FORCES
FOUNDATIONS OF RESILIENT CYBER-PHYSICAL SYSTEMS

Welcome to the FORCES Newsletter

Spring 2017

Welcome to the spring 2017 issue of the FORCES newsletter. In this issue we've drawn links between the current work of FORCES researchers and the National Science Foundation's interest in Smart and Connected Communities as an area of focus and support. As NSF observes, human communities are increasingly reliant on "smart" technology, leading to additional opportunities for advances in infrastructure management and other systems. FORCES researchers, of course, have been working on related issues for a number of years, examining advanced networking and connectivity, sensing, real-time data analytics, control, and automated decision-making. A good example of this is the article contributed by researchers at Berkeley, who describe how unmanned aerial systems traffic management can reduce conflicts by designating virtual pathways. I'm also pleased to share interesting advancements by FORCES researchers at Vanderbilt, Michigan, and MIT, who describe recent work in water networks, security, and air traffic, respectively.

Thanks very much for taking time to read the FORCES spring 2017 newsletter. Your feedback, comments, and suggestions are welcome.

Sincerely,

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

RESEARCH SPOTLIGHT

Unmanned Aerial Systems Traffic Management

by Mo Chen (University of California, Berkeley) and Claire Tomlin (University of California, Berkeley)

On air highways, each UAV operates according to a hybrid system model with "Free," "Leader," and "Follower" modes. Reachability-based controllers ensure the success and safety of mode transitions. The highway and platoon structure greatly reduces the chance of multiple conflicts, enabling the use of pairwise safety analysis. The hybrid system model is shown in Figure 2, and crazyflies following our proposed traffic protocol is shown in Figure 3.

In the unmanned aerial systems traffic management (UTM) project [1][2], we proposed a method for the placement of air highways, which are designated virtual pathways in the airspace that provide a scalable and intuitive way for managing a large number of unmanned aerial vehicles (UAVs) flying in civilian airspace. The method starts with a cost map encoding the desirability of flying in different parts of a region, and computes minimum-cost paths connecting origin and destinations. These paths can be updated in real-time according to changes in the airspace. Trunks and branches of air highways, similar to ground-based highway systems, naturally emerge. An example air highway network over the San Francisco Bay Area is shown in Figure 1.

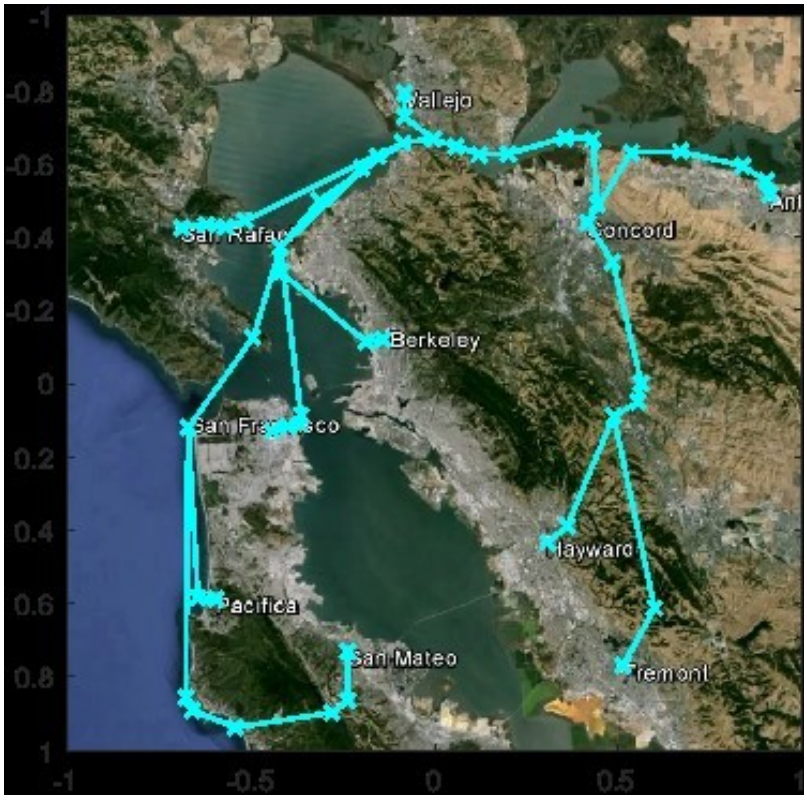

Figure 1

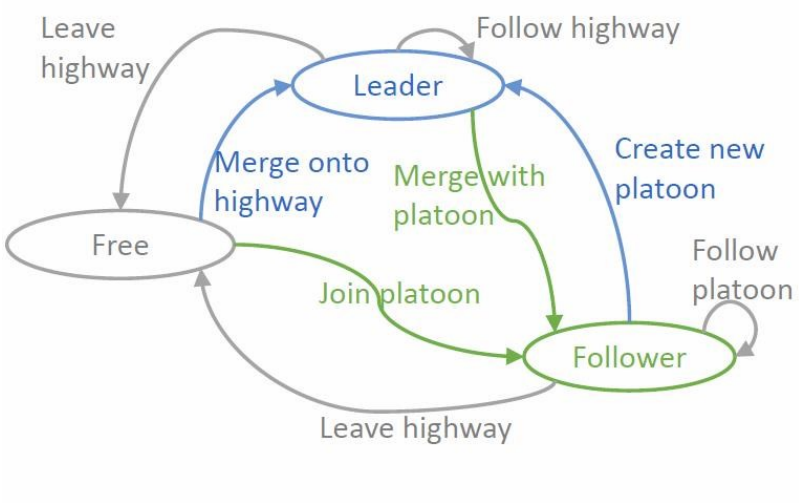

Figure 2

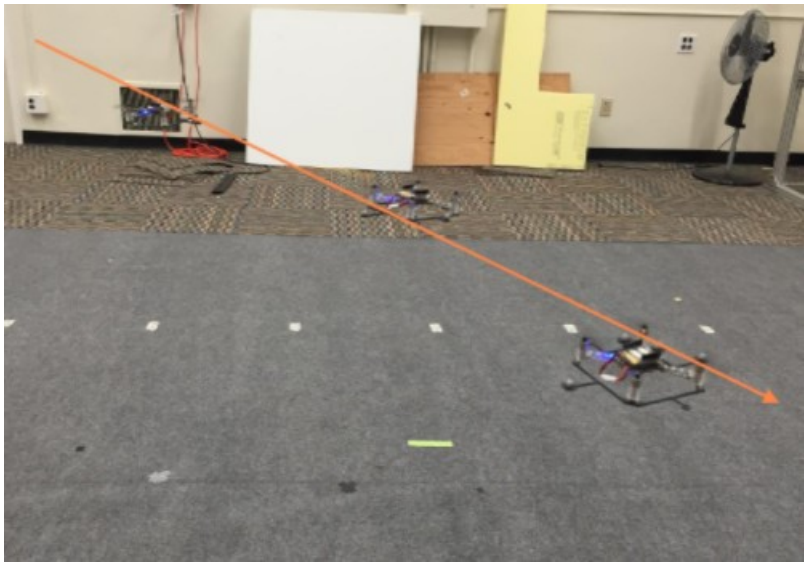

Figure 3

[1] Mo Chen, Qie Hu, Jaime F. Fisac, Kene Akametalu, Casey Mackin, Claire J. Tomlin, "Reachability-Based Safety and Liveness of Unmanned Aerial Vehicle Platoons on Air Highways," AIAA Journal of Guidance, Control, and Dynamics, 2017 (to appear).

[2] Mo Chen, Qie Hu, Casey Mackin, Jaime F. Fisac, Claire J. Tomlin, "Safe Platooning of Unmanned Aerial Vehicles via Reachability," IEEE Conference on Decision and Control, 2015.

Synergic Security for Smart Water Networks: Redundancy, Diversity, and Hardening

by Aron Laszka (Vanderbilt University), Waseem Abbas (Vanderbilt University), Yevgeniy Vorobeychik (Vanderbilt University), and Xenofon Koutsoukos (Vanderbilt University)

Smart water networks promise to provide great benefits to society in terms of efficiency and sustainability. For instance, smart water distribution and waste-water systems may facilitate conserving water, thereby reducing consumer costs and environmental impact at the same time. In a smart water network, physical processes, sensor devices, controllers, and actuators form a connected cyber-physical system. Unfortunately, enhanced capabilities and connectivity also have a downside: previously secluded infrastructure is now susceptible to cyber-attacks.

Cyber-attacks against cyber-physical systems can pose a severe threat to public safety and health. For instance, compromising systems that control the treatment and distribution of drinking water may allow adversaries to suppress warnings about contaminations or to decrease the quality of water. As evidenced by the recent water crisis in Flint, Michigan, measuring the quality of drinking water is of critical importance. Cyber-attacks can also have a devastating environmental impact. For example, in 2000, a disgruntled ex-employee launched a series of attacks against the SCADA system controlling sewage equipment in Maroochy Shire, Australia. As a result of these attacks, approximately 800,000 liters of raw sewage spilt out into local parks and rivers, killing marine life.

Considering the importance of the issue, there has been an increasing concern to develop tools and approaches for assessing vulnerabilities in water networks. In this

direction, the emphasis is on identifying components in water networks that could be exposed to cyber-physical attacks, as well as the types of attacks that could be carried out.

In our work, we consider three canonical approaches for improving the resilience of a smart water network against cyber-attacks: redundancy, diversity, and hardening. *Redundancy* means adding extra components to a system, which are not strictly necessary for achieving desired system functionality, thus increasing the cost of an attack or reducing its probability of success. In cyber-physical systems, an example of redundancy is the deployment of multiple sensors for monitoring the same physical processes. Further, redundancy can be implemented not only for components providing functionality, but also for security mechanisms. For example, multi-factor authentication methods grant a user access to a system only after the user's identity has been successfully verified by multiple authentication methods. The rationale behind redundancy is that an adversary needs to disable or circumvent multiple components to compromise a system, which can significantly decrease the success probability of an attack.

Components that are based on the same hardware or software implementation and that are configured the same way typically suffer from the same vulnerabilities. Consequently, if an adversary can automate the exploitation of vulnerabilities, it may compromise a multitude of components with relatively little effort. *Diversity* can prevent the adversary from compromising a large number of system components using the same vulnerability by means of employing multiple software or hardware implementations and diverse configurations for components that perform the same tasks. In practice, different implementations are typically susceptible to different vulnerabilities, which limits the number of components that the adversary may compromise using a single vulnerability.

Hardening means eliminating potential vulnerabilities from a component of the system. In a deterministic model, hardening increases the effort that an adversary needs to spend in order to find an exploitable vulnerability, while in a non-deterministic model, hardening decreases the probability of finding an exploitable vulnerability. A component can be hardened at multiple levels, ranging from hardware protection to software techniques. On the hardware level, employing tamper-resistant devices can prevent adversaries from mounting simple attacks based on physical access. On the software level, hardening approaches range from following secure-coding principles to setting up firewalls. Operators can also find and eliminate vulnerabilities by hiring security experts for penetration testing or by outsourcing vulnerability discovery through bug-bounty programs.

In this work, we've developed theoretical foundations for finding optimal combinations redundancy, hardening, and diversity in smart water networks. We've also introduced a model of cyber-physical contamination attacks and security investments into redundancy, diversity, and hardening. Based on this model, we performed a case study of a real-world water network using simulated contaminations, as illustrated in Figure 1. In the case study, we evaluated various combinations of the three approaches and compared them with each other. Additional details about the approach can be found in [1].

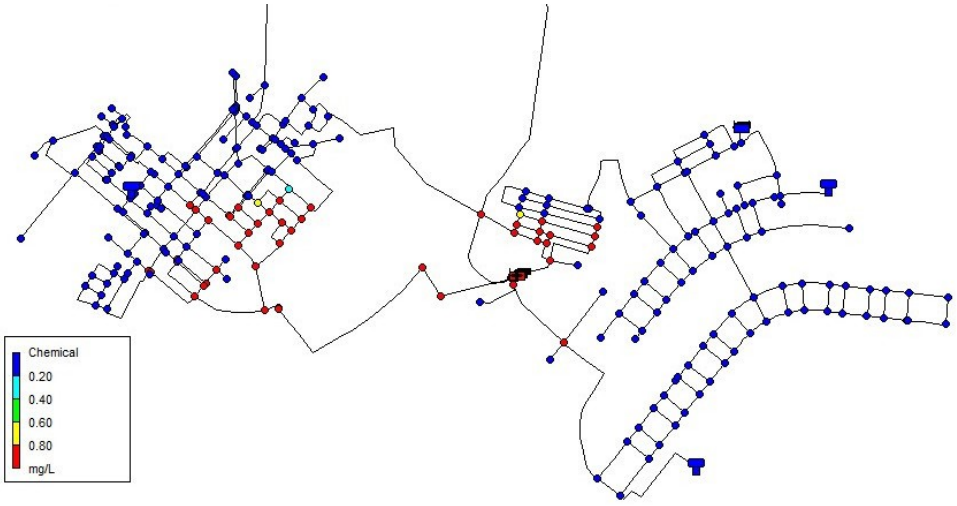

Figure 1. Water-distribution network. Colors show the spread of a chemical contaminant a reservoir two hours after its introduction. Simulations results obtained using EPANET.

[1] Aron Laszka, Waseem Abbas, Yevgeniy Vorobeychik, and Xenofon Koutsoukos. "Synergistic Security for Smart Water Networks: Redundancy, Diversity, and Hardening", 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks (CySWater 2017), Pittsburg, PA, April 21, 2017. To appear. Available at: http://aronlaszka.com/papers/laszka2017synergic.pdf

---

A Dynamic Incentive Mechanism for Security in Networks of Interdependent Agents

by Farzaneh Farhadi (University of Michigan), Hamidreza Tavafoghi (University of Michigan), Demosthenis Teneketzis (University of Michigan), and Jamal Golestani (Sharif University of Technology)

At the University of Michigan, FORCES researchers have been studying a dynamic mechanism design problem for a network of interdependent strategic agents with coupled dynamics. This work incorporates the idea of mechanism design as a framework for thinking about how object-oriented systems will behave when the information necessary to make decisions is dispersed and privately held. In contrast to existing impossibility results for static settings, researchers have presented a dynamic mechanism that is incentive compatible, individually rational, budget balanced, and social welfare maximizing. Researchers utilize the correlation among agents' states over time, and determine a set of inference signals for all agents that enable design of a set of incentive payments that internalize the effect of each agent on the overall network performance. Subsequently, each agent's objective is aligned with the social objective.

The benefit of this work is that real-world allocation problems are more commonly about allocating a limited resource to a network of strategic agents, where each agent's state is dynamic and affected by his interactions with his neighbors in the network. In such networks, information can be privately possessed by the strategic agents, and this may result in inefficiency in resource allocation decisions made by an uninformed decision maker. Dynamic incentive mechanisms, when properly designed, can lead to efficient and reliable allocations. The dynamic mechanism design approach has economic benefits for infrastructure management as it uses real-time analytics to enhance overall performance and responsiveness of networks, and can be used in various applications that include opinion dynamics in social networks, epidemics spreading in networks, dynamic adoption of new products and technologies over networks, and network security.

Delay Propagation in Air Traffic Networks

by Karthik Gopalakrishnan (MIT) and Hamsa Balakrishnan (MIT)

Large-scale infrastructures, such as transportation (air, rail, or ground), power, and communications systems, consist of interacting components, motivating the development of network models to represent them. Most prior work has relied on simplified models of these systems as undirected (and frequently, unweighted) graphs. However, in reality, these systems are large-scale, weighted, directed networks. The weights and the directionalities play an important role in governing the dynamics, and therefore, the behavior of these systems. They also reflect the asymmetries in the interactions between different elements in the system.

In our recent FORCES research, we have developed clustering algorithms for air traffic delay network data, in order to identify characteristic delay states (i.e., weighted directed graphs) as well as characteristic types-of-days (i.e., sequences of such weighted directed graphs). In addition to finding novel connections between traditional network-theoretic and control-theoretic properties of systems, our work generalizes network-theoretic properties such as the eigenvector centralities to weighted directed graphs, as illustrated in Figure 1.

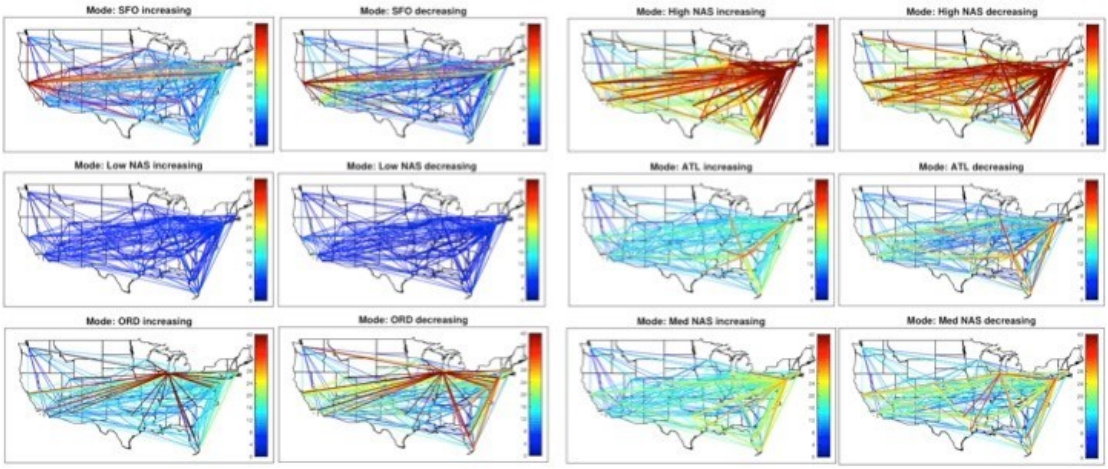

Figure 1. Visualizations of the adjacency matrices of the weighted, directed networks corresponding to the twelve discrete modes identified from 2011-2012 delay data. The links are colored by the average of the weights (median delay) in the two directions. The red links represent a median delay of 90 minutes.

Our analysis techniques yield stochastic switched linear system models of network dynamics that we have, for the first time, validated using real data. They provide methodologies for community detection, that is, the grouping of nodes (airports) based on their similarities. We have also shown that such representations of system state can help better predict future link delays. Most recently, we have shown that even for a 24-hour prediction horizon, our models predict link delays with a mean error of only 4.7 min, and airport delays with a mean error of 9.2 min.

This research promises to yield a set of tools for system diagnostics (for example, congestion or delays), analysis (for example, the relative vulnerability or resilience of different elements in the network), and control (for example, to mitigate the impacts of disruptions). Our initial work on deconstructing delay dynamics received a Best Paper Award at the International Conference for Research in Air Transportation (ICRAT) 2016 [2].

Our methodologies also present an opportunity to study complex multi-layer networks, enabling the analysis of interactions between different infrastructures (such as ground and air transportation). The approaches also open up new, exciting research problems on the optimal recovery of large-scale networks after disruptions such as natural disasters.

References

[1] J.J. Rebollo and H. Balakrishnan. "Characterization and Prediction of Air Traffic Delays," *Transportation Research Part C: Emerging Technologies*, Vol. 44, pp. 231-241, July 2014.

[2] K. Gopalakrishnan, H. Balakrishnan and R. Jordan. "Deconstructing Delay Dynamics: An Air Traffic Delay Example," International Conference on Research in Air Transportation (ICRAT), June 2016.

[3] K. Gopalakrishnan, H. Balakrishnan and R. Jordan. "Clusters and Communities in Air Traffic Delay Networks," American Control Conference, July 2016.

[4] K. Gopalakrishnan, H. Balakrishnan and R. Jordan. "Stability of Networked Systems with Switching Topologies," IEEE Conference on Decision and Control, December 2016.

[5] K. Gopalakrishnan and H. Balakrishnan. "A Comparative Analysis of Models for Predicting Delays in Air Traffic Networks," USA/Europe Air Traffic Management Seminar, under review, June 2017.

PROJECT NEWS

Upcoming Events

FORCES All Hands Meeting
Summer 2017
Date and location TBD