Stealthy Attacker Complexity in Cyber-Physical Systems: Milestone 1

https://c-er.github.io/15400/

Uday Shankar <us@cmu.edu>

Major Changes: There have been no significant changes to the goal of the project so far.

What I Have Accomplished So Far: Thus far, I have read through the paper I am basing my research off of[2] several times and have gotten a reasonable understanding of most of the theoretical framework for the synthesis of stealthy attacks. I have also supplemented this main paper with additional reading from other papers where some of these frameworks were initially developed[3]. Finally, currently I am reading through the first few chapters of a textbook[1] to build up background knowledge in the theory of supervisory control. As I am doing so, I am taking notes and building up a running example that makes concrete the concepts I have learned about thus far. If I am lucky, some of these examples may be of use in my actual research, when I have to look for small systems for which attacker complexity seems to be very high. However, I am not yet at the point where I can evaluate this effectively.

Meeting My Milestone: I think I've made some progress towards the first milestone I initially set, but I haven't met it. I had planned to complete all the necessary "background prep" before the spring semester started, but this hasn't happened yet. I think it's mainly due to lack of time put in. In the spring semester, I am dropping two time-consuming responsibilities I had this past fall (TAing and work for my student organization), so I hope I will have a lot more free time that I can dedicate towards research.

Surprises: The main surprise that I've had thus far is realizing how difficult it is to learn something from the ground up without a course to act as a guide. I plan to work around it just by spending more time reading and maybe setting my own deadlines so I don't procrastinate as much.

Revisions to my 15-400 Milestones: I think it's really important to maximize the time spend on actual research in the spring, but I don't think I have enough background knowledge to start yet. As a result, I will probably be pushing back my 15-400 milestones by 1-2 weeks to give me time to learn more. I will also be reading a bit during the break in order to make this initial period of learning as short as possible.

Resources Needed: All the resources I need are freely available online, and will be easy to procure when I need them.

References

[1] Cassandras, C. G., and Lafortune, S. *Introduction to Discrete Event Systems*, 2nd ed. Springer Publishing Company, Incorporated, 2010.

[2] Góes, R. M., Kang, E., Kwong, R., and Lafortune, S. Stealthy deception attacks for cyber-physical systems. *2017 IEEE 56th Annual Conference on Decision and Control (CDC)* (2017), 4224–4230.

[3] Yin, X., and Lafortune, S. A uniform approach for synthesizing property-enforcing supervisors for partially-observed discrete-event systems. *IEEE Transactions on Automatic Control 61* (2016), 2140–2154.