2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Resilient Containment Control of Multi-Agent Networks in Adversarial Environment

Chan-Yuan Kuo, Bin Du, and Dengfeng Sun

Abstract— **We study the problem of containment control in an adversarial environment, where some of the agents may be adversarial. We identify the security issue of a containment control protocol in such adversarial environment. We propose a resilient containment control protocol that ensures the state of each non-adversarial (normal) follower agent converges to the convex hull spanned by the states of the normal leader agents. Specifically, our protocol is based on the method of resilient convex combination and works for agents with a vector state. For multi-agent networks consisting of one follower agent and multiple leaders, we provide a sufficient condition on the communication topology that guarantees the success of our proposed protocol. In addition, we provide a set of numerical simulations to demonstrate the success of our protocol and verify our theoretical results.**

I. Introduction

As a fundamental problem in networked systems, containment control has received great attention since the early work [1]. The study of containment control is motivated by numerous practical applications such as search missions and convoy missions [2]. For a multi-agent network consists of follower agents and leader agents, the objective of containment control is to design a protocol such that the state of each follower agent will asymptotically converge to the convex hull spanned by the states of the leader agents. In the past decade, numerous containment control protocols have been proposed [3], [4]. A common underlying assumption of these protocols is that all agents in the network are cooperative. Namely, every agent is willing to follow a preset protocol and cooperate with other agents. Such assumption may not hold if an agent is compromised by attackers and becomes adversarial. This security concern motivates the problem of resilient containment control, which seeks to design a protocol such that the state of each non-adversarial (normal) follower agent will asymptotically converge to the convex hull spanned by the states of normal leader agents.

There is, however, a very limited literature that addresses the problem of resilient containment control [5]–[8]. In [5], under the assumption that the identities of the normal agents are known, a protocol based on the use of a virtual resilient communication layer that secures the communication between the normal agents is proposed. The construction of such a resilient layer, however, faces a challenge in practice: it is unlikely to provide full security on every communication between the normal agents, especially as the size of the network scales. Furthermore, the underlying assumption that the identities of the normal agents are known is unrealistic because the targets of the attackers are generally not known in prior. To achieve resilient containment control without knowing the identities of the adversarial agents, protocols [6]–[8] based on resilient consensus algorithms are proposed. These resilient-consensus-based algorithms typically rely on the assumption that the the graph that describes the communication topology of the agents maintains certain connectivity. Depending on whether they are applicable to networks consisting of agents with a vector state, these protocols can be divided into two categories: scalar protocols [6], [7] and vector protocols [8]. The scalar protocols are limited to agents with a scalar state because they are based on resilient scalar consensus algorithms. One potential approach to extend a resilient scalar containment protocol to a vector one is by applying the protocol component-wisely. However, this only guarantees the state of each normal follower to converge to the minimum hypercube that contains the states of the normal leader agents. Since the minimum hypercube takes the convex hull spanned by the states of the normal leader agents as a subset, resilient containment control is not achieved. On the other hand, the vector protocol [8] is applicable to agents with a vector state because it is based on a resilient vector consensus algorithm. The sufficient condition on the communication graph for the vector protocol to work requires the leader agents to have a certain amount of in-neighbors. This condition, however, can not be met because leader agents are agents that do not have any in-neighbors in the context of containment control. As a result, there is currently no resilient vector containment protocol that works under reasonable assumptions in the literature.

In this work, we fill the gap in the literature and propose a resilient containment control protocol that is applicable to networks consisting of agents with a vector state. Specifically, our protocol is based on the method of resilient convex combination [9] and only requires each follower agent to know the upper bound of the number of adversarial in-neighbors and to have a adequate amount of in-neighbors. For networks consisting of one follower agent and multiple leader agents, we provide a sufficient condition on the communication topology that guarantees the success of our protocol. In addition, we provide a set of numerical simulations to demonstrate the success of our protocol and verify the theoretical results.

This work was partially supported by NASA University Leadership Initiative through the project “Secure and Safe Assured Autonomy.”

Chan-Yuan Kuo and Dengfeng Sun are with the School of Aeronautics and Astronautics, Purdue University, IN 47907. {kuo70, dsun}@purdue.edu

Bin Du is with the College of Automation Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China. iniesdu@nuaa.edu.cn

979-8-3503-0123-6/23/$31.00 ©2023 IEEE

II. Notation and Graph Terminology

A. Notation

The set of real numbers is denoted by $\mathbb{R}$, the set of natural numbers by $\mathbb{N}$, and the set of non-negative integers by $\mathbb{Z}_{\geq 0}$. The identity matrix in $\mathbb{R}^{p\times p}$ is denoted by I_p. A vector in $\mathbb{R}^p$ with all its components equal to 1 is denoted by $\mathbf{1}_p$. The zero matrix in $\mathbb{R}^{p\times q}$ is denoted by $\mathbf{0}_{p\times q}$ and the zero vector in $\mathbb{R}^p$ by $\mathbf{0}_p$ for simplicity. For two vectors x and y in $\mathbb{R}^p$, $x \geq y$ means every component of $x - y$ is non-negative. The operation of Kronecker product is denoted by $\otimes$. The transpose of a matrix M in $\mathbb{R}^{m\times n}$ is denoted by $M^T \in \mathbb{R}^{n\times m}$. Let $\mathcal{Z} = \{z_1, z_2, \dots, z_m\}$ be a set of $m \in \mathbb{N}$ points in $\mathbb{R}^p$. The convex hull of $\mathcal{Z}$ is given by $\{\sum_{i=1}^m \theta_i z_i : \theta_i \geq 0, \forall i = 1, 2, \dots, m, \sum_{i=1}^m \theta_i = 1\}$ and is denoted by $\mathcal{H}(\mathcal{Z})$. Any point in $\mathcal{H}(\mathcal{Z})$ is said to be a convex combination of $\mathcal{Z}$. A square matrix $M = \begin{bmatrix} m_{ij} \end{bmatrix}$ in $\mathbb{R}^{p\times p}$ is row-stochastic if $m_{ij} \geq 0$, for all $i, j = 1, 2, \dots, p$, and $\sum_{j=1}^p m_{ij} = 1$, for all $i = 1, 2, \dots, p$.

B. Graph Terminology

A directed graph, or just digraph, is denoted by $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the node set and $\mathcal{E} \subseteq \mathcal{V}\times\mathcal{V}$ is the directed edge set. A directed edge from node j to node i, denoted by (j, i), implies that node j can transmit information to node i and node i can receive information from node j. If edge $(j, i) \in \mathcal{E}$, then node i is said to be an out-neighbor of node j and node j is said to be an in-neighbor of node i. The in-neighborhood of node i is defined as $\mathcal{N}_i = \{j | (j, i) \in \mathcal{E}\}$. A directed path from node i to node j is a sequence of nodes $l_1, l_2, \dots, l_m$ such that $l_1 = i, l_m = j$ and $(l_n, l_{n+1}) \in \mathcal{E}, \forall n = 0, 1, \dots, m - 1$. The cardinality of a finite set $\mathcal{S}$ is denoted by $|\mathcal{S}|$. Suppose $|\mathcal{V}| = N$ and $\mathcal{V} = \{1, 2, \dots, N\}$. A row-stochastic matrix $M = \begin{bmatrix} m_{ij} \end{bmatrix}$ in $\mathbb{R}^{N\times N}$ is said to be associated with $\mathcal{G}$ if the following conditions hold: (a) $m_{ii} > 0, \forall i \in \mathcal{V}$, (b) $m_{ij} > 0$ if $(j, i) \in \mathcal{E}$, and (c) $m_{ij} = 0$ if $(j, i) \notin \mathcal{E}$. Throughout the rest of this paper, we use the terms 'nodes' and 'agents' interchangeably.

III. Problem Formulation

A. Multi-agent Network Model

Consider a multi-agent network consisting of N agents. Specifically, let there be N_F follower agents and $N_L = N - N_F$ leader agents, where a leader agent is an agent with no in-neighbors and a follower agent is an agent with in-neighbors. The communication topology of these agents is described by a digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. The set of leader agents is denoted by $\mathcal{V}_L \subset \mathcal{V}$ and the set of follower agents by $\mathcal{V}_F = \mathcal{V} \setminus \mathcal{V}_F$.

B. Agent Model

The dynamics of each agent $i \in \mathcal{V}$ is described by

$$x_i[k+1] = x_i[k] + u_i[k], \tag{1}$$

where $k \in \mathbb{Z}_{\geq 0}$ is the discrete-time index, $x_i[k] \in \mathbb{R}^p$ and $u_i[k] \in \mathbb{R}^p$ are the state and control input of agent i at time k, respectively, and $p \in \mathbb{N}$.

C. Threat Model

Let the N-agent network be operating in an adversarial environment in which some of the agents become adversarial (malicious) after being attacked. Specifically, the N-agent network is assumed to be under a F-local malicious attack [10], which is a threat model that has been widely studied in the context of consensus [11], [12]. In the following, we present this threat model.

An agent $i \in \mathcal{V}$ is said to be malicious if it either does not follow a preset update rule or sends out the same arbitrary state information to all its out-neighbors at any time $k \in \mathbb{Z}_{\geq 0}$. An agent $i \in \mathcal{V}$ is said to be normal if it is not malicious. The set of malicious agents is denoted by $\mathcal{A} \subset \mathcal{V}$ and the set of normal agents is denoted by $\mathcal{R} = \mathcal{V} \setminus \mathcal{A}$. Notice that both leader agents and follower agents can become malicious after being attacked. The set of normal leader agents is denoted by $\mathcal{R}_L = \mathcal{V}_L \cap \mathcal{R}$ and the set of normal follower agents by $\mathcal{R}_F = \mathcal{V}_F \cap \mathcal{R}$. Furthermore, let $N_R = |\mathcal{R}|$ denote the number of normal agents, $N_{RF} = |\mathcal{R}_F|$ the number of normal follower agents, and $N_{RL} = N_R - N_{RF}$ the number of normal leader agents. To capture the worst case scenario, we further make the following two assumptions on the malicious agents. First, the identities of the malicious agents are unknown to the normal agents. Second, the malicious agents know the communication graph $\mathcal{G}$ and can collaborate with each other to maximize their threats to the normal agents.

Definition 1 (F-local malicious attack): The N-agent network is said to be under a F-local malicious attack if each normal agent $i \in \mathcal{R}$ has no more than F malicious in-neighbors, i.e., $|\mathcal{N}_i \cap \mathcal{A}| \leq F$.

D. Resilient Containment Control Objective

The objective of resilient containment control is to design a control protocol $u_i[k]$ for each agent $i \in \mathcal{V}$ such that, when the N-agent network is under a F-local malicious attack, the state of each normal follower will converge to the convex hull spanned by the states of the normal leaders.

IV. Resilient Containment Control

A. Security Issue of a Containment Control Protocol

Let each agent $i \in \mathcal{V}$ be preset to follow the (cooperative) containment control protocol [3] given by

$$\begin{aligned} u_i[k] &= \sum_{j\in\mathcal{N}_i} d_{ij}(x_j[k] - x_i[k]), && \text{if } i \in \mathcal{V}_F \\ u_i[k] &= 0, && \text{if } i \in \mathcal{V}_L \end{aligned} \tag{2}$$

where d_{ij} is the (i, j)-th entry of a row stochastic matrix D associated with the $\mathcal{G}$. An alternative representation of (2) is given by

$$\begin{aligned} u_i[k] &= (d_{ii}x_i[k] + (1 - d_{ii})v_i[k]) - x_i[k], && \text{if } i \in \mathcal{V}_F \\ u_i[k] &= 0, && \text{if } i \in \mathcal{V}_L \end{aligned} \tag{3}$$

where $v_i[k] = \sum_{j\in\mathcal{N}_i} d_{ij}(1 - d_{ii})^{-1}x_j[k]$. Let $\mathcal{X}_{\mathcal{N}_i}[k] := \{x_j[k], \forall j \in \mathcal{N}_i\}$ denote the set of states of agent i's neighbors. Notice that $v_i[k]$ is a convex combination of

$\mathcal{X}_{\mathcal{N}_i}[k]$ since $\sum_{j\in\mathcal{N}_i} d_{ij} = 1 - d_{ii}$ and $d_{ij}(1-d_{ii})^{-1} \geq 0$, $\forall j \in \mathcal{N}_i$. When the multi-agent network is not under a F-local malicious attack, if $\mathcal{G}$ contains a united directed spanning tree, then the state of each follower agent $i \in \mathcal{V}_F$ will asymptotically converge to the convex hull spanned by the states of the leader agents [3].

Definition 2 (united directed spanning tree): $\mathcal{G}$ contains a united directed spanning tree if, for each follower agent $i \in \mathcal{V}_F$, there exists a directed path from a leader agent $j \in \mathcal{V}_L$ to follower agent i.

Suppose the multi-agent network is under a F-local malicious attack. Consider a normal follower agent $i \in \mathcal{R}_F$. Suppose $\mathcal{N}_i \cap \mathcal{A} \neq \emptyset$ and agent $l \in \mathcal{N}_i$ is malicious. Recall that malicious agent l can send out the same arbitrary state information $x_l[k]$ to all its out-neighbors at any time $k \in \mathbb{Z}_{\geq 0}$. By letting $x_l[k]$ such that $v_i[k] = x_i[k]$, i.e., $x_l[k] = x_i[k] - \sum_{j\in\mathcal{N}_i\setminus\{l\}} d_{ij}d_{il}^{-1}(x_j[k] - x_i[k])$, it follows that $u_i[k] = 0$. This implies that normal follower agent i becomes autonomous and, thus, its state may not converge to the convex hull spanned by the states of the normal leaders. To mitigate the adversarial influence of the malicious agents, one effective way is to replace $v_i[k]$ by a resilient convex combination of $\mathcal{X}_{\mathcal{N}_i}[k]$, i.e., a convex combination of states of agent i's normal in-neighbors.

B. Resilient Convex Combination

Recall the definition of a F-local malicious attack. When the network is under a F-local malicious attack, each normal agent has no more than F malicious in-neighbors. In other words, each normal agent $i \in \mathcal{R}$ has at least $|\mathcal{N}_i| - F$ normal in-neighbors. Thus, if a point lies in every convex hull spanned by $|\mathcal{N}_i| - F$ points in $\mathcal{X}_{\mathcal{N}_i}[k]$, then such a point is a convex combination of states of agent i's normal in-neighbors. To see this, notice that such a point lies in the convex hull spanned by the states $x_i[k]$ of any $|\mathcal{N}_i| - F$ normal in-neighbors of agent i. In the following, we present an effective method called resilient convex combination [9] to find such a point.

Given a set of $m \in \mathbb{N}$ points in $\mathbb{R}^n$, denoted by $\mathcal{X} = \{x_1, x_2, \ldots, x_m\}$, and a non-negative integer $\kappa \in \mathbb{Z}_{\geq 0}$, resilient convex combination [9] is a method for finding a point that lies in every convex hull spanned by $m - \kappa$ points in $\mathcal{X}$. Let $\mathcal{M} = \{1, 2, \ldots, m\}$ and let $\mathcal{M}(\kappa)$ be the set of all subsets of $\mathcal{M}$ with cardinality $\rho := m - \kappa$. Notice that $r := |\mathcal{M}(\kappa)|$, i.e., the total number of such a subset, is given by $\binom{m}{m-\kappa}$. Furthermore, if $\mathcal{M}_i \in \mathcal{M}(\kappa)$, then let $\mathcal{X}_{\mathcal{M}_i} = \{x_j, \forall j \in \mathcal{M}_i\}$. Notice that if a point lies in every convex hull spanned by $m - \kappa$ points in $\mathcal{X}$, then such a point lies in the intersection of every convex hulls spanned by $m - \kappa$ points in $\mathcal{X}$. Thus, $\mathcal{I}$, the set of all points that lies in every convex hull spanned by $m - \kappa$ points in $\mathcal{X}$, is given by

$$\mathcal{I} = \bigcap_{\mathcal{M}_i \in \mathcal{M}(\kappa)} \mathcal{H}(\mathcal{X}_{\mathcal{M}_i}).$$

Lemma 1 ([9]): The set $\mathcal{I} \neq \emptyset$ if $m \geq \kappa(n+1) + 1$.

To solve for a point in $\mathcal{I}$, consider an alternative expression of $\mathcal{I}$ in terms of equality and inequality constraints. For each $\mathcal{M}_i = \{i_1, i_2, \ldots, i_r\} \in \mathcal{M}(\kappa)$, define

$$Y_i = \begin{bmatrix} x_{i_1} & x_{i_2} & \cdots & x_{i_\rho} \end{bmatrix} \in \mathbb{R}^{n\times\rho}.$$

Furthermore, let

$$X = \operatorname{diag}\{Y_i, i = 1, 2, \ldots, r\} \in \mathbb{R}^{nr\times\rho r}$$

be a block diagonal matrix with diagonal blocks $Y_j, j = 1, 2, \ldots, r$. Let $C \in \mathbb{R}^{r\times r}$ be a circulant matrix with the first row in the form of $\begin{bmatrix} 1 & -1 & 0 & \cdots & 0 \end{bmatrix}$. Then, $\mathcal{I}$ can be expressed as

$$\mathcal{I} = \left\{ \frac{1}{r}(\mathbf{1}_r^T \otimes I_n)X\boldsymbol{\beta} : \begin{array}{r} (C\otimes I_n)X\boldsymbol{\beta} = \mathbf{0}_{nr} \\ (I_r \otimes \mathbf{1}_\rho^T)\boldsymbol{\beta} = \mathbf{1}_r, \forall \boldsymbol{\beta} \in \mathbb{R}^{\rho r} \\ \boldsymbol{\beta} \geq \mathbf{0}_{\rho r} \end{array} \right\}.$$

For any $\boldsymbol{\beta} = \begin{bmatrix} \boldsymbol{\beta}_1^T & \boldsymbol{\beta}_2^T & \cdots & \boldsymbol{\beta}_r^T \end{bmatrix} \in \mathbb{R}^{\rho r}$ such that $\boldsymbol{\beta} \geq 0$, where $\boldsymbol{\beta}_i \in \mathbb{R}^\rho$, for all $i = 1, 2, \ldots, r$, the equality constraints $(C \otimes I_n)X\boldsymbol{\beta} = 0$ and $(I_r \otimes \mathbf{1}_p^T)\boldsymbol{\beta} = \mathbf{1}_r$ force all $Y_i\boldsymbol{\beta}_i$ to be identical and each $Y_i\boldsymbol{\beta}_i$ to lie in the convex hull spanned by every $\mathcal{X}_{\mathcal{M}_i}$. Thus, for any $\boldsymbol{\beta} \in \mathbb{R}^{\rho r}$ that satisfies the equality and inequality constraints, $\frac{1}{r}(\mathbf{1}_r^T \otimes I_n)X\boldsymbol{\beta}$ is a point that lies in every convex hull spanned by $m - \kappa$ points in $\mathcal{X}$.

By expressing $\mathcal{I}$ in terms of equality and inequality constraints, a point $z \in \mathcal{I}$ be can obtained by solving the quadratic programming problem given by

$$\begin{aligned} \boldsymbol{\beta}^* := \underset{\boldsymbol{\beta}\in\mathbb{R}^{\rho r}}{\arg\min}\ & \frac{1}{\rho}||\boldsymbol{\beta} - \frac{1}{\rho}\mathbf{1}_{\rho r}||_2^2 \\ \text{subject to}\quad & (C\otimes I_n)X\boldsymbol{\beta} = \mathbf{0}_{nr} \\ & (I_r \otimes \mathbf{1}_\rho^T)\boldsymbol{\beta} = \mathbf{1}_r \\ & \boldsymbol{\beta} \geq \mathbf{0}_{\rho r} \end{aligned} \tag{4}$$

and letting

$$z = \frac{1}{r}(\mathbf{1}_r^T \otimes I_n)X\boldsymbol{\beta}^*. \tag{5}$$

Through the rest of the paper, we let RCC$(\mathcal{X}, \kappa)$ be a function that takes the finite set $\mathcal{X}$ and integer κ as inputs and returns, according to (4) and (5), a point z that lies in every convex hull spanned by $|\mathcal{X}| - \kappa$ points in $\mathcal{X}$. Furthermore, we say the point z is a resilient convex combination of $\mathcal{X}$ with parameter κ.

C. Resilient Containment Control Protocol

Under the assumption that each follower agent $i \in \mathcal{V}_F$ knows in prior the upper bound F on the number of its malicious in-neighbors and $|\mathcal{N}_i| \geq F(p+1)+1$, we propose a resilient containment control protocol given by

$$\begin{aligned} u_i[k] &= (\alpha_i x_i[k] + (1-\alpha_i)r_i[k]) - x_i[k], && \text{if } i \in \mathcal{V}_F \\ u_i[k] &= 0, && \text{if } i \in \mathcal{V}_L \end{aligned} \tag{6}$$

where $0 < \alpha_i < 1$ and $r_i[k] := \text{RCC}(\mathcal{X}_i[k], F)$. Since $r_i[k]$ is a resilient convex combination of $\mathcal{X}_{\mathcal{N}_i}[k]$ with parameter F, it lies in the convex hull spanned by the states of in-neighbors of agent i. Thus, $r_i[k]$ is a convex combination of $\mathcal{X}_{\mathcal{N}_i\cap\mathcal{R}}[k] := \{x_j[k], \forall j \in \mathcal{N}_i \cap \mathcal{R}\}$ and can be expressed as

$$r_i[k] = \sum_{j\in\mathcal{N}_i\cap\mathcal{R}} \bar{d}_{ij}[k]x_j[k],$$

for some weights $\bar{d}_{ij}[k]$ such that $\bar{d}_{ij}[k] \geq 0, \forall j \in \mathcal{N}_i \cap \mathcal{R}$, and $\sum_{j\in\mathcal{N}_i\cap\mathcal{R}} \bar{d}_{ij}[k] = 1$. In the next section, we first assume that every agent is preset to follow the resilient containment control protocol (6) and the network is under a F-local malicious attack. Then, we study the closed-loop dynamics of the normal agents. Last, we focus on networks consisting of a follower agent and multiple leader agents and provide a sufficient condition on the communication topology that is required for the protcol (6) to work.

V. Analysis of the Resilient Containment Control Strategy

By substituting R-CCP (6) into the agent dynamics (1), it follows that the closed-loop dynamics of each normal follower agent $i \in \mathcal{R}_F$ and each normal leader agent $l \in \mathcal{R}_L$ are, respectively, given by

$$\begin{aligned} x_i[k+1] &= x_i[k] + u_i[k] \\ &= \alpha_i x_i[k] + (1-\alpha_i) r_i[k] \\ &= \alpha_i x_i[k] + (1-\alpha_i)\sum_{j\in\mathcal{N}_i\cap\mathcal{R}} \bar{d}_{ij}[k] x_j[k] \\ &= \tilde{d}_{ii}[k] x_i[k] + \sum_{j\in\mathcal{N}_i\cap\mathcal{R}} \tilde{d}_{ij}[k] x_j[k], \end{aligned} \tag{7}$$

where $\tilde{d}_{ii}[k] = \alpha_i, \forall k \in \mathbb{Z}_{\geq 0}$, and $\tilde{d}_{ij}[k] = (1-\alpha_i)\bar{d}_{ij}[k]$, and

$$x_l[k+1] = x_l[k] + u_l[k] = x_l[k] = \tilde{d}_{ll}[k] x_l[k], \tag{8}$$

where $\tilde{d}_{ll}[k] = 1, \forall k \in \mathbb{Z}_{\geq 0}$. Two observations about (7) and (8) can be made. First, the closed-loop dynamics of each normal agent is independent of the malicious agents. Therefore, the adversarial influence of the malicious agents is mitigated. Second, all normal leaders are autonomous and, thus, $x_l[k] = x_l[0], \forall l \in \mathcal{R}_L$. In addition, let $\mathcal{X}_{RL}[k] = \{x_l[k]\}_{l\in\mathcal{R}_L}$ denote the set of states of normal leader agents at time k. It follows that $\mathcal{H}(\mathcal{X}_{RL}[k]) = \mathcal{H}(\mathcal{X}_{RL}[0])$ at any $k \in \mathbb{Z}_{\geq 0}$.

To further study how each normal agent interacts with others, consider the subgraph $\tilde{\mathcal{G}}$ of $\mathcal{G}$ formed by the set of normal agents $\mathcal{R}$. Without loss of generality, assume that agents $1, \ldots, N_{RF}$ are normal follower agents and agents $N_{RF}+1, \ldots, N_R$ are normal leader agents. That is, $\mathcal{R}_F = \{1, \ldots, N_{RF}\}$ and $\mathcal{R}_L = \{N_{RF}+1, \ldots, N_R\}$. Thus, the row-stochastic matrix $\tilde{D}[k] = \left[\tilde{d}_{ij}[k]\right]$ associated with $\tilde{\mathcal{G}}$ is an upper triangular matrix in the form of

$$\tilde{D}[k] = \begin{bmatrix} \tilde{D}_1[k] & \tilde{D}_2[k] \\ \mathbf{0}_{N_{RL}\times N_{RF}} & I_{N_{RL}} \end{bmatrix}. \tag{9}$$

Let $x_R[k] = \begin{bmatrix} x_{RF}[k]^T & x_{RL}[k]^T \end{bmatrix}^T$ denote the state of normal agents, where $x_{RF}[k] = \begin{bmatrix} x_1[k]^T & \ldots & x_{N_{RF}}[k]^T \end{bmatrix}^T$ and $x_{RL}[k] = \begin{bmatrix} x_{N_{RF}+1}[k]^T & \ldots & x_{N_R}[k]^T \end{bmatrix}^T$ denote the state of normal follower agents and the state of normal leader agents, respectively. The closed-loop dynamics of normal agents is given by

$$x_R[k+1] = (\tilde{D}[k] \otimes I_{N_R}) x_R[k]. \tag{10}$$

For any integer m, let $\Pi_{s=0}^{m}\tilde{D}_1[s] = \tilde{D}_1[m-1]\tilde{D}_1[m-2]\cdots\tilde{D}_1[0]$ if $m \geq 0$ and $\Pi_{s=0}^{m}\tilde{D}_1[s] = I_{NF}$ if $m < 0$. By invoking (10) $n \in \mathbb{N}$ times and letting $k = 0$, the state of normal agents at time n is given by

$$\begin{aligned} x_R[n] &= \left(\prod_{s=0}^{n-1} \tilde{D}[s] \otimes I_{N_R}\right) x_R[0] \\ &= \left(\begin{bmatrix} P_1[n] & P_2[n] \\ \mathbf{0}_{N_{RL}\times N_{RF}} & I_{N_{RL}} \end{bmatrix} \otimes I_{N_R}\right) x_R[0], \end{aligned} \tag{11}$$

where

$$P_1[n] = \prod_{s=0}^{n-1} \tilde{D}_1[s]$$

and

$$P_2[n] = \sum_{t=0}^{n-1}\left(\prod_{s=0}^{n-2-t} \tilde{D}_1[(n-1)-s]\right)\tilde{D}_2[t].$$

Specifically, the state of normal follower agents at time $n \in \mathbb{N}$ is given by

$$x_{RF}[n] = (P_1[n] \otimes I_{N_{RF}}) x_{RF}[0] + (P_2[n] \otimes I_{N_{RL}}) x_{RL}[0]. \tag{12}$$

Motivated by the "Loyal Wingman" system [13], which uses multiple unmanned aerial vehicles to protect a manned vehicle on a mission, we now consider a multi-agent network consisting of $N_F = 1$ follower agent and $N_L \geq 1$ leader agents. Specifically, the in-neighborhood of the follower agent consists of all the leader agents. When the network is under a F-local malicious attack, either $\mathcal{R}_F = \emptyset$ or $\mathcal{R}_F \neq \emptyset$ is true. For the case where $\mathcal{R}_F = \emptyset$, the problem becomes trivial because there is no normal follower. For the case where $\mathcal{R}_F \neq \emptyset$, it follows that $\mathcal{R}_F = \mathcal{V}_F = \{1\}$ and $x_{RF}[k] = x_1[k]$. We show that the state of normal follower agent 1 will converge to $\mathcal{H}(\mathcal{X}_{RL}[0])$ when $|\mathcal{N}_1| \geq F(p+1)+1$.

Theorem 1: Consider a multi-agent network consisting of $N_F = 1$ follower agent and $N_L \geq 1$ leader agents whose agent communication topology is described by a digraph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$. Let the dynamics of each agent $i \in \mathcal{V}$ be given by (1) and let each agent i be preset to follow the resilient containment control protocol (6). Suppose the network is under a F-local malicious attack and, without loss of generality, there exists a normal follower whose index is 1. If the in-neighborhood of the normal follower consists of all leader agents and $|\mathcal{N}_1| = N_L \geq F(p+1)+1$, then the state of the normal follower agent will converge to the convex hull spanned by the states of the normal leader agents.

Proof: Since $\mathcal{R}_F = \{1\}$, it follows that $x_{RF}[k] = x_1[k]$ and $\tilde{D}_1[k] = \tilde{d}_{11}[k] = \alpha_1$. By substituting $x_{RF}[k] = x_1[k]$ and $\tilde{D}_1[k] = \alpha_i$ into (12), the state of normal follower agent 1 at any $n \in \mathbb{Z}_{\geq 0}$ is given by

$$\begin{aligned} x_1[n] &= (P_1[n] \otimes I_{N_{RF}}) x_1[0] + (P_2[n] \otimes I_{N_{RL}}) x_{RL}[0] \\ &= \alpha_1^{n-1} x_1[0] + (P_2[n] \otimes I_{N_{RL}}) x_{RL}[0], \end{aligned} \tag{13}$$

where, in this case, $P_2[n] = (\Sigma_{t=0}^{n-1}(\Pi_{s=0}^{n-2-t}\alpha_1)\tilde{D}_2[t])$. An observation about (13) can be made. If $\lim_{n\to\infty} \alpha_1^{n-1} = 0$

and $\lim_{n\to\infty} P_2[n]\mathbf{1}_{N_{RL}} = 1$, i.e., $P_2[n]$ converges to some row-stochastic matrix as $n \to \infty$, then the state of normal follower agent 1 will converge to $\mathcal{H}(\mathcal{X}_{RL}[0])$. Since $0 < \alpha_1 < 1$, it follows that $\lim_{n\to\infty} \alpha_1^{n-1} = 0$. Since $\tilde{D}[k]$ is row-stochastic and $\tilde{D}_1[k] = \alpha_1$, $\tilde{D}_2[k]\mathbf{1}_{N_{RL}} = 1 - \alpha_1, \forall k \in \mathbb{Z}_{\geq 0}$. This implies that

$$\begin{aligned} P_2[n]\mathbf{1}_{RL} &= \left(\sum_{t=0}^{n-1} \left(\prod_{s=0}^{n-2-t} \alpha_1 \right) \tilde{D}_2[t] \right) \mathbf{1}_{N_{RL}} \\ &= \left(\sum_{t=0}^{n-1} \left(\prod_{s=0}^{n-2-t} \alpha_1 \right) \tilde{D}_2[t]\mathbf{1}_{N_{RL}} \right) \\ &= (1-\alpha_1) \sum_{t=0}^{n-1} \left(\prod_{s=0}^{n-2-t} \alpha_1 \right) \\ &= (1-\alpha_1) \frac{1-\alpha_1^{n-1}}{1-\alpha_1} \\ &= 1 - \alpha_1^{n-1}. \end{aligned}$$

Since $0 < \alpha_1 < 1$, it follows that $\lim_{n\to\infty} P_2[n] = 1$. Hence, $x_1[n]$ will asymptotically converge to $\mathcal{H}(\mathcal{X}_{RL}[0])$. ■

In the next section, we demonstrate this result through a numerical simulation.

VI. Simulation

Consider a 7-agent network with $N_F = 1$ follower agent and $N_L = 6$ leader agents whose agent communication topology is described by a digraph shown in Figure 1. Specifically, the in-neighborhood of the follower agent consists of all leader agents. For illustration purpose, an index is assigned to each agent. Agent 1 is the follower agent and agents $2, 3, \ldots, 7$ are the leader agents. Thus, $\mathcal{V}_F = \{1\}$, $\mathcal{V}_L = \{2, 3, \ldots, 7\}$, and $\mathcal{N}_1 = \mathcal{V}_L$. The dynamics of each agent is given by (1) and let the agents be planar agents, i.e., $p = 2$. The states of the agents at time $k = 0$ are summarized in Table I.

To show resilient containment control can be achieved using the resilient containment control protocol (6) and can not be achieved using the cooperative containment control protocol (3), we consider the following three scenarios: (i) each agent $i \in \mathcal{V}$ is preset to follow the cooperative containment control protocol (3) and there are no malicious agents in the network, (ii) each agent $i \in \mathcal{V}$ is preset to follow the cooperative containment control protocol (3) and leader agent 7 is malicious, and (iii) each agent $i \in \mathcal{V}$ is preset to follow the resilient containment control protocol (6) and leader agent 7 is malicious. Notice that, in both scenarios (ii) and (iii), the network is under a F-local malicious attack, where $F = 1$, and $\mathcal{R}_L = \mathcal{V}_L \setminus \{7\}$. Furthermore, in both scenarios (ii) and (iii), by being malicious, leader agent 7 does not follow either preset protocol and changes its state in a way described by

$$x_7[k+1] = x_7[k] + 0.3 \begin{bmatrix} \sin(k/2) \\ \cos(k/2) \end{bmatrix} + 0.001k \begin{bmatrix} 3 \\ -0.5 \end{bmatrix} \quad (14)$$

at every $k \in \mathbb{Z}_{\geq 0}$. For scenario (i), we show mathematically that the state of the leader agent will converge to the convex hull spanned by the states of normal leaders. For each of the scenarios (ii) and (iii), we conduct a numerical simulation to observe the state evolution of each agent from $k = 0$ to $k = 40$. The simulation results of scenarios (ii) and (iii) are shown in Figure 2(a) and Figure 2(b), respectively.

TABLE I

The state of each agent in the 7-agent network at time $k = 0$.

i	1	2	3	4	5	6	7
$x_i[0]$	$\begin{bmatrix} 4 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 2 \\ 0 \end{bmatrix}$	$\begin{bmatrix} 1 \\ \sqrt{3} \end{bmatrix}$	$\begin{bmatrix} -1 \\ \sqrt{3} \end{bmatrix}$	$\begin{bmatrix} -2 \\ 0 \end{bmatrix}$	$\begin{bmatrix} -1 \\ -\sqrt{3} \end{bmatrix}$	$\begin{bmatrix} 1 \\ -\sqrt{3} \end{bmatrix}$

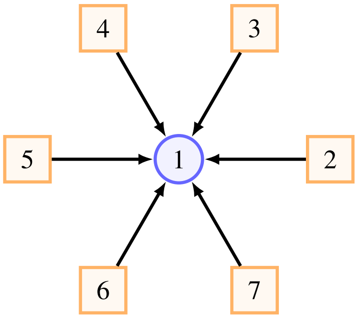


Fig. 1. A digraph that describes the communication topology of the agents in the 7-agent network. The follower agent is represented by the circle marker and the leader agents by the square markers. The number in each marker is the index of each agent. For any two agents $i, j \in \{1, 2, \ldots, 7\}$, if an arrow from agent j is pointing to agent i, then agent j is an in-neighbor of agent i.

Scenario (i): In this scenario, all agents are normal and are preset to follow the cooperative containment control protocol (3). Specifically, for follower agent 1, the weights d_{1j} are assigned as $d_{11} = 0.7$, $d_{1j} = 0.006$, $\forall j \in \{2, 3, \ldots, 6\}$, and $d_{17} = 0.27$. Note that $v_1[k] = \sum_{j\in\mathcal{N}_1} d_{ij}(1-d_{ii})^{-1}x_j[k]$ and that $\mathcal{N}_1 = \mathcal{V}_L$. Since all leader agents are normal and, thus, autonomous according to (2), it follows that, $v_1[k] = v_1[0]$, $\forall k \in \mathbb{Z}_{\geq 0}$, and that, at any time $n \in \mathbb{N}$, the state of follower agent 1 is given by

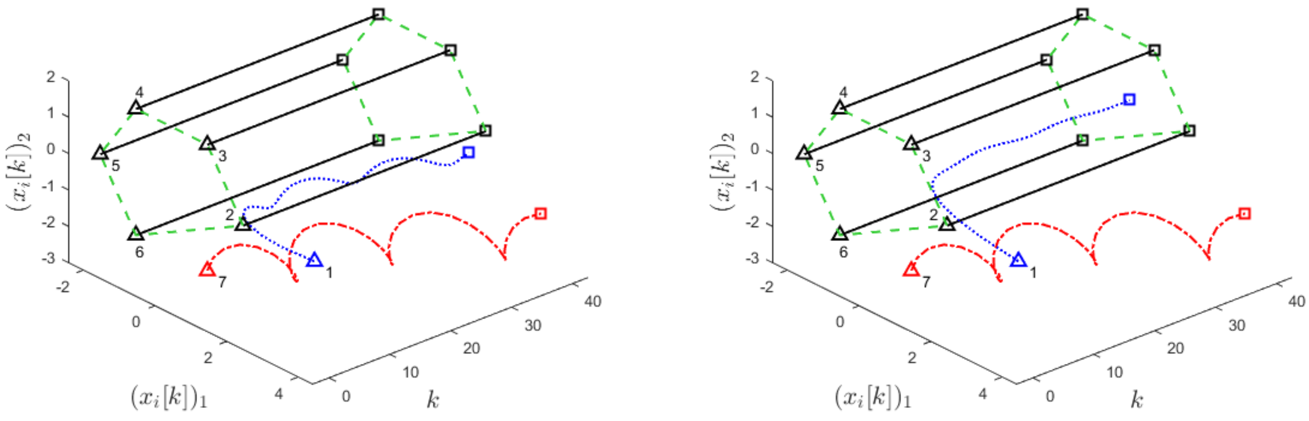
$$\begin{aligned} x_1[n] &= d_{11}^{n-1} x_i[0] + \left(\sum_{t=0}^{n-1} \left(\prod_{s=0}^{n-2-t} d_{11} \right) (1-d_{11}) \right) v_1[0] \\ &= d_{11}^{n-1} x_i[0] + \left((1-d_{11}) \frac{1-d_{11}^{n}}{1-d_{11}} \right) v_1[0] \end{aligned}$$

Since $\lim_{n\to\infty} d_{11}^{n-1} = 0$, it follows that

$$\lim_{n\to\infty} x_1[n] = v_1[0] = \sum_{j\in\mathcal{V}_L} \frac{d_{1j}}{1-d_{11}} x_i[0] = \begin{bmatrix} 0.4 \\ -0.6928 \end{bmatrix}.$$

Since $v_1[0]$ is a convex combination of $\mathcal{X}_{\mathcal{V}_L}[0]$, the state of follower agent 1 asymptotically converges to the $\mathcal{H}(\mathcal{X}_{\mathcal{V}_L}[0])$.

Scenario (ii): In this scenario, all agents except leader agent 7 are normal. The normal agents follow the cooperative containment control protocol (3) and the state of malicious leader agent 7 evolves according to (14). Specifically, follower agent 1 assigns the same weights d_{1j} to the states of



(a)

(b)

Fig. 2. The state $x_i[k]$ of each agent i in the 7-agent network from time $k = 0$ to $k = 40$ for scenarios (ii) and (iii). Here, $(x_i[k])_j$ denotes the jth entry, $j \in \{1, 2\}$, of the state vector $x_i[k]$. The state of each agent at $k = 0$ is marked by the triangle marker, while the state at $k = 40$ is marked by the square marker. The number next to each triangle marker is the index of each agent. The state trajectory of the normal follower agent is marked by the dotted line, the state trajectory of the each normal leader agent is marked by the solid line, and the state trajectory of the malicious leader agent is marked by the dash-dotted line. The boundary of each convex hull spanned by the states of the normal leader agents at $k = 0$ and $k = 40$ is marked by the dash line. (a) In scenario (ii), the state of the (normal) follower agent 1 fails to converge to the convex hull spanned by the states of the (normal) leader agents under the influence of the malicious leader agent 7. (b) In scenario (iii), the state of the (normal) follower agent 1 converges to the convex hull spanned by the states of the (normal) leader agents despite the influence of the malicious leader agent 7.

its in-neighbors as in scenario (a). Since the normal leaders are autonomous, the convex hull spanned by the states of the normal leaders is given by $\mathcal{H}(\mathcal{X}_{\mathcal{R}_L}[0])$. Due to the existence of the malicious leader agent 7 in the network, follower agent 1 fails to converge to $\mathcal{H}(\mathcal{X}_{\mathcal{R}_L}[0])$ as shown in Figure 2(a).

Scenario (iii): As in scenario (ii), in this scenario, all agents except leader agent 7 are normal. The normal agents follow the resilient containment control protocol (6) with $F = 1$ and the state of the malicious leader agent 7 evolves according to (14). The weight of follower agent 1 on its own state is assigned as $\alpha_1 = 0.7$. Notice that follower agent 1 has $|\mathcal{N}_i| = 6 \geq F(p + 1) + 1 = 4$ in-neighbors. Thus, according to Theorem 1, the state of follower agent 1 will asymptotically converge to $\mathcal{H}(\mathcal{X}_{\mathcal{R}_L}[0])$ as shown in Figure 2(b).

VII. Conclusions

In this work, we study the problem of containment control in an adversarial environment. Specifically, we consider a multi-agent network consisting of follower agents and leader agents. We identify the security issue of a cooperative containment control protocol when the network is under a F-local malicious attack. Under the assumption that each follower agent knows in prior the upper bound F on the number of its malicious in-neighbors and has at least $F(p + 1) + 1$ in-neighbors, we propose a resilient containment control protocol based on resilient convex combination. Furthermore, if the network consists of one follower agent and multiple leader agents, we provide a sufficient graph condition that guarantees the success of our proposed protocol. Finally, we provide a numerical simulation to verify our theoretical results.

References

[1] M. Ji, G. Ferrari-Trecate, M. Egerstedt, and A. Buffa, “Containment control in mobile networks,” *IEEE Transactions on Automatic Control*, vol. 53, no. 8, pp. 1972–1975, 2008.

[2] S. Jiang, S. Wang, Z. Zhan, Y. Wu, W. H. Lam, and R. Zhong, “Containment control of discrete-time multi-agent systems with application to escort control of multiple vehicles,” *International Journal of Robust and Nonlinear Control*, vol. 32, no. 12, pp. 6913–6938, 2022.

[3] Z. Li and Z. Duan, *Cooperative control of multi-agent systems: a consensus region approach*. CRC press, 2017.

[4] C. Yuan, P. Stegagno, H. He, and W. Ren, “Cooperative adaptive containment control with parameter convergence via cooperative finite-time excitation,” *IEEE Transactions on Automatic Control*, vol. 66, no. 11, pp. 5612–5618, 2021.

[5] S. Zuo and D. Yue, “Resilient containment of multigroup systems against unknown unbounded fdi attacks,” *IEEE Transactions on Industrial Electronics*, vol. 69, no. 3, pp. 2864–2873, 2021.

[6] M. Santilli, M. Franceschelli, and A. Gasparri, “Dynamic resilient containment control in multirobot systems,” *IEEE Transactions on Robotics*, vol. 38, no. 1, pp. 57–70, 2021.

[7] J. Yan and C. Wen, “Resilient containment control in adversarial environment,” *IEEE Transactions on Control of Network Systems*, vol. 7, no. 4, pp. 1951–1959, 2020.

[8] M. Santilli, M. Franceschelli, and A. Gasparri, “Secure rendezvous and static containment in multi-agent systems with adversarial intruders,” *Automatica*, vol. 143, p. 110456, 2022.

[9] X. Wang, S. Mou, and S. Sundaram, “A resilient convex combination for consensus-based distributed algorithms,” *arXiv preprint arXiv:1806.10271*, 2018.

[10] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, “Resilient asymptotic consensus in robust networks,” *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 4, pp. 766–781, 2013.

[11] S. M. Dibaji, H. Ishii, and R. Tempo, “Resilient randomized quantized consensus,” *IEEE Transactions on Automatic Control*, vol. 63, no. 8, pp. 2508–2522, 2017.

[12] L. Yuan and H. Ishii, “Resilient consensus with multi-hop communication,” in *2021 60th IEEE Conference on Decision and Control (CDC)*, pp. 2696–2701, IEEE, 2021.

[13] E. Levick, “A robot is my wingman,” *IEEE Spectrum*, vol. 57, no. 1, pp. 32–56, 2019.