Proactive Response Strategy for Energy Delivery Systems

Ahmed Fawaz, Carmen Cheh, Uttam Thakore, Atul Bohara, Ben Ujcich, Mohamad Noureddine, Brett Feddersen, William H. Sanders

GOALS

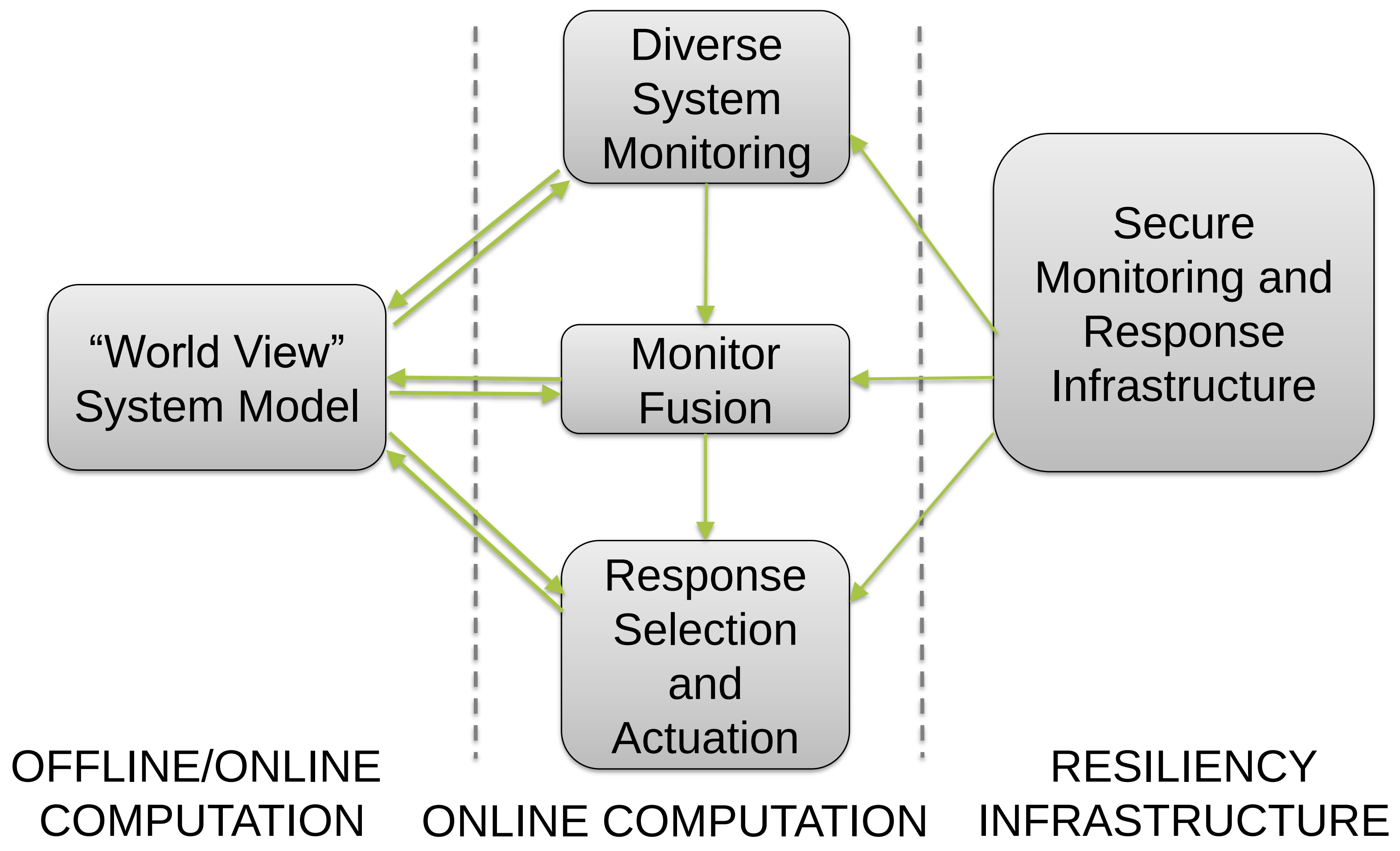
- Develop new monitors to detect behavioral abnormalities using physical ground truth.
- Define a language for response action deployment.
- Define system-specific resiliency metrics for response decision algorithms.
- Design proactive response selection algorithms against adversarial attacks that uses knowledge about the power grid's current security-state and its security requirements.
- Build a response and recovery engine (RRE) as a distributed agent-based system that actively monitors the systems and devises responses.

FUNDAMENTAL QUESTIONS/CHALLENGES

- How to maintain the state of the system in across distributed agents?
- How do we ensure the integrity of the agents if they are part of a compromised hosts?
- How does using diverse sources of information increase the confidence in monitoring information?
- Can low-level physical information provide a base of trust for monitoring information?
- What is the best metric for tolerance and system performance?
- What is the set of decision algorithms needed to find optimal responses?

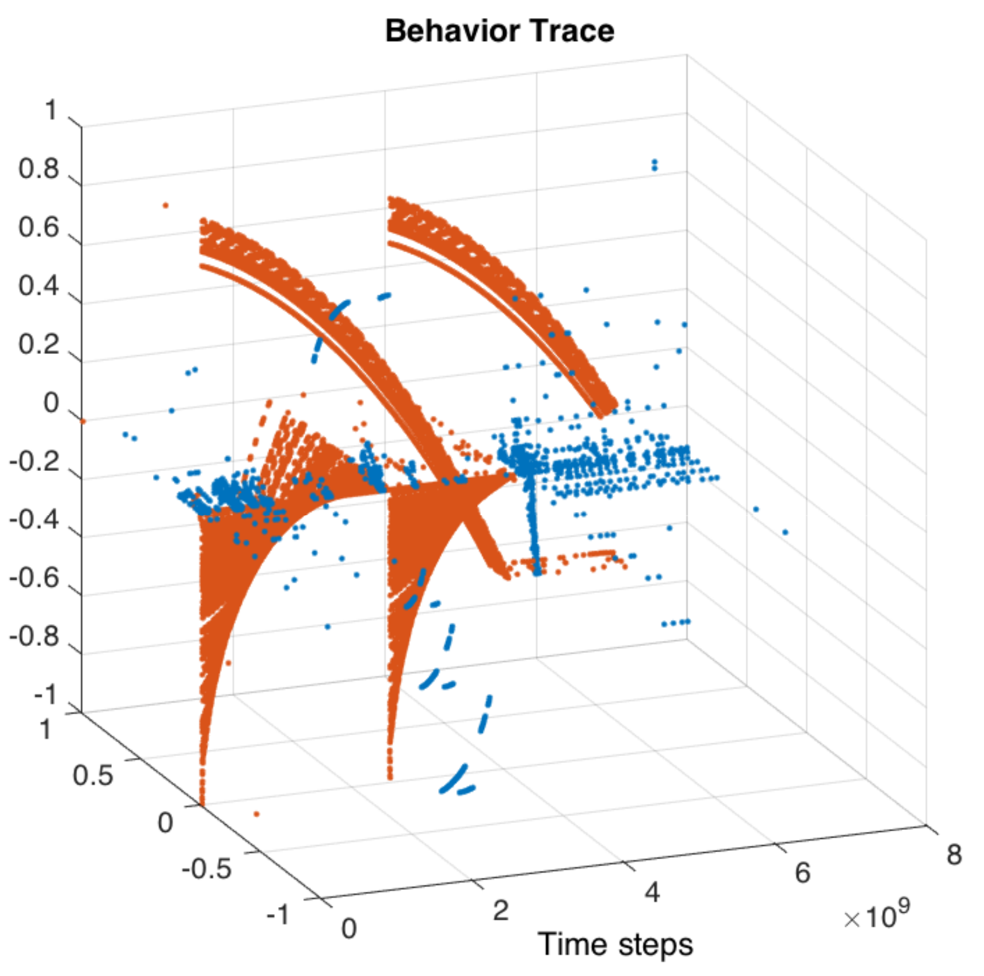
RESEARCH PLAN

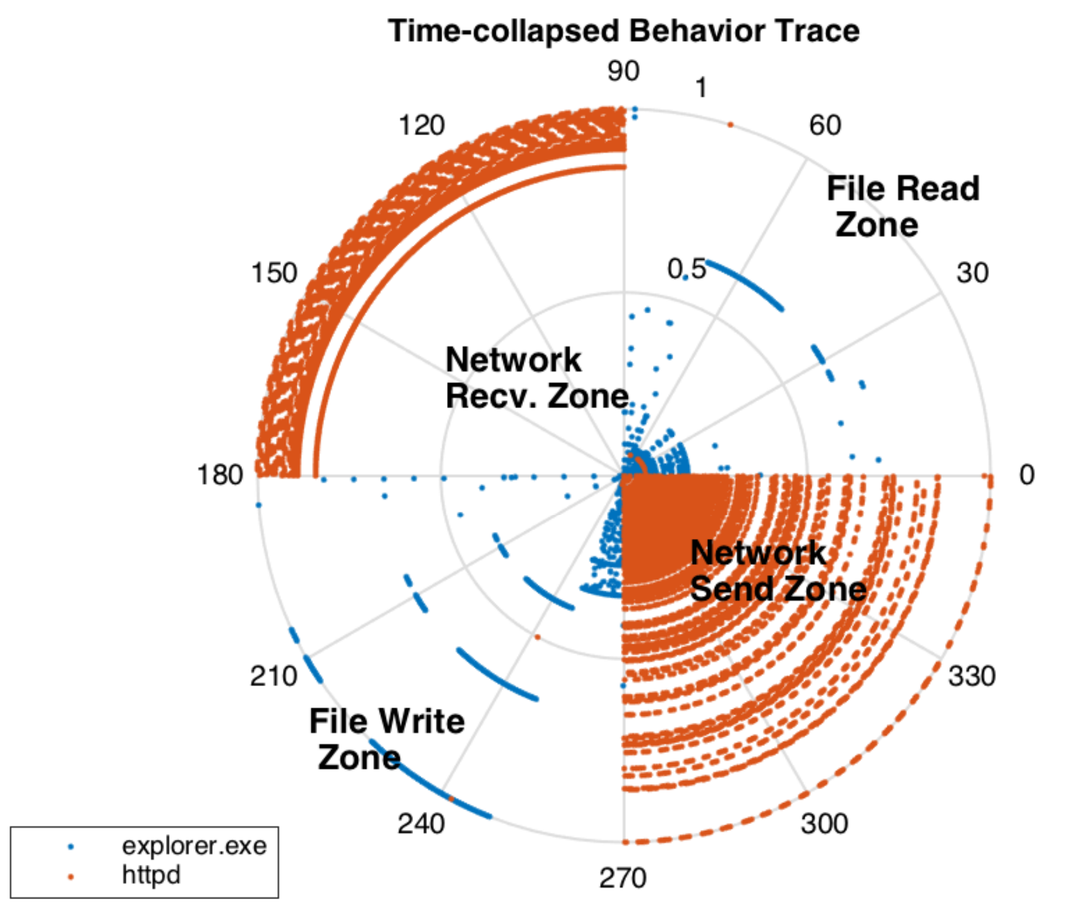
- Develop an anomaly detection algorithm for power grid embedded devices that exploit the regularity of operation. The algorithm learns a sparse representation dictionary that represents the baseline of the operation.
- Implement and deploy the anomaly detector for an embedded system. The detector will use low-level information and fuse power measurements and cyber information from the device.
- Design a set of response mechanisms that use the anomaly detector and the threat model. The response mechanisms should provide optimal performance in terms of security and service level (availability and integrity) in the system.
- Prove that responses are safe in the substation setting. Attackers should not be able to use the mechanisms as a new attack surface.
- Investigate the deployment of physical responses when we detect a cyber intrusion.


Diverse System Monitoring
"World View" System Model
Monitor Fusion
Secure Monitoring and Response Infrastructure
Response Selection and Actuation
OFFLINE/ONLINE COMPUTATION
ONLINE COMPUTATION
RESILIENCY INFRASTRUCTURE

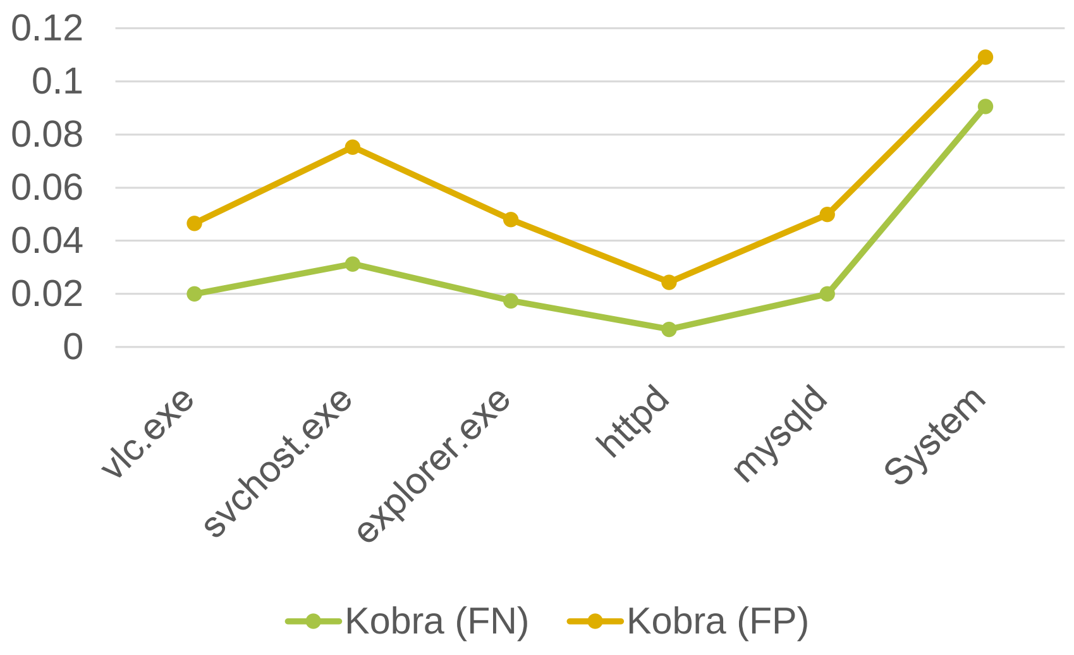
ANOMALY DETECTION

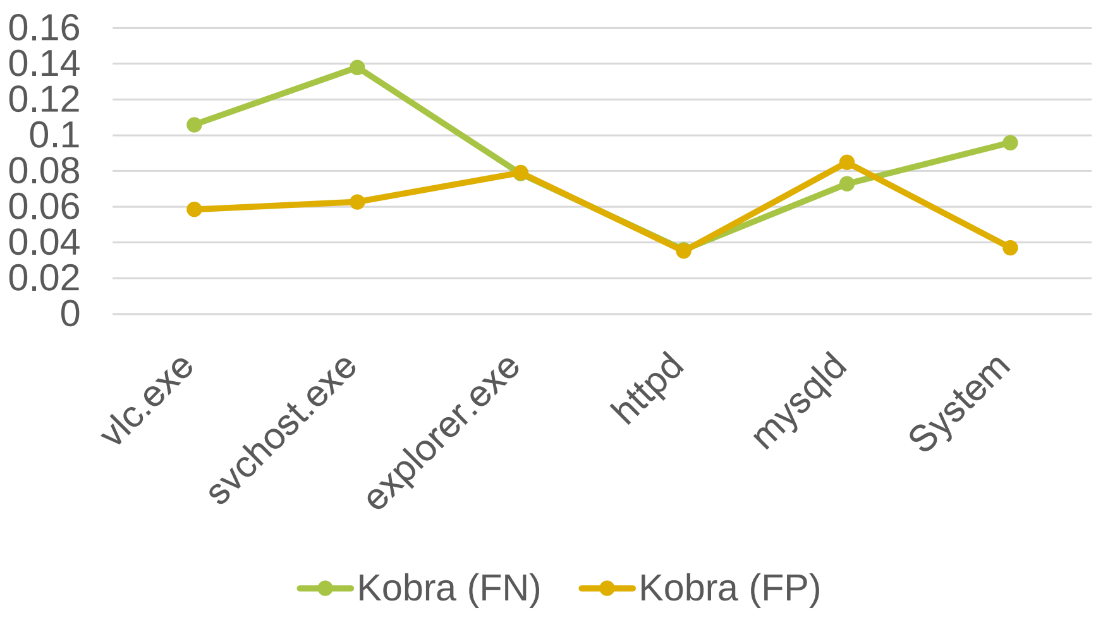
- Kobra is a kernel-level monitoring engine that collects low-level information for anomaly detection.
- Kobra converts application behavior to complex-valued discrete time signal.
- A training set of application behavior is used to establish the normal behavior using sparse representation dictionary learning and latent semantic analysis.
- The anomaly detector flags signals that have a reconstruction error higher than the 95th percentile of that of the training data.





- We inject attack behavior into application behavior. The results show that the false negative rate is low.

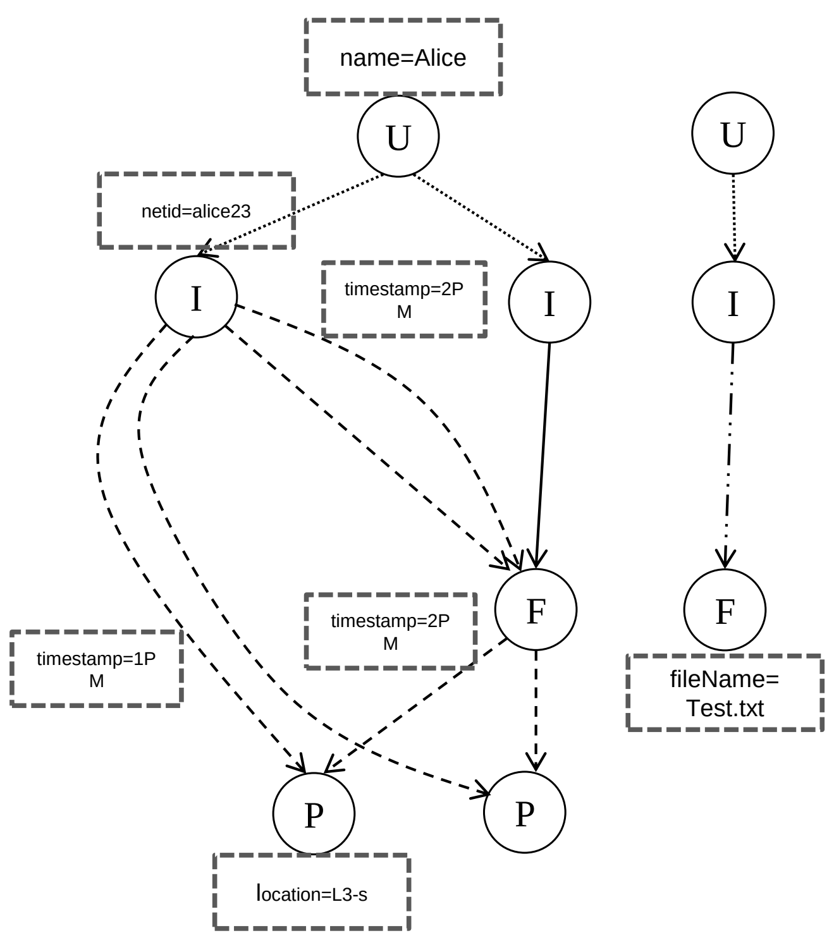




- In the future we want to move our Kobra anomaly detection algorithms to the protective devices of the power grid.
- By cooperating with SEL, we plan to embed Kobra into substation hosts.

CPTL– A WORLD VIEW

- Situational awareness is needed for resiliency.
- In order to drive intrusion detection and response, we need to understand the state of the system.
- CPTL is a human-readable, machine-actionable language to represent and reason about information in cyber-physical systems.
- CPTL includes a suite of operations that integrates graph-theoretic analysis with semantics.



$(G, \mathcal{K})_{\mathcal{I}}$

Concept Name	Icon	Role Name	Icon
User	U	create	-··→
Identity	I	write	→
File	F	prints	---→
Printer	P	hasIdentity	⋯→

Feature Name	Icon
timestamp, fileName, location, netid, name	Feature name=feature value

BROADER IMPACT

- The ultimate goal of providing an automated response capability to power grid control rooms will enable quick reaction against security attacks and failures thus preventing them from causing potentially catastrophic failures.
  - This effort is jointly funded by an NSA Science of Security award.
- Another goal is to study anomaly detection algorithms, the effect of information fusion on accuracy and specificity.

FUTURE EFFORTS

- Design physical models to augment monitor data for integrity checking.
- Implement RRE for embedded devices similar to those found in energy delivery systems by working with SEL.
- Develop behavioral anomaly detection algorithms to detect insider attacks.

CYBER RESILIENT ENERGY DELIVERY CONSORTIUM | CRED-C.ORG

FUNDING SUPPORT PROVIDED BY THE U.S. DEPARTMENT OF ENERGY AND THE U.S. DEPARTMENT OF HOMELAND SECURITY