ON ATTACK-RESILIENT DISTRIBUTED FORMATION CONTROL IN OPERATOR-VEHICLE NETWORKS

MINGHUI ZHU AND SONIA MARTÍNEZ *

Abstract. This paper tackles a distributed formation control problem where a group of vehicles is remotely controlled by a network of operators. Each operator-vehicle pair is attacked by an adversary, who corrupts the commands sent from the operator to the vehicle. From the point of view of operators, each adversary follows an attacking strategy linearly parameterized by some (potentially time-varying) matrix which is unknown *a priori*. In particular, we consider two scenarios depending upon whether adversaries can adapt their attacking tactics online. To assure mission completion in such a hostile environment, we propose two novel attack-resilient distributed control algorithms that allow operators to adjust their policies on the fly by exploiting the latest collected information about adversaries. Both algorithms enable vehicles to asymptotically achieve the desired formation from any initial configuration and initial estimate of the adversaries' strategies. It is further shown that the sequence of the distances to the desired formation is square summable for each proposed algorithm. In numerical examples, the convergence rates of our algorithms are exponential, outperforming the theoretic results.

1. Introduction. Recent advances in communications, sensing and computation have made possible the development of highly sophisticated unmanned vehicles. Applications include, to name a few, border patrol, search and rescue, surveillance, and target identification operations. Unmanned vehicles operate without crew onboard, which lowers their deployment costs in scenarios that are hazardous to humans. More recently, the use of unmanned vehicles by (human) operators has been proposed to enhance information sharing and maintain situational awareness. However, this capability comes at the price of an increased vulnerability of information technology systems. Motivated by this, we consider a formation control problem for an operator-vehicle network where each unmanned vehicle is able to perform real-time coordination with operators (or ground stations) via sensor and communication interfaces. However, the operator-vehicle links can be attacked by adversaries, disrupting the overall network objective. Since we cannot rule out that adversaries are able to successfully amount attacks, it is of prominent importance to provide resilient solutions that assure mission completion despite the presence of security threats.

Literature review. In information technology networks, either reactive or protective mechanisms have been exploited to prevent cyber attacks. Non-cooperative game theory is advocated as a mathematical framework to model the interdependency between attackers and administrators, and predict the behavior of attackers; see an incomplete list of references [1, 15, 26, 32].

Another relevant field is networked control systems in which the effects of imperfect communication channels on remote control are analyzed and compensated. Most of the existing papers focus on; e.g., band-limited channels [19], quantization [11], packet dropout [27], delay [10], and sampling [21].

Very recently, cyber-security of the emerging cyber-physical systems has drawn mounting attention in the control society. *Denial-of-service attacks*, destroying the data availability in control systems, are entailed in recent papers [2, 4, 6, 15]. Another important class of cyber attacks, namely *false data injection*, compromises the data integrity of state estimation and is attracting considerable effort; an incomplete

*M. Zhu is with the Department of Electrical Engineering, Pennsylvania State University, 201 Old Main, University Park, PA, 16802, (muz16@psu.edu). S. Martínez is with the Department of Mechanical and Aerospace Engineering, University of California, San Diego, 9500 Gilman Dr, La Jolla CA, 92093, (soniamd@ucsd.edu). A preliminary version of this paper is published in [35].

reference list includes [20, 24, 30, 33]. In [7, 8], the authors exploit pursuit-evasion games to compute optimal evasion strategies for mobile agents in the face of jamming attacks. Other relevant papers include [3] examining the stability of a SCADA water management system under a class of switching attacks, and our recent paper [36] studying a secure control problem of linear time-invariant systems through a receding-horizon Stackelberg game model. As [3, 36], the current paper is devoted to studying *deception attacks* where attackers maliciously modify the transmitted data. In [31], an attack space defined by the adversary's system knowledge, disclosure and disruption resources is introduced. In the paper [17], a class of trust based distributed Kalman filters is proposed for power systems to prevent data disseminated by untrusted PMUs.

Regarding malicious behavior in multi-agent systems, we distinguish [23, 28] as two representative references mostly relevant to this work. The paper [28] considers the problem of computing arbitrary functions of initial states in the presence of faulty or malicious agents, whereas [23] focuses on consensus problems. In both settings, the faulty or malicious agents are part of the network and subject to unknown (arbitrarily non-zero) inputs. Their main objective is to determine conditions under which the misbehaving agents can (or cannot) be detected and identified, and then devise algorithms to overcome the malicious behavior. This significantly departs from the problem formulation we consider here, where the attackers are external to the operator-vehicle network and can affect inter operator-vehicle connections. Additionally, we make use of a model of attackers as rational decision makers, who can make decisions in a real-time and feedback fashion. Here we aim to design completely distributed algorithms for the operator-vehicle network to maintain mission assurance under limited knowledge of teammates and opponents. Our objective is to determine an algorithm that is independent of the number of adversaries and robust to dynamical changes of communication graphs between operators.

Statement of contributions. The current paper studies a formation control problem for an operator-vehicle network in which each vehicle is remotely controlled by an operator. Each operator-vehicle pair is attacked by an adversary, who corrupts the control commands sent to the vehicle. The adversaries are modeled as rational decision makers and their strategies are linearly parameterized by some (potentially time-varying) matrices which are unknown to operators in advance. We investigate two plausible scenarios depending on the learning capabilities of adversaries. The first scenario involves *unilateral learning*, where adversaries possess (potentially incorrect) private information of operators in advance, but do not update such information during the attacking course. The second scenario assumes *bilateral learning*, where adversaries are intelligent and attempt to infer some private information of operators through their observations. We propose a class of novel distributed attack-resilient formation control algorithms each consisting of two feedback-connected blocks: a formation control block and an online learning block. The online learning mechanism serves to collect information in a real-time fashion and update the estimates of adversaries through continuous contact with them. The formation control law of each operator is adapted online to minimize a local formation error function. To do this, each operator exploits the latest estimate of her opponent and locations of neighboring vehicles. We show how each proposed algorithm guarantees that vehicles achieve asymptotically the desired formation from any initial vehicle configuration and any initial estimates of adversaries. For each proposed algorithm, the sequence of the distances to the desired formation is shown to be square summable. Two numerical examples are provided to verify the performance of the proposed algorithms. In the

simulation, the convergence rates turn out to be exponential, which outperform the analytic results characterizing the worst-case convergence rates.

A preliminary version of this paper is published in [35] where only the scenario of unilateral learning is investigated.

2. Problem formulation. In this section, we first articulate the layout of the operator-vehicle network and its formation control mission. Then, we present the adversary model that is used in the remainder of the current paper. After this, we specify two scenarios investigated in the paper.

2.1. Architecture and objective of the operator-vehicle network. Consider a group of vehicles in $\mathbb{R}^d$, labeled by $i \in V := \{1, \dots, N\}$. The dynamics of each vehicle is governed by the following discrete-time and fully actuated system:

$$p_i(k+1) = p_i(k) + u_i(k), \quad (2.1)$$

where $p_i(k) \in \mathbb{R}^d$ is the position of vehicle i and $u_i(k) \in \mathbb{R}^d$ is its input. Each vehicle i is remotely maneuvered by an operator i , and this assignment is assumed to be one-to-one and fixed over time. For simplicity, we assume that vehicles communicate only with the associated operator and not with other vehicles. Moreover, each vehicle is able to identify its location and send this information to its operator. On the other hand, an operator can exchange information with neighboring operators and deliver control commands to her vehicle. We assume that the communications between operators, and from vehicle to operator are secure¹, while the communications from operator to vehicle can be attacked. Other architectures are possible, and the present

FIG. 2.1. *The architecture of the operator-vehicle network*

one is chosen as a first main class of operator-vehicle networked systems; see Figure 2.1.

The mission of the operator-vehicle network is to achieve some desired formation which is characterized by a formation digraph $\mathcal{G} := (V, \mathcal{E})$. Each edge $(j, i) \in \mathcal{E} \subseteq V \times V \setminus \text{diag}(V)$, starting from vehicle j and pointing to vehicle i , is associated with a vector $\nu_{ij} \in \mathbb{R}^d$. Denote by $\mathcal{N}_i := \{j \in V \mid (j, i) \in \mathcal{E}\}$ the set of in-neighbors of vehicle i in $\mathcal{G}$ and let n_i be the cardinality of $\mathcal{N}_i$; i.e., $n_i = |\mathcal{N}_i|$. The set of in-neighbors of agent i will be enumerated as $\mathcal{N}_i = \{i_1, \dots, i_{n_i}\}$. Being a member of the team, each operator i is only aware of local formation constraints; i.e., ν_{ij} for $j \in \mathcal{N}_i$.

¹Alternatively, it can be assumed that operators have access to vehicles' positions by an external and safe measurement system.

The multi-vehicle formation control mission can be formulated as a team optimization problem where the global optimum corresponds to the desired formation of vehicles. In particular, we encode the problem into the following quadratic program:²

$$\min_p [J(p) := \sum_{(j,i) \in \mathcal{E}} \|p_i - p_j - \nu_{ij}\|_{P_{ij}}^2],$$

where the vector $p := [p_1^T, \dots, p_N^T]^T \in \mathbb{R}^{Nd}$ is the collection of vehicles' locations. The matrix $P_{ij} \in \mathbb{R}^{d \times d}$ is a diagonal and positive-definite weight matrix and represents the preference of operator i on the link (j, i) with $j \in \mathcal{N}_i$. Observe that $J(p)$ is a convex function of p since $\|\cdot\|_{P_{ij}}^2$ is convex and $p_i - p_j - \nu_{ij}$ is affine [9]. Denote by the set of the (global) minimizers $X^* \subset \mathbb{R}^{Nd}$. In this paper, we impose the following on $\mathcal{G}$ and X^* :

Assumption 2.1. *The digraph $\mathcal{G}$ is strongly connected. In addition, $X^* \neq \emptyset$ and $J(p^*) = 0$ for any $p^* \in X^*$.*

The objective function $J(p)$ can describe any shape in $\mathbb{R}^d$ by adjusting the formation vectors ν_{ij} . We assume that operators and vehicles are synchronized. The communication digraph between operators is assumed to be fixed and identical to $\mathcal{G}$. That is, each operator only receives information from in-neighbors in $\mathcal{N}_i$ at each time instant. We later discuss a possible extension to deal with time-varying communication digraphs; see Section 5.

Remark 2.1. *Similar formation functions are used in [13, 14]. When $\nu_{ij} = 0$ for all $(i, j) \in \mathcal{E}$, then the formation control problem reduces to the special case of rendezvous which has received considerable attention [12, 16, 22].* •

2.2. Model of rational adversaries. A group of N adversaries aims to abort the mission of formation stabilization. To achieve this, an adversary is allocated to attack a specific operator-vehicle pair and this relation does not change over time. Thus, we identify adversary i with the operator-vehicle pair i . Each adversary is able to locate her target vehicle, and eavesdrop on incoming messages of her target operator. We further assume that adversaries are able to collect some (potentially imperfect and dynamically changing) information of their opponents. Specifically, adversary i will have estimates $\nu_{ij}^a(k) \in \mathbb{R}^d$ of ν_{ij} at time k and $P_{ij}^a \in \mathbb{R}^{d \times d}$ of P_{ij} , for $j \in \mathcal{N}_i$. Here, the matrix P_{ij}^a is positive-definite and diagonal.

As [7, 8, 15], we assume that adversaries are rational decision makers, and they make real-time decisions based on the latest information available. In particular, at time k , adversary i identifies $p_i(k)$ of her target vehicle, eavesdrops $p_j(k)$ sent from operator $j \in \mathcal{N}_i$ to operator i , and intercepts $u_i(k)$ sent from operator i to vehicle i . The adversary then computes a command $v_i(k)$ which is added to $u_i(k)$ so that vehicle i receives and implements $u_i(k) + v_i(k)$ instead. The command $v_i(k)$ will be the solution to the following program:

$$\max_{v_i \in \mathbb{R}^d} \sum_{j \in \mathcal{N}_i} \|p_j(k) - (p_i(k) + u_i(k) + v_i) - \nu_{ij}^a(k)\|_{P_{ij}^a}^2 - \|v_i\|_{R_i}^2, \quad (2.2)$$

where $R_i \in \mathbb{R}^{d \times d}$ is diagonal and positive definite. The above optimization problem captures two partly conflicting objectives of adversary i . On the one hand, adversary i

²In this paper, we denote by $\|x\|_A^2 := x^T A x$ the weighted norm of vector x for a matrix A with the proper dimensions.

would like to destabilize the formation associated with vehicle i , and this malicious interest is encapsulated in the first term $\sum_{j \in \mathcal{N}_i} \|p_j(k) - (p_i(k) + u_i(k) + v_i) - \nu_{ij}^a(k)\|_{P_{ij}^a}^2$.

On the other hand, adversary i would like to avoid a high attacking cost $\|v_i\|_{R_i}^2$. Here we provide a justification on the attacking cost $\|v_i\|_{R_i}^2$ in problem (2.2). At each time, adversary i has to spend some energy to successfully decode the message and deliver the wrong data to vehicle i . The energy consumption depends upon security schemes; e.g., cryptography and/or radio frequency, employed by operator i . A larger $\|v_i(k)\|$ alerts operator i that there is a greater risk to her vehicle, and consequently operator i will raise the security level $s_i(k+1)$ (e.g., the expansion of radio frequencies) of the link to vehicle i for time $k+1$, increasing the subsequent costs paid by adversary i (e.g. to block all of the radio frequencies following the operator) at the next time instant. That is, $s_i(k+1) = \|v_i(k)\|_{R_i}$. For simplicity, the attacking cost at time $k+1$ is assumed to be identical to the security level $s_i(k+1)$. As a rational decision maker, adversary i is willing to reduce such attacking cost. In the remainder of the paper, we assume the following on the cost matrices of adversaries:

Assumption 2.2. *For each $i \in V$, it holds that $\sum_{j \in \mathcal{N}_i} P_{ij}^a - R_i < 0$.*

In this way, the objective function of the optimization problem (2.2) is strictly concave. This can be easily verified by noticing that the Hessian of $2 \sum_{j \in \mathcal{N}_i} P_{ij}^a - 2R_i$ is negative definite. As a consequence, the optimization problem (2.2) is well defined, and its solution is uniquely determined by:

$$v_i(k) = - \sum_{j \in \mathcal{N}_i} L_{ij}(p_j(k) - (p_i(k) + u_i(k)) - \nu_{ij}^a(k)), \quad (2.3)$$

where $L_{ij} := (R_i - \sum_{j \in \mathcal{N}_i} P_{ij}^a)^{-1} P_{ij}^a \in \mathbb{R}^{d \times d}$ is diagonal and positive definite.

2.3. Justification of the attacker model. Problem (2.2) assumes that each adversary is a rational decision maker, and always chooses the optimal action based on the information available. Compared with [20, 23, 24, 25, 28, 30, 33] focusing on attacking detection, our attacker model limits the actions of adversaries to some extent. Assumptions that restrict the behavior of attackers are usually taken in main references on system control under jamming attacks. For example, the paper [15] limits the number of denial-of-service attacks in a time period. This is based on the consideration that the jammer is energy constrained. Moreover, the paper [7] assumes that the maximum speeds of UAVs and the aerial jammer are identical in a pursuit-evasion game. In addition, the papers [2, 4, 6] restrict the attacking strategies to follow some I.I.D. probability distributions. We argue that the investigation of resilient control policies for constrained jamming attacks is reasonable and can lead to important insights for network vulnerability and algorithm design. Clearly, if the actions of adversaries were omnipotent, no strategy could counteract them. But, even in the case that jammer actions are limited, it is not fully clear what strategy would work or fail. The analysis of these settings can reveal important system and algorithm weaknesses.

2.4. Information about opponents and online adaptation. In a hostile environment, it is not realistic to expect that decision makers have complete and perfect information of their opponents. On the other hand, information about opponents plays a vital role in defending or attacking a system. Throughout this paper, we assume that operator i knows that adversary i is rational and makes decisions

online based on the solution to the optimization problem (2.2). In particular, we will investigate the following two plausible attacking scenarios.

SCENARIO I - Unilateral learning

In the first scenario, adversary i does not update her estimates; i.e., $\nu_{ij}^a(k) = \nu_{ij}^a$ for all $k \geq 0$ even though ν_{ij}^a and P_{ij}^a may be different from the true values of ν_{ij} and P_{ij} . On the other hand, operator i has no access to the values of R_i , P_{ij}^a and ν_{ij}^a which are some private information of adversary i . In order to maintain system resilience, operators can aim to identify the adversarial behavior. To do this, we will novelly exploit the ideas of reinforcement learning [29], and adaptive control [5], which operators can use to learn these parameters through continuous contact with adversaries.

SCENARIO II - Bilateral learning

Adversaries could be intelligent, attempting to learn some unknown information online as well. This motivates us to investigate a second scenario in which adversaries infer private information during the attacking course. For simplicity, we will assume that operator i and adversary i know the cost matrices of each other, and how each other makes real-time decisions on $v_i(k)$ and $u_i(k)$. However, adversary i is unaware of the formation vectors ν_{ij} associated with operator i , and thus attempts to identify these quantities online. In order to play against this class of intelligent adversaries, we show how operators can keep track of the dynamically changing and unmodeled estimates of adversaries, and in turn adapt their defense tactics.

2.5. Discussion. Informally speaking, we pose the formation control problem as a dynamic non-cooperative game between two teams of rational decision makers: operators and adversaries. In SCENARIO I (unilateral learning), adversaries do not adapt their strategies online, but they do in SCENARIO II (bilateral learning). In contrast to [7, 8], decision makers in our problem formulation do not aim to determine a Nash equilibrium, which is a widely used notion in non-cooperative game theory. Instead, the main focus of the current paper is to quantitatively analyze how online adaptation helps operators maintain system functions when they are facing vague and (potentially intelligent) adversaries.

The papers [20, 24, 30, 33] focus on detection of false data injection attacks against state estimation. There, attackers could intelligently take advantage of channel noises and successfully bypass the detectors if they have perfect information of the system dynamics and detectors. The papers [23, 28] aim to detect malicious behavior in a multi-agent setting. Attack detection is a key security variable, and we should mention that this is trivial in the set-up of the current paper. Since we assume communication channels are noise-free, then operators can verify whether their commands are corrupted by simply examining the locations of their associated vehicles. Here, our focus is network resilience to malicious attacks, which is another key security aspect. It is of interest to investigate attack detection in the setting of operator-vehicle networks and this is one of the future work.

In our recent papers [36, 37], we consider deception attacks for a single group of operator, plant and adversary. The plant dynamics in [36, 37] is more complicated than those in the current paper and could be any stabilizable linear time-invariant system. In contrast, the challenge of the current paper is to coordinate multiple vehicles in a distributed way against deception attacks.

Notations. In the sequel, we let tr be the trace operator of matrices, and let $\|A\|_F$ and $\|A\|$ denote the Frobenius norm and 2-norm of a real matrix $A \in \mathbb{R}^{m \times n}$,

respectively. Recall that $\|A\|_F^2 = \text{tr}(A^T A) = \sum_{i=1}^m \sum_{j=1}^n a_{ij}^2$ and $\|A\| \leq \|A\|_F$. We will use the shorthand of $[B_{ij}]_{j \in \mathcal{N}_i} := [B_{ii_1}, \dots, B_{ii_{n_i}}] \in \mathbb{R}^{n \times mn_i}$ where the dimensions of the given $B_{ij} \in \mathbb{R}^{n \times m}$ will be identical for all $j \in \mathcal{N}_i$. Consider the diagonal vector map, $\text{diag}_{\text{ve}} : \mathbb{R}^{d \times d} \rightarrow \mathbb{R}^d$, defined as $\text{diag}_{\text{ve}}(A) = v$, with $v_i = A_{ii}$, for all i . Similarly, define the diagonal matrix map, $\text{diag}_{\text{ma}} : \mathbb{R}^d \rightarrow \mathbb{R}^{d \times d}$, as $\text{diag}_{\text{ma}}(v) = D$, with $D_{ii} = v_i$, $D_{ij} = 0$, for all i, j and $j \neq i$. Let $\mathbb{P}_{\geq 0} : \mathbb{R}^d \rightarrow \mathbb{R}^d$ be the projection operator from $\mathbb{R}^d$ onto the non-negative orthant of $\mathbb{R}^d$. Now define the linear operator $\mathbb{P}_i : \mathbb{R}^{n_i(d+1) \times d} \rightarrow \mathbb{R}^{n_i(d+1) \times d}$ as follows. Given $\Lambda \in \mathbb{R}^{n_i(d+1) \times d}$, then $\mathbb{P}_i(\Lambda) = M \in \mathbb{R}^{n_i(d+1) \times d}$, defined block-wise as follows:

$$\begin{aligned} \text{if } \Lambda^T &:= [[L_{ij}^T]_{j \in \mathcal{N}_i}, [\eta_{ij}^T]_{j \in \mathcal{N}_i}], \quad \text{then } M^T := [[M_{ij}^T]_{j \in \mathcal{N}_i}, [\mu_{ij}^T]_{j \in \mathcal{N}_i}], \text{ with} \\ M_{ij}^T &= \text{diag}_{\text{ma}}(\mathbb{P}_{\geq 0}(\text{diag}_{\text{ve}}(L_{ij}^T))), \quad \mu_{ij}^T = \eta_{ij}^T, \quad j \in \mathcal{N}_i. \end{aligned} \quad (2.4)$$

The linear operator $\mathbb{P}_i$ will be used in the learning rule of the algorithm proposed for SCENARIO I (unilateral learning).

3. Attack-resilient distributed formation control with unilateral learning. In this section, we investigate SCENARIO I (unilateral learning) and propose a novel formation control algorithm, namely ALGORITHM I (unilateral learning), to guarantee the formation control mission under malicious attacks. It is worthy to recall that in this scenario adversary i does not update her estimates in this scenario; i.e., $\nu_{ij}^a(k) = \nu_{ij}^a$ for all $k \geq 0$.

3.1. A linearly parametric interpretation of attacking policies. Recall that operator i is aware that the decisions of adversary i are based on the solution to the optimization problem (2.2). This implies that operator i knows that $v_i(k)$ is in the form of (2.3), but does not have access to the real values of L_{ij} and ν_{ij}^a . A more compact expression for $v_i(k)$ is given in the following.

LEMMA 3.1. *The vector $v_i(k)$ can be written in the following form:*

$$\begin{aligned} v_i(k) &= \Theta_i^T \Phi_i(k) = - \sum_{j \in \mathcal{N}_i} \{L_{ij}(p_j(k) - (p_i(k) + u_i(k)) - \nu_{ij}) + \eta_{ij}\} \\ &= - \sum_{j \in \mathcal{N}_i} L_{ij}((p_j(k) - (p_i(k) + u_i(k)) - \nu_{ij}) + (\nu_{ij} - \nu_{ij}^a)), \end{aligned}$$

where $\eta_{ij} := L_{ij}(\nu_{ij} - \nu_{ij}^a) \in \mathbb{R}^d$, and matrices $\Theta_i \in \mathbb{R}^{n_i(d+1) \times d}$, $\phi_i(k) \in \mathbb{R}^{n_i d}$, $\Phi_i(k) \in \mathbb{R}^{n_i(d+1)}$ are given by:

$$\begin{aligned} \phi_i(k) &:= - \begin{bmatrix} p_{i_1}(k) - (p_i(k) + u_i(k)) - \nu_{ii_1} \\ \vdots \\ p_{i_{n_i}}(k) - (p_i(k) + u_i(k)) - \nu_{ii_{n_i}} \end{bmatrix}, \\ \Theta_i^T &:= [[L_{ij}]_{j \in \mathcal{N}_i} \quad [\eta_{ij}]_{j \in \mathcal{N}_i}], \quad \Phi_i(k) := -[\phi_i(k)^T \quad 1 \dots 1]^T. \end{aligned} \quad (3.1)$$

Proof. This fact can be readily verified. $\square$

In the light of the above lemma, we will equivalently assume that operator i is aware of $v_i(k)$ being the product of Θ_i and $\Phi_i(k)$, where the unknown parameter Θ_i is referred to as the target parameter of operator i , and the vector $\Phi_i(k)$ is referred

to as the regression vector of operator i at time k . In other words, from the point of view of operator i , the attacking strategy of adversary i is linearly parameterized by the unknown (but fixed) matrix Θ_i .

3.2. ALGORITHM I (unilateral learning) and its convergence properties.

[*Informal description*] Overall, ALGORITHM I (unilateral learning) can be roughly described as follows. At each time instant, each operator first collects the current locations of neighboring operators' vehicles. Then, the operator computes a control command $u_i(k)$ minimizing a local formation error function by assuming that her neighboring vehicles do not move. This computation is based on the certainty equivalence principle; i.e., operator i exploits her latest estimate $\Theta_i(k)$ to predict that adversary i corrupts her command by adding $v_i^o(k) := \Theta_i(k)^T \Phi_i(k)$ as if $\Theta_i(k)$ were identical to Θ_i . After that, the operator sends the new command $u_i(k)$ to her associated vehicle. Adversary i then corrupts the command by adding the signal $v_i(k)$ linearly parameterized by Θ_i . Vehicle i receives, implements, and further sends back to operator i the new position $p_i(k+1)$. After that, operator i computes the new estimation error of Θ_i , and updates her estimate to minimize a local estimation error function.

We now formally state the interactions of the i^{th} group consisting of operator, vehicle and adversary i in Algorithm 1. The rule to compute $u_i(k)$, and the precise update law for $\Theta_i(k)$ can be found there. The notations used to describe ALGORITHM I (unilateral learning) are summarized in Table 3.1.

TABLE 3.1
Notations used in ALGORITHM I (unilateral learning)

$p_i(k) \in \mathbb{R}^d$	the location of vehicle i at time k
$p_i(k+1 k) \in \mathbb{R}^d$	the prediction of $p_i(k+1)$ produced by operator i at time k
$P_{ij} \in \mathbb{R}^{d \times d}$	the weight matrix assigned by operator i to the formation vector ν_{ij} for $j \in \mathcal{N}_i$
$P_{ii} \in \mathbb{R}^{d \times d}$	the weight matrix assigned by operator i to her own current location
$u_i(k) \in \mathbb{R}^d$	the control command of operator i at time k
$v_i(k) \in \mathbb{R}^d$	the command generated by adversary i at time k and given in (2.3)
$v_i^o(k) \in \mathbb{R}^d$	the prediction of $v_i(k)$ generated by operator i
$\Theta_i \in \mathbb{R}^{n_i(d+1) \times d}$	the target parameter of operator i given in (3.1)
$\Theta_i(k) \in \mathbb{R}^{n_i(d+1) \times d}$	the estimate of Θ_i produced by operator i at time k
$\Phi_i(k) \in \mathbb{R}^{n_i(d+1)}$	the regression vector of operator i at time k given in (3.1)
$m_i(k) := \sqrt{1 + \ \Phi_i(k)\ ^2}$	the normalized term of operator i
$\mathbb{P}_i$	a projection operator defined by (2.4)

Remark 3.1. We denote $P_i := P_{ii} + \sum_{j \in \mathcal{N}_i} P_{ij}$ and let $\Theta_i(k)^T$ be partitioned in the form of $\Theta_i(k)^T = [[L_{ij}(k)]_{j \in \mathcal{N}_i} \quad [\eta_{ij}(k)]_{j \in \mathcal{N}_i}]$, where $L_{ij}(k) \in \mathbb{R}^{d \times d}$ and $\eta_{ij}(k) \in$

Algorithm 1 ALGORITHM I (unilateral learning) for group i

Initialization: Operator i chooses any $\tilde{\Theta}_i \in \mathbb{R}^{n_i(d+1) \times d}$ and lets $\Theta_i(0) = \mathbb{P}_i[\tilde{\Theta}_i]$ as the initial estimate of Θ_i .

Iteration: At each $k \geq 0$, adversary, operator, and vehicle i execute the following steps:

- 1: Operator i receives $p_j(k)$ from operator $j \in \mathcal{N}_i$, and solves the following quadratic program:

$$\begin{aligned} \min_{u_i(k) \in \mathbb{R}^d} \quad & \sum_{j \in \mathcal{N}_i} \|p_j(k) - p_i(k+1|k) - \nu_{ij}\|_{P_{ij}}^2 + \|p_i(k) - p_i(k+1|k)\|_{P_{ii}}^2, \\ \text{s.t.} \quad & p_i(k+1|k) = p_i(k) + u_i(k) + v_i^o(k), \end{aligned} \quad (3.2)$$

to obtain the optimal solution $u_i(k)$ where $v_i^o(k) := \Theta_i(k)^T \Phi_i(k)$ and P_{ii} is a positive-definite and diagonal matrix.

- 2: Operator i sends $u_i(k)$ to vehicle i , and generates a prediction of $p_i(k+1)$ in such a way that $p_i(k+1|k) = p_i(k) + u_i(k) + v_i^o(k)$.
 - 3: Adversary i identifies $p_i(k)$, eavesdrops on $p_j(k)$ sent from operator $j \in \mathcal{N}_i$ to operator i , and corrupts $u_i(k)$ by adding $v_i(k) = \Theta_i^T \Phi_i(k)$.
 - 4: Vehicle i receives and implements the corrupted command $u_i(k) + v_i(k)$, and then sends back the new location $p_i(k+1) = p_i(k) + u_i(k) + v_i(k)$ to operator i .
 - 5: Operator i computes the estimation error $e_i(k) = p_i(k+1) - p_i(k+1|k)$, and updates her parameter estimate as $\Theta_i(k+1) = \mathbb{P}_i[\Theta_i(k) + \frac{1}{m_i(k)^2} \Phi_i(k) e_i(k)^T]$, where $m_i(k) := \sqrt{1 + \|\Phi_i(k)\|^2}$.
 - 6: Repeat for $k = k+1$.
-

$\mathbb{R}^d$, for $j \in \mathcal{N}_i = \{1, \dots, n_i\}$. Then, the solution $u_i(k)$ to the quadratic program in Step 1 of ALGORITHM I (unilateral learning) can be explicitly computed as follows:

$$\begin{aligned} u_i(k) = & \left(I + \sum_{j \in \mathcal{N}_i} L_{ij}(k) \right)^{-1} \times \left\{ \sum_{j \in \mathcal{N}_i} P_i^{-1} P_{ij} (p_j(k) - p_i(k) - \nu_{ij}) \right. \\ & \left. + \sum_{j \in \mathcal{N}_i} L_{ij}(k) (p_j(k) - p_i(k) - \nu_{ij}) + \sum_{j \in \mathcal{N}_i} \eta_{ij}(k) \right\}. \end{aligned} \quad (3.3)$$

Hence, the program in Step 1 of ALGORITHM I (unilateral learning) is equivalent to the computation (3.3). In Step 5 of ALGORITHM I (unilateral learning), operator i utilizes a projected parameter identifier to learn Θ_i online. This scheme extends the classic (vector) normalized gradient algorithm; e.g., in [5], to the matrix case and further incorporates the projection operator $\mathbb{P}_i$ to guarantee that $u_i(k)$ is well defined. That is, the introduction of $\mathbb{P}_i$ ensures that the estimate $L_{ij}(k)$ is positive definite, and that $I + \sum_{j \in \mathcal{N}_i} L_{ij}(k)$ is nonsingular. As in [5], the term $\frac{1}{m_i(k)^2} \Phi_i(k) e_i(k)^T$ in the update law of $\Theta_i(k)$ is to minimize the error cost $\frac{e_i(k)^T e_i(k)}{m_i(k)^2}$. Here, $e_i(k)$ is the position estimation error, and $m_i(k)$ is a normalizing factor. •

The following theorem guarantees that our proposed ALGORITHM I (unilateral learning) is attack-resilient and allows the multi-vehicle to achieve the desired formation in SCENARIO I (unilateral learning).

THEOREM 3.2. (Convergence properties of ALGORITHM I (unilateral learning)): Consider SCENARIO I (unilateral learning) with any initial configura-

tion $p(0) \in \mathbb{R}^{Nd}$ of vehicles. If Assumptions 2.1 and 2.2 hold, then ALGORITHM I (unilateral learning) for every group i ensures that the vehicles asymptotically achieve the desired formation; i.e., $\lim_{k \rightarrow +\infty} \text{dist}(p(k), X^*) = 0$. Furthermore, the convergence rate of ALGORITHM I (unilateral learning) ensures the following:

$$\sum_{k=0}^{+\infty} \sum_{(i,j) \in \mathcal{E}} \|p_j(k) - p_i(k) - \nu_{ij}\|^2 < +\infty.$$

Proof. The proof is provided in the appendix. $\square$

3.3. A numerical example for ALGORITHM I (unilateral learning).

Here we evaluate the performance of ALGORITHM I (unilateral learning) through a numerical example. Consider a group of 15 vehicles which are initially randomly deployed over a square of 50×50 length units as shown in Figure 3.1(a). Figure 3.1(c) delineates the trajectory of each vehicle in the first 60 iterations of the algorithm. The configuration of the vehicles at the 60th iteration of ALGORITHM I (unilateral learning) is given by Figure 3.1(b) and this one is identical to the desired formation. This fact can be verified by Figure 3.1(d), which shows the evolution of the formation errors of ALGORITHM I (unilateral learning). Figure 3.1(d) also demonstrates that the convergence rate of ALGORITHM I (unilateral learning) in the simulation is exponential and this is faster than our analytical result in Theorem 3.2.

(a) Initial configuration of vehicles for ALGORITHM I (unilateral learning).

(b) The configuration of vehicles at the 60th iteration under ALGORITHM I (unilateral learning).

4. Attack-resilient distributed formation control with bilateral learning. In this section, we investigate the more challenging SCENARIO II (bilateral learning) and we propose ALGORITHM II (bilateral learning) to defeat the intelligent adversaries.

In SCENARIO II (bilateral learning), adversary i is aware of P_{ij} (i.e., $P_{ij}^a = P_{ij}$) and the policy of operator i to compute $u_i(k)$. However, adversary i has no access to the formation vectors of ν_{ij} for $j \in \mathcal{N}_i$ in advance. This motivates adversary i to learn ν_{ij} . In what follows, the quantity $\nu_{ij}^a(k)$ is an estimate of ν_{ij} maintained by adversary i at time k . On the other hand, operator i is assumed to know R_i and the rule of adversary i making decisions without accessing the instantaneous estimate $\nu_{ij}^a(k)$. In order to play against her opponent, operator i has to keep track of the time-varying quantity $\nu_{ij}^a(k)$. Operator i is completely unaware of the learning dynamics associated with the estimates $\nu_{ij}^a(k)$, and thus $\nu_{ij}^a(k)$ is totally unmodeled for operator i . The best

(c) Trajectories of the vehicles during the first 60 iterations of ALGORITHM I (unilateral learning). The green squares stand for initial locations and red circles represent final locations.

(d) The evolution of formation errors during the first 60 iterations of ALGORITHM I (unilateral learning).

operator i can do is to observe some quantity that depends on $\nu_{ij}^a(k)$ at time k , and generate a posterior estimate $\nu_{ij}^o(k+1)$ of $\nu_{ij}^a(k)$. Through the certainty equivalence principle, the actions of operator i and adversary i at time k employ the estimates of $\nu_{ij}^a(k)$ and $\nu_{ij}^o(k)$, respectively.

In the remainder of this section, the subscripts of a and o are used to indicate the target parameters of adversaries and operators, respectively, and the superscripts of a and o are employed to indicate the estimates of target parameters or other local variables of adversaries and operators, respectively. Towards this end, let us make the following notations: $\Omega_{a,i} = [[\nu_{ij}^T]_{j \in \mathcal{N}_i}]^T$ (resp. $\Psi_{o,i}(k) = \Omega_i^a(k)$) is the target parameter of adversary i (resp. operator i), and $\Omega_i^a(k) = [[\nu_{ij}^a(k)^T]_{j \in \mathcal{N}_i}]^T$ (resp. $\Psi_i^o(k) = [[\nu_{ij}^o(k)^T]_{j \in \mathcal{N}_i}]^T$) represents the estimate of $\Omega_{a,i}$ (resp. $\Psi_{o,i}(k-1)$) produced by adversary i (resp. operator i) at time k .

4.1. A linearly parametric interpretation of attacking policies and local formation control laws. In this part, we first find a linearly parametric interpretation of attacking policies from the point of view of operators. Then we devise a local formation control law for each operator. Before it, we adopt the following notation³:

$$L_{ij} := (R_i - \sum_{j \in \mathcal{N}_i} P_{ij})^{-1} P_{ij}, \quad L_i := \sum_{j \in \mathcal{N}_i} L_{ij},$$

$$M_{ij} := (I + L_i)^{-1} P_i^{-1} P_{ij}, \quad M_i := \sum_{j \in \mathcal{N}_i} M_{ij}.$$

Throughout this section, we assume that the cost matrices of each operator are homogeneous, and this assumption is formally stated as follows:

Assumption 4.1. *For each $i \in V$, there is a diagonal and positive-definite matrix $\bar{P}_i$ such that $P_{ij} = \frac{1}{n_i} \bar{P}_i$ for all $j \in \mathcal{N}_i$.*

With this assumption, it is easy to see that:

$$L_{ij} = \frac{1}{n_i} (R_i - \bar{P}_i)^{-1} \bar{P}_i, \quad L_{ij} = \frac{1}{n_i} L_i, \quad M_{ij} = \frac{1}{n_i} M_i.$$

³Note that similar letters do not exactly match their meaning in the previous section.

LEMMA 4.1. *The vector $v_i(k)$ can be written in the following way:*

$$v_i(k) = - \sum_{j \in \mathcal{N}_i} L_{ij}(p_j(k) - p_i(k) - u_i(k)) + (\Phi_i^o)^T \Psi_{o,i}(k), \quad (4.1)$$

where the matrices of Φ_i^o and $\Psi_{o,i}(k)$ are given by:

$$(\Phi_i^o)^T := [[L_{ij}]_{j \in \mathcal{N}_i}], \quad \Psi_{o,i}(k) := [[\nu_{ij}^a(k)^T]_{j \in \mathcal{N}_i}^T]^T \quad (4.2)$$

Proof. It is straightforward to verify this result. $\square$

In SCENARIO II (bilateral learning), operator i knows that adversary i bases her decisions on the solution to the optimization problem (2.2) which is parameterized by the unknown quantity $\nu_{ij}^a(k)$. Lemma 4.1 indicates that, from operator i 's point of view, the attacking strategy of adversary i is linearly parameterized by the unknown and time-varying matrix $\Psi_{o,i}(k)$. The quantity Φ_i^o is referred to as the regression vector of operator i .

We are now in the position to devise a local formation control law for each operator. In particular, with $p_j(k)$ for $j \in \mathcal{N}_i$, operator i computes the control command $u_i(k)$ by solving the following program to minimize the local formation error:

$$\begin{aligned} \min_{u_i(k) \in \mathbb{R}^d} \quad & \sum_{j \in \mathcal{N}_i} \|p_j(k) - p_i(k+1|k) - \nu_{ij}\|_{P_{ij}}^2 + \|p_i(k) - p_i(k+1|k)\|_{P_{ii}}^2, \\ \text{s.t.} \quad & p_i(k+1|k) = p_i(k) + u_i(k) + v_i^o(k), \end{aligned} \quad (4.3)$$

where $v_i^o(k)$ is a prediction of $v_i(k)$ and defined as follows:

$$v_i^o(k) := - \sum_{j \in \mathcal{N}_i} L_{ij}(p_j(k) - (p_i(k) + u_i(k))) + (\Phi_i^o)^T \Psi_i^o(k). \quad (4.4)$$

The solution to (4.3) is uniquely determined by:

$$\begin{aligned} u_i(k) = (I + L_i)^{-1} \{ & \sum_{j \in \mathcal{N}_i} P_i^{-1} P_{ij}(p_j(k) - p_i(k) - \nu_{ij}) \\ & + \sum_{j \in \mathcal{N}_i} L_{ij}(p_j(k) - p_i(k) - \nu_{ij}^o(k)) \}. \end{aligned} \quad (4.5)$$

4.2. A linearly parametric interpretation and estimates of formation control commands. In SCENARIO II (bilateral learning), adversary i , on the one hand, is unaware of the formation vector ν_{ij} for $j \in \mathcal{N}_i$; and on the other hand, is able to intercept $u_i(k)$ produced by operator i . This motivates adversary i to infer ν_{ij} through the observation of $u_i(k)$. To achieve this, she generates the following estimate $u_i^a(k)$ of the control command $u_i(k)$ before receiving $u_i(k)$:

$$\begin{aligned} u_i^a(k) = (I + L_i)^{-1} \{ & \sum_{j \in \mathcal{N}_i} P_i^{-1} P_{ij}(p_j(k) - p_i(k) - \nu_{ij}^a(k)) \\ & + \sum_{j \in \mathcal{N}_i} L_{ij}(p_j(k) - p_i(k) - \nu_{ij}^a(k)) \}, \end{aligned} \quad (4.6)$$

and computes the estimation error $e_i^a(k) = u_i(k) - u_i^a(k)$ via the comparison with $u_i(k)$ and $u_i^a(k)$. In the next part, we will explain how adversary i updates her estimates of ν_{ij} based on $e_i^a(k)$.

4.3. ALGORITHM II (bilateral learning) and convergence properties.

[*Informal description*] We informally describe ALGORITHM II (bilateral learning) as follows. At each time instant k , operator i , adversary i and vehicle i implement the following steps.

- (1) Each operator first receives the information of $p_j(k)$ from neighboring operator j . The operator then computes a control command $u_i(k)$ to minimize a local formation error function by assuming that her neighboring vehicles do not move and the strategy of adversary i is linearly parameterized by $\Theta_i^o(k)$. After this computation, the operator sends the generated command $u_i(k)$ to vehicle i .
- (2) Adversary i intercepts $p_j(k)$ for $j \in \mathcal{N}_i$ and $u_i(k)$, and further corrupts $u_i(k)$ by adding the signal $v_i(k)$ linearly parameterized by Θ_i^o . Adversary i maintains a scheduler T_i^a ⁴ which determines the collection of time instants to update her estimate $\Omega_i^a(k)$. In particular, if $k \in T_i^a$, then adversary i generates an estimate $u_i^a(k)$ of $u_i(k)$, identifies her estimation error and then produces her estimate $\Omega_i^a(k)$ by minimizing some local estimation error function.⁵
- (3) Vehicle i receives, implements, and further sends back to operator i the new position $p_i(k+1)$.
- (4) After that, operator i determines the estimation error of $\Psi_{o,i}(k)$, and updates her estimate to minimize a local estimation error function.

We proceed to formally state ALGORITHM II (bilateral learning) in Algorithm 2. The notations used in Algorithm 2 are summarized in Table 4.1.

We now set out to analyze ALGORITHM II (bilateral learning). First of all, let us spell out the estimation errors $e_i^a(k)$ and $e_i^o(k)$ as follows:

$$\begin{aligned} e_i^o(k) &= p_i(k+1) - p_i(k+1|k) = (\Phi_i^o)^T(\Psi_{o,i}(k) - \Psi_i^o(k)), \\ e_i^a(k) &= u_i(k) - u_i^a(k) = r_i^a(k) + (I + L_i)^{-1}e_i^o(k), \end{aligned} \quad (4.9)$$

where $r_i^a(k) := (\Phi_i^a)^T(\Omega_{a,i} - \Omega_i^a(k))$. In addition, we notice that operator i is attempting to identify some time-varying quantities, and the evolution of her time-varying target parameters is given by:

$$\Psi_i^o(k+1) = \Psi_i^o(k) + \frac{\mu_i^a}{m_i^2} \Phi_i^a e_i^a(k), \quad (4.10)$$

which can be readily obtained from the update rules of (4.7) in Algorithm 2 by noting that $\Psi_i^o(k) = \Omega_{a,i}(k)$. The following lemma describes a linear relation between the regression vectors Φ_i^a and Φ_i^o . This fact will allow us to quantify the estimation errors of operators which are introduced by the variations of time-varying target parameters.

LEMMA 4.2. *The regression vectors of the i^{th} adversary-operator pair satisfy $\Phi_i^a = \Phi_i^o L_i^{-1} M_i$.*

Proof. It follows from Assumption 4.1 and the non-singularity of corresponding matrices. $\square$

⁴Without loss of any generality, we assume that $0 \in T_i^a$.

⁵Note that the scheduler just marks the update of the attack policy, but the attacker corrupts the control commands at every k .

TABLE 4.1
The notations of ALGORITHM II (bilateral learning)

$p_i(k) \in \mathbb{R}^d$	the location of vehicle i at time k
$p_i(k+1 k) \in \mathbb{R}^d$	the prediction of $p_i(k+1)$ produced by operator i at time k
$u_i(k) \in \mathbb{R}^d$	the control command of operator i at time k
$u_i^a(k) \in \mathbb{R}^d$	the estimate of $u_i(k)$ maintained by adversary i at time k and given in (4.6)
$v_i(k) \in \mathbb{R}^d$	the command generated by adversary i at time k
$v_i^o(k) \in \mathbb{R}^d$	the prediction of $v_i(k)$ produced by operator i at time k and given by (4.4)
$\Omega_{a,i} = [\nu_{ij}^T]_{j \in \mathcal{N}_i}^T$	the target parameter of adversary i
$\Omega_i^a(k) = [\nu_{ij}^a(k)^T]_{j \in \mathcal{N}_i}^T$	the estimate of $\Omega_{a,i}$ produced by adversary i at time k
$\Psi_{o,i}(k) = \Omega_i^a(k)$	the target parameter of operator i
$\Psi_i^o(k) = [\nu_{ij}^o(k)^T]_{j \in \mathcal{N}_i}^T$	the posterior estimate of $\Psi_{o,i}(k-1)$ produced by operator i at time k
$(\Phi_i^a)^T := [M_{ij}]_{j \in \mathcal{N}_i}$	the regression vector of adversary i
$(\Phi_i^o)^T := [L_{ij}]_{j \in \mathcal{N}_i}$	the regression vector of operator i
$m_i := \sqrt{1 + \ \Phi_i^o\ ^2 + \ \Phi_i^a\ ^2}$	the normalized term of group i
$\mu_i^a \in (0, 1]$	the step-size of adversary i
$\mu_i^o \in (0, 1]$	the step-size of operator i
T_i^a	the scheduler of adversary i

For each $k \geq 1$, we denote by $\tau_i^a(k)$ the largest time instant in T_i^a that satisfies $\tau_i^a(k) < k$. The following proposition summarizes the convergence properties of the estimation errors of the learning schemes in ALGORITHM II (bilateral learning).

PROPOSITION 4.3. *Consider SCENARIO II (bilateral learning) with any initial configuration $p(0) \in \mathbb{R}^{Nd}$ of vehicles and any initial estimates of $\Omega_i^a(0)$ and $\Psi_i^o(0)$. Suppose Assumptions 2.1, 2.2 and 4.1 hold and the following inequalities are satisfied:*

$$\begin{aligned}
& -2\mu_i^a + 5(\mu_i^a)^2 + \left(\frac{\mu_i^a}{\mu_i^o}\right)^2 \|L_i^{-1} M_i\|^2 + \left(\frac{\mu_i^a}{\mu_i^o}\right)^2 \|(I + L_i)^{-1}\|^2 < 0, \\
& -2\mu_i^o + 4(\mu_i^o)^2 + 4(\mu_i^a)^2 \|(I + L_i)^{-1}\|^2 + 2\mu_i^a \|L_i^{-1} M_i\| \|(I + L_i)^{-1}\| < 0. \quad (4.11)
\end{aligned}$$

The following statements hold for the sequences generated by ALGORITHM II (bilateral learning):

1. The sequence of $\{\Psi_i^a(k)\}$ is uniformly bounded.
2. The sequence of $\{e_i^o(k)\}$ is square summable and the sequence of $\{r_i^a(k)\}$ is diminishing.
3. If there is an integer $T_B \geq 1$ such that $k - \tau_i^a(k) \leq T_B$ for any $k \geq 0$, then the sequence of $\{e_i^a(k)\}$ is square summable.

Proof. The proof is given in the appendix. $\square$

Based on Proposition 4.3, we are able to characterize the asymptotic convergence properties of ALGORITHM II (bilateral learning) as follows.

THEOREM 4.4. (**Convergence properties of ALGORITHM II (bilateral learning)**): *Consider SCENARIO II (bilateral learning) with any initial position $p(0) \in \mathbb{R}^{Nd}$ of vehicles and any initial estimates of $\Omega_i^a(0)$ and $\Psi_i^o(0)$. Suppose As-*

Algorithm 2 ALGORITHM II (bilateral learning) for group i

Initialization: Vehicle i informs operator i of its initial location $p_i(0) \in \mathbb{R}^d$. Operator i chooses initial estimate $\Psi_i^o(0)$, and adversary i chooses initial estimates of $\Omega_i^a(0)$.

Iteration: At each $k \geq 0$, adversary, operator, and vehicle i execute the following steps:

- 1: Operator i receives $p_j(k)$ from operator $j \in \mathcal{N}_i$, solves the quadratic program (4.3), and obtains the optimal solution $u_i(k)$. Operator i then sends $u_i(k)$ to vehicle i , and generates the prediction of $p_i(k+1|k) = p_i(k) + u_i(k) + v_i^o(k)$.
- 2: Adversary i identifies the location $p_i(k)$ of vehicle i , eavesdrops on $p_j(k)$ sent from operator $j \in \mathcal{N}_i$ to operator i , and corrupts $u_i(k)$ by adding $v_i(k)$ in (2.3). Adversary i produces an estimate $u_i^a(k)$ of $u_i(k)$ in the way of (4.6), and computes her estimation error $e_i^a(k) = u_i(k) - u_i^a(k)$. If $k \notin T_i^a$, then $\Omega_i^a(k+1) = \Omega_i^a(k)$; otherwise,

$$\Omega_i^a(k+1) = \Omega_i^a(k) + \frac{\mu_i^a}{m_i^2} \Phi_i^a e_i^a(k), \quad (4.7)$$

with the step-size $\mu_i^a \in (0, 1]$ and the normalized term $m_i := \sqrt{1 + \|\Phi_i^o\|^2 + \|\Phi_i^a\|^2}$.

- 3: Vehicle i receives and implements the corrupted command $u_i(k) + v_i(k)$, and then sends back its new location $p_i(k+1) = p_i(k) + u_i(k) + v_i(k)$ to operator i .
- 4: Operator i computes the estimation error $e_i^o(k) = p_i(k+1) - p_i(k+1|k)$, and updates her parameter estimate in the following manner:

$$\Psi_i^o(k+1) = \Psi_i^o(k) + \frac{\mu_i^o}{m_i^2} \Phi_i^o e_i^o(k), \quad (4.8)$$

with the step-size $\mu_i^o \in (0, 1]$.

- 5: Repeat for $k = k+1$.
-

sumptions 2.1, 2.2 and 4.1 and condition (4.11) hold. Then ALGORITHM II (bilateral learning) ensures that the vehicles asymptotically achieve the desired formation; i.e., $\lim_{k \rightarrow +\infty} \text{dist}(p(k), X^*) = 0$. Furthermore, the convergence rate of the algorithm can

be estimated in such a way that $\sum_{k=0}^{+\infty} \sum_{(i,j) \in \mathcal{E}} \|p_j(k) - p_i(k) - \nu_{ij}\|^2 < +\infty$.

Proof. The proof can be found in the appendix. $\square$

Through the comparison of Theorem 4.4 and Theorem 3.2, it is not difficult to see that ALGORITHM II (bilateral learning) shares analogous convergence properties with ALGORITHM I (unilateral learning), but requires an additional condition (4.11). The following provides a set of sufficient conditions that can ensure (4.11).

LEMMA 4.5. *The following statements hold:*

1. For any pair of step-sizes $\mu_i^a \in (0, \frac{2}{5})$ and $\mu_i^o \in (0, \frac{1}{2})$, there is a $\bar{P}_i$ such that condition (4.11) holds.
2. For any given triple of $\mu_i^o \in (0, \frac{1}{2})$, $\|(I + L_i)^{-1}\|$ and $\|L_i^{-1}M_i\|$, then there is $\bar{\mu}_i^a \in (0, \frac{2}{5})$ such that for any $\mu_i^a \in (0, \bar{\mu}_i^a]$, condition (4.11) holds.

Proof. Note that $-2\mu_i^a + 5(\mu_i^a)^2 < 0$ and $-2\mu_i^o + 4(\mu_i^o)^2 < 0$ in (4.11) for $\mu_i^a \in (0, \frac{2}{5})$ and $\mu_i^o \in (0, \frac{1}{2})$.

Let us investigate the first condition. If we take the limit on $R_i - \bar{P}_i$ to 0, then we have $\|(I + L_i)^{-1}\| \rightarrow 0$ and $\|L_i^{-1}M_i\| \rightarrow 0$. This means that operator i can always choose $\bar{P}_i$ such that $\|(I + L_i)^{-1}\|$ and $\|L_i^{-1}M_i\|$ are sufficiently small. As a result, operator i can always choose $\bar{P}_i$ to enforce condition (4.11). We now consider the second condition. When μ_i^a is sufficiently small, then $-2\mu_i^a$ and $-2\mu_i^o$ dominate in the two inequalities of condition (4.11), respectively. By continuity, there exists $\bar{\mu}_i^a \in (0, \frac{2}{5})$ such that condition (4.11) holds for any $\mu_i^a \in (0, \bar{\mu}_i^a]$. $\square$

To conclude this section, we leverage singular perturbation theory (e.g., in [18]) to provide an informal interpretation of the conditions in Lemma 4.5. This will help us draw some insights from Proposition 4.3 and Theorem 4.4. From (4.9) and Lemma 4.2, we know the following:

$$e_i^a(k) = (\Phi_i^o L_i^{-1} M_i)^T (\Omega_{a,i} - \Omega_i^a(k)) + (I + L_i)^{-1} e_i^o(k).$$

The first condition in Lemma 4.5 renders that $\|(I + L_i)^{-1}\|$ and $\|L_i^{-1}M_i\|$, and thus $\|e_i^a(k)\|$, are sufficiently small. The second condition in Lemma 4.5 renders $\mu_i^a \approx 0$ and thus $\|e_i^a(k)\| \approx 0$ as well. Hence, under any condition in Lemma 4.5, the dynamics (4.7) approximates $\Omega_i^a(k+1) \approx \Omega_i^a(k)$; i.e., the learning dynamics of adversary i evolves on a slow manifold. On the other hand, for any fixed Ω_i^a , (4.8) becomes:

$$\Psi_i^o(k+1) = \Psi_i^o(k) + \frac{\mu_i^o}{m_i^2} \Phi_i^o(\Psi_i^o(k) - \Omega_i^a), \quad (4.12)$$

and the trajectories of (4.12) asymptotically reach the set of $\{\Psi_i^o \mid \|\Phi_i^o(\Psi_i^o - \Omega_i^a)\| = 0\}$ where the estimation error of operator i vanishes.

If we informally interpret μ_i^a and μ_i^o as learning rates of adversary i and operator i , respectively, then the second condition in Lemma 4.5 demonstrates that operators can win the game if their learning rates are sufficiently faster than their opponents.

4.4. A numerical example for ALGORITHM II (bilateral learning). In order to compare with the performance of ALGORITHM I (unilateral learning), we consider the same problem where a group of 15 vehicles are initially randomly deployed over the square of 50×50 . Figure 4.1(e) shows the initial configuration, and Figure 4.1(g) then presents the trajectory of each vehicle in the first 100 iterations of the algorithm. The group configuration at the 100th iteration is provided in Figure 4.1(f). We can verify the fact that the desired formation is exponentially achieved from Figure 4.1(h) of the evolution of the formation errors of ALGORITHM II (bilateral learning).

The simulations provide some insights of the algorithms. Comparing Figures 3.1(d) and 4.1(h), it can be seen that ALGORITHM I (unilateral learning) converges faster than ALGORITHM II (bilateral learning). Figure 3.1(c) shows that vehicles stay close to the region where they start from while Figure 4.1(g) shows that vehicles drift significantly away from the starting area. These two facts verify the fact that the damage induced by intelligent adversaries is greater.

5. An extension to time-varying inter-operator communication digraphs.

So far, we have only considered a fixed communication digraph of operators. ALGORITHM I (unilateral learning), together with Theorem 3.2, can be extended to a simple case of time-varying inter-operator digraphs with some additional assumptions. Let $\mathcal{N}_i^C(k) \subseteq \mathcal{N}_i$ be the set of operators who can send data to operator i at time k . We define an operator communication digraph as $\mathcal{G}^C(k) := (V, \mathcal{E}^C(k))$ where $\mathcal{E}^C(k) := \{(j, i) \mid j \in \mathcal{N}_i^C(k)\}$. It can be seen that $\mathcal{G}^C(k)$ is a subgraph of $\mathcal{G}$. We

(e) Initial configuration of vehicles for ALGORITHM II (bilateral learning).

(f) The configuration of vehicles at the 100th iteration under ALGORITHM II (bilateral learning).

(g) Trajectories of the vehicles during the first 100 iterations of ALGORITHM II (bilateral learning). The green squares stand for initial locations and red circles represent final locations.

(h) The evolution of formation errors during the first 100 iterations of ALGORITHM II (bilateral learning).

slightly modify ALGORITHM I (unilateral learning) as follows. If $\mathcal{N}_i^C(k) \neq \mathcal{N}_i$, then operator i does nothing at this time instant. Since operator i does not send out any information, then adversary and vehicle i will have to keep idle at this time instant as well. If $\mathcal{N}_i^C(k) = \mathcal{N}_i$, then operator i , adversary i and vehicle i implement one iteration of ALGORITHM I (unilateral learning). In other words, this situation models a type of asynchronous operator interactions under the assumption that vehicles can maintain their positions. To ensure the convergence of the modified algorithm, we require that the frequency that the set $\mathcal{N}_i$ can be recovered by operators is high enough. Formally, we need the following to hold:

Assumption 5.1. *There is some integer $T \geq 1$ such that the event of $\mathcal{N}_i^C(k) = \mathcal{N}_i$ occurs at least once within any T consecutive steps.*

This assumption in conjunction with Assumption 2.1 ensures that for all $k_0 \geq 0$, the digraph $(V, \bigcup_{k=0}^{B-1} \mathcal{E}^C(k_0 + k))$ is strongly connected with the integer $B := NT$. The proof of Theorem 3.2 can be carried out almost exactly by only changing $T_k := k(NB - 1)$ in the proof of Claim 1 of the proofs for Theorem 3.2 in the appendix, as we did in [34]. This extension applies to ALGORITHM II (bilateral learning) as well. The possible solution aforementioned allows for tolerating unexpected changes of communication digraphs between operators, but this robustness comes with the expense of potentially slowing down the algorithms. An interesting future research problem is to maintain the convergence rates of algorithms under switching topologies.

6. Conclusions. We have studied a distributed formation control problem for an operator-vehicle network which is threatened by a team of adversaries. We have proposed a class of novel attack-resilient distributed formation control algorithms and analyzed their asymptotic convergence properties. Our results have demonstrated the capability of online learning to enhance network resilience, and suggest a number of future research directions which we plan to investigate. For example, the current operator-vehicle architecture can be enlarged to allow for more complex interactions. Moreover, the types of malicious attacks can be broadened and the models of attackers can be further refined. In addition, it would be interesting to study the cyber-security of other cooperative control problems in the operator-vehicle setting.

7. Appendix. In this section, we provide the proofs for Theorem 3.2, Proposition 4.3 and Theorem 4.4. Before doing that, we give two instrumental facts as follows where the second one is a direct result of the first one.

LEMMA 7.1. *The following statements hold:*

1. *Let $\{a(k)\}$ be a non-negative scalar sequence. If $\{a(k)\}$ is summable, then it converges to zero.*
2. *Consider non-negative scalar sequences of $\{V(k)\}$ and $\{b(k)\}$ such that $V(k+1) - V(k) \leq -b(k)$. Then it holds that $\lim_{k \rightarrow +\infty} b(k) = 0$.*

It is worthy to remark that the second fact in Lemma 7.1 is a discrete-time version of Barbalat's lemma (e.g., in [18]) and plays an important role in our subsequent analysis. We are now in the position to show Theorem 3.2 for ALGORITHM I (unilateral learning).

Proof of Theorem 3.2:

Proof. First of all note that, through the choice of $u_i(k)$, $p_i(k+1|k)$ is the minimizer of $\sum_{j \in \mathcal{N}_i} \|p_j(k) - p_i - \nu_{ij}\|_{P_{ij}}^2 + \|p_i(k) - p_i\|_{P_{ii}}^2$ in p_i . Therefore,

$$p_i(k+1|k) = p_i(k) + \sum_{j \in \mathcal{N}_i} P_i^{-1} P_{ij} (p_j(k) - p_i(k) - \nu_{ij}),$$

where we use the fact that P_{ij} is diagonal and positive definite. Recall that $e_i(k) = p_i(k+1) - p_i(k+1|k)$. The above relation leads to:

$$p_i(k+1) = p_i(k+1|k) + e_i(k) = p_i(k) + \sum_{j \in \mathcal{N}_i} P_i^{-1} P_{ij} (p_j(k) - p_i(k) - \nu_{ij}) + e_i(k). \quad (7.1)$$

Pick any $p^* := [p_i^*]_{i \in V} \in X^*$. Then $p_j^* - p_i^* = \nu_{ij}$ for any $(j, i) \in \mathcal{E}$. Denote $y_i(k) = p_i(k) - p_i^*$, for $i \in V$. Subtracting p_i^* on both sides of (7.1) leads to:

$$\begin{aligned} y_i(k+1) &= y_i(k) + \sum_{j \in \mathcal{N}_i} P_i^{-1} P_{ij} ((p_j(k) - p_j^*) - (p_i(k) - p_i^*)) \\ &\quad - \sum_{j \in \mathcal{N}_i} P_i^{-1} P_{ij} (-p_j^* + p_i^* + \nu_{ij}) + e_i(k) \\ &= y_i(k) + \sum_{j \in \mathcal{N}_i} P_i^{-1} P_{ij} (y_j(k) - y_i(k)) + e_i(k). \end{aligned} \quad (7.2)$$

Since the P_{ij} are diagonal and positive definite, system (7.2) can be viewed as d parallel first-order dynamic consensus algorithms in the variables $y_i(k)$ subject to the time-varying signals $e_i(k)$. We can guarantee convergence of the vehicles to the desired formation if consensus in the $y_i(k)$ is achieved. In other words, $\lim_{k \rightarrow +\infty} \|y_i(k) - y_j(k)\| = 0$,

for all $(i, j) \in \mathcal{E}$, is equivalent to $\lim_{k \rightarrow +\infty} \|p_i(k) - p_j(k) - (p_i^* - p_j^*)\| = 0$. Since $p_i^* - p_j^* = \nu_{ij}$, consensus on the $y_i(k)$ is equivalent to $\lim_{k \rightarrow +\infty} \|p_i(k) - p_j(k) - \nu_{ij}\| = 0$. The rest of the proof is devoted to verify this consensus property.

For each $\ell \in \{1, \dots, d\}$, we denote the following:

$$g_\ell(k) := \max_{i,j \in V} \|e_{i\ell}(k) - e_{j\ell}(k)\|, \quad D_\ell(k) := \max_{i,j \in V} \|y_{i\ell}(k) - y_{j\ell}(k)\|.$$

Here, the quantity $D_\ell(k)$ represents the maximum disagreement of the ℓ^{th} consensus algorithm. The following claim characterizes the input-to-state stability properties of consensus algorithms, and it is based on the analysis of dynamic average consensus algorithms of our paper [34]:

Claim 1: There exist $D_\ell(0), \beta > 0$, and $\sigma \in (0, 1)$, such that the following holds:

$$D_\ell(k+1) \leq \sigma^{k+1} D_\ell(0) + \beta \sum_{s=0}^k \sigma^{k-s} g_\ell(s). \quad (7.3)$$

Proof. Denote $T_k := k(N-1)$ and, for any integer $k \geq 0$, let ℓ_k be the largest integer such that $\ell_k(N-1) \leq k$. From (16) in the proof of Theorem 4.1 in [34], we know that there exists some $\eta \in (0, 1)$ such that

$$\begin{aligned} D_\ell(k) &\leq (1-\eta)^{\ell_k} D_\ell(0) + (1-\eta)^{\ell_k-1} \sum_{s=0}^{T_1-1} g_\ell(s) + \dots \\ &+ (1-\eta) \sum_{s=T_{\ell_k-2}}^{T_{\ell_k-1}-1} g_\ell(s) + \sum_{s=T_{\ell_k-1}}^{T_{\ell_k}-1} g_\ell(s) + \sum_{s=T_{\ell_k}}^{k-1} g_\ell(s). \end{aligned}$$

This relation can be rewritten as follows:

$$D_\ell(k) \leq (1-\eta)^{\ell_k} D_\ell(0) + \sum_{s=0}^{k-1} (1-\eta)^{\ell_k-\ell_s} g_\ell(s). \quad (7.4)$$

Since $k \leq \ell_k(N-1)$ and $\frac{k-s}{N-1} - 1 \leq \ell_k - \ell_s$ for $k \geq s$, then it follows from (7.4) that

$$D_\ell(k) \leq (1-\eta)^{\frac{k}{N-1}} D_\ell(0) + \sum_{s=0}^{k-1} (1-\eta)^{\frac{k-s}{N-1}-1} g_\ell(s). \quad (7.5)$$

We get the desired result by letting $\sigma = (1-\eta)^{\frac{1}{N-1}}$ and $\beta = \frac{1}{1-\eta}$ in (7.5). $\square$

Define now an auxiliary scalar sequence $\{z(k)\}$:

$$z(k+1) = \sigma^{k+1} z(0) + \sum_{s=0}^k \sigma^{k-s} f(s), \quad k \geq 0, \quad (7.6)$$

where $z(0) = \max_{\ell \in \{1, \dots, d\}} D_\ell(0)$, and $f(k) = \beta \max_{\ell \in \{1, \dots, d\}} g_\ell(k)$. It is not difficult to verify that $\{z(k)\}$ is an upper bound of $\{D_\ell(k)\}$ in such a way that $0 \leq D_\ell(k) \leq z(k)$, for all $k \geq 0$ and $\ell \in \{1, \dots, d\}$. In order to show the convergence of $\{D_\ell(k)\}$ to zero for

any $i \in \{1, \dots, d\}$, it suffices to show that $\{z(k)\}$ converges to zero. We do this in the following. Observe that $\{z(k)\}$ satisfies the following recursion:

$$\begin{aligned} z(k+1) &= \sigma^{k+1}z(0) + \sum_{s=0}^k \sigma^{k-s}f(s) \\ &= \sigma(\sigma^k z(0) + \sum_{s=0}^{k-1} \sigma^{k-1-s}f(s)) + f(k) = \sigma z(k) + f(k). \end{aligned} \quad (7.7)$$

For any $\lambda > 0$, it follows from (7.7) that

$$z(k+1)^2 \leq (1+\lambda)\sigma^2 z(k)^2 + (1+\frac{1}{\lambda})f(k)^2, \quad (7.8)$$

by noting that $2\sigma z(k)f(k) \leq \lambda\sigma^2 z(k)^2 + \frac{1}{\lambda}f(k)^2$. From the definition of $f(k)$, it is not difficult to see that $f(k)^2 \leq 4\beta^2 \sum_{i \in V} \|e_i(k)\|^2$. Therefore, we have the bound:

$$z(k+1)^2 \leq (1+\lambda)\sigma^2 z(k)^2 + 4(1+\frac{1}{\lambda})^2 \beta^2 \sum_{i \in V} \|e_i(k)\|^2.$$

In the sequel, we choose a (sufficiently small) $\lambda > 0$ such that $(1+\lambda)\sigma^2 < 1$. The following claim finds a bound for $\|e_i(k)\|$ in terms of $z(k)^2$, for each $i \in V$.

Claim 2: For each $i \in V$, there are a positive and summable sequence $\{\gamma_i(k)\}$, and positive constants λ_1, λ_2 , such that the following holds:

$$\|e_i(k)\|^2 \leq \gamma_i(k)(1+n_i+\lambda_1 z(k)^2+\lambda_2). \quad (7.9)$$

Furthermore, $\{\|\Theta_i(k)\|\}$ is uniformly bounded.

Proof. Denote $\hat{\Theta}_i(k) := \Theta_i(k) + \frac{1}{m_i(k)^2} \Phi_i(k)e_i(k)^T$. Subtracting Θ_i on both sides leads to the following:

$$\hat{\Theta}_i(k) - \Theta_i = (\Theta_i(k) - \Theta_i) + \frac{1}{m_i(k)^2} \Phi_i(k)e_i(k)^T. \quad (7.10)$$

Recall that $\|A\|_F^2 = \sum_{i=1}^m \sum_{j=1}^n a_{ij}^2$ for a matrix $A \in \mathbb{R}^{m \times n}$. Similarly to the vector

normalized gradient algorithm in [5], one can compute $\frac{1}{2}\|\hat{\Theta}_i(k) - \Theta_i\|_F^2 = \frac{1}{2}\text{tr}((\hat{\Theta}_i(k) - \Theta_i)^T(\hat{\Theta}_i(k) - \Theta_i))$, just plugging in (7.10), as follows:

$$\frac{1}{2}\|\hat{\Theta}_i(k) - \Theta_i\|_F^2 = \frac{1}{2}\|\Theta_i(k) - \Theta_i\|_F^2 - \frac{1}{2m_i(k)^2} \text{tr}(e_i(k)(2 - \frac{\Phi_i(k)^T \Phi_i(k)}{m_i(k)^2})e_i(k)^T), \quad (7.11)$$

where we use the fact that tr is a linear operator, and that $e_i(k) = (\Theta_i - \Theta_i(k))^T \Phi_i(k)$. As a consequence, the difference of $\frac{1}{2}\|\hat{\Theta}_i(k) - \Theta_i\|_F^2 - \frac{1}{2}\|\Theta_i(k) - \Theta_i\|_F^2$ can be characterized in the following way:

$$\frac{1}{2}\|\hat{\Theta}_i(k) - \Theta_i\|_F^2 - \frac{1}{2}\|\Theta_i(k) - \Theta_i\|_F^2 \leq -\frac{1}{2m_i(k)^2} \text{tr}(e_i(k)e_i(k)^T) = -\frac{\|e_i(k)\|^2}{2m_i(k)^2}, \quad (7.12)$$

where we have used that $2 - \frac{\Phi_i(k)^T \Phi_i(k)}{m_i(k)^2} \geq 1$, since $m_i(k)$ is a normalizing term. Since the projection operator $\mathbb{P}_i$ is applied block-wise, then $\|\Theta_i(k+1) - \Theta_i\|_F^2 \leq \|\hat{\Theta}_i(k) - \Theta_i\|_F^2$. Then from (7.12) we have:

$$\|\Theta_i(k+1) - \Theta_i\|_F^2 - \|\Theta_i(k) - \Theta_i\|_F^2 \leq -\frac{\|e_i(k)\|^2}{m_i(k)^2}. \quad (7.13)$$

The above relation implies that $\{\|\Theta_i(k) - \Theta_i\|_F^2\}$ is non-increasing and uniformly bounded. Further, this ensures that $\{\|\Theta_i(k)\|\}$ is uniformly bounded by noting that:

$$\|\Theta_i(k)\|^2 = \|(\Theta_i(k) - \Theta_i) + \Theta_i\|^2 \leq \|(\Theta_i(k) - \Theta_i) + \Theta_i\|_F^2 \leq 2\|\Theta_i(k) - \Theta_i\|_F^2 + 2\|\Theta_i\|_F^2.$$

Denote $\gamma_i(k) := \|\Theta_i(k) - \Theta_i\|_F^2 - \|\Theta_i(k+1) - \Theta_i\|_F^2$. It is noted that

$$\sum_{k=0}^K \gamma_i(k) = \|\Theta_i(0) - \Theta_i\|_F^2 - \|\Theta_i(K+1) - \Theta_i\|_F^2.$$

The previous discussion implies that the sequence $\{\gamma_i(k)\}$ is non-negative, summable, and thus converges to zero by Lemma 7.1. Now, from (7.13) we obtain the following upper bound on $\|e_i(k)\|^2$ in terms of $\gamma_i(k)$:

$$\|e_i(k)\|^2 \leq \gamma_i(k) m_i(k)^2 = \gamma_i(k) (1 + \|\Phi_i(k)\|^2) \leq \gamma_i(k) (1 + n_i + \|\phi_i(k)\|^2). \quad (7.14)$$

We would like to find now a relation between $\|\phi_i(k)\|$ and $z(k)$. To do this, recover from (3.3) the expression for $u_i(k)$:

$$\begin{aligned} u_i(k) &= (I + \sum_{j \in \mathcal{N}_i} L_{ij}(k))^{-1} \times \left\{ \sum_{j \in \mathcal{N}_i} P_i^{-1} P_{ij} (y_j(k) - y_i(k)) \right. \\ &\quad \left. + \sum_{j \in \mathcal{N}_i} L_{ij}(k) (y_j(k) - y_i(k)) + \sum_{j \in \mathcal{N}_i} \eta_{ij}(k) \right\}. \end{aligned} \quad (7.15)$$

Recall that $L_{ij}(k)$ and P_{ij} are positive definite and diagonal. This gives us that $\|(I + \sum_{j \in \mathcal{N}_i} L_{ij}(k))^{-1}\| \leq 1$. Now, it follows from (7.15) that

$$\|u_i(k)\| \leq \sum_{j \in \mathcal{N}_i} \|P_i^{-1} P_{ij}\| \sqrt{d} z(k) + \sum_{j \in \mathcal{N}_i} \sqrt{d} \|L_{ij}(k)\| z(k) + \sum_{j \in \mathcal{N}_i} \|\eta_{ij}(k)\|.$$

Since $\{\|\Theta_i(k)\|\}$ is uniformly bounded, there exists some $\theta_1, \theta_2 > 0$ such that $\|u_i(k)\| \leq \theta_1 z(k) + \theta_2$, for all $k \geq 0$ and all $i \in V$. Notice that $\phi_i(k)$ can be rewritten as follows:

$$\phi_i(k) := \begin{bmatrix} y_{i_1}(k) - y_i(k) - u_i(k) \\ \vdots \\ y_{i_{n_i}}(k) - y_i(k) - u_i(k) \end{bmatrix}.$$

This implies that there exists some $\lambda_1, \lambda_2 > 0$ such that the following holds for all $k \geq 0$ and all $i \in V$:

$$\begin{aligned} \|\phi_i(k)\|^2 &\leq \lambda_1 z(k)^2 + \lambda_2, \\ \|e_i(k)\|^2 &\leq \gamma_i(k) (1 + n_i + \|\phi_i(k)\|^2) \leq \gamma_i(k) (1 + n_i + \lambda_1 z(k)^2 + \lambda_2). \end{aligned}$$

□

Using the upper bound on the $\|e_i(k)\|^2$, and the uniform bound on the $\|\Theta_i(k)\|$, we can now obtain an inequality involving the $\{z(k)^2\}$ and other diminishing terms. This is used to determine the stability properties of $\{z(k)^2\}$.

Claim 3: The sequence $\{z(k)\}$ is square summable.

Proof. From the recursion for $z(k)$, we found that

$$z(k+1)^2 \leq (1+\lambda)\sigma^2 z(k)^2 + 4(1+\frac{1}{\lambda})\beta^2 \sum_{i \in V} \|e_i(k)\|^2, \quad (7.16)$$

where a (sufficiently small) $\lambda > 0$ is chosen such that $(1+\lambda)\sigma^2 \in (0, 1)$. We now define $V(k) := z(k)^2 + \sum_{i \in V} \|e_i(k)\|^2$ to be a Lyapunov function candidate for ALGORITHM I (unilateral learning), and have that:

$$\begin{aligned} V(k+1) - V(k) &= z(k+1)^2 + \sum_{i \in V} \|e_i(k+1)\|^2 - z(k)^2 - \sum_{i \in V} \|e_i(k)\|^2 \\ &\leq z(k+1)^2 + \sum_{i \in V} \|e_i(k+1)\|^2 - z(k)^2. \end{aligned}$$

Using now the bound for $\|e_i(k+1)\|^2$ in Claim 2, we obtain:

$$V(k+1) - V(k) \leq (1+\lambda_1 \sum_{i \in V} \gamma_i(k+1))z(k+1)^2 + \sum_{i \in V} \gamma_i(k+1)(1+n_i+\lambda_2) - z(k)^2.$$

Finally, upper-bounding $z(k+1)^2$ as in (7.16), we get:

$$\begin{aligned} V(k+1) - V(k) &\leq (1+\lambda_1 \sum_{i \in V} \gamma_i(k+1))((1+\lambda)\sigma^2 z(k)^2 \\ &\quad + (1+\frac{1}{\lambda})4\beta^2 \sum_{i \in V} \|e_i(k)\|^2) - z(k)^2 + \sum_{i \in V} \gamma_i(k+1)(1+n_i+\lambda_2). \end{aligned} \quad (7.17)$$

Substituting the upper bound on $\|e_i(k)\|^2$ from (7.9) of Claim 2 into (7.17), we find that there exists $\alpha \in (0, 1)$ and two sequences $\{\pi_1(k)\}$ and $\{\pi_2(k)\}$ such that

$$V(k+1) - V(k) \leq (\alpha - 1 + \pi_1(k))z(k)^2 + \pi_2(k), \quad (7.18)$$

where $\{\pi_1(k)\}$ is positive and diminishing and $\{\pi_2(k)\}$ is positive and summable by using that each sequence of $\{\gamma_i(k)\}$ is summable. There is a finite $K \geq 0$ such that $1 - \alpha - \pi_1(k) \leq 1 - \frac{\alpha}{2}$ for all $k \geq K$. Then, for $k \geq K$, we have the following:

$$(1 - \frac{\alpha}{2})z(k)^2 \leq (1 - \alpha - \pi_1(k))z(k)^2 \leq V(k) - V(k+1) + \pi_2(k).$$

This implies that

$$(1 - \frac{\alpha}{2}) \sum_{k=K}^{+\infty} z(k)^2 \leq V(K) + \sum_{k=K}^{+\infty} \pi_2(k). \quad (7.19)$$

Upper-bounding $\|e_i(k)\|^2$ by (7.9) from Claim 2 in the recursion (7.16), it can be found that $z(k)$ is finite for any finite k . As a consequence, $e_i(k)$, and thus $V(k)$, are

finite for every finite time. In this way, $V(K)$ is finite in (7.19) and, since $\{\pi_2(k)\}$ is summable, so is $\{z(k)^2\}$. $\square$

Claim 3 guarantees that $\{z(k)\}$, and thus $\{D_\ell(k)\}$, for all $\ell \in \{1, \dots, d\}$, converge to zero by Lemma 7.1. Therefore, $\{p(k)\}$ asymptotically converges to the set X^* . In order to estimate the convergence rate, note that

$$\sum_{k=0}^{+\infty} \sum_{(i,j) \in \mathcal{E}} \|p_j(k) - p_i(k) - \nu_{ij}\|^2 = \sum_{k=0}^{+\infty} \sum_{(i,j) \in \mathcal{E}} \|y_j(k) - y_i(k)\|^2 \leq d|\mathcal{E}| \sum_{k=0}^{+\infty} z(k)^2 < +\infty,$$

where $|\mathcal{E}|$ is the cardinality of $\mathcal{E}$, and in the last inequality we use the summability of $\{z(k)^2\}$ from Claim 3. This completes the proof of Theorem 3.2. $\square$

We now turn our attention to show Proposition 4.3 for ALGORITHM II (bilateral learning).

The proof of Proposition 4.3:

Proof. We will divide the proof into several claims.

Claim 4: For adversary i , then the following relation holds when $k \in T_i^a$:

$$\begin{aligned} \|\Omega_i^a(k+1) - \Omega_{a,i}\|_F^2 - \|\Omega_i^a(k) - \Omega_{a,i}\|_F^2 &\leq -2(\mu_i^a - (\mu_i^a)^2) \frac{\|r_i^a(k)\|^2}{m_i^2} \\ &+ 2\mu_i^a \|(I + L_i)^{-1}\| \frac{\|r_i^a(k)\| \|e_i^o(k)\|}{m_i^2} + 2(\mu_i^a)^2 \|(I + L_i)^{-1}\|^2 \frac{\|e_i^o(k)\|^2}{m_i^2}. \end{aligned} \quad (7.20)$$

If $k \notin T_i^a$, then the following holds:

$$\|\Omega_i^a(k+1) - \Omega_{a,i}\|_F^2 = \|\Omega_i^a(k) - \Omega_{a,i}\|_F^2. \quad (7.21)$$

Proof. First of all, we notice that, analogous to (7.11), the following holds for adversary i when $k \in T_i^a$:

$$\begin{aligned} \|\Omega_i^a(k+1) - \Omega_{a,i}\|_F^2 &= \|\Omega_i^a(k) - \Omega_{a,i}\|_F^2 + \left(\frac{\mu_i^a}{m_i^2}\right)^2 \text{tr}(e_i^a(k)^T (\Phi_i^a)^T \Phi_i^a e_i^a(k)) \\ &+ 2 \text{tr}((\Omega_i^a(k) - \Omega_{a,i})^T \frac{\mu_i^a}{m_i^2} \Phi_i^a e_i^a(k)). \end{aligned} \quad (7.22)$$

For the last term on the right-hand side of the relation (7.22), we have

$$\begin{aligned} (\Omega_i^a(k) - \Omega_{a,i})^T \frac{\mu_i^a}{m_i^2} \Phi_i^a e_i^a(k) &= (\Omega_i^a(k) - \Omega_{a,i})^T \frac{\mu_i^a}{m_i^2} \Phi_i^a (r_i^a(k) + (I + L_i)^{-1} e_i^o(k)) \\ &= -\frac{\mu_i^a}{m_i^2} r_i^a(k)^T r_i^a(k) - \frac{\mu_i^a}{m_i^2} r_i^a(k)^T (I + L_i)^{-1} e_i^o(k). \end{aligned} \quad (7.23)$$

The trace of the second term in the last term of (7.23) can be upper bounded in the following way:

$$\frac{\mu_i^a}{m_i^2} \|\text{tr}(r_i^a(k)^T (I + L_i)^{-1} e_i^o(k))\| \leq \frac{\|(I + L_i)^{-1}\| \mu_i^a}{m_i^2} \|r_i^a(k)\| \|e_i^o(k)\|. \quad (7.24)$$

Let us consider the second term on the right-hand side of the relation (7.22). Note that $(\Phi_i^a)^T \Phi_i^a = \text{diag}(M_{ij}^2)$ is a diagonal matrix from the fact that M_{ij} is a diagonal matrix.

Using the definition of m_i as a normalizing term and $e_i^a(k) = r_i^a(k) + (I + L_i)^{-1}e_i^o(k)$, we have

$$\begin{aligned} \left(\frac{\mu_i^a}{m_i^2}\right)^2 \text{tr}(e_i^a(k)^T (\Phi_i^a)^T \Phi_i^a e_i^a(k)) &\leq \frac{(\mu_i^a)^2}{m_i^2} \|e_i^a(k)\|^2 \\ &\leq 2 \frac{(\mu_i^a)^2}{m_i^2} (\|r_i^a(k)\|^2 + \|(I + L_i)^{-1}\|^2 \|e_i^o(k)\|^2), \end{aligned} \quad (7.25)$$

where in the last inequality we use the relations of $\|a + b\|^2 \leq 2(\|a\|^2 + \|b\|^2)$ and $\|cd\| \leq \|c\|\|d\|$. Substitute the bounds of (7.24) and (7.25) into (7.22), and we have the desired relation (7.20) for $k \in T_i^a$ by using the fact that tr is a linear operator. The relation for $k \notin T_i^a$ is trivial to verify. $\square$

Claim 5: For operator i , the following relation holds when $k \in T_i^a$:

$$\begin{aligned} &\|\Psi_i^o(k+1) - \Psi_{o,i}(k+1)\|_F^2 - \|\Psi_i^o(k) - \Psi_{o,i}(k)\|_F^2 \\ &\leq (-2\mu_i^o + (\mu_i^o)^2 + 2(\mu_i^a)^2 \|(I + L_i)^{-1}\|^2 + 2\mu_i^a \|L_i^{-1}M_i\| \|(I + L_i)^{-1}\|) \frac{\|e_i^o(k)\|^2}{m_i^2} \\ &\quad + 2(\mu_i^a)^2 \frac{\|r_i^a(k)\|^2}{m_i^2} + 2(\mu_i^a \|L_i^{-1}M_i\| + \mu_i^o \mu_i^a) \frac{\|r_i^a(k)\| \|e_i^o(k)\|}{m_i^2}. \end{aligned} \quad (7.26)$$

If $k \notin T_i^a$, then the following holds:

$$\|\Psi_i^o(k+1) - \Psi_{o,i}(k+1)\|_F^2 - \|\Psi_i^o(k) - \Psi_{o,i}(k)\|_F^2 \leq (-2\mu_i^o + (\mu_i^o)^2) \frac{\|e_i^o(k)\|^2}{m_i^2}. \quad (7.27)$$

Proof. We first discuss the case when both adversary i and operator i update their estimates at time k . Note that the following holds for operator i :

$$\Psi_i^o(k+1) - \Psi_{o,i}(k+1) = \Psi_i^o(k) + \frac{\mu_i^o}{m_i^2} \Phi_i^o e_i^o(k) - \Psi_{o,i}(k) - \frac{\mu_i^a}{m_i^2} \Phi_i^a e_i^a(k). \quad (7.28)$$

Analogous to (7.11), it follows from (7.28) that

$$\begin{aligned} &\|\Psi_i^o(k+1) - \Psi_{o,i}(k+1)\|_F^2 = \|\Psi_i^o(k) - \Psi_{o,i}(k)\|_F^2 \\ &\quad + \frac{\mu_i^o}{m_i^2} \text{tr}((\Psi_i^o(k) - \Psi_{o,i}(k))^T \Phi_i^o e_i^o(k)) - \frac{\mu_i^a}{m_i^2} \text{tr}((\Psi_i^o(k) - \Psi_{o,i}(k))^T \Phi_i^a e_i^a(k)). \end{aligned} \quad (7.29)$$

One can verify that

$$(\Psi_i^o(k) - \Psi_{o,i}(k))^T \frac{\mu_i^o}{m_i^2} \Phi_i^o e_i^o(k) = -\frac{\mu_i^o}{m_i^2} e_i^o(k)^T e_i^o(k), \quad (7.30)$$

which produces the following upper bounds for the second term on the right-hand side of (7.29):

$$\|\text{tr}(\Psi_i^o(k) - \Psi_{o,i}(k))^T \frac{\mu_i^o}{m_i^2} \Phi_i^o e_i^o(k)\| \leq \frac{\mu_i^o}{m_i^2} \|e_i^o(k)\|^2. \quad (7.31)$$

From (7.30), we can derive the following upper bounds for the third term on the right-hand side of (7.29):

$$\begin{aligned}
& \|(\Psi_i^o(k) - \Psi_{o,i}(k))^T \frac{\mu_i^a}{m_i^2} \Phi_i^a e_i^a(k)\| = \frac{\mu_i^a}{m_i^2} \|(\Psi_i^o(k) - \Psi_{o,i}(k))^T \Phi_i^o L_i^{-1} M_i e_i^a(k)\| \\
& = \frac{\mu_i^a}{m_i^2} \|e_i^o(k)^T L_i^{-1} M_i e_i^a(k)\| \leq \mu_i^a \|L_i^{-1} M_i\| \left\| \frac{e_i^o(k)}{m_i} \right\| \left\| \frac{e_i^a(k)}{m_i} \right\| \\
& \leq \mu_i^a \|L_i^{-1} M_i\| \left\| \frac{e_i^o(k)}{m_i} \right\| \left(\left\| \frac{r_i^a(k)}{m_i} \right\| + \|(I + L_i)^{-1}\| \left\| \frac{e_i^o(k)}{m_i} \right\| \right), \tag{7.32}
\end{aligned}$$

where in the first equality we use Lemma 4.2, in the second equality we use the definition of $e_i^o(k)$, and the third equality follows from the definition of $e_i^a(k)$. The combination of (7.29), (7.31) and (7.32) gives (7.26). When $k \notin T_i^a$, then $\Psi_i^o(k+1) = \Psi_i^o(k)$ and thus (7.26) reduces to (7.27). $\square$

Denote the following to characterize the estimation errors of the i^{th} group:

$$U_i(k) := \|\Omega_i^a(k) - \Omega_{a,i}\|_F^2 + \|\Psi_i^o(k) - \Psi_{o,i}(k)\|_F^2.$$

With the two claims just proved, one can characterize $U_i(k+1) - U_i(k)$ as follows:

$$U_i(k+1) - U_i(k) \leq \frac{1}{m_i^2} \begin{bmatrix} \|r_i^a(k)\| & \|e_i^o(k)\| \end{bmatrix} \Pi_i(k) \begin{bmatrix} \|r_i^a(k)\| \\ \|e_i^o(k)\| \end{bmatrix}, \tag{7.33}$$

where the time-varying matrix $\Pi(k)$ is given that: if $k \in T_i^a$, then

$$\Pi_i(k) = \Pi_i^{(1)} = \begin{bmatrix} \xi_1 & 0 \\ 0 & \xi_2 \end{bmatrix},$$

with $\xi_1 := -2\mu_i^a + 5(\mu_i^a)^2 + \left(\frac{\mu_i^a \|L_i^{-1} M_i\|}{\mu_i^o}\right)^2 + \left(\frac{\|(I+L_i)^{-1}\| \mu_i^a}{\mu_i^o}\right)^2$ and $\xi_2 := -2\mu_i^o + 4(\mu_i^o)^2 + 4(\mu_i^a)^2 \|(I + L_i)^{-1}\|^2 + 2\mu_i^a \|L_i^{-1} M_i\| \|(I + L_i)^{-1}\|$; otherwise,

$$\Pi_i(k) = \Pi_i^{(2)} = \begin{bmatrix} 0 & 0 \\ 0 & -2\mu_i^o + (\mu_i^o)^2 \end{bmatrix}.$$

Claim 6: The matrix $\Pi_i^{(2)}$ are negative semi-definite and $\Pi_i^{(1)}$ is negative definite.

Proof. Since $\mu_i^o \in (0, 1)$, then it is easy to see that $\Pi_i^{(2)}$ is negative semi-definite. From (4.11), it can be seen that $\Pi_i^{(2)}$ is negative definite. $\square$

Claim 7: The sequence of $\{\Psi_i^o(k)\}$ is uniformly bounded. Furthermore, the sequence of $\{r_i^a(k)\}$ is diminishing, and the sequence of $\{e_i^o(k)\}$ is square summable.

Proof. It follows from Claim 6 and (7.33) that the sequence of $\{U_i(k)\}$ is non-increasing and uniformly bounded. Since $\|\Omega_i^a(k) - \Omega_{a,i}\|_F^2$ and $\|\Psi_i^o(k) - \Psi_{o,i}(k)\|_F^2$ are non-negative, they are uniformly bounded. Since Ω_i is constant, so $\{\Omega_i^a(k)\}$ and thus $\{\Psi_{o,i}(k)\}$ are uniformly bounded. It further implies that $\{\Psi_i^o(k)\}$ are uniformly bounded. Sum (7.13) over $[0, K]$, and we have the following relation:

$$\begin{aligned}
& -\frac{\lambda_{\max}(\Pi^{(2)})}{m_i^2} \sum_{0 \leq k \leq K, k \in T_i^a} (\|e_i^o(k)\|^2 + \|r_i^a(k)\|^2) + \frac{2\mu_i^o - (\mu_i^o)^2}{m_i^2} \sum_{0 \leq k \leq K, k \notin T_i^a} \|e_i^o(k)\|^2 \\
& \leq U_i(0) - U_i(K+1) < +\infty.
\end{aligned}$$

This implies that the sequence of $\{\|e_i^o(k)\|^2\}$ and the subsequence $\{\|r_i^a(k)\|^2\}_{k \in T_i^a}$ are summable. Then the subsequence of $\{\|r_i^a(k)\|^2\}_{k \in T_i^a}$ diminishing by Lemma 7.1.

Notice that $r_i^a(s) = r_i^a(\tau_i^a(k) + 1)$ for all $\tau_i^a(k) + 1 \leq s \leq k$. We are now in the position to show the convergence of the whole sequence $\{e_i^a(k)\}$. Pick any $\epsilon > 0$, there is $K(\epsilon) \geq 0$ such that the following holds for any $k', k'' \geq K(\epsilon)$ with $k', k'' \in T_i^a$:

$$\|r_i^a(k') - r_i^a(k'')\| \leq \epsilon. \quad (7.34)$$

Pick any $k_1, k_2 \geq K(\epsilon)$, then $\|r_i^a(k_1) - r_i^a(k_2)\|$ can be characterized as follows:

$$\|r_i^a(k_1) - r_i^a(k_2)\| = \|r_i^a(\tau_i^a(k_1)) - r_i^a(\tau_i^a(k_2))\| \leq \epsilon, \quad (7.35)$$

where the last inequality is a result of (7.34). As a result, the sequence of $\{r_i^a(k)\}_{k \geq 0}$ is a Cauchy sequence and thus converges. Since $\{r_i^a(k)\}_{k \in T_i^a}$ is a subsequence of $\{r_i^a(k)\}_{k \geq 0}$, it implies that $\{r_i^a(k)\}_{k \geq 0}$ has the same limit as $\{r_i^a(k)\}_{k \in T_i^a}$ and thus $\{r_i^a(k)\}_{k \geq 0}$ goes to zero. Since $e_i^a(k) = r_i^a(k) + (I + L_i)^{-1}e_i^o(k)$, this gives that $\{e_i^a(k)\}$ is diminishing. $\square$

Claim 8: If $k - \tau_i^a(k) \leq T_B$, then the sequence of $\{e_i^a(k)\}$ is square summable.

Proof. Since $k - \tau_i^a(k) \leq T_B$, then we have

$$\sum_{k=0}^{+\infty} \|r_i^a(k)\|^2 \leq T_B \sum_{k \in T_i^a} \|r_i^a(k)\|^2 < +\infty. \quad (7.36)$$

Recall that $e_i^a(k) = r_i^a(k) + (I + L_i)^{-1}e_i^o(k)$. It follows from the square summability of $\{e_i^o(k)\}$ and $\{r_i^a(k)\}$ that $\{e_i^a(k)\}$ is square summable. $\square$

This completes the proof of Proposition 4.3. $\square$

We are now ready to show Theorem 4.4 for ALGORITHM II (bilateral learning).

The proof of Theorem 4.4:

Proof. The proof is analogous to Theorem 3.2, and we only provide its sketch here. From Proposition 4.3, we know that $\{e_i^o(k)\}$ is square summable and $\{\Psi_i^o(k)\}$ is uniformly bounded. This result is the counterpart of Claim 2 in the proof of Theorem 3.2. The remainder of the proof can be finished by following analogous lines in Claim 1 and Claim 3 in Theorem 3.2. The details are omitted here. $\square$

REFERENCES

- [1] T. Alpcan and T. Basar. *Network Security: A Decision And Game Theoretic Approach*. Cambridge University Press, 2011.
- [2] S. Amin, A. Cardenas, and S.S. Sastry. Safe and secure networked control systems under denial-of-service attacks. In *Hybrid systems: Computation and Control*, pages 31–45, 2009.
- [3] S. Amin, X. Litrico, S.S. Sastry, and A.M. Bayen. Stealthy deception attacks on water SCADA systems. In *Hybrid systems: Computation and Control*, pages 161–170, Stockholm, Sweden, 2010.
- [4] S. Amin, G.A. Schwartz, and S.S. Sastry. Security of interdependent and identical networked control systems. *Automatica*, 49(1):186–192, 2013.
- [5] K.J. Åström and B. Wittenmark. *Adaptive control*. Dover Publications, 2008.
- [6] G.K. Befekadu, V. Gupta, and P.J. Antsaklis. Risk-sensitive control under a class of denial-of-service attack models. In *American Control Conference*, pages 643–648, San Francisco, USA, June 2011.
- [7] S. Bhattacharya and T. Basar. Game-theoretic analysis of an aerial jamming attack on a UAV communication network. In *American Control Conference*, pages 818–823, Baltimore, USA, June 2010.
- [8] S. Bhattacharya and T. Basar. Graph-theoretic approach for connectivity maintenance in mobile networks in the presence of a jammer. In *IEEE Int. Conf. on Decision and Control*, pages 3560–3565, Atlanta, USA, December 2010.

- [9] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.
- [10] M.S. Branicky, S.M. Phillips, and W. Zhang. Stability of networked control systems: explicit analysis of delay. In *American Control Conference*, pages 2352–2357, Chicago, USA, 2000.
- [11] R. W. Brockett and D. Liberzon. Quantized feedback stabilization of linear systems. *IEEE Transactions on Automatic Control*, 45(7):1279–1289, 2000.
- [12] M. Cao, A. S. Morse, and B. D. O. Anderson. Reaching a consensus in a dynamically changing environment - convergence rates, measurement delays and asynchronous events. *SIAM Journal on Control and Optimization*, 47(2):601–623, 2008.
- [13] J. Cortés. Global and robust formation-shape stabilization of relative sensing networks. *Automatica*, 45(12):2754–2762, 2009.
- [14] W. B. Dunbar and R. M. Murray. Distributed receding horizon control for multi-vehicle formation stabilization. *Automatica*, 42(4):549–558, 2006.
- [15] A. Gupta, C. Langbort, and T. Basar. Optimal control in the presence of an intelligent jammer with limited actions. In *IEEE Int. Conf. on Decision and Control*, pages 1096–1101, Atlanta, USA, December 2010.
- [16] A. Jadbabaie, J. Lin, and A. S. Morse. Coordination of groups of mobile autonomous agents using nearest neighbor rules. *IEEE Transactions on Automatic Control*, 48(6):988–1001, 2003.
- [17] T. Jiang, I. Matei, and J.S. Baras. A trust based distributed Kalman filtering approach for mode estimation in power systems. In *Proceedings of The First Workshop on Secure Control Systems*, pages 1–6, Stockholm, Sweden, April 2010.
- [18] H. K. Khalil. *Nonlinear Systems*. Prentice Hall, 3 edition, 2002.
- [19] D. Liberzon and J.P. Hespanha. Stabilization of nonlinear systems with limited information feedback. *IEEE Transactions on Automatic Control*, 50(6):910–915, 2005.
- [20] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *IEEE Int. Conf. on Decision and Control*, pages 5967–5972, Atlanta, USA, December 2010.
- [21] D. Nešić and A. Teel. Input-output stability properties of networked control systems. *IEEE Transactions on Automatic Control*, 49(10):1650–1667, 2004.
- [22] R. Olfati-Saber and R. M. Murray. Consensus problems in networks of agents with switching topology and time-delays. *IEEE Transactions on Automatic Control*, 49(9):1520–1533, 2004.
- [23] F. Pasqualetti, A. Bicchi, and F. Bullo. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control*, 57(1):90–104, February 2012.
- [24] F. Pasqualetti, R. Carli, and F. Bullo. A distributed method for state estimation and false data detection in power networks. In *IEEE Int. Conf. on Smart Grid Communications*, pages 469–474, October 2011.
- [25] 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.
- [26] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu. A survey of game theory as applied to network security. In *Int. Conf. on Systems Sciences*, pages 1–10, Hawaii, USA, 2010.
- [27] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry. Kalman filtering with intermittent observations. *IEEE Transactions on Automatic Control*, 49(9):1453–63, 2004.
- [28] S. Sundaram and C.N. Hadjicostis. Distributed function calculation via linear iterative strategies in the presence of malicious agents. *IEEE Transactions on Automatic Control*, 56(7):1731–1742, 2011.
- [29] R. S. Sutton and A. G. Barto. *Reinforcement Learning: An Introduction*. MIT Press, 1998.
- [30] A. Teixeira, S. Amin, H. Sandberg, K.H. Johansson, and S.S. Sastry. Cyber security analysis of state estimators in electric power systems. In *IEEE Int. Conf. on Decision and Control*, pages 5991–5998, Atlanta, USA, December 2010.
- [31] A. Teixeira, D. Perez, H. Sandberg, and K.H. Johansson. Attack models and scenarios for networked control systems. In *Int. Conf. on High Confidence Networked Systems*, pages 55–64, 2012.
- [32] G. Theodorakopoulos and J. S. Baras. Game theoretic modeling of malicious users in collaborative networks. *IEEE Journal of Selected Areas in Communications*, 26(7):1317–1327, 2008.
- [33] L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. In *IEEE Int. Conf. on Smart Grid Communications*, pages 226–231, Gaithersburg, USA, October 2010.

- [34] M. Zhu and S. Martínez. Discrete-time dynamic average consensus. *Automatica*, 46(2):322–329, 2010.
- [35] M. Zhu and S. Martínez. Attack-resilient distributed formation control via online adaptation. In *IEEE Int. Conf. on Decision and Control*, pages 6624–6629, Orlando, FL, USA, December 2011.
- [36] M. Zhu and S. Martínez. Stackelberg game analysis of correlated attacks in cyber-physical system. In *American Control Conference*, pages 4063–4068, June 2011.
- [37] M. Zhu and S. Martínez. On the performance of resilient networked control systems under replay attacks. *IEEE Transactions on Automatic Control*, 59(3):804–808, 2014.