Resilient Multi-Robot Target Pursuit

Jiani Li
jiani.li@vanderbilt.edu
Institute for Software Integrated Systems
Vanderbilt University, Nashville, TN

Mudassir Shabbir
mudassir@rutgers.edu
Computer Science Department
Information Technology University, Lahore, Pakistan

Waseem Abbas
waseem.abbas@vanderbilt.edu
Institute for Software Integrated Systems
Vanderbilt University, Nashville, TN

Xenofon Koutsoukos
xenofon.koutsoukos@vanderbilt.edu
Institute for Software Integrated Systems
Vanderbilt University, Nashville, TN

ABSTRACT

We consider the problem of networked agents cooperating together to perform a task of optimizing the parameters of a global cost function. Agents receive linearly correlated noisy streaming data that can be used to learn the target parameters via Least-Mean-Squares (LMS) approaches. Diffusion scheme is incorporated such that at each step after agents adapt the parameters by the current received data, a combination step is included for agents to aggregate the information coming from its one-hop neighbors. It has been demonstrated that by introducing the aggregation step, diffusion algorithms greatly improve the learning accuracy of the parameters measured by the network Mean-Square-Deviation (MSD) [1].

However, the aggregation step is susceptible to attacks. In the presence of Byzantine agents, the aggregation of Byzantine information can easily disrupt the convergence of normal robots and even one Byzantine agent can drive its normal neighbors to converge to some point desired by the attacker [2]. To address this, we propose a resilient aggregation rule based on the notion of *centerpoint* [3, 4], which is a generalization of median in the higher dimensional Euclidean space. We show that if a normal robot implements the centerpoint based aggregation rule for distributed diffusion, then it can guarantee the aggregated result to lie inside the convex hull of its normal neighbors, given at most $\lceil \frac{n}{d+1} \rceil - 1$ neighbors are Byzantine with n total negihbors and d-dimensional state vectors exchanged among agents. Further, we demonstrate all normal robots implementing centerpoint based distributed diffusion converge resiliently to the true target state. In addition, we demonstrate that widely adopted aggregation rules such as coordinate-wise median [5] and geometric median [6] based are not resilient under certain conditions. The main reason is that unlike centerpoint based aggregation, these rules do not guarantee the aggregation result to be inside the convex hull of the states of normal agents. We carried out experiments on Robotarium, a multirobot testbed developed at the Georgia Institute of Technology to demonstrate the cases where diffusion with coordinate-wise median and geometric median based aggregation rules fail to converge to the true target state, whereas diffusion with centerpoint based rule resiliently converge to the true target state in the same scenario.

KEYWORDS

Resilient diffusion, multirobot target pursuit, centerpoint

1 SYSTEM MODEL

We use distributed diffusion algorithm for a mobile adaptive network [7] where N agents move in a cooperative manner to pursue a target located at $w^o \in \mathbb{R}^d$. The location of agent k at time i is denoted by $x_{k,i} \in \mathbb{R}^d$, and we can express the distance between agent k and target at time i as

$$d_k^o(i) = u_{k,i}^o(w^o - x_{k,i}), \tag{1}$$

where $u_{k,i}^o$ denotes the unit direction vector pointing from $x_{k,i}$ to w^o. We assume agents have only noisy observations $\{d_k(i), u_{k,i}\}$ of the distance and the unit direction vector, i.e.,

$$d_k(i) = d_k^o(i) + n_k^d(i), \qquad u_{k,i} = u_{k,i}^o + n_{k,i}^u, \tag{2}$$

where $n_{k,i}^u$ and $n_k^d(i)$ denote noise terms. Here, $d_k(i) \in \mathbb{R}$ and $u_{k,i} \in \mathbb{R}^d$. From (1) and (2), we have

$$d_k(i) = u_{k,i}(w^o - x_{k,i}) + n_k(i),$$

where $n_k(i) \triangleq -n_{k,i}^u(w^o - x_{k,i}) + n_k^d(i)$. Let $\hat{d}_k(i) \triangleq d_k(i) + u_{k,i}x_{k,i}$, then we can derive a linear model for variables $\{\hat{d}_k(i), u_{k,i}\}$ as

$$\hat{d}_k(i) = u_{k,i}w^o + n_k(i).$$

Two agents are neighbors if they exchange information with each other. At each iteration i, agent k knows its location $x_{k,i} \in \mathbb{R}^d$ and velocity $v_{k,i} \in \mathbb{R}^d$, and it can observe its neighbors' location $x_{l,i}$ for $l \in \mathcal{N}_k(i)$. Agents update the velocity according to the following update rule in order to move towards the unknown target:

$$v_{k,i+1} = \begin{cases} w_{k,i} - x_{k,i}, & \text{if } \|w_{k,i} - x_{k,i}\| \le s \\ s \cdot \frac{w_{k,i} - x_{k,i}}{\|w_{k,i} - x_{k,i}\|}, & \text{otherwise} \end{cases} \tag{3}$$

where $w_{k,i}$ is the estimate of the target location by k at time i, and the positive scaling factor s is used to bound the speed in pursuing the target.

Agents then update their location according to

$$x_{k,i+1} = x_{k,i} + \Delta t \cdot v_{k,i+1},$$

where Δt represents the time step.

To obtain velocity, agents need to know the estimate of the target location $w_{k,i}$, which should be the unique minimizer of the following cost function:

$$J^{glob}(w) = \sum_{k \in \mathcal{N}^+} \mathbb{E}\|\hat{d}_k(i) - u_{k,i}w\|^2,$$

where $\mathcal{N}^+$ denotes the set of normal agents in the network. Agents estimate the term by the diffusion algorithm and the adaptation and combination steps take the following form:

$$\psi_{k,i} = w_{k,i} + \mu u_{k,i}^*(\hat{d}_k(i) - u_{k,i}w_{k,i-1}),$$

$$w_{k,i} = \text{Aggr}^w(\psi_{1,i}, \psi_{2,i}, \ldots, \psi_{|\mathcal{N}_k|,i}), \qquad (4)$$

where μ is the step size, Aggr^w represents certain aggregation rule and $|\mathcal{N}_k|$ denotes the size of $\mathcal{N}_k$.

2 EXPERIMENTS

Experiments are carried out on Robotarium [8], a multirobot testbed developed at the Georgia Institute of Technology. The robots are 11 cm wide, 10 cm long, and operate on a 3m x 2m area. We denote the bottom-left corner of the arena to be the original point with coordinates $[0, 0]$ and the upper-right corner to be $[3, 2]$.

We evaluate the diffusion algorithm with three different aggregation rules, including coordinate-wise median (CM), geometric median (GM), and centerpoint based for the aggregation of $w_{k,i}$ in (4). We consider a network of 11 normal robots that remain fully connected throughout the simulation. Parameters are selected to be $s = 1, \Delta t = 1s$. The target location is set to be $w^o = [2.4, 1.7]$. The regression vector $u_{k,i}$ has uniform covariance matrix $R_{u,k} = \sigma_{u,k}^2 I_2$, $\sigma_{u,k}^2 \in [0.1, 0.5]$ where I_2 is the identity matrix of size 2. The noise variance of distance $\sigma_{d,k}^2 \in [0.5, 5.0]$. Both $\sigma_{d,k}^2$ and $\sigma_{u,k}^2$ decrease linearly as the distance to the target decreases. The step size $\mu = 0.2$. In the case of attack, 5 more Byzantine robots are introduced making the total number of robots to be 16. Since centerpoint based aggregation rule is resilient up to $\lceil \frac{16}{3} \rceil - 1 = 5$ Byzantine robots, we expect it to be resilient in the experiment.

Figure 1 and Figure 2 show the initial and final network deployments using CM/GM/centerpoint based diffusion without attack/with attack. The Byzantine robots are indicated by the red circle, and the target location is denoted by the blue star. Byzantine robots stay stationary throughout the experiment and continuously send wrong estimates of the target location $[0, 0]$ and velocity vector $[0, 0]$ to normal robots. We adopt the collision avoidance mechanism implemented by Robotarium and in our experiment, no collision has been recorded.

We find that without attacks, robots adopting diffusion with CM/GM/centerpoint aggregation all converge to the target. However, in the presence of Byzantine agents, only robots adopting the centerpoint based diffusion converge to the target. At the same time, robots implementing CM or GM based diffusion converge to somewhere in the middle of the arena, showing that centerpoint has better resilience properties than the other two rules under the same scenario.
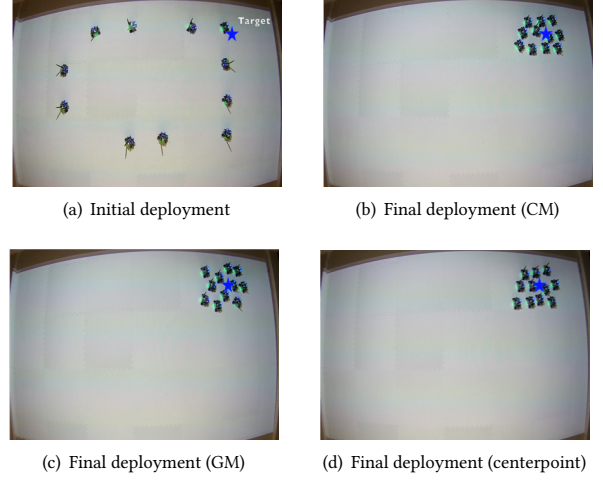

(a) Initial deployment   (b) Final deployment (CM)

(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)
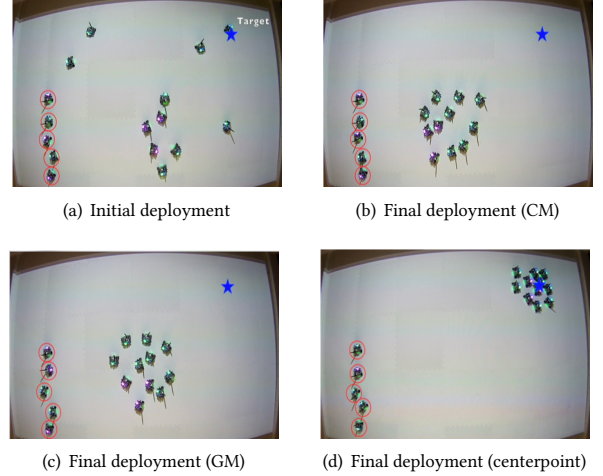
Figure 2: Network deployment with five Byzantine robots.

REFERENCES

[1] A. H. Sayed, S. Tu, J. Chen, X. Zhao, and Z. J. Towfic. Diffusion strategies for adaptation and learning over networks: An examination of distributed strategies and network behavior. *IEEE Signal Process. Mag.*, 30(3):155–171, 2013.

[2] J. Li, W. Abbas, and X. Koutsoukos. Resilient distributed diffusion in networks with adversaries. *IEEE Transactions on Signal and Information Processing over Networks*, 6:1–17, 2020.

[3] M. Shabbir, J. Li, W. Abbas, and X. Koutsoukos. Resilient vector consensus in multi-agent networks using centerpoints. In *the 2020 American Control Conference*, July, 2020.

[4] J. Li, W. Abbas, M. Shabbir, and X. Koutsoukos. Resilient distributed diffusion for multi-robot systems using centerpoint. In *Robotics: Science and Systems*, 2020.

[5] D. Yin, Y. Chen, K. Ramchandran, and P. L. Bartlett. Byzantine-robust distributed learning: Towards optimal statistical rates. In *Proceedings of the 35th International Conference on Machine Learning (ICML)*, pages 5636–5645, 2018.

[6] Y. Chen, L. Su, and J. Xu. Distributed statistical machine learning in adversarial settings: Byzantine gradient descent. *Proc. ACM Meas. Anal. Comput. Syst.*, 1(2):44:1–44:25, December 2017.

[7] S. Tu and A. H. Sayed. Mobile adaptive networks. *IEEE Journal of Selected Topics in Signal Processing*, 5(4):649–664, 2011.

[8] D. Pickem, P. Glotfelter, L. Wang, M. Mote, A. D. Ames, E. Feron, and M. Egerstedt. The robotarium: A remotely accessible swarm robotics research testbed. In *IEEE International Conference on Robotics and Automation (ICRA)*, pages 1699–1706, 2017.