FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

FORCES News

Winter 2015

The FORCES project is now in its third year and we've made great strides in research and focus since the program launched. This issue of the FORCES newsletter summarizes some recent findings from our university researchers while also including a perspective on the importance of the work of the FORCES program from one of our industry partners.

The FORCES group continues to be engaged in examining societal scale cyber-physical systems, including how incentives can change consumer behavior and improve our daily lives. As a group, we've developed a foundation for integrating resilient control algorithms with economic incentives schemes, looked at how infrastructure systems can work towards better design of mechanisms for efficient operation, and examined how emerging data markets can protect privacy and encourage greater resilience to failures and network-level attacks. Current studies are also exploring the potential for developing resilience in home energy systems, automotive and air traffic safety, as well as in other critical infrastructure systems, including water, oil, and gas delivery systems. A few of those projects are highlighted in this issue of our newsletter.

We're already looking ahead and considering how to refine our findings and increase reliability and preventive maintenance for systems being studied. Next steps for the FORCES group includes identifying and addressing new areas of vulnerabilities, increasing opportunities for collaboration, and advancing research from the lab to practice.

Thanks for taking time to read the FORCES newsletter and, 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

Denial of Service Attacks on Mobility as a Service System:

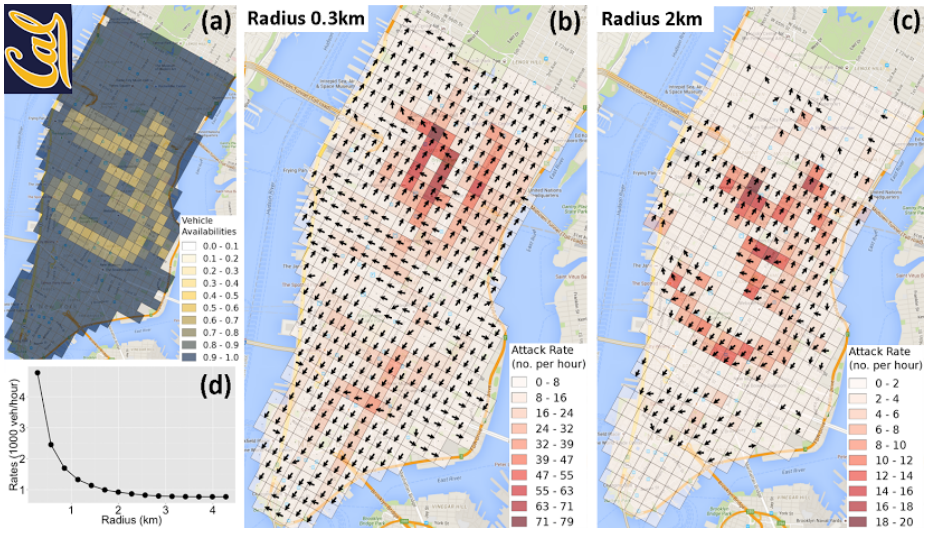
Analysis and Remediation

by Jerome Thai, Chenyang Yuan, and Alexandre Bayen

Mobility-as-a-Service (MaaS) systems such as ride-sharing services have expanded very quickly over the past years, while car ownership is dropping rapidly in cities. Uber has launched in more than 120 cities worldwide, Lyft operates in 60 cities, both taking millions of rides away from taxis everyday. This revolution in Personal Urban Mobility has the potential to fulfill the transportation needs in dense cities, which will count more than 3B urbanites by 2050. To achieve this, MaaS sytems will require optimal fleet size and dispatching, and experts agree that a fleet of 8,000 autonomous vehicles (70% of NY taxi fleet size) will be sufficient to satisfy taxi demand in Manhattan.

However, the popularity of MaaS systems make them increasingly vulnerable to Denial-of-Service (DoS) attacks, where attackers attempt to disrupt the system to make it unavailable to the customers. In fact, such attacks already exist and have been experienced by several MaaS companies at large scale. Between them, Uber and Lyft claim to have been forced to cancel thousands of rides, while hackers have gained access to a Jeep's internet-connected feature (Uconnect) to control it, suggesting that it is possible to control a fleet of 471,000 vehicles with Uconnect. Such cyber-attacks can have real-world physical consequences, and security breaches have already been exploited in several other transportation systems, ranging from controlling traffic lights to spoofing Waze.

Calibrating a queuing model for a MaaS system in Manhattan from 1B taxi rides, we dynamically simulated a system under attack and estimated the passenger loss under different scenarios, such as arbitrarily depleting taxis (see figure below) or maximizing the passenger loss.



A simulation of a traffic attack in progress

Combined with an economic model of supply and demand for attacks, we show that countermeasures raising the expected cost of attacks (such as increasing ride cancellation fees, higher level of security of the cyber components, and better fraud detection by law enforcement agencies) removes economical incentives for DoS attacks. We can see the benefits of this research not only in the analytical work which enabled the modeling and analysis work of the network, but also in the practical conclusions in terms of financial countermeasures to counteract the attacks.

Large-scale Networked Systems: Towards a Theory of Cyber-Security

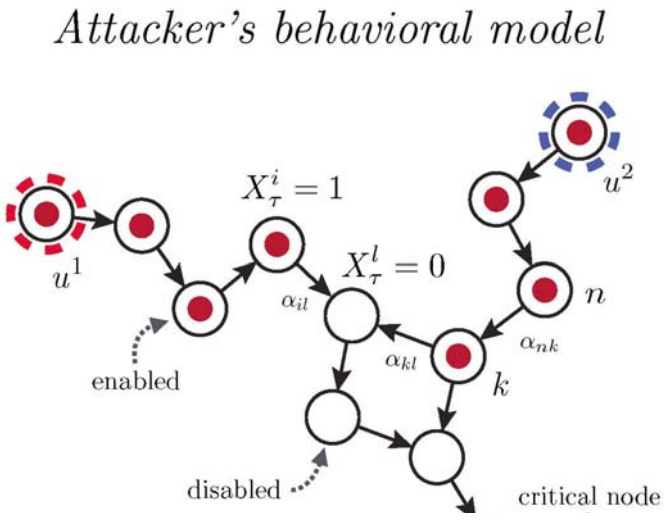
by Erik Miehling, Mohammad Rasouli, and Demosthenis Teneketzis

The increasing connectivity of networks and smart devices allows for greater efficiency and flexibility in the operation of complex networked systems. One instance of such complex networked systems is the power grid. The modernized power grid, commonly referred to as the smart grid, brings increased measurement, communication, and control functionality, in addition to distributed generation and demand response.

With the support of the FORCES program, researchers are working to design the necessary mechanisms in order to ensure that the increased capabilities of the smart grid translate into efficient operation. For deregulated energy market settings, researchers were able to design a pricing mechanism that ensures market participants (generation companies, distribution companies, and transmission companies) reach a Pareto efficient competitive equilibrium even in the presence of market nonlinearities and asymmetric information. In another problem, researchers have investigated the issue of generation expansion planning, which strives to determine the optimal long-term plan to adopt in order to ensure that society's future energy demands will be met. This problem is complicated by the changing, and highly unpredictable, technological, political, and economic landscape of the future. Researchers were able to design an allocation rule, termed a block mechanism, that ensured that strategic generation companies were incentivized to behave in a manner that results in a social-welfare maximizing future plan.

Unfortunately, the conveniences that arise due to the high connectivity of modern systems come at the cost of the introduction of multiple vulnerabilities in the network. Particularly concerning is that the operation of critical infrastructure services is becoming increasingly reliant upon (potentially insecure) networked devices, generating significant vulnerabilities in many systems, and consequently, in many areas of society.

Driven by these concerns, researchers are aiming to develop a formal methodology for cyber-security that is rich enough to model realistic security settings while scaling effectively. A behavioral model of the attacker is developed which allows the network operator to form a belief about the attacker's level of intrusion in the network, as seen in the figure below, and deploy the optimal countermeasure action.



Thanks to FORCES funding, the researchers have been able to not only design mechanisms that ensure efficient operation of large-scale networks, but also to develop theoretical tools for securing them. The current results have helped to identify obstacles in applying these tools to realistic problems, and consequently guide future research to overcome these obstacles.

A Testbed for Resilient and Secure Cyber-physical Systems

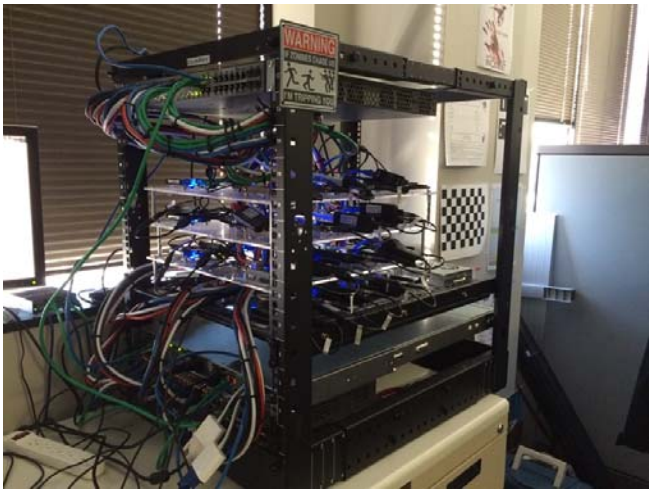
by William Emfinger, Pranav Srinivas Kumar, Gabor Karsai

Experimental evaluation of theoretical results is a requirement for good science and engineering, and research on Resilient Cyber-Physical Systems (RCPS) is no exception. We created an RCPS testbed as the foundational infrastructure for executing experiments with actual CPS computing hardware and software. A critical part of a CPS is the tight coupling and interaction with the physical world, so the integration of a high-fidelity, real-time physics simulation engine increases the fidelity of our experimental results with respect to the system we are analyzing. Another part of the CPS is the network used for communication among the computing needs – we use emulation for this purpose. The testbed also comes with a software tool-suite: the modeling, analysis, generation, deployment, and management tools we have developed drastically reduce the complexity and effort of CPS software development. This allows us to focus on the research experiments we want to run and the systems we want to analyze.

Resilient CPS Testbed

The RCPS testbed is composed of the following components:

- 32 embedded Linux computers (Beaglebone Black) with ARMv7L architecture;
- OpenFlow-capable smart gigabit network switch, which allows the network characteristics of the system to be enforced on all network traffic – thus emulating the performance of a network that connects the embedded controllers;
- Physics simulator, which allows the physical dynamics of the physical plant and its environment to be simulated along with the sensor data and actuator control. We have integrated the Orbiter Space Flight Simulator, the Kerbal Space Program simulator, SUMO (a traffic simulator), and are working on integrating Gridlab-D (a power grid simulator).
- Standard gigabit network switch, which allows a fast communication between the physics simulator and the nodes of the cluster; and
- Development host, for modeling, generation, development, deployment, and monitoring of the application code that runs on the controllers.



RCPS testbed

Summary

Using this testbed, we have shown how we can analyze the resilience of a system to realistic network attacks, such as Distributed Denial-of-Service (DDoS) attacks, e.g. attacking a traffic light control system in a road network. The effects produced in the physical simulation caused by this cyber-attack demonstrated the direct coupling of the cyber and physical aspects of the systems. This testbed allowed us to not only measure the software service degradation (with respect to missed control-loop deadlines) but also measure the degradation in the physical system's performance.

INDUSTRY NEWS

Secure Connectivity: A Case for IT and Cyber R&D on the Electric Grid

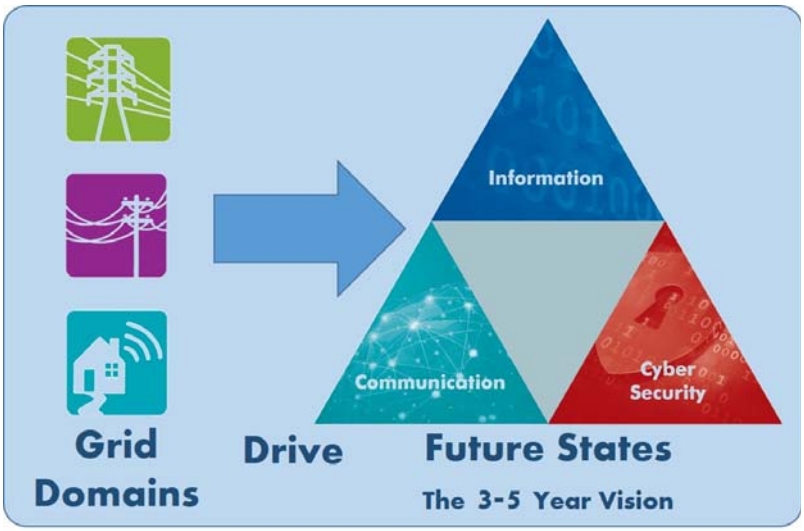
By Matt Wakefield, Director, ICCS, EPRI

Information, Communication, and Cyber Security (ICCS) technologies are necessary to maintain a secure, reliable, affordable and environmentally responsible electric grid. Secure connectivity can help the power system better integrate advanced digital functionality to become more flexible and resilient. As the existing power system adjusts to accommodate distributed energy resources such as renewable energy, energy storage, and demand response, its ability to also support lightning fast, two-way communications between the utility and customer, becomes ever more critical, so that all of these new technologies and new forms of energy can be used on the grid without causing strain or overload.

As we see more innovation at the edge of the grid and behind the meter, particularly driven by the growing penetration of solar photovoltaics, home and business energy management systems and sensors, and as telecommunication networks assume a more prevalent role in connecting consumers with the grid, continued industry collaboration with efforts such as FORCES are important to address the complex and emerging issues associated with grid modernization.

The Electric Power Research Institute (EPRI) recently completed a three-year ICCS R&D roadmap with industry stakeholders to identify ideal "future states" and needed

guidance on necessary action plans to help achieve those goals.



Challenges to overcome include the sheer volume of data; interfacing with proprietary systems; need for enhanced security; varying life-cycle timescales between utility assets and new connected devices; and effective integration into the power system. More than 20 “future states” were identified--relating to cyber security threat management, secure communications, incident response, security architecture, network management, interoperability, communications, enterprise architecture, and advanced metering.

Roadmaps, by their nature, are living documents--this roadmap will evolve. I invite the FORCES community to review this roadmap to inform the important work you are doing as well as provide feedback that will result in improved grid flexibility and resiliency.

NEWS AND EVENTS

Upcoming Events

Watch this space for additional details about these upcoming meetings:

FORCES All Hands Meeting
May - June 2016 (date and location TBD)

Celebrating 10 Years of CPS
Late summer 2016

Recent Events

IPAM Workshop
November 16 - 20, 2015

NSF CPS PI meeting
November 16- 17, 2015

FORCES NSF Review meeting
November 4-5, 2015

FORCES In the News

ENERGY INFRASTRUCTURE RESEARCH FINDS NEW SOURCE OF SUPPORT

A new collaborative project, the Siebel Energy Institute (SEI), has been established at UC Berkeley to accelerate advancements in the safety, security, and reliability of modern energy systems. The Institute builds on FORCES and other NSF-funded research in cyber-physical systems, and is focused on developing engineering and computer solutions to promote efficient management of the country's energy infrastructure and energy resources.

The Institute awards a small amount of funding to researchers at member institutions (eight universities worldwide) to help them develop ideas that they then submit as large grant requests to government agencies, including the

Department of Energy and the National Science Foundation. In the first round of grants, FORCES researchers at MIT and Berkeley received awards for projects that advance our understanding of vulnerabilities and sustainability of energy systems.
