Resilient Multi-Robot Target Pursuit

Jiani Li, Waseem Abbas, Mudassir Shabbir, Xenofon Koutsoukos

[1]*Institute for Software Integrated Systems, Vanderbilt University, Nashville, TN*

Abstract This work studies the resilient distributed diffusion in multi-robot networks where robots, some of which might be adversarial, move in a cooperative manner to pursue some target. We consider a well-known adapt-then-combine diffusion algorithm whereby each non-adversarial robot computes its estimate about the target by optimizing a local cost function (adapt), and then aggregates the estimates received from neighbors (combine) that robot uses in optimizing the local cost function.

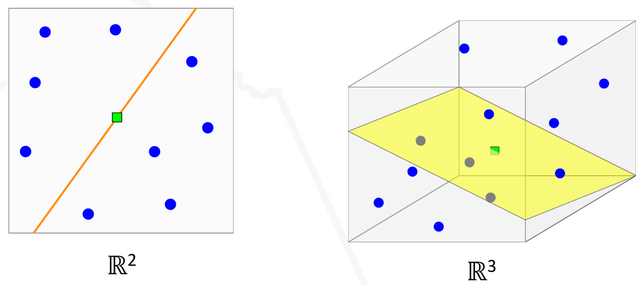
Problem The output of the aggregation step can be adversely impacted if a robot has Byzantine neighbors sending arbitrary estimates. Consequently, robot's estimate of the target can be far from the true value. Moreover, a robot cannot distinguish between normal and Byzantine neighbors. So, how can we design a resilient aggregation rule for diffusion?

Solution A robot aggregates by computing a *centerpoint* (generalization of median in higher dimensions) of its neighbors' estimates.

Main Result If each normal robot has at most $\left\lceil \frac{n}{d+1} \right\rceil - 1$ Byzantine neighbors, and normal robots use centerpoint-based aggregation in the diffusion algorithm, then they converge resiliently to the true target.

(*n* is the total neighbors, and *d* is the dimension of the state vector exchanged between robots.)

Centerpoint Given a set of n points in $\mathbb{R}^d$, a centerpoint is a point such that any hyperplane that goes through that point divides the set of points in two subsets, each of which contains at least $\lceil n/(d+1) \rceil$ of the points.



$\mathbb{R}^2$ $\mathbb{R}^3$

Adapt-then-Combine Diffusion

Unknown target: $w^o \in \mathbb{R}^d$

Streaming data: $\{d_k(i),\ u_{k,i}\} \qquad k = 1, 2, \ldots, N$

Agent k's estimate at time i: $w_{k,i}$

Adaptation: $\psi_{k,i} = w_{k,i-1} + \mu u^*_{k,i}[d_k(i) - u_{k,i} w_{k,i-1}]$

Combination: $w_{k,i} = \mathrm{Aggr}\left(\psi_{1,i}, \psi_{2,i}, \cdots, \psi_{|N_k|,i}\right)$

Experiments Carried out on Robotarium testbed at Georgia Tech.

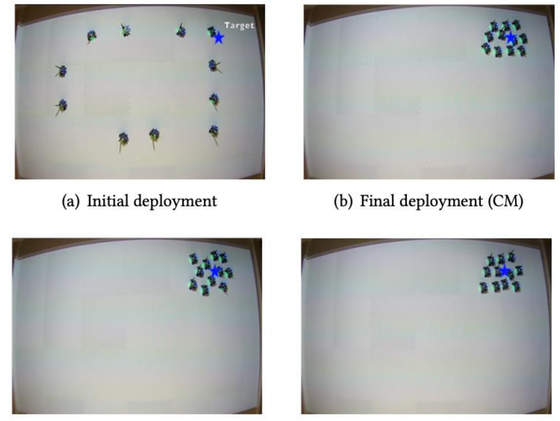
– Complete network – **11** normal robots – **5** Byzantine robots

Byzantine robots stayed stationary and continuously sent wrong estimates of the target location and velocity vector.

We compared aggregation rules based on:

- coordinate-median (CM),
- geometric median (GM),
- centerpoint.

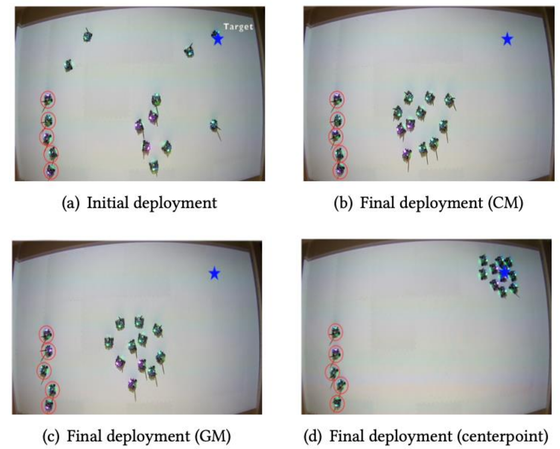
In the presence of Byzantine agents, only robots using the centerpoint-based diffusion converged to the target whereas the other rules failed.



(a) Initial deployment (b) Final deployment (CM)

(c) Final deployment (GM) (d) Final deployment (centerpoint)

Figure 1: Network deployment under no attack.



(a) Initial deployment (b) Final deployment (CM)

(c) Final deployment (GM) (d) Final deployment (centerpoint)

Figure 2: Network deployment with five Byzantine robots.

HOTSOS 2020
7TH ANNUAL
HOT TOPICS *in the* **SCIENCE OF SECURITY**
SEPTEMBER 22-23, 2020 | LAWRENCE, KANSAS