Attack-resilient distributed formation control via online adaptation

Minghui Zhu and Sonia Martínez

***Abstract*— This paper investigates a distributed formation control problem in an operator-vehicle network where each vehicle is remotely controlled by an operator. Each operator-vehicle pair is attacked by an adversary, who corrupts the commands sent from the operator to the vehicle following a partially unknown strategy. We propose a novel distributed control algorithm that allows operators to adapt their policies online by exploiting the latest collected information about adversaries. The algorithm enables vehicles to asymptotically achieve the desired formation from any initial configuration and initial estimate of the adversaries' strategies. It is shown that the sequence of the distances to the desired formation is summable. A numerical example is provided to illustrate the performance of the algorithm. In particular, we observe that the rate of convergence to the desired formation is exponential, outperforming our theoretical result.**

I. Introduction

Recent advances in communications, sensing and computation have made possible the development of highly sophisticated unmanned vehicles. Applications include 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 the increased vulnerability of cyber and communication systems. Motivated by this, we consider a formation control problem for an operator-vehicle group 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 link can be attacked by an adversary, disrupting the overall group objective. Our main goal is to provide a resilient solution that assures mission completion despite the presence of security threats.

Literature review. Information networks have had a great impact on the way modern control systems operate today. Unfortunately, they have also become an attractive target of causal and organized attacks. In practice, either reactive or protective mechanisms have been exploited to deal with cyber attacks. Non-cooperative game theory [15] has been 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], [16], [30], [35].

The authors are with Department of Mechanical and Aerospace Engineering, University of California, San Diego, 9500 Gilman Dr, La Jolla CA, 92093, {mizhu,soniamd}@ucsd.edu

The area of networked control systems focuses on the effect of imperfect communication channels on remote control. Most of the existing papers focus on; e.g., band-limited channels [20], [24], quantization [11], [23], packet dropout [17], [31], delay [10], [36], and sampling [25].

Very recently, the security of the new generation of control systems, namely *cyber-physical systems*, has drawn mounting attention in the control society, and our current paper falls into this field. *Denial-of-service attacks*, destroying the data availability in control systems, are entailed in recent papers [2], [4], [6], [16]. Another important class of cyber attacks, namely *false data injection*, compromises the data integrity of state estimation and is attracting considerable effort; an incomplete reference list includes [21], [28], [34], [37]. *Replay attacks* maliciously repeat transmitted data, and their impact to control systems is first studied in [22]. The papers [3], [38] are devoted to studying *deception attacks* where attackers intentionally modify measurements and control commands. In [7], [8], the authors exploit pursuit-evasion games to compute optimal evasion strategies for mobile agents in the face of jamming attacks. The paper [3] examines the stability of a SCADA water management system under a class of switching attacks, and the authors in [19] propose a class of trust based distributed Kalman filters for power systems to prevent data disseminated by untrusted phase measurement units.

Regarding malicious behavior in multi-agent systems, we distinguish [27], [32] as two representative references relevant to this work. The paper [32] consider the problem of distributed function calculation in the presence of faulty or malicious agents, whereas [27] 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 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 group 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 real-time and feedback fashion. In contrast, the malicious model in [27], [32] may not be sufficient to capture the features of human adversaries. Here, we aim to design completely distributed algorithms for the operator-vehicle group to maintain mission assurance under limited knowledge of teammates and opponents. The 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 where 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 unknown matrix. We propose a distributed resilient formation control algorithm which consists of two feedback-connected blocks: a formation control block and an online learning block. The novel 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 the proposed algorithm guarantees that vehicles achieve asymptotically the desired formation from any initial vehicle configuration and any initial estimates of adversaries. The sequence of the distances to the desired formation is shown to be summable. In our simulation, the convergence rate turns out to be exponential, which outperforms the analytic result characterizing a worst-case convergence rate.

II. Problem formulation

Here, 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 rest of the manuscript. After this, we specify the information assumptions that operators have on adversaries.

A. Architecture and objective of the operator-vehicle network

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

$$p_i(k+1) = p_i(k) + u_i(k), \tag{1}$$

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 one-to-one and fixed. 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 secure[1], while the communications from operator to vehicle can be attacked. Other architectures are possible, and the present one is chosen as a first main class of operator-vehicle networked systems; see Figure 1.

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

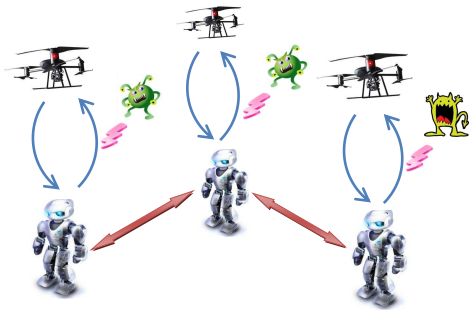

Fig. 1. The architecture of the operator-vehicle network

The mission of the operator-vehicle network is to achieve some desired formation which is characterized by a (directed) formation graph $\mathcal{G} := (V, \mathcal{E})$. Each edge $(j,i) \in \mathcal{E} \subseteq V \times V \setminus \mathrm{diag}(V)$, 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 $\mathcal{N}_i = \{i_1, \ldots, i_{n_i}\}$. Being a member of the team, each operator i is only aware of local formation constraints; i.e., ν_{ij} for $j \in \mathcal{N}_i$.

The multi-vehicle formation control mission can be encoded into the following optimization problem[2]:

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

where $p = [p_1^T, \cdots, p_N^T]^T \in \mathbb{R}^{Nd}$, $P_{ij} \in \mathbb{R}^{d\times d}$ is a diagonal and positive-definite weight matrix assigned to the link (j,i). The objective function $J(p)$ can describe any shape in $\mathbb{R}^d$ by adjusting ν_{ij}. Notice that $J(p)$ is a convex function of p since $\|\cdot\|^2_{P_{ij}}$ is convex and $p_i - p_j - \nu_{ij}$ is affine; c.f. [9]. Denote by the set of the (global) minimizers $X^* \subset \mathbb{R}^{Nd}$. We impose the following to ensure the desired formation is well-defined:

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

We assume that operators and vehicles are synchronized. Each operator only receives information from neighbors in $\mathcal{N}_i$ at each time instant. The communication graph between operators is then assumed to be fixed and identical to $\mathcal{G}$.

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], [18], [26], [29]. •

B. 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

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

adversary i with the operator-vehicle pair i. Each adversary is able to eavesdrop on incoming messages of her target operator. We further assume that adversaries are able to collect some imperfect information of their opponents in advance. Specifically, adversary i will have estimates $\hat{\nu}_{ij} \in \mathbb{R}^d$ of ν_{ij} and $\hat{P}_{ij} \in \mathbb{R}^{d\times d}$ of P_{ij}, for $j \in \mathcal{N}_i$. Here, $\hat{P}_{ij} \in \mathbb{R}^{d\times d}$ is positive-definite and diagonal.

Adversaries make real-time decisions based on the latest information available. In particular, at time k, adversary i eavesdrops $p_j(k)$ sent from operator $j \in \mathcal{N}_i$ to operator i, and intercepts $p_i(k)+u_i(k)$ sent from operator i to vehicle i. The adversary then computes a $v_i(k)$ which is added to $p_i(k) + u_i(k)$ so that vehicle i implements $p_i(k) + u_i(k) + v_i(k)$ instead. The command $v_i(k)$ will be the solution to the program:

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

where $R_i \in \mathbb{R}^{d\times d}$ is diagonal and positive definite. The above optimization problem captures two partly conflicting objectives. On the one hand, adversary i would like to destabilize the formation associated with vehicle i, and this interest is encapsulated in the term $\sum_{j\in\mathcal{N}_i} \|p_j(k) - (p_i(k)+u_i(k)+v_i) - \hat{\nu}_{ij}\|^2_{\hat{P}_{ij}}$. On the other hand, adversary i would like to avoid a high attacking cost $\|v_i(k)\|^2_{R_i}$, which represents the energy consumption of adding the signal $v_i(k)$. We assume the following on the cost matrices of adversaries:

Assumption 2.2: For all $j \in \mathcal{N}_i$, $\sum_{j\in\mathcal{N}_i} \hat{P}_{ij} - R_i < 0$.

In this way, the objective function of the optimization problem (2) is strictly concave. This can be verified by noticing that the Hessian $2\sum_{j\in\mathcal{N}_i} \hat{P}_{ij} - 2R_i$ is negative definite. As a consequence, the solution to the optimization problem (2) is unique and given by:

$$v_i(k) = -\sum_{j\in\mathcal{N}_i} L_{ij}(p_j(k) - (p_i(k) + u_i(k)) - \hat{\nu}_{ij}), \quad (3)$$

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

C. Justification of attacking costs and our attacker model

Here we provide a justification on the attacking cost $\|v_i\|^2_{R_i}$ in problem (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 alerts operator i that there is a greater risk to her vehicle, and consequently operator i will raise the security level (e.g., the expansion of radio frequencies) of the link to vehicle i, increasing the subsequent costs paid by adversary i (e.g. to block all of the radio frequencies following the operator). The term $\|v_i(k)\|^2_{R_i}$ represents the consideration of adversary i for her *subsequent* energy consumption which is directly determined by $v_i(k)$. As a rational decision maker, adversary i is willing to reduce such security cost, which, for simplicity, we model as a weighted 2-norm.

Problem (2) assumes that each adversary is a rational decision maker, and always chooses the optimal action based on the information available. Compared with [21], [27], [28], [32], [34], [37] 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 [16] 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.

D. Information about adversaries and online adaptation

In an adversarial environment, it is not realistic to expect that operators have complete and perfect information on their opponents. In this paper, we assume that operator i knows that adversary i makes decisions online based on the solution to the optimization problem (2), but has no access to the value of R_i, $\hat{P}_{ij}$ and $\hat{\nu}_{ij}$, which is some private information of adversary i. This implies that operator i knows that $v_i(k)$ is in the form of (3), but is unaware of the real value of L_{ij} and $\hat{\nu}_{ij}$. A more compact expression for $v_i(k)$ is given next.

Lemma 2.1: The vector $v_i(k)$ can be written in the following compact form:

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

where $\eta_{ij} := L_{ij}(\nu_{ij} - \hat{\nu}_{ij}) \in \mathbb{R}^d$, 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:

$$\begin{aligned} \Theta_i^T &:= [L_{ii_1} \ \cdots \ L_{ii_{n_i}} \ \eta_{ii_1} \ \cdots \ \eta_{ii_{n_i}}], \\ \phi_i(k) &:= -\begin{bmatrix} p_{i_1}(k) - (p_i(k) + u_i(k)) - \nu_{ii_1} \\ \vdots \\ p_{i_{n_i}}(k) - (p_i(k) + u_i(k)) - \nu_{ii_{n_i}} \end{bmatrix}, \\ \Phi_i(k) &:= -[\phi_i(k)^T \ 1 \cdots 1]^T, \end{aligned}$$

where $\mathcal{N}_i = \{i_1, \ldots, i_{n_i}\}$.

Proof: This fact can be readily verified. ■

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 $\Phi_i(k)$, without knowing the parameter Θ_i. It would be hard

to gather the private information Θ_i of adversaries *a priori*. We will exploit the ideas of reinforcement learning [33], and adaptive control [5], that operators can use to estimate Θ_i through continuous contact with adversaries. This will allow operators to adapt their policies *online* and eventually defeat adversaries.

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 $\|A\|_F^2 = \mathrm{tr}(A^TA) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}^2$ and $\|A\| \le \|A\|_F$.

Consider the diagonal vector map, $\mathrm{diag}_{\mathsf{ve}} : \mathbb{R}^{d\times d} \to \mathbb{R}^d$, defined as $\mathrm{diag}_{\mathsf{ve}}(A) = v$, with $v_i = A_{ii}$, for all i. Similarly, define the diagonal matrix map, $\mathrm{diag}_{\mathsf{ma}} : \mathbb{R}^{d\times d} \to \mathbb{R}^{d\times d}$, as $\mathrm{diag}_{\mathsf{ma}}(A) = D$, with $D_{ii} = A_{ii}$, $D_{ij} = 0$, for all i, j and $j \neq i$. Let $\mathbb{P}_{\ge 0} : \mathbb{R}^d \to \mathbb{R}^d$ be the projection operator from $\mathbb{R}^d$ onto the non-negative orthant of $\mathbb{R}^d$. Now define $\mathbb{P}_i : \mathbb{R}^{n_i(d+1)\times d} \to \mathbb{R}^{n_i(d+1)\times d}$ as follows. Given $\Lambda \in \mathbb{R}^{n_i(d+1)\times d}$, then $\mathbb{P}_i(\Lambda) = \tilde{\Lambda} \in \mathbb{R}^{n_i(d+1)\times d}$, where

$$\begin{aligned}
&\Lambda^T := [L_{ii_1}^T \ \cdots \ L_{ii_{n_i}}^T \ \eta_{ii_1}^T \ \cdots \ \eta_{ii_{n_i}}^T],\\
&\tilde{\Lambda}^T := [\tilde{L}_{ii_1}^T \ \cdots \ \tilde{L}_{ii_{n_i}}^T \ \tilde{\eta}_{ii_1}^T \ \cdots \ \tilde{\eta}_{ii_{n_i}}^T],\\
&\tilde{L}_{ij}^T = \mathrm{diag}_{\mathsf{ma}}(\mathbb{P}_{\ge 0}(\mathrm{diag}_{\mathsf{ve}}(L_{ij}^T))), \ \ \eta_{ij}^T = \tilde{\eta}_{ij}^T, \quad j \in \mathcal{N}_i.
\end{aligned}$$

The block-decomposition of Λ and $\tilde{\Lambda}$ is analogous to that of Θ_i in Lemma 2.1. The operator $\mathbb{P}_i$ will be used in the learning step of the proposed algorithm below.

III. Attack-resilient formation control algorithm and analysis

In this section, we propose a novel **attack-resilient formation control algorithm**, AR-FORM for short, and then summarize its properties of guaranteeing the formation control mission under malicious attacks. Due to the space limitation, we omit the proofs for the main results.

Overall, the algorithm can be roughly described as follows:

> At each time instant, each operator first collects the latest locations of neighboring operators' vehicles. Then, the operator computes a control law $u_i(k)$ 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 how adversary i corrupts her command as if $\Theta_i(k)$ were identical to Θ_i. After that, the operator sends the new command $p_i(k) + u_i(k)$ to her associated vehicle. Adversary i then corrupts the command by adding the signal $v_i(k)$ parameterized by Θ_i. Vehicle i receives, implements, and further sends back to operator i the corrupted command $p_i(k) + u_i(k) + v_i(k)$. After receiving the new location of her vehicle, operator i computes the estimation error of Θ_i, and updates her estimate to minimize an 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.

Algorithm 1 The AR-FORM Algorithm for group i

Initialization: Initial value $\tilde{\Theta}_i \in \mathbb{R}^{n_i(d+1)\times d}$ and estimate $\Theta_i(0) = \mathbb{P}_i[\tilde{\Theta}_i]$ of the adversary parameter.

Iteration: At each $k \ge 0$, adversary, operator, and vehicle i interact through the following sequence of steps:

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

$$\begin{aligned}
&\min_{u_i(k)\in\mathbb{R}^d} \sum_{j\in\mathcal{N}_i} \|p_j(k) - p_i(k+1|k) - \nu_{ij}\|_{P_{ij}}^2,\\
&\text{s.t. } \ p_i(k+1|k) = p_i(k) + u_i(k) + \Theta_i(k)^T\Phi_i(k), \quad (4)
\end{aligned}$$

to obtain the optimal solution $u_i(k)$.

2: Operator i sends $p_i(k)+u_i(k)$ to vehicle i, and generates the estimate:

$$p_i(k+1|k) = p_i(k) + u_i(k) + \Theta_i(k)^T\Phi_i(k).$$

3: Adversary i eavesdrops on $p_j(k)$ sent from operator $j \in \mathcal{N}_i$ to operator i, and corrupts $p_i(k) + u_i(k)$ by adding $v_i(k) = \Theta_i^T\Phi_i(k)$.

4: Vehicle i receives and implements $p_i(k)+u_i(k)+v_i(k)$, and then sends back $p_i(k+1) = p_i(k) + u_i(k) + v_i(k)$ to operator i.

5: Operator i computes the estimation error $e_i(k) = p_i(k+1) - p_i(k+1|k)$, and updates the 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 $k = k + 1$.

Remark 3.1: Let $\Theta_i(k)^T$ be partitioned in the form:

$$\Theta_i(k)^T = [L_{ii_1}(k) \ \cdots \ L_{ii_{n_i}}(k) \ \eta_{ii_1}(k) \ \cdots \ \eta_{ii_{n_i}}(k)],$$

where $L_{ij}(k) \in \mathbb{R}^{d\times d}$ and $\eta_{ij}(k) \in \mathbb{R}^d$, for $j \in \mathcal{N}_i = \{1, \cdots, n_i\}$. Then, the solution $u_i(k)$ to the quadratic program in Step 1 can be explicitly computed as follows:

$$\begin{aligned}
u_i(k) = &\big(\sum_{j\in\mathcal{N}_i} P_{ij}(I + \sum_{l\in\mathcal{N}_i} L_{il}(k))\big)^{-1}\\
&\times \sum_{j\in\mathcal{N}_i} P_{ij}\big\{(p_j(k) - p_i(k) - \nu_{ij})\\
&+ \sum_{l\in\mathcal{N}_i} L_{il}(k)(p_l(k) - p_i(k) - \nu_{il}) + \sum_{l\in\mathcal{N}_i}\eta_{il}(k)\big\}. \quad (5)
\end{aligned}$$

Hence, the program in Step 1 is equivalent to the computation (5). In Step 5, 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 a projection 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 the proposed algorithm allows the operator-vehicle network to achieve the desired formation despite the malicious attacks of adversaries.

Theorem 3.1: (Convergence properties of the AR-FORM **algorithm):** Consider any initial position $p(0) \in \mathbb{R}^{Nd}$ of vehicles. If Assumptions 2.1 and 2.2 hold, then the AR-FORM algorithm for every group i ensures that the vehicles asymptotically achieve the desired formation; i.e., $\lim_{k\to+\infty} \mathrm{dist}(p(k), X^*) = 0$. Furthermore, the rate of convergence of the algorithm ensures

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

We provide a coupled of remarks to conclude this section. Persistent excitation (e.g., in [5]) is not guaranteed to be satisfied by the AR-FORM algorithm, thus the formation convergence rate may not be exponential. Furthermore, without persistent excitation, we cannot guarantee either the convergence of the estimate $\Theta_i(k)$ to the true value Θ_i. Note that the regressor $\Phi_i(k)$ is coupled by the locations of different vehicles. Thus, we would need full coordination between operators at each time instant to guarantee persistent excitation. The absence of a centralized authority makes this task challenging.

IV. Simulation

We now set out to elucidate the performance of our proposed algorithm through a numerical example. Consider a group of 15 vehicles which are initially randomly deployed over the square of 50×50 as in Figure 2. Figure 3 delineates the trajectory of each vehicle in the first 60 iterations of the algorithm. The configuration of the vehicles at the 60^{th} iteration is given by Figure 4 and this one is identical to the desired formation. This fact can be verified by Figure 5, which shows the evolution of the formation errors. Figure 5 also demonstrates that the convergence rate in the simulation is exponential and this is faster than our analytical result.

V. Conclusions

In this paper, we have studied a formation control problem for a operator-vehicle network in the presence of a team of adversaries. We have proposed a novel attack-resilient distributed formation control algorithm, the AR-FORM, and analyzed its asymptotic convergence properties. Our results have demonstrated the potential of online learning to enhance network resilience, and suggest a number of future research directions which we plan to investigate. For example, more challenging scenarios can be created by considering intelligent adversaries who can learn some private information of operators; e.g., ν_{ij} and P_{ij}, and adapt their attacking policies online. The current operator-vehicle architecture can be enlarged to allow for more complex interactions. In addition, it would be interesting to study the impact of other attacks; e.g., denial-of-service attacks and replay attacks, to cooperative control in the operator-vehicle network.

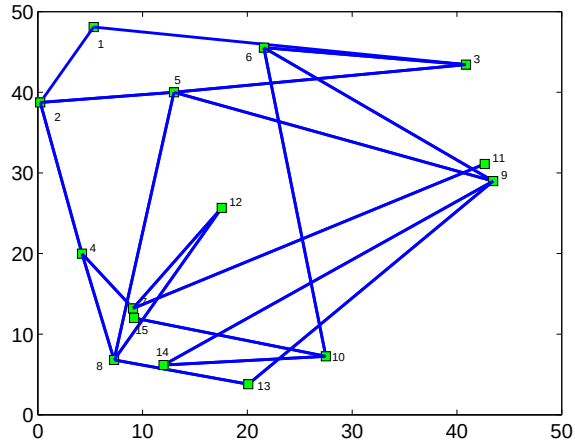

Fig. 2. Initial configuration of vehicles.

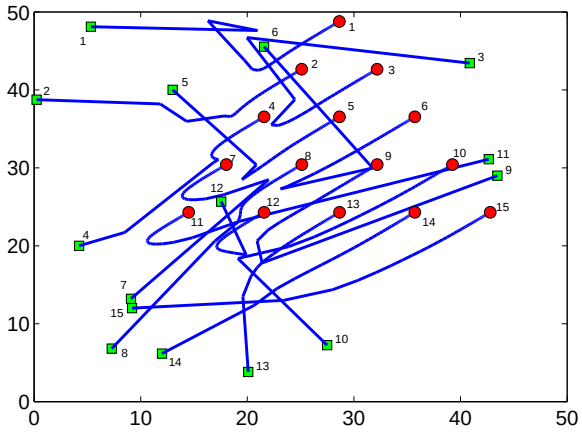

Fig. 3. Trajectories of the vehicles during the first 60 iterations. The green squares stand for initial locations and red circles represent final locations.

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. Sastry, and A. M. Bayen. Stealthy deception attacks on water SCADA systems. In *Proceedings of the 13th ACM International Conference on 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*, July 2010. submitted.

[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.

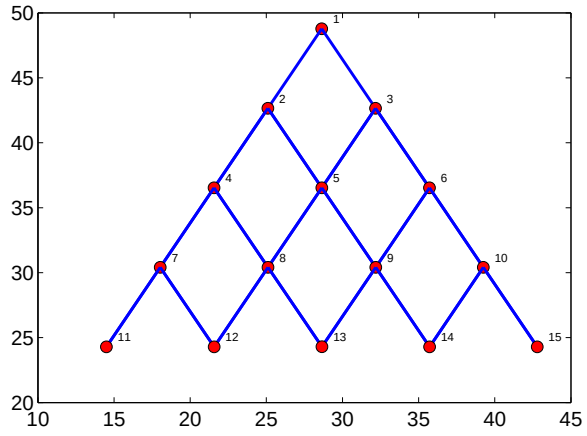

Fig. 4. The configuration of vehicles at the 60^{th} iteration.

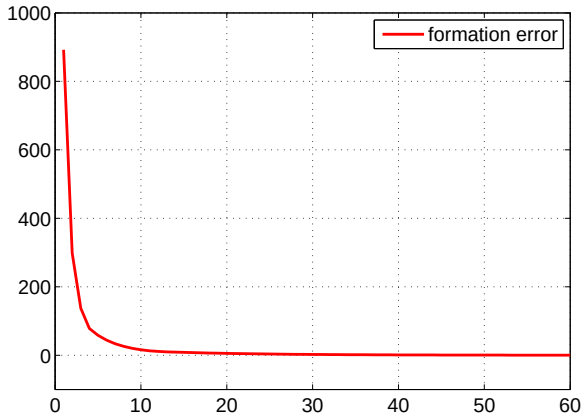

Fig. 5. The evolution of formation errors during the first 60 iterations.

[8] S. Bhattacharya and T. Basar. Graph-theoretic approach for connectivity maintenance in mobile networks in the presence of a jammer. In *IEEE 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 *Proceedings of 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] D. Fudenberg and J. Tirole. *Game theory*. The MIT press, 1991.

[16] A. Gupta, C. Langbort, and T. Basar. Optimal control in the presence of an intelligient jammer with limited actions. In *IEEE Conf. on Decision and Control*, pages 1096–1101, Atlanta, USA, December 2010.

[17] V. Gupta and N. Martins. On stability in the presence of analog erasure channels between controller and actuator. *IEEE Transactions on Automatic Control*, 55(1):175–179, 2010.

[18] 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.

[19] 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*, Stockholm, Sweden, April 2010.

[20] D. Liberzon and J. P. Hespanha. Stabilization of nonlinear systems with limited information feedback. *IEEE Transactions on Automatic Control*, 50(6):910–915, 2005.

[21] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *IEEE Conf. on Decision and Control*, pages 5967–5972, Atlanta, USA, December 2010.

[22] Y. Mo and B. Sinopoli. Secure control against replay attacks. In *Forty-Seventh Annual Allerton Conference*, UIUC, Illinois, USA, September 2009.

[23] G. N. Nair, R. J. Evans, I. M. Y. Mareels, and W. Moran. Topological feedback entropy and nonlinear stabilization. *IEEE Transactions on Automatic Control*, 49(9):1585–1597, 2004.

[24] G. N. Nair, F. Fagnani, S. Zampieri, and R. J. Evans. Feedback control under data rate constraints: an overview. *Proceddings of IEEE Special Issue on Technology of Networked Control Systems*, 95(1):108–137, 2007.

[25] D. Nesic and A. Teel. Input-output stability properties of networked control systems. *IEEE Transactions on Automatic Control*, 49(10):1650–1667, 2004.

[26] 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.

[27] F. Pasqualetti, A. Bicchi, and F. Bullo. Consensus computation in unreliable networks: A system theoretic approach. *IEEE Transactions on Automatic Control*, February 2010. To appear.

[28] F. Pasqualetti, R. Carli, and F. Bullo. Distributed estimation and false data detection with application to power networks. *Automatica*. submitted.

[29] W. Ren and R. Beard. *Distributed Consensus in Multi-vehicle Cooperative Control*. Communications and Control Engineering. Springer-Verlag, London, 2008.

[30] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu. A survey of game theory as applied to network security. In *Proceedings of the 43rd Hawaii International Conference on System Sciences*, pages 1–10, Hawaii, USA, 2010.

[31] L. Schenato, B. Sinopoli, M. Franceschetti, K. Poolla, and S. S. Sastry. Foundations of control and estimation over lossy networks. *Proceddings of IEEE Special Issue on Technology of Networked Control Systems*, 95(1):163–187, 2007.

[32] S. Sundaram and C. N. Hadjicostis. Distributed function calculation via linear iterative strategies in the presence of malicious agents. *IEEE Transactions on Automatic Control*. To appear.

[33] R. S. Sutton and A. G. Barto. *Reinforcement Learning: An Introduction*. MIT Press, 1998.

[34] 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 Conf. on Decision and Control*, pages 5991–5998, Atlanta, USA, December 2010.

[35] G. Theodorakopoulos and J. S. Baras. Game theoretic modeling of malicious users in collaborative networks. *IEEE Journal on Selected Areas in Communications*, 7:1317–1327, 2008.

[36] Z. Wang and F. Paganini. Global stability with time-delay in network congestion control. In *Proceedings of the 41st IEEE Conference on Decision and Control*, pages 3632–3637, Las Vegas, USA, 2002.

[37] L. Xie, Y. Mo, and B. Sinopoli. False data injection attacks in electricity markets. In *2010 First International Conference on Smart Grid Communications*, pages 226–231, Gaithersburg, USA, October 2010.

[38] M. Zhu and S. Martínez. Stackelberg game analysis of correlated attacks in cyber-physical systems. In *2011 American Control Conference*, pages 4063–4068, June 2011.