FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Welcome to the FORCES newsletter

Spring 2016

Welcome to the latest issue of the FORCES newsletter. This issue considers the idea of cyber threats and adversaries and describes how we protect against them in different cyber-physical systems, including water systems and electrical grids. We are featuring perspectives from FORCES researchers at our partner universities, as well as observations from advisory board members Bill Streilein and Hamed Okhravi at MIT Lincoln Labs.

The FORCES project has made tremendous advances since its inception, and we continue to move ahead with our studies of areas of vulnerability in our critical infrastructure. This issue of the newsletter provides an excellent summary of the variety of work being conducted in our group, and I'd like to extend our thanks to the National Science Foundation for supporting this work.

Thanks for taking time to read the FORCES Spring newsletter. As always, if you have feedback, comments, and suggestions I'd appreciate hearing from you.

Sincerely,

S. Shankar Sastry
Professor and Dean of Engineering
University of California, Berkeley

RESEARCH SPOTLIGHT

Sustainable and Resilient Urban Water Systems

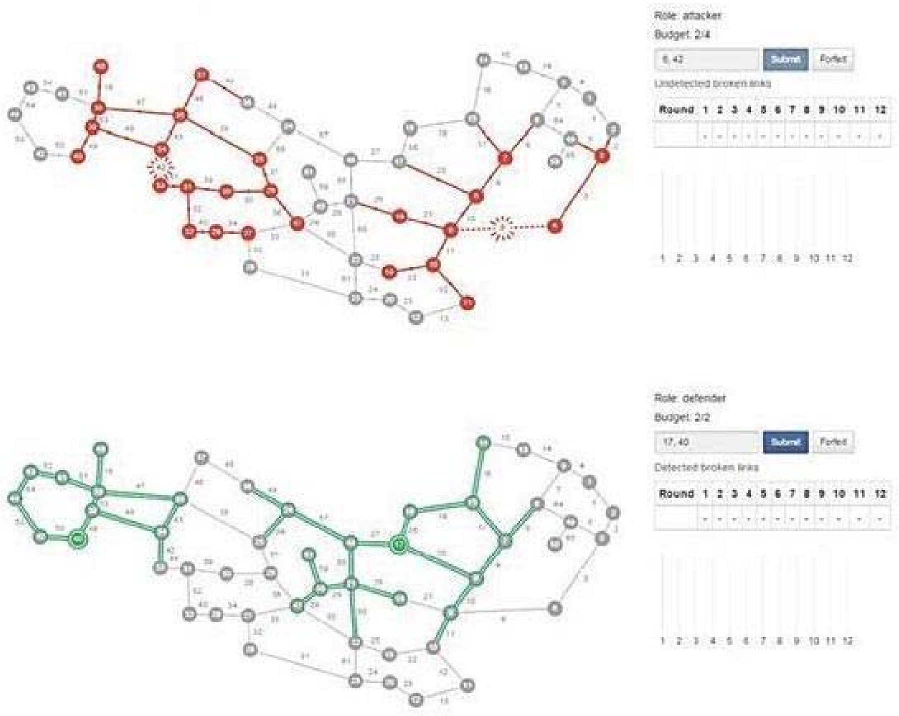
by Saurabh Amin, Massachusetts Institute of Technology

Our urban water systems are facing three major challenges: growing demand due to rapid urbanization, depleting water resources, and deteriorating water transmission and distribution networks. Water resources and systems also face threats of disruptions due to natural disasters, and more recently, to malicious cyber-physical attacks. Ensuring safe, clean, and reliable water supply to our cities requires exploring new opportunities and justifying investment in them. Chief among these are new water treatment and desalination plants, efficient and cost-effective design of water supply networks, and management of problems related to water quality and losses such as leaks and bursts. In the FORCES project, we are working on the deployment of modern technologies for monitoring and diagnostics, combined with better strategies for network control and demand management. Our objective is to design tools that significantly improve the operational efficiency of water systems and reduce the risks of service disruptions.

Random events such as leaks and bursts can lead to substantial water losses. If not addressed in a timely manner, they can lead to service disruptions, and even pose public health risks. Significant advancements have been reported in recent years on sensor networks for hydraulic and quality monitoring. Real-time data acquired from these sensor networks can enable “smart” capabilities such as better and cost-effective water treatment, leak detection, pump optimization, valve operation, and customer demand prediction. Successful deployments of sensor networks in real-world water systems have demonstrated the economic and environmental benefits of these capabilities.

In our recent work with the FORCES project, we have addressed a key challenge: how to optimally place and operate a small number of sensor nodes to achieve network-wide monitoring and diagnostics. Specifically, we are working on computational tools that can help extend the capabilities of sensor networks to both detect and localize a broad range of fault events in water system, and by executing timely rectification actions in response to the active faults. Network observability through sensor placement has been widely studied in the context of fault detection. However, sensor placement for fault isolation, i.e. the ability to distinguish between faults, has not been commonly sought after, especially in the context of water systems. Our algorithmic contribution achieves both detection and location identification of component failures in large-scale (~ 10,000 nodes) water networks using the minimum number of sensors.

Critical water system components such as main pipes, reservoirs, or treatment plants may fail due to a variety of reasons. We are working on vulnerability analysis, which is a crucial first-step towards improving the survivability of water systems during such “what-if” scenarios. Our goal is to obtain structural results that can be directly useful for network reinforcement and repair. Classical methods of vulnerability/risk analysis typically adopt a probabilistic approach, where the objective is to compute both the probability and impact of a class of failure scenarios. However, these estimates are often not meaningful or appropriate for planners and operators. We are using network interdiction models to develop a practically useful and computationally scalable approach to vulnerability analysis. In extending these models to water systems we model the costs due to loss of service and component failures, account for the nonlinearity between head-losses and flow in water networks, and include the possibility of both cyber and physical component interdictions.


Role: attacker

Budget: 2/4

6, 42

Undetected broken links

Round	1	2	3	4	5	6	7	8	9	10	11	12
	-	-	-	-	-	-	-	-	-	-	-	-

Role: defender

Budget: 2/2

17, 40

Detected broken links

Round	1	2	3	4	5	6	7	8	9	10	11	12
	-	-	-	-	-	-	-	-	-	-	-	-

Playing security games on infrastructure networks

Another challenge in vulnerability/risk analysis of water systems is to expand the classical methods to include security threats. In this regard, we are working on network monitoring games where the attacker disrupts one or more links, and the defender deploys sensing resources to detect adversary-induced link disruptions. Our goal is to find (randomized) sensing strategies subject to limitations on sensing range and resource constraints. We account for a general sensing model with heterogeneous range sensors, and obtain structural insights on the equilibrium strategies. Interestingly enough, our work also extends the earlier work that relied on (approximate) solutions of the set cover problem to environments where randomized sensing strategies are needed to defend against a strategic opponent.

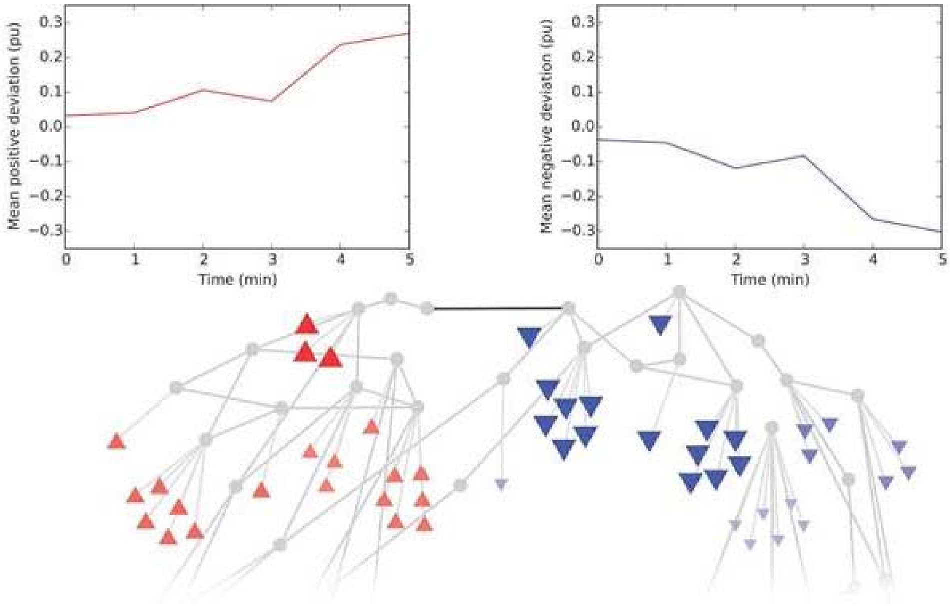
We believe that these developments can also help strengthen regulations on auditing and reporting losses from public water systems by providing more accurate and consistent estimates of the network state.

Ensuring Secure Electric Grids

by Ian Hiskens, University of Michigan

Access to reliable electricity is an important standard in many parts of the modern world. To provide this service, bulk electric transmission networks are typically built and operated to ensure that the loss of any single component will not disrupt the network's ability to operate. However, significant events such as widespread storms or an intelligent coordinated attack on various parts of the physical infrastructure can create situations where many components are simultaneously removed from the network. System operators must make critical decisions about how the physical network should be managed during these periods, with limited time to analyze the impact of control decisions on the future operation of the network.

In an effort to aid system operators during these precarious situations, FORCES researchers at the University of Michigan have been developing a control scheme which identifies, in real-time, optimal control actions for restoring the system to acceptable operation. Based on model predictive control (MPC), the controller adjusts the dispatch of controllable generation and energy storage, curtails renewables, and enacts demand response programs in order to satisfy transmission line temperature constraints and device capabilities over the subsequent 10 to 30 minute horizon. As an event continues to unfold across the network, MPC reruns periodically to determine and implement updated control actions.



Actions of the proposed control scheme showing generator response to an overloaded transmission line

Initial testing on realistic electric grids (up to 5000 nodes) suggests that the controller is capable of identifying control decisions that restore secure operation following large disturbances, with the chosen actions being minimally disruptive. Ongoing work is focused on extending modelling and control capabilities to incorporate voltage collapse events. Investigations are also considering ways of improving the network reduction algorithm that underpins large-scale applications.

Deploying Intrusion Detection Systems in Distributed Cyber Physical Systems

by Aron Laszka (University of California, Berkeley), Waseem Abbas (Vanderbilt University), S. Shankar Sastry(University of California, Berkeley), Yevgeniy Vorobeychik (Vanderbilt University), and Xenofon Koutsoukos (Vanderbilt University)

In recent years, we have seen a number of successful cyber-attacks against high-profile targets, which have demonstrated that resourceful and determined adversaries can penetrate even highly secure and isolated systems. In light of these attacks, it becomes apparent that the attack-resilience of a cyber-physical system depends on the defender's ability to detect and mitigate intrusions before they could cause significant damage. However, in anticipation of the defender's mitigation efforts, adversaries can mount stealthy attacks that aim to stay covert until damage is irreversible. To detect stealthy attacks, the defender can deploy an intrusion detection system (IDS). An IDS is a device or software that monitors a computer system for malicious activity, and when such activity is detected, it raises an alarm that can be investigated by the defender.

Unfortunately, practical intrusion detection systems are imperfect. On the one hand, they might raise a false alarm when there is no attack, which results in wasting resources on unnecessary investigations. On the other hand, they might fail to raise an alarm when there is an actual attack. Moreover, there is a tradeoff between false alarms and missed attacks: decreasing the sensitivity of an IDS decreases the number of false alarms but increases the probability of missing an attack, and vice versa. Consequently, the configuration of an IDS has to strike a balance between the cost of false alarms and losses due to missed attacks.

Configuration is a particularly challenging problem when intrusion detection systems are deployed on computer systems in a distributed CPS. Since these computer systems control the same physical processes, they are interdependent with respect to the damage that an adversary can cause by compromising them. Consequently, the configuration of each IDS must take into account not only the computer systems on which it is deployed, but the structure and configuration of the entire CPS. This challenge is further complicated by intelligent adversaries, who target a set of computer systems based on both the potential for causing damage and the probability of remaining undetected.

To address this challenge, our team of researchers proposed a game-theoretic model of stealthy attacks and intrusion detection in distributed systems. We showed that solving the game is computational hard, and we proposed a simulated-annealing based algorithm for finding an IDS configurations in practice. Finally, we evaluated the proposed algorithm numerically based on a real-world water-distribution network. Our numerical results show that the proposed algorithms significantly outperforms baseline configurations that do not take the structure of the system into account.

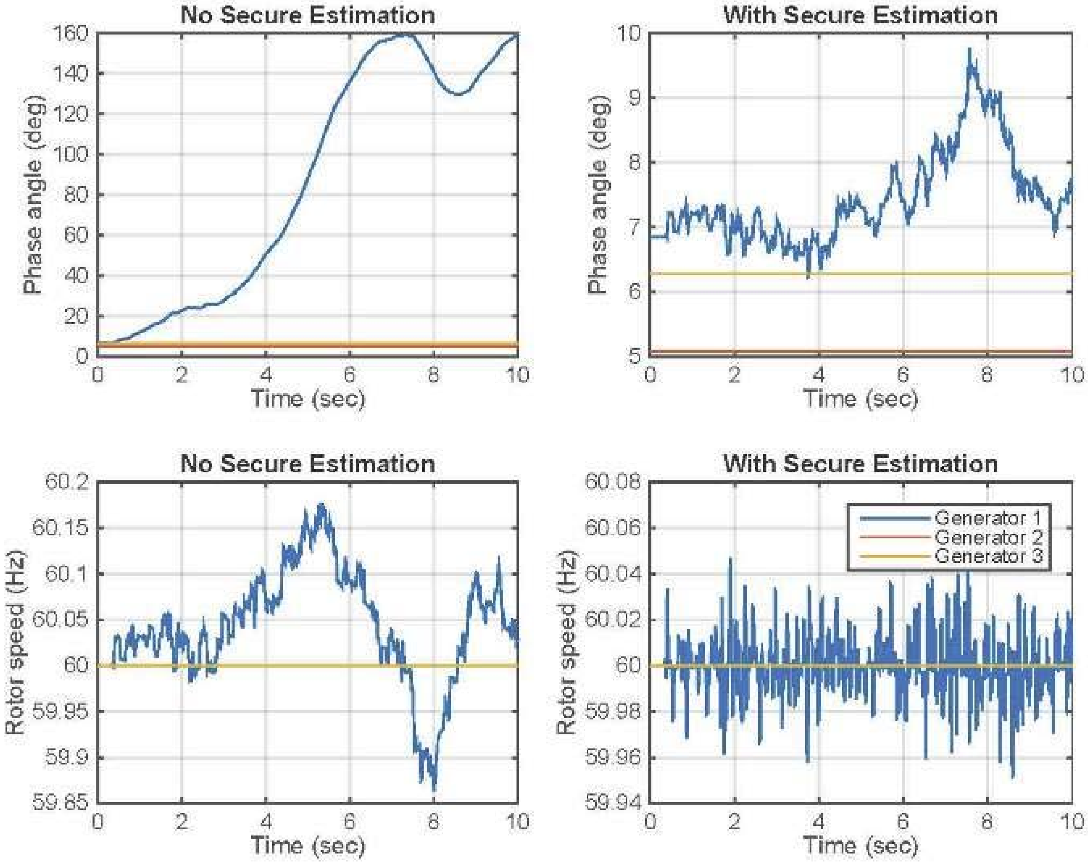
Secure State Estimation for Nonlinear Power Systems Under Cyber Attack

by Qie Hu (University of California, Berkeley), Dariush Fooladivanda (University of Toronto), Young Hwan Chang (Oregon Health and Science University), Claire J Tomlin (University of California, Berkeley)

Today’s critical infrastructures are mostly managed by cyber physical systems (CPS) that consist of several actuators, sensors, and controllers. Securing these systems against malicious attacks or communication failures is an important problem.

Extensive work has been done on secure estimation for linear dynamical systems, but none of them propose a secure state estimator for nonlinear systems as we do. Our group focuses on securely estimating the state of a nonlinear dynamical system from a set of corrupted measurements. In particular, our work focuses on two broad classes of nonlinear systems, and proposes a technique that enables us to transform the nonlinear dynamics into a set of linear equations. We then apply the classical error correction method to the equivalent linear system, and provide guarantees on the achievable state estimation error against arbitrary corruptions. For this research, we do not assume the sensor attacks or corruptions to follow any particular model. The only assumption concerning the corrupted sensors will be about the number of sensors that was corrupted due to attacks or failures. Our analytical results characterize the number of errors that can be perfectly corrected by an estimator.

In order to illustrate how the proposed nonlinear state estimation approach can be applied to practical systems, we consider an interconnected power system comprising several synchronous generators, transmission lines and energy storage units. We assume that all these physical devices are controlled via a wide area control systems (WACS) as well as local controllers which use the synchrophasor technology to maintain the system's stability. More specifically, several phasor measurement units (PMU) are installed at different generator buses in the power network. These PMUs are connected through a communication network, which sends PMU measurements, including rotors' speeds and generators' phase angles, to different controllers and the WACS in the system. However the communication channels in the network are not secured and subject to cyber attacks and failures.



Evolution of phase angle and rotor speed of generators, with and without secure estimation

We numerically demonstrate the effectiveness of the proposed state estimation algorithm using the New England power system comprising 10 generators and 39 buses. We show that when the network is subject to malicious attacks targeted at generator 1 and if no secure estimation-based protection was implemented, then the phase angle of generator 1 would deviate rapidly from its equilibrium value and would reach 159◦ within 7.3 sec. When the phase angle difference between two generators exceeds 90◦, the generators can potentially lose synchrony and trip. We can incorporate our proposed secure estimator such that the WACS performs secure state estimation to reconstruct the rotor angles and rotational speeds of the generators before using the received data for computing wide area control signals, and to monitor the operation of local controllers installed in the system. As a result, generator 1's phase angle is maintained close to its equilibrium value, even when it was under attack, and all possible system failures are prevented.

INDUSTRY NEWS

Threat-based Approaches for Cyber-Physical Resilience

by William Streilein and Hamed Okhravi, MIT Lincoln Laboratory

Increased interconnectivity of once isolated or air gapped cyber-physical and critical infrastructure systems has enabled new functionality, such as remote status monitoring and remote control in routine and emergency situations. This newfound connectivity, however, also exposes these systems to threats that were not anticipated in their design. Work is needed to understand how to deal with targeted cyber attacks by intelligent and capable adversaries that leverage this new connectivity.

A first step involves understanding and modeling the methods, capabilities, and goals of the adversary, in what is known as a "threat model", so that more effective defenses can be developed. Consider the case of Stuxnet, in which cyber attackers leveraged infected USB devices to inject malware into widely deployed programmable logic controllers (PLCs) in order to allegedly cause damage to nuclear centrifuges controlled by them [1]. If the defender had known more about the potential threat, defenses could have been created to protect the system. Knowing that USB devices were a possible threat vector, the defender could have disabled USB use to and from the isolated computer-controlled centrifuge networks. Similarly, knowledge that the malware might target the logic of the PLC as part of the attack could enable the defender to employ periodic software integrity checks on the PLC to ensure its proper function. The more that is understood about potential threats, the more resilient cyber-physical systems can be made.

As important as it is to understand the threat, it is equally important to be able to measure progress toward achieving resilience of these defended systems. Work is being done to develop metrics for enterprise systems [2], however, more research is needed to characterize risk to and recovery from attacks on cyber-physical systems by sophisticated cyber adversaries. Cyber modeling and simulation capabilities [3], including emulation and testbed experimentation [4] can be leveraged to explore the range of possible attack scenarios on cyber-physical systems and to quantify their effects.

[1] http://www.symantec.com/connect/blogs/exploring-stuxnet-s-plc-infection-process, Symantec. 23 2014

[2] Lippmann, R., Riordan, J., Yu, T., Watson, K., **Continuous Security Metrics for Prevalent Network Threats: Introduction and First Four Metrics**, Project Report IA-3, MIT Lincoln Laboratory, Lexington, MA, 22 May 2012.

[3] Wagner N., Lippmann R., Winterrose M., Riordan J., Yu T., and Streilein W., *Agent-based Simulation for Assessing Network Security Risk due to Unauthorized Hardware*, in **Proceedings of the 2015 ACM Spring Simulation Multi-Conference - Agent Directed Simulation Symposium**, Alexandria, VA, April, 2015.

[4] Hamed Okhravi, James Riordan, and Kevin Carter, "Quantitative Evaluation of Dynamic Platform Techniques as a Defensive Mechanism," Proceedings of the 17th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID), Sep 2014

This material is based upon work supported under Air Force Contract No. FA8721-05-C-0002 and/or FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the U.S. Air Force.

Upcoming Events

FORCES All Hands Meeting

June 9-10, 2016
Cambridge, MA

FORCES In the News

ASUMAN OZDAGLAR APPOINTED TO KEITHLEY PROFESSORSHIP

FORCES researcher Asu Ozdaglar at MIT has been appointed to the Joseph F. and Nancy P. Keithley Professorship in Electrical Engineering. The Keithley Chair was originally created as a career development chair, and in 1990 the chair was converted to a senior professorship.

“Professor Ozdaglar is a star in the research areas of optimization theory, economic and social networked systems, and game theory,” wrote Anantha P. Chandrakasan, the Vannevar Bush Professor of Electrical Engineering and Computer Science, in an email announcing the appointment. “She has made truly outstanding contributions related to interdisciplinary research, curriculum development and teaching, mentoring, and service."