Secure Rendezvous and Static Containment in Multi-Agent Systems with Adversarial Intruders

Matteo Santilli [a], Mauro Franceschelli [b*], Andrea Gasparri [a]

[a] *Department of Engineering, Roma Tre University, Rome, Italy.*

[b] *Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy.*

Abstract

In this paper we propose a novel distributed local interaction protocol for networks of multi-agent systems (MASs) in a multi-dimensional space under directed time-varying graph with the objective to achieve secure rendezvous or static containment within the convex hull of a set of leader agents. We consider the scenario where a set of anonymous adversarial agents may intrude the network (or may be hijacked by a cyber-attack) and show that the proposed strategy guarantees the achievement of the global objective despite the continued influence of the adversaries which can not be detected nor identified by the collaborative agents. We characterize the convergence properties of the proposed protocol in terms of the characteristics of the underlying network topology of the multi-agent system. Numerical simulations and examples corroborate the theoretical results.

Key words: Multi-agent systems; Resilient control; Secure Rendezvous; Secure Containment.

1 Introduction

Large scale networks or swarms of mobile agents, such as autonomous vehicles, are envisioned to play a role in future civilian and military applications (Macwan et al. (2015), Liu and Foina (2016)).

One of the fundamental open problems in the design of distributed coordination algorithms for large scale autonomous teams is the resiliency of the control protocols with respect to the unexpected behavior of team members when faults or cyber-physical attacks occur.

While there is strength in numbers, there is also an increased probability of faults and opportunity for cyber-attacks against single agents, members of the network. Current coordination protocols developed to enable the functioning of the group of agents by exploiting only local information and limited sensing are developed under the assumption that all agents execute the same nominal protocol, thus even one among thousands of agents which does not execute the prescribed nominal control protocol is able to disrupt the emerging behavior of most coordination algorithms based on consensus protocols. Given the multiple applications that utilize these kind of coordination protocols, research on resiliency and robustness against such adversities has gained a lot of interest in recent years.

In this paper we aim to overcome this vulnerability by proposing a secure strategy for multi-dimensional rendezvous (consensus) and static containment of the MAS within a specified area defined by a set of agents of the network. The proposed control strategy is secure, under proper topological conditions of the underlying directed time-varying graph, against the presence of adversarial agents assumed to be members of the network who either i) have been affected by a cyber-physical attack and are thus remotely controlled by a third party or ii) have suffered a fault that made them unable to execute the nominal prescribed control protocol. Notably, the proposed protocol exploits only local sensing of relative positions of neighboring agents with respect to their own reference frame in a multi-dimensional space.

⋆ Mauro Franceschelli is the corresponding author.

Email addresses: matteo.santilli@uniroma3.it (Matteo Santilli), mauro.franceschelli@unica.it (Mauro Franceschelli), gasparri@dia.uniroma3.it (Andrea Gasparri).

[1] This work was supported partially by the Fondazione di Sardegna with grant "Formal Methods and Technologies for the Future of Energy Systems", n. F72F20000350007, call 2019, and partially by the European Commission under the grant agreement number 101016906 – Project CANOPIES.

1.1 Literature Review

In the past decades distributed cooperative control and in particular the consensus problem, i.e., the problem of designing a local interaction protocol in order to reach a common agreement among the agents of a network, has attracted much interest as in Chen et al. (2011), Cao and Ren (2014), Franceschelli et al. (2015), Franceschelli et al. (2017), Cortés (2006), Chen et al. (2012), and Wang and Xiao (2010). Given the development of cyber-physical systems (Pasqualetti et al. (2013), Sridhar et al. (2012), Khaitan and McCalley (2015), Mo and Sinopoli (2016)), over the last decade people have shifted their efforts to enhance the physical and cyber security of MASs. One of the problems that has attracted recent attention is the resilient consensus problem, i.e., the problem of designing a local update law to reach consensus over a network in the presence of adversarial or faulty agents, with recent examples as Zhang and Sundaram (2012), Leblanc et al. (2013), Wu et al. (2020), Wang and Ishii (2020), and Abbas et al. (2018). In these works, as well as in the rest of the literature, the resilient consensus and the adversarial agents are often referred to with different names. One of the keyword that is often used as a synonym for resilient and that we use throughout the rest of the paper is *secure*. Synonyms for adversarial agents are instead adversaries, intruders, attackers, malicious agents, and misbehaving nodes. In this work we mainly refer to them using the adjective *adversarial*.

In this context the first significant results are Zhang and Sundaram (2012), and Leblanc et al. (2013) where the authors introduced a topological property known as *robustness* in order to enhance the resiliency of the network to adversarial nodes and provided a distributed robust protocol to achieve consensus when a bound on the number of adversarial agents in the network is known. Said topological property is able to capture the idea of redundancy of information in a network in a better way than the previously used notions of connectivity and minimum degree of a graph. Depending on the locality of the bound on the number of adversarial agents in the network, i.e., if it is local only to the neighborhood of the agents or if it is global with respect to the whole network, two different models have been considered: the *F-local* model which assumes that each single agent can be influenced at maximum by F malicious agents in its own neighborhood, and the *F-total* model which assumes that there are at maximum F malicious agents in the whole network. Given a topology condition of the network related to the considered model, the proposed distributed algorithm, known as *Weighted-Mean-Subsequence-Reduced* (*W-MSR*), discards part of the data collected from the neighborhood that could have been compromised by the adversarial agents and it is capable of guaranteeing the resilient consensus in a one-dimensional space independently from the considered model.

The W-MSR algorithm became very popular within the secure control community and inspired a lot of works such as Sundaram and Gharesifard (2019), Shang (2020), Liu et al. (2018), Wu and He (2017), Dibaji and Ishii (2017), Yiğit Öksüz and Akar (2018), Usevitch and Panagou (2017), Usevitch and Panagou (2020), and Leblanc and Koutsoukos (2018). For example, Shang (2020) adapted the W-MSR algorithm in order to achieve resilient consensus for an hybrid multi-agent system composed of both continuous time and discrete time dynamical agents. Liu et al. (2018) addressed the problem of bipartite consensus under the F-local and F-total model attack extending the W-MSR algorithm to consider the absolute value of the neighbors giving rise to the AW-MSR (Absolute W-MSR) algorithm. In addition upon considering the delay factor that natural information transmission could have, Wu and He (2017) improved the W-MSR to achieve consensus even under delayed transmissions whereas Dibaji and Ishii (2017) slightly modified the base algorithm in order to work with agents whose dynamics are described by a double integrator law.

All the works mentioned above, however, are one-dimensional, meaning that the state of agents evolves in $\mathbb{R}$; on the contrary, under the same topological assumptions, our work allows to achieve a secure rendezvous in a multi-dimensional space.

Works that achieve resilient objectives in multi-dimensional space such as consensus (Leblanc and Koutsoukos (2018)), flocking (Saulnier et al. (2017)), formation control and leader tracking (Usevitch et al. (2018), Zegers et al. (2021)) exist but propose results based either on separating the position coordinates or using a norm-based version of the W-MSR algorithm, which both require the presence of common reference frames or the access to the absolute positions of the agents (GPS).

A different approach to the secure consensus problem consists in adopting the so called secure localization approach (Liu et al. (2008), Lazos and Poovendran (2005)) in which the agents try to detect the adversarial agents in order to fulfill the global objective isolating such agents. Notable examples of this approach can be found in Quan et al. (2017), Boem et al. (2017) where the authors developed local state observers to estimate the presence of adversarial agents or faults in the network. These methods, however, rely on communication among the agents and presence of common reference frames. In our context, on the contrary, the agents are anonymous and their interactions are sensing-based. Furthermore, our work does not require the presence of a common reference frame shared among the agents.

The containment problem consist in designing a local interaction rule in order to let a set of agents, namely

the cooperative agents, enter and then remain within an area defined by another set of agents, namely the leaders (Ji et al. (2008), Cao et al. (2012), Xiao et al. (2019), Fu et al. (2019), Mu and Liu (2016)). In Ji et al. (2008) the authors proposed hybrid control schemes based on stop-go rules in order to ensure that the cooperative agents remain in the convex polytope spanned by both the leaders and the cooperative agents. Cao et al. (2012) provided necessary and sufficient conditions to achieve the containment problem in the convex hull of the leaders for both stationary and dynamic leaders under fixed and switching topology. In addition, in Xiao et al. (2019) the authors developed a distributed algorithm for heterogeneous multi-agent systems whose dynamics change on successive time intervals, able to asymptotically achieve containment under the hypothesis of a directed path from each follower to at least a leader.

To the best of the authors' knowledge, there is no prior work that has addressed directly the secure containment problem. Resilient distributed optimization frameworks could theoretically encode it but this would be either constrained to a one-dimensional space (Sundaram and Gharesifard (2019)) or require the presence of a common reference frame (Kuwaranancharoen et al. (2020)) whereas our work consider a multi-dimensional space with no requirement on shared common coordinate systems. Under the assumption of a common reference frame and measurements for bearing angles in Santilli et al. (2019) and Santilli et al. (2022) we proposed a distributed control protocol based on bearing angles measurements capable of achieving secure containment within the hypercube of the leaders. In this work we remove the assumption on the common reference frame and we improve the description of the containment region, which in this case is the convex hull of the positions of the leaders, rather than the hypercube.

1.2 Main Contribution

In this paper we propose a distributed control protocol for multi-dimensional MASs described by directed time-varying graphs which is secure against the influence of a finite set of anonymous adversarial agents.

The objective of the MAS is to perform rendezvous or containment within a given area while the adversarial agents have the objective to either stop the convergence to a common position or to make the collaborative agents get out of their containment area. We characterize the convergence properties of the proposed algorithm and provide a sufficient theoretical condition on the robustness of the underlying directed time-varying graph under which the algorithm is secure against the existence of up to F adversarial agents in each neighborhood of the agents (F-local model). The proposed control strategy can be computed by using local information on the neighborhood of the agents thus making the cooperative framework completely distributed and scalable. The adversarial agents are assumed to benefit from unbounded control actions and knowledge of the full network state.

To the best of the authors' knowledge this is the first work to achieve secure rendezvous and secure containment in a multi-dimensional environment without requiring access to global position (GPS) or common reference frames.

1.3 Structure of the paper

The rest of the paper is structured as follows. In Section 2, preliminary results concerning graph theory and topology definitions along with the introduction of notions that are used in the rest of the paper are provided. In Section 3, the problem setting of our work and the model of the agents are described. In Section 4, the proposed secure distributed protocol is discussed. In Section 5, the theoretical analysis of the proposed distributed algorithm is carried out. In Section 6, the results of numerical validation are described. Finally, in Section 7, the conclusion is drawn and future work is discussed.

2 Preliminaries

In this section we review and introduce notions about graph theory and notation that we adopt in the rest of the paper.

A set K in a vector space $\mathcal{X} \subseteq \mathbb{R}^d$ is called *convex*, if for every $x, y \in K$ and every $\alpha \in [0,1]$, the point $(1-\alpha)\,x + \alpha\,y \in K$. The *convex hull* of K, denoted $\mathrm{co}\,(K)$, is the smallest set containing K. We denote by $\partial\,\mathrm{co}\,(K)$ the border of the convex hull $\mathrm{co}\,(K)$ and by $\Omega\,\mathrm{co}\,(K)$ the set of its vertices.

Consider a non-self-intersecting closed polygon P in $\mathbb{R}^d$, we define the mean of all the points of P the *centroid* of the polygon P to which we refer as $\mathsf{C}(\mathsf{P}) \in \mathbb{R}^d$ (Protter and Morrey (1977)). In addition, we denote with $\mathbb{R}_{\geq 0}$ the set of non negative real numbers and with $|S|$ the cardinality of the set S. The term $\binom{a}{b}$ with $a \geq b \geq 0$ denotes the binomial coefficient, that is all the possible ways to select an unordered subset of a elements from a set of b elements and it is computed as $\frac{a!}{b!(a-b)!}$.

Let us introduce the definition of a lexicographic order, that is a relationship between pairs of elements of a set S such that $\forall (x,y),(z,w) \in S$, $(x,y) < (z,w)$ holds only if either $x < z$ is verified or both $x = z$ and $y < w$ are verified.

Let $\mathcal{G}(t) = (\mathcal{V}, \mathcal{E}(t))$ be a directed time-varying graph, where $\mathcal{V} = \{1, \ldots, n\}$ is the set of nodes representing

agents and $\mathcal{E}(t) \subseteq \{\mathcal{V} \times \mathcal{V}\}$ is the set of edges representing their ability to sense their relative position. Let $(j,i) \in \mathcal{E}(t)$ be the edge joining the agents j and i meaning that agent i can receive information from agent j at time t, i.e., agent i can sense agent j at time t. We denote by $\mathcal{N}_i(t) = \{j \in \mathcal{V} : (j,i) \in \mathcal{E}(t)\}$ the set of neighbors of agent i. Moreover, let $\overline{\mathcal{N}}_i(t) = \mathcal{N}_i(t) \cup \{i\}$ be the set of the extended neighbors of the agent i, i.e., its neighbors plus itself.

A directed path $p_{ij} = \{(i,r),(r,k),\ldots,(s,t),(t,j)\}$ between node i and j in a graph $\mathcal{G}$ is a sequence of consecutive edges, all with same direction, which starts from node i and ends with node j. A directed graph is said to be *strongly connected* if there exists a directed path between any pair of nodes. A graph possess a rooted spanning tree if there exists a node, called root, that is able to reach every other node by a directed path starting from the root.

We now report the notions of reachability and robustness for directed graphs introduced in Zhang and Sundaram (2012).

Definition 1 (r-reachable set) *Consider a directed graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ with node set $\mathcal{V}$, edge set $\mathcal{E}$ and a nonempty node subset $\mathcal{S} \subset \mathcal{V}$. We say that $\mathcal{S}$ is an* r-reachable *set if $\exists i \in \mathcal{S}$ such that $|\mathcal{N}_i \setminus \mathcal{S}| \geq r$, where $r \in \mathbb{Z}_{\geq 0}$.*

Basically, a subset of nodes $\mathcal{S} \subset \mathcal{V}$ is r-reachable according to Definition 1 if there exists at least one node in set $\mathcal{S}$ with at least r neighbors outside set $\mathcal{S}$. The next definition makes use of the concept of r-reachability to define the so-called r-robust graph.

Definition 2 (r-robust graph) *Consider a directed graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ with node set $\mathcal{V}$ and edge set $\mathcal{E}$. We say that $\mathcal{G}$ is* r-robust *if for all pairs of nonempty, disjoint subsets $\mathcal{S}_1, \mathcal{S}_2 \subset \mathcal{V}$, at least one of $\mathcal{S}_1$ or $\mathcal{S}_2$ is r-reachable, where $r \in \mathbb{Z}_{\geq 0}$.*

From Definition 2 it follows that in a r-robust graph there is always a subset of nodes $\mathcal{S}$ with a least one of them that has at least r neighbors outside $\mathcal{S}$. Moreover, a graph is r-robust if and only if it contains a rooted spanning tree (Leblanc et al. (2013)). To conclude this section we report a variation of the concept of r-robustness, known as strong r-robustness.

Definition 3 (strongly r-robust graph) *Consider a directed graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ with node set $\mathcal{V}$ and edge set $\mathcal{E}$. We say that $\mathcal{G}$ is* strongly r-robust *if for any subset $\mathcal{S} \subset \mathcal{V}$, either $\mathcal{S}$ is r-reachable or there exists a node $i \in \mathcal{S}$ such that $\mathcal{V} \setminus \mathcal{S} \subseteq \mathcal{N}_i$ where $r \in \mathbb{Z}_{\geq 0}$.*

The difference between Definition 2 and Definition 3 is that while the former requires one of the two subset of nodes to satisfy the r-reachability property, the latter requires *every* subset to be r-reachable, or to have at least a node that is connected to every node outside the set. Clearly strong r-robustness implies r-robustness while the inverse is generally not true. A strongly r-robust graph is also strongly connected. Furthermore, in a strongly r-robust graph, as well as in a r-robust graph, each node has at least r neighbors. The reader is referred to Zhang and Sundaram (2012) and Leblanc et al. (2013) for more insight and properties of r-robust graphs and related notions.

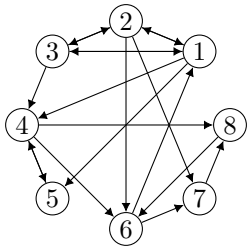


Figure 1. Example of a graph with 8 nodes that is 2-robust.

Figure 1 depicts a directed graph composed of 8 nodes. It can be verified by applying Definition 2 that the graph is 2-robust. Moreover, applying Definition 3, it can be verified that the graph is strongly 1-robust. It is not strongly 2-robust since the subset $\mathcal{S} = \{2,3\}$ is not 2-reachable and nodes 2 and 3 are not connected to all the rest of the network, thus not satisfying Definition 3.

3 Problem Setting

Let us consider a multi-agent system where three different sets of agents are considered, namely cooperative agents, leaders, and adversarial agents. More specifically, the set of "cooperative agents", denoted as $\mathcal{V}_c$, represents those agents that execute a distributed protocol based on the sensing of relative positions of their neighbors with respect to their own inertial reference frame. In the following we refer to the cooperative agents also as "followers". Furthermore, we consider a set of so-called "leaders", denoted as $\mathcal{V}_\ell$, representing those agents which do not execute the proposed control protocol and are possibly autonomous or remotely controlled. In this paper leaders are static and can be also considered as anchor nodes. The positions of the leaders define a containment area that the followers are expected to reach and not escape from. The set of leaders can be empty, in that case only cooperative and adversarial agents are considered. Finally, the set of "adversaries", denoted as $\mathcal{V}_a$, represents those agents tasked with preventing the cooperative agents to fulfill their goal, or the agents that suffered a fault and are thus unable to execute the prescribed control protocol. Clearly the node set $\mathcal{V}$ of the network $\mathcal{G}(t)$ is such that $\mathcal{V} = \mathcal{V}_c \cup \mathcal{V}_\ell \cup \mathcal{V}_a$.

In this paper, mobile agents (possibly representing

autonomous vehicles) with positions in an arbitrary d-dimensional space are modeled as discrete-time multi-dimensional integrators with fixed step-size and state $x_i \in \mathbb{R}^d$ which evolve according to the dynamics shown next as

$$x_i(t+1) = x_i(t) + \varepsilon\, u_i^c(t), \qquad i \in \mathcal{V}_c, \qquad (1)$$
$$x_i(t+1) = x_i(0), \qquad i \in \mathcal{V}_\ell, \qquad (2)$$
$$x_i(t+1) = x_i(t) + \varepsilon\, u_i^a(t), \qquad i \in \mathcal{V}_a, \qquad (3)$$

where $u_i^c(t) \in \mathbb{R}^d$ is the local control input of the cooperative agents $i \in \mathcal{V}_c$ to be later specified, $x_i(0) \in \mathbb{R}^d$ is the initial position at time $t = 0$, and $u_i^a(t) \in \mathbb{R}^d$ is the dynamic of the adversarial agents $i \in \mathcal{V}_a$. For the sake of simplicity and analysis we express the variables in eq. (1)–(3) in a common reference frame but we stress that the agents do not share one. Otherwise, local variables $\hat{x}_{i,\Sigma_i(t)}(t), \hat{u}_{i,\Sigma_i(t)}(t) \in \mathbb{R}^d$ with $i \in \mathcal{V}$ could be introduced to represent the presence of possibly time-varying local reference frames $\Sigma_i(t) = (R_i, t_i)$ encoding rigid body transformations that uniquely identify the local reference frames with respect to an unknown common reference frame. Furthermore, for the sake of analysis we collect the state of all the agents in the stacked vector $\mathbf{x}(t) = [x_1(t)^T, \ldots, x_n(t)^T]^T$. In addition, we refer to the cardinality of the sets $\mathcal{V}_c$, $\mathcal{V}_\ell$, and $\mathcal{V}_a$ respectively as n_c, n_ℓ and n_a, i.e. $|\mathcal{V}_c| = n_c$, $|\mathcal{V}_\ell| = n_\ell$, and $|\mathcal{V}_a| = n_a$.

Let us now introduce the working assumptions of our multi-agent system.

(A1) The adversarial agents are assumed to be embedded with unbounded control inputs and full knowledge of the network model and state (worst case scenario);
(A2) There are a maximum of F adversarial agents in the neighborhood of each cooperative agent (F-local model);
(A3) The cooperative agents are able to measure the relative distance and bearing of their neighbors with respect to their own reference frame;
(A4) The interactions of the agents are described by a directed time-varying graph.

We are now ready to state two coordination problems addressed by the algorithm proposed in this work, that is a cooperative protocol $u_i^c(t)$ for the followers $i \in \mathcal{V}_c$ so that they can i) asymptotically achieve rendezvous when there are adversarial agents and no leader in the network and ii) asymptotically reach a containment region defined according to the position of the leaders despite the influence of adversarial agents.

Problem 1 (Secure Rendezvous) *Consider a multi-agent system composed of n_c cooperative agents and n_a adversaries with dynamics (1) and (3) under Assumptions (A1)–(A4). Our goal is to design a distributed control law $u_i^c(t)$ for the cooperative agents $i \in \mathcal{V}_c$ so that for any initial condition $\mathbf{x}(0)$ and for any input $u_i^a(t)$ of the anonymous adversarial agents in the set $\mathcal{V}_a$, the following holds true:*

$$\lim_{t\to\infty} x_i(t) = p,\ \forall i \in \mathcal{V}_c,\ p \in \mathbb{R}^d. \qquad (4)$$

Problem 2 (Secure Containment) *Consider a multi-agent system composed of n_c cooperative agents, n_ℓ leaders and n_a adversaries with dynamics (1)–(3) under Assumptions (A1)–(A4). Consider a containment region $\mathcal{C}_\ell$ defined according to the position of the leaders. Our goal is to design a distributed control law $u_i^c(t)$ for the cooperative agents $i \in \mathcal{V}_c$ so that for any initial condition $\mathbf{x}(0)$, and for any input $u_i^a(t)$ of the anonymous adversarial agents in the set $\mathcal{V}_a$, the following holds true:*

$$\lim_{t\to\infty} x_i(t) \in \mathcal{C}_\ell,\ \forall i \in \mathcal{V}_c. \qquad (5)$$

4 Proposed local interaction protocol

In this section we provide the distributed control strategy capable of solving Problems 1 and 2 under proper topological conditions of the graph $\mathcal{G}(t)$.

To this end, let us now introduce the definition of the convex hull of the state variables of the agents belonging to a set $\mathcal{S} \subseteq \mathcal{V}$, that is

$$\mathrm{co}\,(\mathbf{x}, \mathcal{S}) = \left\{ y \in \mathbb{R}^d, y = \sum_{i\in\mathcal{S}} \alpha_i x_i : \sum_{i\in\mathcal{S}} \alpha_i = 1, \alpha_i \geq 0 \right\}. \qquad (6)$$

In our case $\mathrm{co}\,(\mathbf{x}, \mathcal{S})$ is a compact set and, in fact, a convex polytope. Let us now introduce the definitions of secure convex hull and F-secure convex hull.

Definition 4 (Secure convex hull) *We refer to the convex hull of cooperative agents as* secure convex hull, *which is defined as*

$$\text{s-co}\,(\mathbf{x}) = \mathrm{co}\,(\mathbf{x}, \mathcal{V}_c)\,. \qquad (7)$$

Definition 5 (F-Secure convex hull) *We define as* F-secure convex hull *for the agent i, the safe area obtained as follows*

$$\text{F-co}\,(\mathbf{x}, \mathcal{N}_i) = \bigcap_{\substack{\forall\, \mathcal{I} \subseteq \mathcal{N}_i \\ |\mathcal{I}| = \min\{F, |\mathcal{N}_i|\}}} \mathrm{co}\left(\mathbf{x}, \overline{\mathcal{N}}_i \backslash \mathcal{I}\right). \qquad (8)$$

The F-Secure convex hull is built from the intersection of the convex hull of the state variables of the neighbors where each time a different subset of the neighbors of cardinality equal to $\min\{F, |\mathcal{N}_i(t)|\}$ has been removed.

Algorithm 1 *F-Secure Rendezvous and Containment Protocol*

States of the agents: $x_i(t)$ for all $i \in \mathcal{V}_c$;
Protocol execution: At each time instant t, all the agents repeat the following operations, here reported for the agent i:
1) Collect the neighbors relative positions $x_i(t) - x_j(t)$ in its own local reference frame;
2) According to eq. (8) compute the F-secure convex hull F-co $(\mathbf{x}(t), \mathcal{N}_i(t))$;
3) Compute the centroid $m_i(t)$ of the F-secure convex hull as

$$m_i(t) = \mathsf{C}\Big(\text{F-co}\,(\mathbf{x}(t), \mathcal{N}_i(t))\Big), \tag{9}$$

where $\mathsf{C}\,(\text{F-co}\,(\mathbf{x}(t), \mathcal{N}_i(t)))$ is the centroid of the F-secure convex hull computed with respect to the local reference frame of the agent;
4) Compute the relative control action $u_i^c(t)$ as

$$u_i^c(t) = m_i(t) - x_i(t); \tag{10}$$

5) Update the state $x_i(t)$ as

$$x_i(t+1) = x_i(t) + \varepsilon u_i^c(t) = x_i(t) + \varepsilon(m_i(t) - x_i(t)). \tag{11}$$

It should be noticed that Definition 5 has been also used in Wang et al. (2019) where the authors developed a geometrical method to obtain the so-called resilient convex combination from a set of vectors which may contain malicious data. In our case instead we use the above definition to build a secure area where the agents are allowed to move.

Algorithm 1 describes the local coordination protocol that is proven to solve Problems 1 and 2. The basic idea of the algorithm is to let the cooperative agents move in an area, i.e., the F-secure convex hull, that cannot be arbitrarily influenced by the adversarial agents. The area is built intersecting a combination of convex hulls of the state variables of the neighbors of the agent that is computing the secure area, where each time F of the neighbors (or all of them) have been removed from consideration. In this way, under proper topological conditions, the agents are able to move freely in such area and actively work towards the collaborative objective undisturbed. Notice how the intersection includes the state of the agent i, which is considered by definition secure, whereas the subset $\mathcal{I}$ does not. This implies that in the worst case the F-secure convex hull is a singleton consisting of the state of the agent i. Finally, we point out that in order to compute eq. (8), each agent i has to analyze exactly $\binom{|\mathcal{N}_i|}{F}$ combinations of convex hulls.

Among all the possible points in the F-secure convex hull, the one that we choose to move towards is its centroid. Indeed the centroid, being the mean of all the points in the F-secure convex hull, is always defined independently if the hull is a single point, a line, or an area. In the first case, the centroid is the single point itself; in second case, the centroid is the mean of the two endpoints of the line; whereas in the case the F-secure convex hull is an area, it is possible to compute it from the vertices of the area itself (further details are given in Section 6).

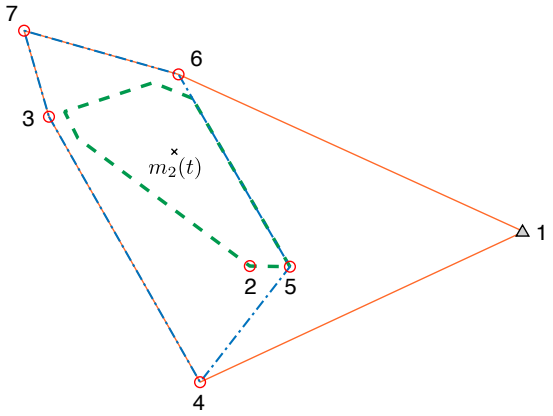


Figure 2. A two dimensional MAS where the control term $m_2(t)$ of the cooperative agent 2 is highlighted. Agent 1 is an adversarial agent. The F-secure convex hull is depicted with a dashed green line. The orange solid line represents the convex hull of the states of the extended neighborhood of agent 2 whereas the dash-dotted blue line depicts the Secure convex hull s-co.

Notice also how the steps described in Algorithm 1 can be implemented by each agent by relying on relative information measured with respect to their own reference frame only. Notably, the control input in eq. (10) is invariant with respect to any rotation and/or translation of the agent's reference frame. Hence, for this reason, the presence of a common reference frame among the agents is not required.

Figure 2 depicts the control term $m_2(t)$ of agent 2 in a two-dimensional MAS with 7 agents in which one of them (agent 1) is an adversarial intruder. The control term $m_2(t)$ is the centroid of the 1-secure convex hull F-co $(\mathbf{x}(t), \mathcal{N}_2(t))$ and it is represented by a black cross whereas the secure convex hull itself is portrayed with dashed green lines.

5 Theoretical Analysis

In this section we provide the theoretical properties of the F-secure convex hull and consequently the theoretical results of the problems introduced in Section 3. In particular, first we prove three structural properties on the F-secure convex hull and then we use them to demonstrate the convergence properties of Algorithm 1 in regards to Problems 1 and 2.

Proposition 1 *The F-secure convex hull in eq.* (8) *built*

by each agent $i \in \mathcal{V}_c$ is never an empty set, that is

$$\text{F-co}\left(\mathbf{x}(t), \mathcal{N}_i(t)\right) \neq \{\emptyset\}. \tag{12}$$

PROOF. The result follows from the fact that for each agent $i \in \mathcal{V}_c$, the convex hulls $\text{co}\left(\mathbf{x}(t), \overline{\mathcal{N}}_i(t) \setminus \mathcal{I}\right)$ built in eq. (8), for any $\mathcal{I} \subseteq \mathcal{N}_i(t)$, always include the state $x_i(t)$. Therefore, the F-secure convex hull $\text{F-co}\left(\mathbf{x}(t), \mathcal{N}_i(t)\right)$ is never empty. □

From Proposition 1 it follows that the centroid $m_i(t)$ can always be computed by any cooperative agent of the network.

Proposition 2 *Consider a cooperative agent $i \in \mathcal{V}_c$ under Assumption (A2), then its F-secure convex hull is a subset of the secure convex hull, that is,*

$$\text{F-co}\left(\mathbf{x}(t), \mathcal{N}_i(t)\right) \subseteq \text{s-co}\left(\mathbf{x}(t)\right) \tag{13}$$

PROOF. The proof follows from the construction of eq. (8).

Denote as C_{safe} the convex hull of cooperative agents in the neighborhood of agent i, i.e.,

$$C_{\text{safe}} = \text{co}\left(\mathbf{x}(t), \overline{\mathcal{N}}_i(t) \cap \mathcal{V}_c\right). \tag{14}$$

Moreover, denote with $C_{\mathcal{I}}$ the subsets that made up the convex hulls involved in the intersection in eq. (8), i.e., $C_{\mathcal{I}} = \overline{\mathcal{N}}_i(t) \setminus \mathcal{I}$ with $\mathcal{I}$ such that $\mathcal{I} \subseteq \mathcal{N}_i(t)$ and $|\mathcal{I}| = \min\{F, |\mathcal{N}_i(t)|\}$.

Since by assumption there are a maximum of F adversarial agents, and rule (8) removes $\min\{F, |\mathcal{N}_i(t)|\}$ elements each time from the set $\overline{\mathcal{N}}_i$, it follows that it must exists a set $C_{\mathcal{I}}$ that contains only elements of the set C_{safe}, i.e., $C_{\mathcal{I}} \subseteq C_{\text{safe}}$.

By definition the convex hull of the set $C_{\mathcal{I}}$ is considered in the intersection in eq. (8) so it holds that

$$\text{F-co}\left(\mathbf{x}(t), \mathcal{N}_i(t)\right) \subseteq C_{\mathcal{I}} \subseteq C_{\text{safe}} \subseteq \text{s-co}\left(\mathbf{x}(t)\right). \tag{15}$$

The result follows. □

Proposition 3 *Consider a cooperative agent $i \in \mathcal{V}_c$ which is a vertex of the secure convex hull* $\text{s-co}(\mathbf{x}(t))$ *in a d-dimensional space. If $|\mathcal{N}_i(t)| \geq F(d+1)+1$ and $\text{co}\left(\mathbf{x}(t), \mathcal{V}_c \cap \mathcal{N}_i(t)\right) \neq \{x_i(t)\}$, then there exists at least a point $y \in \mathbb{R}^d$ different from $x_i(t)$, i.e., such that $y \neq x_i(t)$, which is inside the F-secure convex hull, i.e.,*

$$y \in \text{F-co}\left(\mathbf{x}(t), \mathcal{N}_i(t)\right). \tag{16}$$

Furthermore, all points $z \in \mathbb{R}^d$ of the convex combination $z = \alpha\, x_i(t) + (1-\alpha)\, y$ with $\alpha \in (0,1)$ belong to the F-secure convex hull as well, i.e., $z \in \text{F-co}\left(\mathbf{x}(t), \mathcal{N}_i(t)\right)$.

PROOF. The proof follows from the application of (Wang et al., 2019, Lemma 3) where $\mathcal{R}$ is the equivalent of our intersection operation in eq. (8) in which the agent i is not considered, i.e., $\mathcal{R}$ represents the following

$$\mathcal{R} = \bigcap_{\substack{\forall\, \mathcal{I} \subseteq \mathcal{N}_i(t) \\ |\mathcal{I}| = \min\{F, |\mathcal{N}_i(t)|\}}} \text{co}\left(\mathbf{x}(t), \mathcal{N}_i(t) \setminus \mathcal{I}\right). \tag{17}$$

In particular, since $|\mathcal{N}_i(t)| \geq F(d+1)+1$ holds, then it follows that $\mathcal{R}$ is not empty and contains at least a point $y \in \mathbb{R}^d$. In addition, since $\mathcal{R}$ is built without including the state of the agent i then it holds that $\mathcal{R} \subset \text{F-co}\left(\mathbf{x}(t), \mathcal{N}_i(t)\right)$, hence, it must necessarily also hold that $y \neq x_i(t)$.

In addition, since the F-secure convex hull is convex by construction and eq. (16) holds, then the points $z = \alpha\, x_i(t) + (1-\alpha)\, y$ with $\alpha \in (0,1)$ belong to the F-secure convex hull as well, i.e., $z \in \text{F-co}\left(\mathbf{x}(t), \mathcal{N}_i(t)\right)$. The result follows. □

As it will be shown later, the results of Proposition 3 imply that if its conditions are met, then the centroid $m_i(t)$ computed by each agent i, vertex of the convex hull $\text{s-co}(\mathbf{x}(t))$, is located in the interior of the F-secure convex hull.

5.1 Secure Rendezvous

We now provide our theoretical result concerning the solution of Problem 1.

Theorem 1 *Consider a multi-agent system consisting of n_c cooperative agents and n_a adversaries agents with dynamics as in eqs.* (1) *and* (3) *under Assumptions (A1)–(A4). Let the cooperative agents execute the control protocol in Algorithm 1. If the graph $\mathcal{G}(t)$ is $(F(d+1)+1)$-robust $\forall\, t \geq 0$, then the cooperative agents asymptotically reach rendezvous, i.e.*

$$\lim_{t \to \infty} x_i(t) = p,\ \forall\, i \in \mathcal{V}_c,\ p \in \text{s-co}\left(\mathbf{x}(0)\right), \tag{18}$$

where $\text{s-co}\left(\mathbf{x}(0)\right)$ *is the secure convex hull introduced in Definition 4 at time $t = 0$.*

PROOF. In order to prove this result, let us consider the secure convex hull $\text{s-co}\left(\mathbf{x}(t)\right)$ composed of the states of the cooperative agents $\mathcal{V}_c$ at time t and its volume $V(\mathbf{x}(t)) : \mathbb{R}^{nd} \to \mathbb{R}_{\geq 0}$. Note that $V(\mathbf{x}(t))$ is a positive and continuous function of the state $\mathbf{x}(t)$. In what follows for the sake of brevity we denote the volume at time t simply as $V(t)$.

If all the cooperative agents have reached the rendezvous point then s-co $(\mathbf{x}(t))$ is a singleton, i.e., the rendezvous point, and the volume is zero. Now, suppose that the cooperative agents are not in a rendezvous state at time t.

As stated in Proposition 2, the F-secure convex hull F-co $(\mathbf{x}(t), \mathcal{N}_i(t))$ for each agent i is a subset of the secure convex hull of cooperative agents s-co $(\mathbf{x}(t))$. Then for the centroid $m_i(t)$ the following statements hold

$$m_i(t) \in \text{co}\left(\mathbf{x}(t), \overline{\mathcal{N}}_i(t) \setminus \mathcal{V}_a\right), \tag{19}$$

and

$$m_i(t) \in \text{s-co}\left(\mathbf{x}(t)\right). \tag{20}$$

Moreover, in virtue of eq. (11), each agent moves towards its computed centroid $m_i(t)$. Since at time t both $x_i(t)$ and $m_i(t)$ belong to the convex hull s-co $(\mathbf{x}(t))$, then it also holds

$$x_i(t+1) \in \text{s-co}\left(\mathbf{x}(t)\right), \quad i \in \mathcal{V}_c, \tag{21}$$

because it is defined as a convex combination of $x_i(t)$ and $m_i(t)$ (see eq. (11)).

Since eq. (21) holds for all $i \in \mathcal{V}_c(t)$, it follows that

$$\text{s-co}\left(\mathbf{x}(t+1)\right) \subseteq \text{s-co}\left(\mathbf{x}(t)\right), \tag{22}$$

and thus the volume of the convex hull of the cooperative agents is non-increasing with respect to time

$$V(t+1) \leq V(t). \tag{23}$$

Consider now the cooperative agents belonging to $\Omega\,\text{s-co}\left(\mathbf{x}(t)\right)$ at time t, i.e., agents that are vertices of the set s-co $(\mathbf{x}(t))$.

We want now to prove that either the volume V is strictly decreasing or that, even if the volume stays the same, there exists at least a cooperative agent in the set $\Omega\,\text{s-co}\left(\mathbf{x}(t)\right)$ moving towards the rendezvous point p at time t that eventually leads to the decrease of the convex hull s-co $(\mathbf{x}(t))$ and hence of its volume V.

First, consider the case where cooperative agents do not overlap during the execution of Algorithm 1. Recall that by assumption the graph is $(F(d+1)+1)$-robust, implying that $|\mathcal{N}_i(t)| \geq F(d+1)+1$ holds for each agent i of the network. It then follows that the conditions of Proposition 3 are satisfied.

Then, in virtue of eq. (19) and Proposition 3, it is guaranteed that the centroid of each agent i which is vertex of the convex hull of the cooperative agents s-co $(\mathbf{x}(t))$ is located in the interior of the convex hull $\text{co}(\mathbf{x}(t), \overline{\mathcal{N}}_i(t) \setminus \mathcal{V}_a)$. Hence it follows that

$$\text{s-co}\left(\mathbf{x}(t+1)\right) \subset \text{s-co}\left(\mathbf{x}(t)\right). \tag{24}$$

Eq. (24) holds true as long as for each agent i vertex of s-co $(\mathbf{x}(t))$ it holds $\text{co}(\mathbf{x}(t), \overline{\mathcal{N}}_i(t) \setminus \mathcal{V}_a) \neq \{x_i(t)\} = p$, i.e., until the agents reach the rendenzvous point p. This implies that $V(t+1) < V(t)$ holds as long as $V(t) > 0$ if no agent overlaps its position with others.

Now consider the case where some agents may overlap their position with others at certain times. In particular, suppose there exists h subsets $\mathcal{S}_1, \ldots, \mathcal{S}_h \subset \mathcal{V}_c$ of agents that overlap at different vertices of the convex hull s-co $(\mathbf{x}(t))$ during the execution of Algorithm 1 at time t, i.e.,

$$\mathcal{S}_q = \Big\{ i \in \mathcal{V}_c : x_i(t) = x_q,\ x_q \in \Omega\,\text{s-co}\left(\mathbf{x}(t)\right) \Big\}, \tag{25}$$

with $q \in \{1, \ldots, h\}$.

In this case, eq. (24) is no longer guaranteed to hold since there could exists agents in those subsets such that

$$x_i(t+1) = x_i(t), \tag{26}$$

i.e., such that F-co $(\mathbf{x}(t), \mathcal{N}_i(t)) = \{x_i(t)\}$, potentially leading to

$$\text{s-co}\left(\mathbf{x}(t+1)\right) = \text{s-co}\left(\mathbf{x}(t)\right) \quad \text{and} \quad V(t+1) = V(t). \tag{27}$$

However, by Definition 2 it must hold for each pair of subsets $\mathcal{S}_a, \mathcal{S}_b$, with $a, b \in \{1, \ldots, h\}$ that there exists at least an agent i, with either $i \in \mathcal{S}_a$ or $i \in \mathcal{S}_b$, that is connected to at least $F(d+1)+1$ neighbors not overlapped with him outside its respective subset. Then, since for agent i the conditions of Proposition 3 hold, we can assert that

$$\text{F-co}\left(\mathbf{x}(t), \mathcal{N}_i(t)\right) \neq \{x_i(t)\}. \tag{28}$$

This implies that eq. (19) holds as well. Define now the variable $\Psi(t)$ as the number of agents overlapped at the vertices of the convex hull s-co $(\mathbf{x}(t))$, i.e.,

$$\Psi(t) = \sum_{q=1}^{h} |\mathcal{S}_q|. \tag{29}$$

Then, in virtue of eq. (11) and what has been derived above, for each pair of subsets of overlapped agents there always exists at least an agent i that moves towards the neighbors not overlapped with him, hence reducing the number of agents overlapped at the vertices, that is

$$\Psi(t+1) < \Psi(t). \tag{30}$$

Since $\Psi(t)$ is upper bounded by n_c, it is guaranteed that in a finite number of consecutive time instants $T_\Psi \leq n_c - 2$, either the volume of the convex hull decreases again or the rendezvous point p has been reached by all cooperative agents.

Summarizing, during the evolution of the multi-agent system the following three scenarios are possible:

i) $V(t+1) < V(t)$;
ii) $V(t+1+\tau) = V(t+\tau)$ and $\Psi(t+1+\tau) < \Psi(t+\tau)$ with $\tau \geq 0$;
iii) $V(t+1) = V(t) = 0$ and $\Psi(t+1) = \Psi(t) = n_c$ and s-co $(\mathbf{x}(t)) = \{p\}$.

Consider now the lexicographic ordered function $V_L(t)$ defined as

$$V_L(t) = \Big(V(t), \Psi(t)\Big), \tag{31}$$

consisting of volume $V(t)$ and function $\Psi(t)$. We have proven above and summarized in i) and ii) that $V_L(t)$ decreases at each iteration until the cooperative agents reach the rendezvous point p.

We point out that the time variability of the graph does not change the reasoning of the proof as long as the graph is $(F(d+1)+1)$-robust for all time instants. In other words, the edge set $\mathcal{E}(t)$ is allowed to change during the evolution of the system as long as the $(F(d+1)+1)$-robustness property is satisfied for all $t \geq 0$.

In conclusion we notice that since the convex hull of cooperative agents is not increasing in size, the rendezvous point satisfies $p \in$ s-co $(\mathbf{x}(0))$. The result follows. □

In addition, we want to point out that the usage of the concept of (r,s)-robustness introduced in Leblanc et al. (2013), i.e., considering a time-varying $(F(d+1)+1, s)$-robust graph with $s > 1$, does not guarantee a strict decrease of the volume. However, increasing the parameter s guarantees a minor upper bound on the time bound T_Ψ. In particular, having a network $(F(d+1)+1, s)$-robust would increase the speed by a factor of s time steps since at each time instant there would exists at least s cooperative agents moving towards the interior of the convex hull hence decreasing the value of the function $\Psi(t)$ by at least s at each t.

Figure 2 gives insights on the inclusion properties of the different convex hulls in place: the F-secure convex hull F-co $(\mathbf{x}(t), \mathcal{N}_i(t))$ depicted with a dashed green line is contained in the secure convex hull s-co $(\mathbf{x}(t))$ depicted with a dashed dotted blue line, which is, in turn, contained in the convex hull of all the agents co $(\mathbf{x}(t), \mathcal{V})$ depicted with a solid orange line.

Remark 1 *If a necessary and sufficient condition for the result in (Wang et al., 2019, Lemma 3) were to be found, then the same graph theoretical condition would become necessary and sufficient for Theorem 1.*

5.2 Secure Containment

We now provide our theoretical result concerning the solution of Problem 2. The containment region that the cooperative agents $\mathcal{V}_c$ have to reach and then remain contained within is the convex hull of the initial positions of the leaders $\mathcal{V}_\ell$.

Theorem 2 *Consider a multi-agent system consisting of n_c cooperative agents, n_ℓ leaders, and n_a adversaries agents with dynamics as in eqs. (1), (2), and (3) respectively, under Assumptions (A1)–(A4). Let the cooperative agents execute the control protocol in Algorithm 1. If the graph $\mathcal{G}(t)$ is strongly $(F(d+1)+1)$-robust $\forall\, t \geq 0$, then the cooperative agents asymptotically reach and remain contained in the convex hull defined by the initial positions of the leaders, that is*

$$\lim_{t\to\infty} \mathbf{x}(t) \in \mathcal{C}_\ell, \tag{32}$$

where the containment region is the convex hull of the initial positions of the leaders, i.e., $\mathcal{C}_\ell =$ co $(\mathbf{x}(0), \mathcal{V}_\ell)$.

PROOF. To prove this result we follow the same steps as done in Theorem 1. To this end, consider the convex hull composed of the states of the cooperative agents $\mathcal{V}_c$ and leaders $\mathcal{V}_\ell$ combined at time t, co $(\mathbf{x}(t), \mathcal{V}_c \cup \mathcal{V}_\ell)$ and its volume $V(\mathbf{x}(t)) : \mathbb{R}^{nd} \to \mathbb{R}_{\geq 0}$, positive and continuous function of the state $\mathbf{x}(t)$.

We now prove that the volume $V(t)$ of the convex hull of cooperative agents and leaders combined co $(\mathbf{x}(t), \mathcal{V}_c \cup \mathcal{V}_\ell)$ decreases as long as it is not entirely contained in the convex hull of the leaders co $(\mathbf{x}(0), \mathcal{V}_\ell)$ at time $t = 0$.

Clearly, if at time $t = 0$ the convex hull of cooperative agents s-co $(\mathbf{x}(0))$ is entirely contained within the convex hull of the leaders co $(\mathbf{x}(0), \mathcal{V}_\ell)$, then Problem 2 is solved. Suppose that s-co $(\mathbf{x}(0))$ is not entirely contained in co $(\mathbf{x}(0), \mathcal{V}_\ell)$, that is,

$$\text{co}\,(\mathbf{x}(0), \mathcal{V}_c \cup \mathcal{V}_\ell) \not\subseteq \text{co}\,(\mathbf{x}(0), \mathcal{V}_\ell)\,. \tag{33}$$

As discussed in the proof of Theorem 1, the F-secure convex hull F-co $(\mathbf{x}(t), \mathcal{N}_i(t))$ for each agent i is a subset of the secure convex hull s-co $(\mathbf{x}(t))$ (Proposition 2), hence the centroid $m_i(t)$ is such that

$$m_i(t) \in \text{co}\left(\mathbf{x}(t), \overline{\mathcal{N}}_i(t) \setminus \mathcal{V}_a\right). \tag{34}$$

In this case then it holds that

$$\text{co}\left(\mathbf{x}(t), \overline{\mathcal{N}}_i(t) \setminus \mathcal{V}_a\right) \subseteq \text{co}\,(\mathbf{x}(t), \mathcal{V}_c \cup \mathcal{V}_\ell)\,. \tag{35}$$

Then, it follows that for every $i \in \mathcal{V}_c$ the following holds

$$m_i(t) \in \text{co}\,(\mathbf{x}(t), \mathcal{V}_c \cup \mathcal{V}_\ell)\,, \tag{36}$$

leading to

$$x_i(t+1) \in \text{co}\left(\mathbf{x}(t), \mathcal{V}_c \cup \mathcal{V}_\ell\right), \quad i \in \mathcal{V}_c, \tag{37}$$

in virtue of eq. (11). Moreover, since eq. (37) holds for all $i \in \mathcal{V}_c(t)$, it holds that

$$\begin{aligned} &\text{co}\left(\mathbf{x}(t+1)\mathcal{V}_c \cup \mathcal{V}_\ell\right) \subseteq \text{co}\left(\mathbf{x}(t)\mathcal{V}_c \cup \mathcal{V}_\ell\right), \\ &\text{and} \quad V(t+1) \leq V(t). \end{aligned} \tag{38}$$

As in the case of secure rendezvous, let us now consider the case when agents at the vertices of the convex hull s-co $(\mathbf{x}(t))$ do not overlap during the execution of Algorithm 1.

Recalling that by assumption the network is strongly $(F(d+1)+1)$-robust, we have that $|\mathcal{N}_i(t)| \geq F(d+1)+1$ holds for every agent. For the agents vertices of s-co $(\mathbf{x}(t))$ then Proposition 3 holds. From eq. (11) and eq. (34) we can then infer that

$$\text{co}\left(\mathbf{x}(t+1), \mathcal{V}_c \cup \mathcal{V}_\ell\right) \subset \text{co}\left(\mathbf{x}(t), \mathcal{V}_c \cup \mathcal{V}_\ell\right), \tag{39}$$

that is, the convex hull of the followers and leaders combined is strictly decreasing. As a consequence, its volume V decreases as well, i.e., $V(t+1) < V(t)$, as long as the convex hull of the cooperative agents is not entirely contained in the convex hull of the leaders.

In the case the cooperative agents overlap at the vertices of the convex hull of cooperative agents only, we can collect them in the subsets $\mathcal{S}_q \subset \mathcal{V}_c$ defined as in eq. (25) and apply the same reasoning as Theorem 1. In this case, however, to account for the missed contribution of the leaders (that are static and hence not actively involved in the convergence of the convex hull co $(\mathbf{x}(t), \mathcal{V}_c \cup \mathcal{V}_\ell)$) the network requires a greater level of robustness. The strongly $(F(d+1)+1)$-robustness property of the time-varying network guarantees that there always exists at least a cooperative agent in one of the subsets $\mathcal{S}_q$ of overlapped agents that possess at least $F(d+1)+1$ neighbors not overlapped with him outside its set, leading to the decrease of either the volume V or the value of the function $\Psi(t)$ defined as in eq. (29).

Considering the lexicographic ordered function $V_L(t)$ defined as $V_L(t) = (V(t), \Psi(t))$ consisting of volume $V(t)$ and function $\Psi(t)$ as done in the proof of Theorem 1, we can prove that at each iteration such that the convex hull s-co $(\mathbf{x}(t))$ is not entirely contained in the convex hull of the initial positions of the leaders, the lexicographic function $V_L(t)$ decreases. The cooperative agents then asymptotically reach and remain contained in convex hull of the initial position of the leaders $\mathcal{C}_\ell$ thus proving the result. □

We want to remark that the network graph $\mathcal{G}(t)$ is allowed to change as long as the strongly $(F(d+1)+1)$-robustness property is satisfied for all time instants $t \geq 0$.

We also point out that the same argument as Remark 1 holds in the case of secure containment, i.e., if a graph theoretical necessary and sufficient condition were to be found for the result in Wang et al. (2019) then the same condition would become necessary and sufficient for Theorem 2.

6 Numerical simulations

In this section we provide numerical simulations to corroborate the theoretical findings, we present two different scenarios: i) a MAS with no leaders in which the cooperative agents are performing secure rendezvous under the presence of two adversarial agents and ii) a MAS in which the cooperative agents are tasked to reach and remain contained in an area defined by the positions of a set of leaders under the disruptive behaviour of two adversarial agents.

In both scenarios the agents do not share a common reference frame nor have access to absolute positions but rely on measurements with respect to their own reference frame only to execute the proposed Algorithm 1.

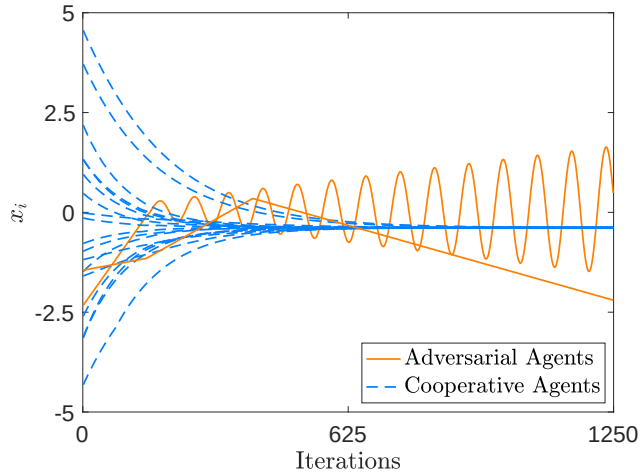
The simulations are carried out in a two-dimensional space for the sake of clearness. The centroid of a polygon in this case assumes a well known form. In particular, considering a non-self-intersecting closed polygon P defined by v vertices $\{(x_0, y_0), (x_1, y_1), \ldots, (x_{v-1}, y_{v-1})\}$ numbered in order of their occurrence along the polygon's perimeter, the centroid of P is the point $\mathsf{C}(\mathsf{P}) = [C_x,\, C_y]^T$ defined as

$$\begin{aligned} C_x &= \frac{1}{6\,A} \sum_{i=0}^{v-1} (x_i + x_{i+1})(x_i y_{i+1} - x_{i+1} y_i), \\ C_y &= \frac{1}{6\,A} \sum_{i=0}^{v-1} (y_i + y_{i+1})(x_i\, y_{i+1} - x_{i+1} y_i), \end{aligned} \tag{40}$$

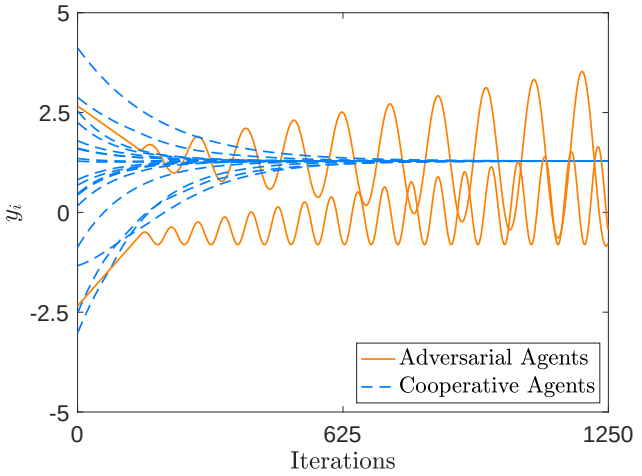
where the vertex $(x_v, y_v) = (x_0, y_0)$ and A is the area of the polygon expressed by

$$A = \frac{1}{2} \sum_{i=0}^{v-1} (x_i y_{i+1} - x_{i+1} y_i). \tag{41}$$

In the case $d = 3$, the centroid can be computed by performing proper polygon triangulations: after the polygon has been decomposed in w triangular faces, its centroid is given from the mean value of the centroids of the w triangular faces (Protter and Morrey (1977)).

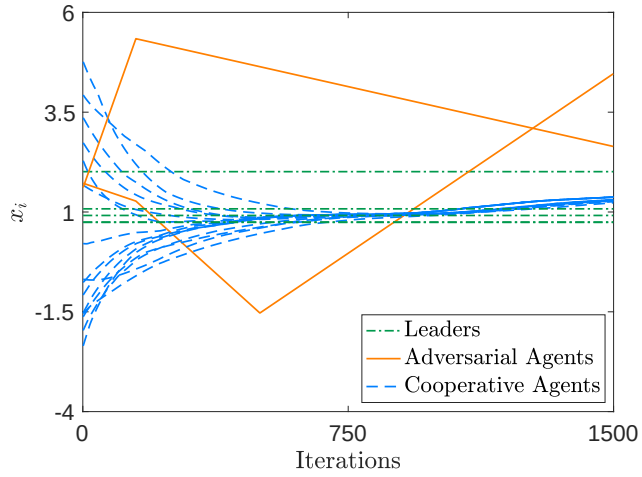


(a) Evolution of the multi agent-system along the x-axis.

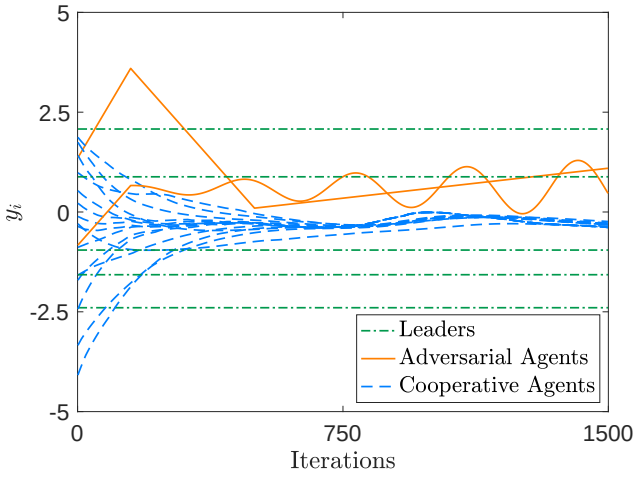


(b) Evolution of the multi agent-system along the y-axis.

Figure 3. A multi-agent system composed of 18 cooperative agents and 2 adversarial agents with $d = 2$ performing secure rendezvous with interactions described by a directed time-varying 7-robust graph.



(a) Evolution of the multi agent-system along the x-axis.



(b) Evolution of the multi agent-system along the y-axis.

Figure 4. A multi-agent system composed of 15 cooperative agents, 5 leaders and 2 adversarial agents with $d = 2$ performing secure containment with interactions described by a directed time-varying strongly 7-robust graph.

6.1 Secure Rendezvous

For the case of secure rendezvous we consider a multi-agent system described by a directed 7-robust time-varying graph composed of 18 cooperative agents, 2 adversarial agents and no leaders. The cooperative agents execute Algorithm 1 with parameter $F = 2$. The two adversarial agents evolve using the following control inputs:

$$
\begin{aligned}
u^a_{19}(t) &= \left[\tfrac{3}{2}, -\tfrac{3}{4}\right]^T, && t \in \{1, \dots, 150\},\\
u^a_{19}(t) &= \left[\tfrac{t}{100}\cos\left(\tfrac{7t}{90}\right), \tfrac{t}{100}\sin\left(\tfrac{t}{18}\right)\right]^T, && t \in \{151, \dots, 700\},\\
u^a_{20}(t) &= \left[\tfrac{1}{5}, \tfrac{6}{5}\right]^T, && t \in \{1, \dots, 150\},\\
u^a_{20}(t) &= \left[\tfrac{3}{5}, \tfrac{t}{100}\sin\left(\tfrac{t}{10}\right)+\tfrac{1}{10}\right]^T, && t \in \{151, \dots, 400\},\\
u^a_{20}(t) &= \left[-\tfrac{3}{10}, \tfrac{t}{100}\sin\left(\tfrac{t}{10}\right)+\tfrac{1}{10}\right]^T, && t \in \{401, \dots, 700\}.
\end{aligned}
\tag{42}
$$

Figure 3 depicts the evolution of the states of the agents; in particular in Figure 3a it is depicted the evolution along the x-axis whereas in Figure 3b it is portrayed the evolution along the y-axis. The evolution of the cooperative agents is depicted with a light blue dashed line whereas the evolution of the intruders is portrayed with a solid orange line. Until time $t = 150$ the intruders behave in a similar way to the rest of the agents. After that time, however, they start executing a disruptive beha-

viour. Nevertheless all the cooperative agents correctly achieve the rendezvous as expected from the results of Theorem 1.

6.2 Secure Containment

For the case of secure containment we consider a multi-agent system described by a directed strongly 7-robust time-varying graph. The network is composed of 15 cooperative agents executing Algorithm 1 with parameter $F = 2$, 5 static leaders and 2 intruders. The first intruder evolves using the following control inputs:

$$\begin{aligned} u^a_{21}(t) &= \left[-\tfrac{3}{10}, \tfrac{3}{2}\right]^T, && t \in \{1, \dots, 150\}, \\ u^a_{21}(t) &= \left[-\tfrac{4}{5}, -1\right]^T, && t \in \{151, \dots, 500\}, \\ u^a_{21}(t) &= \left[\tfrac{3}{5}, \tfrac{1}{10}\right]^T, && t \in \{501, \dots, 1500\}, \end{aligned} \tag{43}$$

whereas the second one with the followings:

$$\begin{aligned} u^a_{22}(t) &= \left[\tfrac{5}{2}, 1\right]^T, && t \in \{1, \dots, 150\}, \\ u^a_{22}(t) &= \left[-\tfrac{1}{5}, \tfrac{t}{1000}\sin\left(\tfrac{t}{10}\right)\right]^T, && t \in \{151, \dots, 1500\}. \end{aligned} \tag{44}$$

The evolution of the states of the agents are depicted in Figure 4 in which the dash dotted green line, the dashed light blue line, and the solid orange line represent the evolution of the leaders, of the cooperative agents and of the adversarial agent, respectively. As can be seen from Figures 4a and 4b even thought the behaviour of the intruder is capable of influencing the behaviour of the cooperative agents, they remain contained in the confinement region defined by the leaders as expected from the result of Theorem 2. Figure 5 depicts the evolution over time of the MAS where the convex hulls of the leaders (light blue) and cooperative agents (green) can be clearly seen.

7 Conclusions

In this paper we investigated the secure rendezvous and static containment problems for multi-agents system described by directed time-varying networks under the presence of anonymous adversarial intruders which attempt to disrupt the desired behaviour of the system. We proposed a novel distributed local interaction protocol able to achieve a secure rendezvous and secure containment within the convex hull of set of agents of the system under proper topological conditions known as r-robustness. Future work will focus on developing a control strategy able to guarantee containment with dynamic leaders.

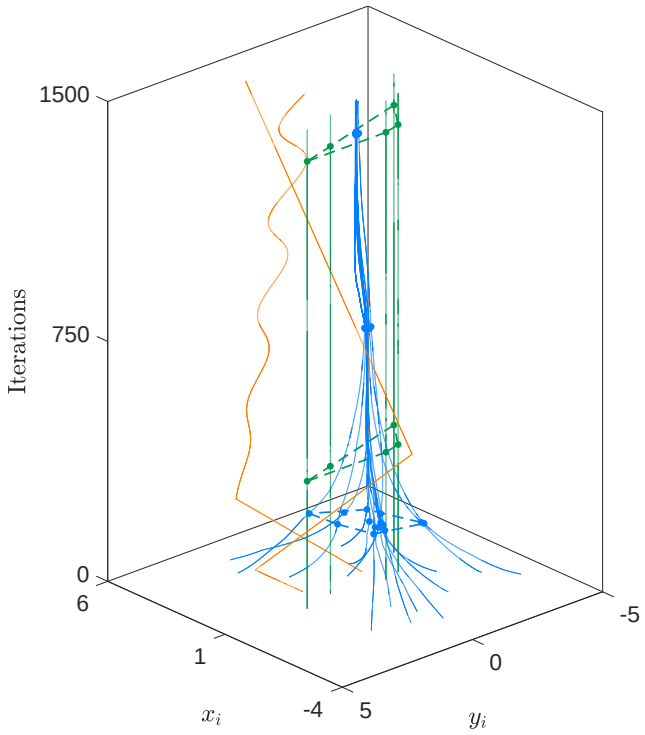


Figure 5. Evolution over time of the MAS performing the secure containment.

References

A. Macwan, J. Vilela, G. Nejat, and B. Benhabib. A multirobot path-planning strategy for autonomous wilderness search and rescue. *IEEE Transactions on Cybernetics*, 45(9):1784–1797, 2015.

Z. Liu and A.G. Foina. An autonomous quadrotor avoiding a helicopter in low-altitude flights. *IEEE Aerospace and Electronic Systems Magazine*, 31(9): 30–39, 2016.

G. Chen, F.L. Lewis, and L. Xie. Finite-time distributed consensus via binary control protocols. *Automatica*, 47(9):1962–1968, 2011.

Y. Cao and W. Ren. Finite-time consensus for multi-agent networks with unknown inherent nonlinear dynamics. *Automatica*, 50(10):2648–2656, 2014.

M. Franceschelli, A. Pisano, A. Giua, and E. Usai. Finite-time consensus with disturbance rejection by discontinuous local interactions in directed graphs. *IEEE Transactions on Automatic Control*, 60(4): 1133–1138, 2015.

M. Franceschelli, A. Giua, and A. Pisano. Finite-time consensus on the median value with robustness properties. *IEEE Transactions on Automatic Control*, 62 (4):1652–1667, 2017.

J. Cortés. Finite-time convergent gradient flows with applications to network consensus. *Automatica*, 42 (11):1993–2000, 2006.

F. Chen, Y. Cao, and W. Ren. Distributed average tracking of multiple time-varying reference signals with

bounded derivatives. *IEEE Transactions on Automatic Control*, 57(12):3169–3174, 2012.

L. Wang and F. Xiao. Finite-time consensus problems for networks of dynamic agents. *IEEE Transactions on Automatic Control*, 55(4):950–955, 2010.

F. Pasqualetti, F. Dorfler, and F. Bullo. Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control*, 58(11): 2715–2729, 2013.

S. Sridhar, A. Hahn, and M. Govindarasu. Cyber-physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1):210–224, 2012.

S.K. Khaitan and J.D. McCalley. Design techniques and applications of cyberphysical systems: A survey. *IEEE Systems Journal*, 9(2):350–365, 2015.

Y. Mo and B. Sinopoli. On the performance degradation of cyber-physical systems under stealthy integrity attacks. *IEEE Transactions on Automatic Control*, 61 (9):2618–2624, 2016.

H. Zhang and S. Sundaram. Robustness of information diffusion algorithms to locally bounded adversaries. In *2012 American Control Conference (ACC)*, pages 5855–5861, 2012.

H.J. Leblanc, H. Zhang, X. Koutsoukos, and S. Sundaram. Resilient asymptotic consensus in robust networks. *IEEE Journal on Selected Areas in Communications*, 31(4):766–781, 2013.

Y. Wu, M. Xu, N. Zheng, and X. He. Event-triggered resilient consensus for multi-agent networks under deception attacks. *IEEE Access*, 8:78121–78129, 2020.

Y. Wang and H. Ishii. Resilient consensus through event-based communication. *IEEE Transactions on Control of Network Systems*, 7(1):471–482, 2020.

W. Abbas, A. Laszka, and X. Koutsoukos. Improving network connectivity and robustness using trusted nodes with application to resilient consensus. *IEEE Transactions on Control of Network Systems*, 5(4): 2036–2048, 2018.

S. Sundaram and B. Gharesifard. Distributed optimization under adversarial nodes. *IEEE Transactions on Automatic Control*, 64(3):1063–1076, 2019.

Y. Shang. Consensus of hybrid multi-agent systems with malicious nodes. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 67(4):685–689, 2020.

H. Liu, M. Xu, Y. Wu, N. Zheng, Y. Chen, and M. Z. A. Bhuiyan. Resilient bipartite consensus for multi-agent networks with antagonistic interactions. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering*, pages 1262–1269, 2018.

Y. Wu and X. He. Secure consensus control for multiagent systems with attacks and communication delays. *IEEE/CAA Journal of Automatica Sinica*, 4(1):136–142, 2017.

S.M. Dibaji and H. Ishii. Resilient consensus of second-order agent networks: Asynchronous update rules with delays. *Automatica*, 81:123–132, 2017.

H. Yiğit Öksüz and M. Akar. Approximate byzantine group consensus in robust networks. In *2018 Annual American Control Conference (ACC)*, pages 6590–6595, 2018.

J. Usevitch and D. Panagou. r-robustness and (r, s)-robustness of circulant graphs. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 4416–4421, 2017.

J. Usevitch and D. Panagou. Resilient leader-follower consensus to arbitrary reference values in time-varying graphs. *IEEE Transactions on Automatic Control*, 65 (4):1755–1762, 2020.

H.J. Leblanc and X. Koutsoukos. Resilient first-order consensus and weakly stable, higher order synchronization of continuous-time networked multiagent systems. *IEEE Transactions on Control of Network Systems*, 5(3):1219–1231, 2018.

K. Saulnier, D. Saldaa, A. Prorok, G. J. Pappas, and V. Kumar. Resilient flocking for mobile robot teams. *IEEE Robotics and Automation Letters*, 2(2):1039–1046, 2017.

J. Usevitch, K. Garg, and D. Panagou. Finite-time resilient formation control with bounded inputs. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 2567–2574, 2018.

F. Zegers, M. Hale, J. M. Shea, and W. E. Dixon. Event-triggered formation control and leader tracking with resilience to byzantine adversaries: A reputation-based approach. *IEEE Transactions on Control of Network Systems*, pages 1–1, 2021.

Donggang Liu, Peng Ning, An Liu, Cliff Wang, and Wenliang Kevin Du. Attack-resistant location estimation in wireless sensor networks. *ACM Trans. Inf. Syst. Secur.*, 11(4), July 2008. ISSN 1094-9224.

Loukas Lazos and Radha Poovendran. Serloc: Robust localization for wireless sensor networks. *ACM Trans. Sen. Netw.*, 1(1):73100, August 2005. ISSN 1550-4859.

Y. Quan, W. Chen, Z. Wu, and L. Peng. Distributed fault detection for second-order delayed multi-agent systems with adversaries. *IEEE Access*, 5:16478–16483, 2017.

F. Boem, A. J. Gallo, G. Ferrari-Trecate, and T. Parisini. A distributed attack detection method for multi-agent systems governed by consensus-based control. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 5961–5966, 2017.

M. Ji, G. Ferrari-Trecate, M. Egerstedt, and A. Buffa. Containment control in mobile networks. *IEEE Transactions on Automatic Control*, 53(8):1972–1975, 2008.

Y. Cao, W. Ren, and M. Egerstedt. Distributed containment control with multiple stationary or dynamic leaders in fixed and switching directed networks. *Automatica*, 48(8):1586–1597, 2012.

Q. Xiao, F.L. Lewis, and Z. Zeng. Containment control for multiagent systems under two intermittent control schemes. *IEEE Transactions on Automatic Control*, 64(3):1236–1243, 2019.

J. Fu, Y. Wan, G. Wen, and T. Huang. Distributed robust global containment control of second-order mul-

tiagent systems with input saturation. *IEEE Transactions on Control of Network Systems*, 6(4):1426–1437, 2019.

X. Mu and K. Liu. Containment control of single-integrator network with limited communication data rate. *IEEE Transactions on Automatic Control*, 61 (8):2232–2238, 2016.

Kananart Kuwaranancharoen, Lei Xin, and Shreyas Sundaram. Byzantine-resilient distributed optimization of multi-dimensional functions. In *2020 American Control Conference (ACC)*, pages 4399–4404, 2020.

M. Santilli, M. Franceschelli, and A. Gasparri. Robust containment control in multi-agent systems with common coordinate frames and bearing angle measurements. In *2019 IEEE 58th Conference on Decision and Control (CDC)*, pages 3710–3717, 2019.

Matteo Santilli, Mauro Franceschelli, and Andrea Gasparri. Dynamic resilient containment control in multirobot systems. *IEEE Transactions on Robotics*, 38 (1):57–70, 2022.

M.H. Protter and C.B. Morrey. *College Calculus with Analytic Geometry*. Addison-Wesley VLSI Systems Series. Addison-Wesley Publishing Company, 1977.

X. Wang, S. Mou, and S. Sundaram. A resilient convex combination for consensus-based distributed algorithms. *Numerical Algebra, Control and Optimization*, 9(3):269–281, 2019.