Resilient Control and Safety for Cyber-Physical Systems

Anna Lukina
and Radu Grosu
Cyber-Physical Systems Group
Technische Universität
Wien, Austria
Email: anna.lukina@tuwien.ac.at

Ashish Tiwari
Microsoft, USA

Scott A. Smolka
and Junxing Yang
Department of Computer Science
Stony Brook University
New York, USA

Lukas Esterle
Aston University
Birmingham, UK

***Abstract*—Many Cyber-Physical Systems (CPSs) comprise a multitude of computing entities that can collectively exhibit an *emergent behavior*. A compelling example of such a system is the *drone swarm*, which are beginning to see increasing application in battlefield surveillance and reconnaissance. The emergent behavior they exhibit is that of *flight formation*. A particularly interesting flight configuration is *V-formation*, especially for long-range missions. V-formation is emblematic of migratory birds such as Canada geese, where a bird flying in the *upwash region* of the bird in front of it can enjoy significant energy savings. In addition, the V-formation offers a *clear view* benefit, as no bird's field of vision is obstructed by another bird in the formation. Hence, it is important to quantify the resiliency of the control algorithms underlying this class of CPSs to various kinds of attacks. This question provides the motivation for the investigation put forth in this abstract and detailed in [4].**

I. Problem Statement and Summary of Results

V-formation games are two-player games, where the goal of the controller is to maneuver the plant (a simple model of flocking dynamics) into a V-formation, and the goal of the attacker is to prevent the controller from doing so. Controllers in V-formation games utilize a version of model-predictive control (MPC) we developed called *Adaptive-Horizon MPC* (AMPC), giving them the power, under certain controllability conditions, to attain V-formation with probability one. We define classes of attackers, including those that in one move can select a small number of victim agents and remove them from the flock or randomly displace them. We consider both *naive attackers*, whose strategies are purely probabilistic, and *AMPC-enabled attackers*, putting them on par strategically with the controller. The architecture of a V-formation game with an AMPC-enabled attacker is shown in Fig. 1. While a controller is expected to win every game with probability one, in practice, it is *resource-constrained*: its maximum prediction horizon and the maximum number of execution steps are fixed in advance. Under these conditions, an attacker has a much better chance of winning a V-formation game.

AMPC is a key contribution of the work presented in this abstract and in more detail in [4]. Traditional MPC uses a fixed *prediction horizon* to determine the optimal control action. The AMPC procedure chooses the prediction horizon dynamically. Thus, AMPC can adapt to the severity of the adversarial action played by choosing its own horizon accordingly. While the concept of MPC with an adaptive horizon has been investigated before [3], [1], our approach for choosing the prediction horizon based on the progress toward a fitness goal is novel, and has a more general appeal compared to previous work. Experimenting with different objectives, such as drone surveillance, and constraints, such as battery consumption, is future work.

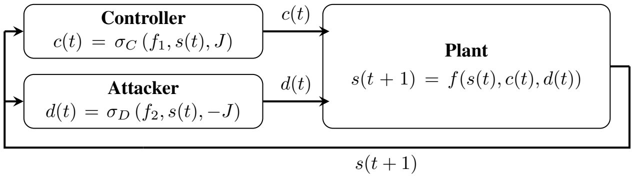
Controller
$c(t) = \sigma_C(f_1, s(t), J)$
Attacker
$d(t) = \sigma_D(f_2, s(t), -J)$
$c(t)$
$d(t)$
Plant
$s(t+1) = f(s(t), c(t), d(t))$
$s(t+1)$

Fig. 1. Controller-Attacker Game Architecture. The controller and the attacker use randomized strategies σ_C and σ_D to choose actions $c(t)$ and $d(t)$ based on dynamics, respectively, where $s(t)$ is the state at time t, and f is the dynamics of the plant model. The controller tries to minimize the cost J, while the attacker tries to maximize it.

Our evaluation of V-formation games uses statistical model checking [2] with $2 \cdot 10^3$ independent experiments to estimate the probability that an attacker can thwart the controller. Our results show that for the bird-removal game in Fig. 2 (on the diagonal of the left plot) with one bird being removed, the controller almost always wins (restores the flock to a V-formation). When two birds are removed, the outcome critically depends on the choice of birds (e.g., for removed birds 2 and 6 the success rate is 0.986). For the displacement game, our results again demonstrate that an intelligent attacker, i.e., the one using AMPC, outperforms its naive counterpart (who is randomly carrying out its attack) by over 0.9 probability. See Fig. 2 (right). Encouraged by these results, our future goal is to develop monitoring algorithms that can detect attacks of these types.

Acknowledgment

Research supported in part by the Doctoral Program Logical Methods in Computer Science and the Austrian National Research Network RiSE/SHiNE (S11412-N23) project funded by the Austrian Science Fund (FWF) project W1255-N23,

978-1-5386-6748-4/18/$31.00 ©2018 IEEE
DOI 10.1109/MT-CPS.2018.00015

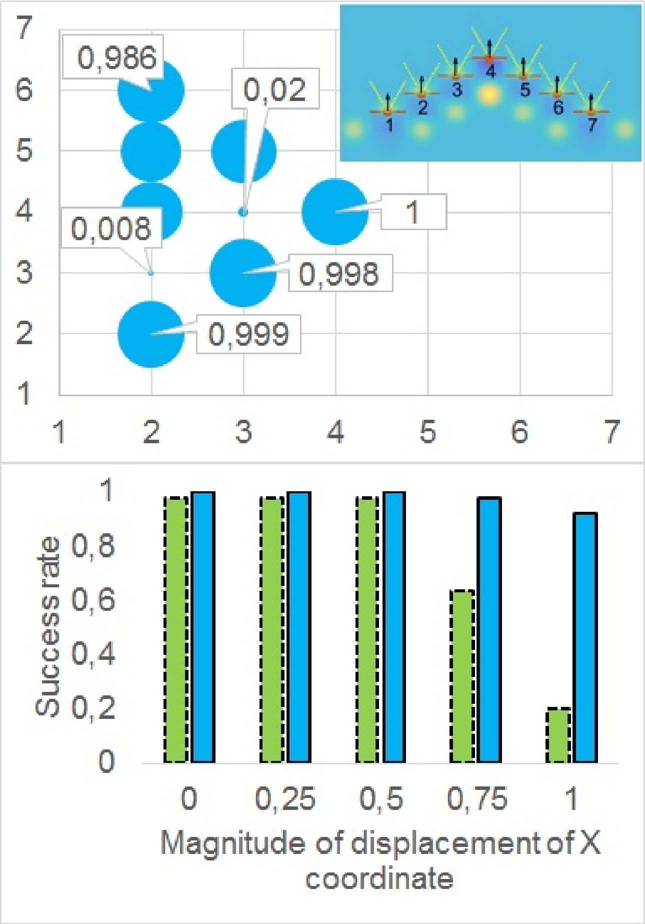

Fig. 2. Left: numbering of the birds in the upper right corner. Axis are the numbers of birds. Bubbles are the probabilities of success after removing birds in intersection. Right: The blue bars with solid outline are for the random displacement game and the green bars with dashed outline are for the AMPC-enabled attacker.

AFOSR Grant FA9550-14-1-0261 and NSF Grants CCF-1423296, CNS-1423298, IIS-1447549, CNS-1446832, CNS-1445770, CNS-1445770.

References

[1] Droge, G., Egerstedt, M.: Adaptive time horizon optimization in model predictive control. In: American Control Conference (ACC), 2011. pp. 1843-1848. IEEE (2011)

[2] Grosu, R., Peled, D., Ramakrishnan, C.R., Smolka, S.A., Stoller, S.D., Yang, J.: Using statistical model checking for measuring systems. In: Proceedings of the International Symposium Leveraging Applications of Formal Methods, Verification and Validation. LNCS, vol. 8803, pp. 223-238. Springer (2014)

[3] Krener, A.J.: Adaptive horizon model predictive control. arXiv preprint arXiv:1602.08619 (2016)

[4] Tiwari, A., Smolka, S.A., Esterle, L., Lukina, A., Yang, J., Grosu, R.: Attacking the V: on the resiliency of adaptive-horizon MPC. In: Automated Technology for Verification and Analysis - 15th International Symposium, ATVA 2017, Pune, India, October 3-6, 2017, Proceedings. Lecture Notes in Computer Science, vol. 10482, pp. 446-462. Springer (2017)