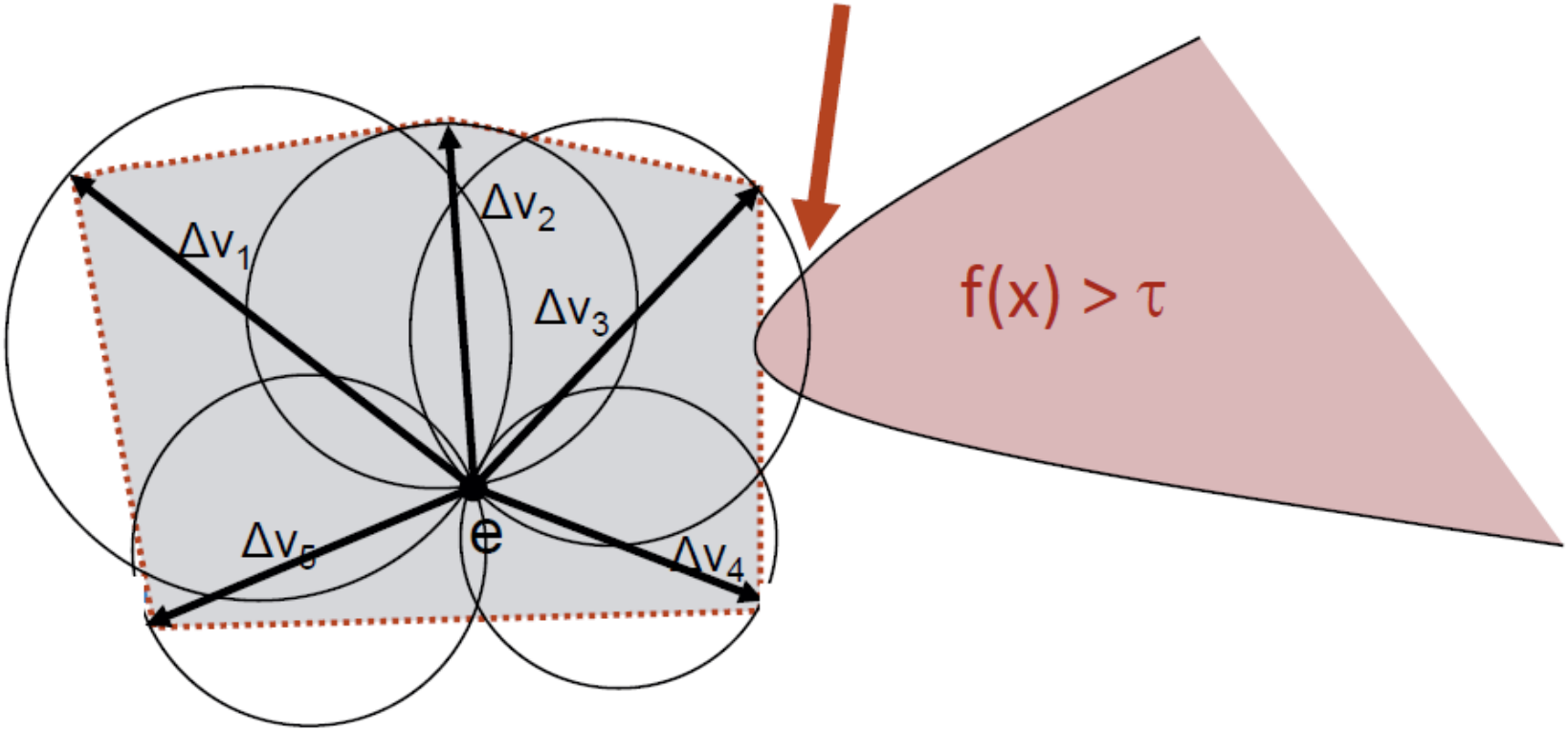


Monochromatic Region

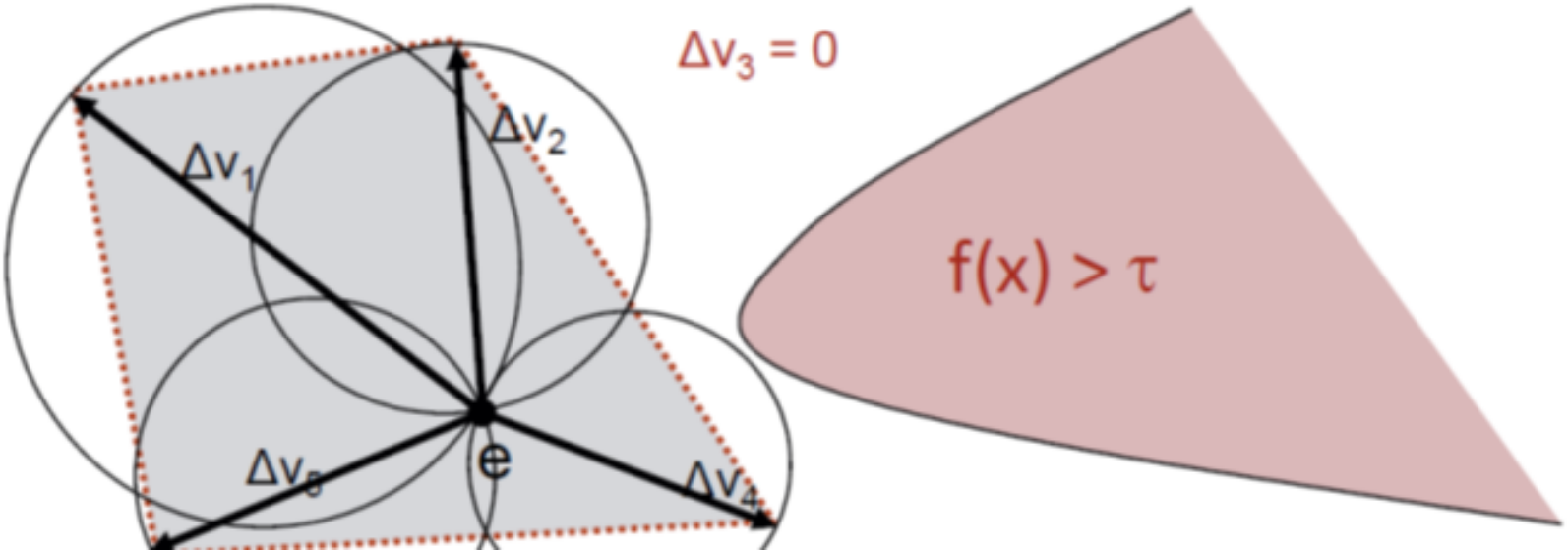
- Monochromatic Region: For all x in region, f(x)is on the same side of the threshold (f(x) > τ or f(x) ≤ τ)
- Each site independently checks its sphere is monochromatic
  - Find max and min for f()in local sphere region (may be costly)
- Send updated value of v_i if not monochrome



Restoring monotonicity



- After update, $||\Delta v_i||_2 = 0 \Rightarrow$ Sphere at i is monochromatic
  - Global estimate e is updated, which may cause more site update broadcasts
- Coordinator case: Can allocate local slack vectors to sites to enable "localized" resolutions
  - Drift (=radius) depends on slack (adjusted locally for subsets)



Advantages and Power of the Approach

Overcoming Replay Attack

- Replay attack:
  - Attacker records a sequence of sensor measurements and replays the same at a later point of time which could cause havoc to the system later on.
  - Also one of the attacks used by Stuxnet.
- Suppose the attack is at T corresponding to values read at t, T > t
- It will be allowed only if the reference vector at T is within the known limits of that at t.
- Hence safe

Overcoming Stealth Attacks

Safe

- ***Surge attack*:** here, the attacker wants to maximize the damage as soon as possible.
- ***Bias attack*:** In this case, the attacker wants to attack over a period of time through incremental perturbations.
- ***Geometric attack*:** here the adversary wants to drift slowly in the beginning and finally maximize the damage.
- **False positives** -- Could be minimized based on sampling

Conclusions

- Extremely useful in Detecting Black Swan Events
- Scalable and overcomes false positives
- Inductive Learning/Machine Learning

Conclusions

- **Tunable for generalizations like**
  - Same analysis of correctness holds when spheres are allowed to be ellipsoids
  - Different reference vectors → to increase radius when close to threshold values
  - Combining these observations allows additional cost savings
  - More general theory of **"Safe Zones" --** Convex subsets of the admissible region

Conclusions

- Approach in conjunction with IT security provides a safe operation.
- As most SCADA vendors do not divulge details the approach is promising.
- Applicable for varieties of SCADA deployments including power grids, smart grids etc. (note that the data is quite quite often very sensitive)
- Experimental work in progress.

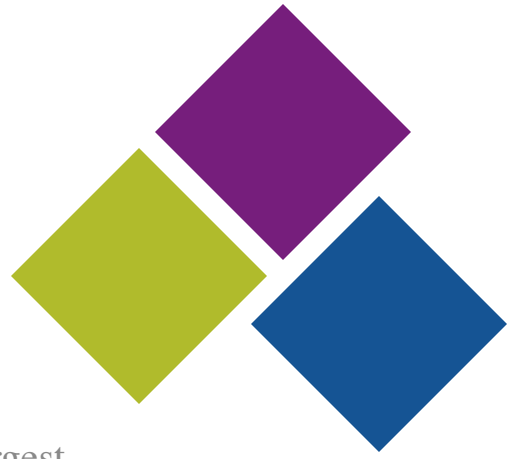
The Distinguished Speakers Program is made possible by

Association for Computing Machinery

Advancing Computing as a Science & Profession

For additional information, please visit http://dsp.acm.org/

About ACM



ACM, the Association for Computing Machinery is the world's largest educational and scientific computing society, uniting educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges.

ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence.

ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

With over 100,000 members from over 100 countries, ACM works to advance computing as a science and a profession. www.acm.org

Thank you

Questions?