Stealthy Attacker Complexity in Cyber-Physical Systems: Milestone 4

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

Uday Shankar <us@cmu.edu>

Major Changes: There seems to have been a slight adjustment to the goal of the project. Instead of focusing on finding and proving lower bounds for attacker complexity, we're more focused on the related problem of trying to determine if attackers with restricted capabilities can carry out successful attacks.

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 [2;3]. I have continued by brainstorming some potential measures of stealthy attacker complexity. Some measures seem to be addressed by the framework from the original paper [2], but others seem to require some additional machinery. Currently, I am focused on formally defining the simpler notions of complexity and proving that they are handled by the framework from the original paper.

This status report is much the same as from two weeks ago, as I recently got access to the full-length version of the paper that made a lot of things clearer and uncovered some misconceptions I had. As a result, some of the ideas that I had for handling the simpler notions of complexity turned out to be incorrect. However, I do have some new ideas that seem promising and I think I should have them on paper before long.

Meeting My Milestone: Considering the roadblock I described above, I think I'm about one milestone behind right now. I think I need to work on research more frequently so that I can hit and resolve these roadblocks sooner.

Surprises: No big surprises so far.

Revisions to my 15-400 Milestones: As mentioned in the last report, my first few milestones are reversed, in the sense that I am brainstorming and working with potential measures of complexity before evaluating them on actual examples. I've now received the software to work with examples from the authors of the paper, which should make coming up with examples a lot easier.

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.