Stealthy Attacker Complexity in Cyber-Physical Systems: Milestone 2

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

Uday Shankar <us@cmu.edu>

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

What I Have Accomplished So Far: Thus far, I've completed my initial background knowledge acquisition, which included the first three chapters of this book[1] as well as two papers[3;4]. I have continued by brainstorming some potential measures of stealthy attacker complexity, but none of these have been very interesting yet, in that they are all easily handled by the framework proposed in the original paper[3].

Meeting My Milestone: Given that the goals for the first couple milestones are now somewhat reversed, I think I am almost meeting my milestones. If I had one interesting measure of complexity, I'd say I've met my milestone. There are some measures in the literature[2] that can potentially be applied here; I just had a busy weekend due to coursework and haven't had a chance to go through this paper properly yet.

Surprises: No big surprises so far. Having the reduced course load really helps with having time to spend on research.

Revisions to my 15-400 Milestones: The first goal in the original set of milestones was to come up with a bunch of examples where the synthesized attacker is intuitively complex. Unfortunately, this seems prohibitively hard to do, even for small examples, without the help of software. My advisor is currently waiting on a response from the co-authors of the stealthy attacker paper[3] to an email asking if they have software available; if not, I will be developing it. Because of this blocker, I am focusing on developing some potential notions of complexity before we have examples to test them out.

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] CURY, J. E. R., AND KROGH, B. H. Robustness of supervisors for discrete-event systems. *IEEE Transactions on Automatic Control 44*, 2 (Feb 1999), 376–379.

[3] 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.

[4] 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.