Cooperative Systems in Presence of Cyber-Attacks: A Unified Framework for Resilient Control and Attack Identification

Azwirman Gusrialdi and Zhihua Qu

***Abstract*— This paper considers a cooperative control problem in presence of unknown attacks. The attacker aims at destabilizing the consensus dynamics by intercepting the system's communication network and corrupting its local state feedback. We first revisit the virtual network based resilient control proposed in our previous work and provide a new interpretation and insights into its implementation. Based on these insights, a novel distributed algorithm is presented to detect and identify the compromised communication links. It is shown that it is not possible for the adversary to launch a harmful and stealthy attack by only manipulating the physical states being exchanged via the network. In addition, a new virtual network is proposed which makes it more difficult for the adversary to launch a stealthy attack even though it is also able to manipulate information being exchanged via the virtual network. A numerical example demonstrates that the proposed control framework achieves simultaneously resilient operation and real-time attack identification.**

***Index Terms*— Resilient control, attack identification, leaderless consensus, cyber-attacks.**

I. INTRODUCTION

Cooperative control has been demonstrated to provide an efficient way for controlling and coordinating a large-number of distributed small devices over a communication network due to its scalability and robustness to a single point of failure. Cooperative control has been applied to various problems including smart grids, intelligent transportation systems, and robotics [1]–[4]. Even though open and pervasive Information and Communication Technologies (ICT) such as wireless communication technologies facilitates the implementation of cooperative control, its use comes at a price of making the cooperative system vulnerable to cyber-attacks which may cause physical damage to the systems [5]. Since in practice cyber-attacks cannot be foreseen in advance, it is therefore highly desirable to design control algorithms which can maintain or restore systems performance under unknown attacks, commonly referred to as resilient control algorithms. A variety of resilient cooperative control algorithms have been proposed in the literature to attenuate the impact of cyber-attacks in the cooperative systems, see for example [6]–[10]. Among those strategies, a mean subsequence reduced algorithm [6] has been shown to be powerful to achieve resilient consensus without requiring any assumptions on the attacker's behavior. However, the strategy requires a knowledge on the upper bound of the maximum number of attacks and also poses a restriction on the network topology. On the other hand, a virtual network based approach originally proposed in [9], [11] for leaderless consensus has been shown to be promising to deal with unknown cyber-attacks due to the following reasons: (i) it requires no assumptions on the maximum number of attacks; (ii) it can deal with different type of attacks on actuator, sensor and/or communication network [12]–[14]; (ii) it can be extended and applied to different cooperative control problems including leader-following consensus [15], formation containment [12] and also cooperative heterogeneous system with plug and play operation [14]. Furthermore, it has been applied to resilient control of smart grid [16], [17] and connected vehicles [18]. However, despite its promise, it is still not totally clear how to implement the virtual network and how to interpret it.

In this paper, we consider a cooperative system in presence of cyber-attacks where the attacker intercepts the system's communication network and corrupts its local state feedback to destabilize the system. First, we revisit the virtual network based resilient control algorithm proposed in our previous work [9] and provide a new interpretation and insights into its implementation. Based on the insights, a novel distributed algorithm is proposed to detect and identify the compromised communication links, resulting in a unified framework for achieving resilient control and real-time attack identification. Specifically, it is shown that it is not possible for the adversary to launch a harmful and stealthy attack by only manipulating the physical states being exchanged through the network. When an adversary is also able to manipulate the information exchanged via the virtual network, a new virtual network with time-varying weights is proposed which makes it more difficult for the adversary to launch a stealthy attack compared to the virtual network with constant weights.

The paper is organized as follows. After formally formulating the problem in Section II, the virtual network based resilient control algorithm is revisited and a new interpretation on its implementation is provided in Section III. Distributed algorithms to identify cyber-attacks for different scenarios are discussed in Sections IV and V. The proposed algorithms are demonstrated via a numerical example in Section VI. Concluding remarks are presented in Section VII.

II. PROBLEM FORMULATION

In this section, we first provide a brief overview of graph theory followed by describing the problem formulation.

A. Gusrialdi is with Faculty of Engineering and Natural Sciences, Tampere University, Tampere 33014, Finland. Z. Qu is with Department of Electrical and Computer Engineering, University of Central Florida, Orlando 32816, USA. Emails: *azwirman.gusrialdi@tuni.fi* and *qu@ucf.edu*. The work of A. Gusrialdi was supported by Academy of Finland under academy project decision no. 330073. The work of Z. Qu was supported in part by US Department of Energy's awards DE-EE0007998, DE-EE0009028, DE-EE0009152, and DE-EE0009339.

A. Notation and Preliminaries

Let $\mathbb{R}$ be the set of real numbers; vector $\mathbf{1}_n \in \mathbb{R}^n$ denotes the vector of all ones. Given a vector $b \in \mathbb{R}^n$, we denote the i-th element of b as b_i. Furthermore, diag$(b) \in \mathbb{R}^{n\times n}$ represents the diagonal matrix with the vector $b \in \mathbb{R}^n$ on its diagonal. The identity matrix $I_n \in \mathbb{R}^{n\times n}$ is given by $I_n = \text{diag}(\mathbf{1}_n)$. Cardinality of a set $\mathcal{N}$ is denoted by $|\mathcal{N}|$.

Let $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ be an undirected graph with a set of nodes $\mathcal{V} = \{1, 2, \cdots, n\}$ and a set of edges $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$. An edge $(j, i) \in \mathcal{E}$ denotes that node i can receive information from node j. Since graph $\mathcal{G}$ is undirected, we have $(j, i) \in \mathcal{E} \Leftrightarrow (i, j) \in \mathcal{E}$. The neighbor set of node i is defined as $\mathcal{N}_i = \{j|(j, i) \in \mathcal{E}, j \neq i\}$. The undirected graph $\mathcal{G}$ is connected if there exists no isolated nodes in the graph. The entries of Laplacian matrix $L = [L]_{ij}$ associated with an undirected graph $\mathcal{G}$ are defined as $[L]_{ii} = |\mathcal{N}_i|$, $[L]_{ij} = -1$ if $j \in \mathcal{N}_i$ and $[L]_{ij} = 0$ if otherwise. If the graph $\mathcal{G}$ is connected, the null space of L associated with $\mathcal{G}$ is 1-dimensional and spanned by the vector $\mathbf{1}_n$. Furthermore, the eigenvalues of L are given by $0 = \lambda_1(L) < \lambda_2(L) \leq \cdots \leq \lambda_n(L)$.

B. Cooperative Systems

Consider the following cooperative system Σ_s consisting of n nodes:

$$\dot{x} = -L_s x \tag{1}$$

where $x \in \Re^n$ is the state of physical variables to be controlled toward a *consensus* (in the sense that $x \to c_s\mathbf{1}$ with $c_s \in \Re$) and L_s is the Laplacian matrix. Interactions between nodes within the cooperative system can be represented by a graph $\mathcal{G}_s$. In this paper, we assume that the graph $\mathcal{G}_s$ corresponding to Laplacian matrix L_s is *undirected* and *connected*. Under this topological condition, it is well known [19] that the system (1) reaches consensus with value c_s is equal to $\mathbf{1}_n^T x(0)/n$ where $x(0)$ denotes the initial state. It is worth noting that systematic designs are presented in [20] for general classes of nonlinear and linear networked systems and, more importantly, their dynamic behaviors at the network level are shown therein to be equivalent to system (1). Therefore, the design proposed in this paper has broad implications for general networked systems and is not restricted to linear cooperative dynamics.

C. Cooperative Systems under Cyber-Attacks

In practice, the communication network may be subject to attack and thus its state equation is now represented by

$$\dot{x} = -L_s(x - d), \tag{2}$$

where $d(t) \in \Re^n$ is an unknown exogenous injection. That is, $d_i(t) \neq 0$ means that the information received from node i is being compromised and the local state feedback of node i is corrupted. The attacker could have up to the full knowledge on the Laplacian L_s and also have access to the state x. In addition, it is assumed that the adversary inserts a bounded injection. This assumption is reasonable in practice as an intelligent attacker would aim at destabilizing the system with a limited change to avoid any detection. Moreover, an injection of unbounded magnitude can be easily rejected by a threshold check [15]. The bounded injections can take of the following forms [10], [13], [15], [18], [21]:

1) Uniformly bounded injections: That is, $\|d(t)\|_\infty \leq \overline{d}$ and $\|\dot{d}(t)\|_\infty \leq \overline{d}_d$ for some constant $\overline{d}, \overline{d}_d$. This type of injection is easy to launch since it does not require the information about the system and may deviate the desired consensus value.
2) Finite-gain injections: Injection vector $d(t)$ is generated by exogenous finite-L_2-gain dynamics of the state x, that is, $d(t)$ satisfies the following differential equation
$$\dot{d} = f(d, x), \tag{3}$$
in which d would vanish when state x settles so any potential attack would not be visible when system is idle or at the steady state.

Finally, let

$$\check{x}_j = x_j + d_j \tag{4}$$

denote the compromised information sent by j and $\hat{x}_{ij}$ is the estimation of the (compromised) information x_j at node i. We introduce the following definition of a *stealthy* attack.

Definition 1: An attack launched at $t = t_a$ on the link $(j, i) \in \mathcal{E}_s$ is *stealthy* if $\hat{x}_{ij}(t) = \check{x}_j(t)$, $\forall t \geq t_a$.

D. Paper's Objectives

The objective of this paper is twofold:

1) design a network enabled control algorithm u so that the following system
$$\dot{x} = -L_s(x - d) + u \tag{5}$$
remains to operate close to its nominal consensus value $(\mathbf{1}_n^T x(0)/n)\mathbf{1}_n$ under all possible unknown and possibly stealthy cyber-attack d
2) detect and identify in a distributed fashion all the compromised communication links.

III. Revisiting Virtual Network based Resilient Control: A New Interpretation

The cooperative system Σ_s can be made resilient against unknown cyber-attacks by introducing a virtual system Σ_h, as proposed in [9], whose number of nodes is equal to n and interconnected with the cooperative system (2). In particular, the defender's strategy u in (5) is given by

$$u = \beta L_s z, \;\; \dot{z} = -L_s z - \beta L_s x$$

and the resulting interconnected system can be written as

$$\begin{aligned} \dot{x} &= -L_s(x - d) + \beta L_s z, \\ \dot{z} &= -L_s z - \beta L_s x, \end{aligned} \tag{6}$$

where $z \in \Re^n$ is the state of virtual network and $\beta > 0$ is a design parameter to be chosen. In contrast to the state of cooperative system x, the virtual state z does not have any physical meaning and its initial condition $z(0)$ can be set to any arbitrary values. It is shown in [9] that by increasing β, the state x of interconnected system (6) is forced to converge to an arbitrary small neighbourhood around $(\mathbf{1}_n^T x(0)/n)\mathbf{1}_n$.

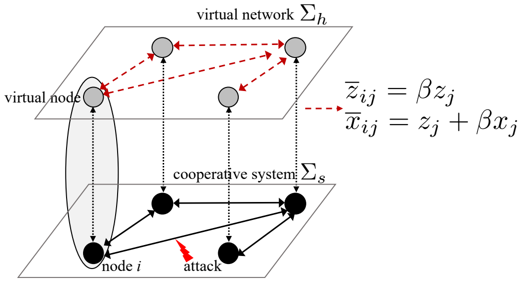

virtual network Σ_h
virtual node
$\overline{z}_{ij} = \beta z_j$
$\overline{x}_{ij} = z_j + \beta x_j$
cooperative system Σ_s
node i
attack

Fig. 1: Implementation of virtual network based resilient control strategy

However, it is still not totally clear how to implement the above virtual network. One contribution of the paper is to describe how we can implement the above virtual network to achieve resilient cooperative system.

The implementation of the virtual network based resilient control (6) is illustrated in Fig. 1. The resilient control at the i-th node can be written as

$$\begin{aligned}\dot{x}_i &= -[L_s]_{i*}(x-d) + \beta|\mathcal{N}_i|z_i - \sum_{j\in\mathcal{N}_i}\beta z_j,\\ \dot{z}_i &= -|\mathcal{N}_i|z_i - \beta|\mathcal{N}_i|x_i + \sum_{j\in\mathcal{N}_i}[z_j+\beta x_j]\end{aligned} \tag{7}$$

where $[L_s]_{i*}$ denote the i-th row of Laplacian matrices L_s. From Fig. 1 and individual dynamics (7), the steps for implementing resilient control (6) are as follows:

1) Each node maintains a local virtual node which can be implemented as an internal signal to that particular node. Hence, the communication between node i and its corresponding local virtual node is not subject to attack. Furthermore, virtual node i has a copy of the physical state of the i-th node x_i and a virtual state z_i.
2) In addition to the physical state x_j, each node also sends the following information
$$\overline{z}_{ij} = \beta z_j, \quad \overline{x}_{ij} = z_j + \beta x_j, \tag{8}$$
to its neighboring nodes $i \in \mathcal{N}_j$ using communication channels (e.g., via clouds) different than the one used for exchanging x_j. This requirement can be realized by taking advantage of networking technologies, namely network slicing approach for partitioning a shared physical infrastructure into multiple virtual networks [22] and software-defined networking to direct traffic in the network.
3) After receiving all the required information via different communication channels, each node then updates both its physical and virtual states according to (7).

IV. Attack Identification

After guaranteeing resiliency of the cooperative system, we now proceed with identifying distributively communication links $(j,i) \in \mathcal{E}_s$ that are being attacked using the new interpretation on the virtual network's implementation. The proposed attack identification algorithm consists of the following two steps:

1) using information $\overline{x}_{ij}, \overline{z}_{ij}$ defined in (8) and received via virtual network Σ_h, node i estimates the neighboring physical state x_j whose estimation is given by $\hat{x}_{ij}$. Specifically, the estimated x_j at node i can be computed from (8) as
$$\hat{x}_{ij} = \frac{1}{\beta}\left(\overline{x}_{ij} - \frac{\overline{z}_{ij}}{\beta}\right). \tag{9}$$
2) node i then compares the estimated state $\hat{x}_{ij}$ with its (possibly compromised) neighboring physical state $\breve{x}_j$ in (4) directly communicated in Σ_s to detect and identify whether the communication link $(j,i) \in \mathcal{E}_s$ is being attacked.

Using the information on $\hat{x}_{ij}$ and $\breve{x}_j$, we propose the following test criterion for node i to detect if link $(j,i) \in \mathcal{E}_i$ is compromised:

$$\textbf{Detection test:} \quad \hat{x}_{ij} = \breve{x}_j. \tag{10}$$

Note that in order to perform detection test (10), node i only requires local information available or received via Σ_s and virtual network Σ_h. The only common information (i.e., global information) for all nodes is the scalar gain $\beta > 0$. However, since the gain β is constant, its value can be fixed and assigned to all the nodes in advance before deploying the cooperative system and executing resilient control law (6).

The distributed and real-time attack identification using test criterion (10) is summarized in the following lemma.

Lemma 1: Given a communication link $(j,i) \in \mathcal{E}_s$ and detection test criterion (10). We have the following results.

1) Node j or communication link $(j,i) \in \mathcal{E}_s$ is being compromised if and only if $\hat{x}_{ij} \neq \breve{x}_j$
2) Injection d_j which results in a stealthy attack is given by $d_j = 0$.

Proof: To prove the first statement, observe that since it is assumed that the adversary can only insert injection to the cooperative system in Σ_s, the estimate $\hat{x}_{ij}$ in (9) will result in the true (uncorrupted) value of x_j. Hence, the condition $\hat{x}_{ij} \neq \breve{x}_j$ indicates that the information on x_j received at node i via the communication network in Σ_s has been manipulated. Therefore, it can be concluded that node j or the communication link $(j,i) \in \mathcal{E}_s$ has been compromised.

To prove the second statement, observe from definition 1 that the stealthy attack has to satisfy $\hat{x}_{ij} = \breve{x}_j$. Since the virtual network is not attacked, we have $\hat{x}_{ij} = x_j$. Hence, the stealthy injection d_j needs to satisfy $x_j = x_j + d_j$, resulting in $d_j = 0$. ■

Lemma 1 shows that it is not possible for the adversary to launch a harmful and stealthy attack when it can only have access to the communication network in Σ_s. In the next section, we discuss a scenario where an adversary has access also to the virtual network Σ_h.

V. Preventing Stealthy Attacks on the Virtual Network

Let us now consider a scenario in which the adversary is able to attack the communication network in the virtual network Σ_h. That is, the adversary can manipulate the information $\overline{x}_{ij}, \overline{z}_{ij}$ being exchanged in the virtual network by injecting bounded signals $\overline{d}^x_{ij}, \overline{d}^z_{ij}$ respectively. The test criterion (10) under this new scenario becomes

$$(\overline{x}_{ij} + \overline{d}^x_{ij}) - \frac{(\overline{z}_{ij} + \overline{d}^x_{ij})}{\beta} = \beta(x_j + d_j). \tag{11}$$

We then have the following result on the impact of the attack on the cooperative system.

Lemma 2: Assume that the adversary can attack both networks in Σ_s and Σ_h and knows the relation between the physical and virtual states. The adversary can then destabilize the cooperative system. Furthermore, the adversary can launch stealthy attacks by choosing non-zero injections $d_j, \overline{d}^x_{ij}, \overline{d}^z_{ij}$ satisfying (11).

Proof: It is shown in [23] that if the attacker also gains access to the virtual network Σ_h and is able to learn the relation between noth the physical and virtual states, then the attacker can destabilize the overall system for all large values of $\beta > 0$. In addition, in order to be stealthy, the attacker also needs to insert injections which satisfy $\hat{x}_{ij} = \check{x}_j$ for each compromised communication link yielding the condition (11). It is clear that there are many combinations of injections $d_j, \overline{d}^x_{ij}, \overline{d}^z_{ij}$ satisfying (11). ■

Next, we present a distributed strategy to prevent the adversary from launching a stealthy attack, i.e., to learn the relation between both physical and virtual states, given that he/she has access to both networks Σ_s and Σ_h. The idea is to introduce time-varying weights to the Laplacian matrices associated with the virtual network Σ_h. To this end, the interconnected system (6) is modified as follows

$$\begin{aligned} \dot{x} &= -L_s(x - d) + \beta L_s \Gamma(t) z, \\ \dot{z} &= -Hz - \beta \Gamma(t) L_s x, \end{aligned} \tag{12}$$

where matrices

$$H = L_s + I_n, \;\; \Gamma(t) = \mathrm{diag}\{[\alpha_1(t), \cdots, \alpha_n(t)]^T\}.$$

Here, scalar $\alpha_i(t) > 0$ for $i \in \{1, \cdots, n\}$ are time-varying functions individually known at the ith node within both the physical network and the virtual network. Furthermore, $\alpha_i(t)$ is chosen such that $\alpha_i(t)$ is uniformly bounded away from zero and that $\dot{\alpha}_i(t)$ exists and is uniformly bounded.

Similar to resilient control (6), for the newly design resilient control (12) the i-th node executes the following update law

$$\begin{aligned} \dot{x}_i &= -[L_s]_{i*}(x - d) + \beta |\mathcal{N}_i| \alpha_i(t) z_i - \sum_{j \in \mathcal{N}_i} \beta \alpha_j(t) z_j, \\ \dot{z}_i &= -(|\mathcal{N}_i| + 1) z_i - \beta |\mathcal{N}_i| \alpha_i(t) x_i + \sum_{j \in \mathcal{N}_i} [z_j + \beta \alpha_i(t) x_j]. \end{aligned} \tag{13}$$

To implement (13), in addition to the physical state x_j, each node also sends the information given by

$$\overline{z}^n_{ij} = \beta \alpha_j(t) z_j, \;\; \overline{x}^n_{ij} = z_j + \beta \alpha_i(t) x_j, \tag{14}$$

to its neighboring nodes $i \in \mathcal{N}_j$ using different channels than the one used for sending x_j. Note that in order to send $\overline{x}^n_{ij}$ two neighboring nodes i, j have to share their functions $\alpha_i(t)$ and $\alpha_j(t)$. Since the functions $\alpha_i(t)$ are independent of the states x, z the neighboring nodes can share their functions $\alpha_i(t)$ in advance before the deployment of cooperative system and later individually update the values $\alpha_i(t)$ in real-time. Hence, resilient control (13) can be designed in a distributed manner. Next, we analyze stability of interconnected system (6) both in the absence and presence of cyber-attacks on the network Σ_s.

A. Analysis of Nominal Interconnected System

The following lemma shows that in the absence of attacks the newly designed virtual network does not impact the convergence of state x to the consensus value of $(\mathbf{1}_n^T x(0)/n)\mathbf{1}_n$.

Lemma 3: Consider interconnected system (12) with $d = 0$. Then the same consensus of x can be ensured, that is $x \to (\mathbf{1}_n^T x(0)/n)\mathbf{1}_n$ as $t \to \infty$.

Proof: Setting $d = 0$ and computing the time derivative of $\eta_{s1} = \mathbf{1}_n^T x$ along the trajectory (12) yields

$$\dot{\eta}_{s1} = \mathbf{1}_n^T(-L_s x + \beta L_s \Gamma(t) z) = 0.$$

Hence, we know that η_{s1} is invariant.

Now let us define the following error vectors $e_x = x - \frac{\mathbf{1}^T x(0)}{n}\mathbf{1}$ and transformation matrix $T = \begin{bmatrix} \frac{1}{\sqrt{n}}\mathbf{1}_n & \nu_2 & \cdots & \nu_n \end{bmatrix}^T$ where $\nu_i \in \mathbb{R}^n$ denotes the eigenvector of Laplacian L_s corresponding to eigenvalue $\lambda_i(L_s)$. We then have

$$Te_x = \begin{bmatrix} 0 \\ \tilde{e}_x \end{bmatrix}. \tag{15}$$

Using (15), we can write (12) with $d = 0$ as

$$\begin{aligned} \dot{\tilde{e}}_x &= -\Lambda \tilde{e}_x + \beta W \Gamma(t) z \\ \dot{z} &= -Hz - \beta \Gamma(t) W^T \tilde{e}_x \end{aligned} \tag{16}$$

where $\Lambda = \mathrm{diag}\{[\lambda_2(L_s), \cdots, \lambda_n(L_s)]^T\}$ and

$$TL_s = \begin{bmatrix} 0 \\ W \end{bmatrix}, \;\; L_s T^{-1} = \begin{bmatrix} 0 & W^T \end{bmatrix}, \;\; W \in \mathbb{R}^{(n-1)\times n}.$$

Now, consider the following Lyapunov function

$$V = \tilde{e}_x^T \tilde{e}_x + z^T z.$$

Taking the derivative of V along trajectories (16) yields

$$\begin{aligned} \dot{V} &= -2\tilde{e}_x^T \Lambda \tilde{e}_x + 2\beta \tilde{e}_x^T W \Gamma(t) \tilde{e}_z - 2z^T H z - 2\beta z^T \Gamma(t) W^T \tilde{e}_x \\ &= -2\tilde{e}_x^T \Lambda \tilde{e}_x - 2z^T H z < 0 \end{aligned}$$

Hence, it can be concluded that the equilibrium points of (16) given by $\tilde{e}_x^e = 0$ and $z^e = 0$ are asymptotically stable. Therefore, from (15) we have $x \to \frac{\mathbf{1}^T x(0)}{n}\mathbf{1}$. ■

B. Analysis of Cooperative Systems with Newly Designed Virtual Network against Cyber-Attacks

The following theorem shows that using the newly designed virtual network, the state x converges to the neighborhood of consensus value $(\mathbf{1}_n^T x(0)/n)\mathbf{1}_n$ given that the adversary only has access to the network Σ_s.

Theorem 1: Consider the interconnected system (12). For a sufficiently large value of $\beta > 0$, the state x asymptotically converges to a small neighborhood of $(\mathbf{1}_n^T x(0)/n)\mathbf{1}_n$.

Proof: For the sake of simplicity we consider attacks given by a uniformly bounded injections. The proof for attacks given by finite-gain injections can be done in a similar manner and by combining it with the steps in [9]. Similar to the proof of Lemma 3, applying (15) into (12) yields

$$\begin{aligned}\dot{\tilde{e}}_x &= -\Lambda\tilde{e}_x + \beta W\Gamma(t)z + Wd \\ \dot{z} &= -Hz - \beta\Gamma(t)W^T\tilde{e}_x\end{aligned} \tag{17}$$

Let us now take the following Lyapunov function

$$V = \beta\tilde{e}_x^T\tilde{e}_x + \beta z^T z + 2z^T d',$$

where $d' = \Gamma(t)^{-1}d$. It follows that both d' and $\dot{d}'$ are uniformly bounded as $d, \dot{d}, \alpha_i(t), \dot{\alpha}_i(t)$ are uniformly bounded. Taking the derivative of V along trajectories (17) yields

$$\begin{aligned}\dot{V} &= -2\beta\tilde{e}_x^T\Lambda\tilde{e}_x + 2\beta^2\tilde{e}_x^T WD(t)z + 2\beta\tilde{e}_x^T Wd - 2\beta z^T Hz \\ &\quad - 2\beta^2 z^T D(t)W^T\tilde{e}_x + 2z^T\dot{d}' - 2z^T Hd' \\ &\quad - 2\beta\tilde{e}_x^T WD(t)d' \\ &= -2\beta\tilde{e}_x^T\Lambda\tilde{e}_x - 2\beta z^T Hz + 2z^T\dot{d}' - 2z^T Hd'.\end{aligned}$$

Hence, for a large value of β we have $\dot{V} < -Q(x) < 0$ where $Q(x)$ is positive definite which demonstrates robust stability against attack d. ■

C. Identifying Stealthy Attacks on the Virtual Network

Consider the case where the adversary has access to the virtual network Σ_h and can manipulate the exchanged information $\overline{z}_{ij}^n, \overline{x}_{ij}^n$ in (14) by injecting bounded signals $\overline{d}_{ij}^x, \overline{d}_{ij}^z$ respectively. The (possibly) corrupted information $\overline{z}_{ij}^n, \overline{x}_{ij}^n$ received at node i is then given by

$$\check{x}_{ij}^n = \overline{x}_{ij}^n + \overline{d}_{ij}^x, \;\; \check{z}_{ij}^n = \overline{z}_{ij}^n + \overline{d}_{ij}^x.$$

In order to detect such attacks on links $(j,i) \in \mathcal{E}_s$ and $(j,i) \in \mathcal{E}_h$, consider the following detection test criterion for node i

$$\textbf{Detection test:} \quad \hat{x}_{ij}^n = \check{x}_j. \tag{18}$$

where (possibly corrupted) estimation $\hat{x}_{ij}^n$ can be computed from (14) and is given by

$$\hat{x}_{ij}^n = \frac{1}{\beta\alpha_i(t)}\left[\check{x}_{ij}^n - \frac{\check{z}_{ij}^n}{\beta\alpha_j(t)}\right]. \tag{19}$$

In order to launch a harmful and stealthy attack the adversary has to choose the injections $d_j, \overline{d}_{ij}^x, \overline{d}_{ij}^z$ which satisfy

$$(\overline{x}_{ij}^n + \overline{d}_{ij}^x) - \frac{(\overline{z}_{ij}^n + \overline{d}_{ij}^x)}{\beta\alpha_j(t)} = \beta\alpha_i(t)(x_j + d_j). \tag{20}$$

In other words, the adversary has to know both the structure of detection test (20) and time-varying functions $\alpha_i(t)$. However, the scalar gain β and functions $\alpha_i(t), \alpha_j(t)$ corresponding to the nodes $(j,i) \in \mathcal{E}_s$ are local information to nodes i, j (assuming the nodes are not malicious) and not being directly communicated as can be observed from (14). Furthermore, the functions $\alpha_i(t)$ can be arbitrarily constructed by the designer as long as $\alpha_i(t)$ is uniformly bounded away from zero and that $\dot{\alpha}_i(t)$ exists and is uniformly bounded. Hence, it will be difficult for the adversary to accurately learn these time-varying functions $\alpha_i(t), \alpha_j(t)$ in real-time solely from information on $\overline{z}_{ij}^n, \overline{x}_{ij}^n$. This suggests that it is more difficult for the adversary to launch a stealthy and harmful attack under the new virtual network compared to the one proposed in [9]. Once the compromised links are identified, the cooperative system can then remove that links or reconfigure the network to maintain the stability.

VI. Numerical Example

Consider a cooperative system Σ_s with four nodes with initial condition given by $x(0) = [2, 3, 5, 6]^T$. The communication network topology in Σ_s is shown in Fig. 2. When there is no attack, i.e., $d = 0$ and under dynamics (1), the states of the nodes converge to the consensus value $x \to 4.\mathbf{1}_4$.

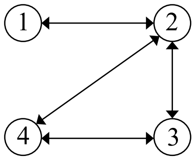
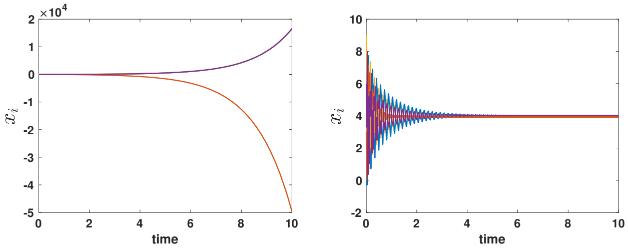


Fig. 2: Communication network topology

Now assume that there is an adversary who aims to destabilize the cooperative system by injecting d as shown in (2) whose dynamics (unknown to the defender) is set to be $\dot{d} = F_a d + B_a x$ with

$$F_a = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -0.6 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \; B_a = -\frac{3}{2}\begin{bmatrix} 0 & 0 & 0 & 0 \\ 3 & 2 & 3 & 4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}. \tag{21}$$

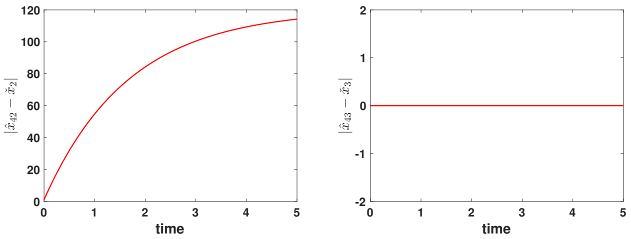
In other words, the adversary manipulates the information sent (via the communication network $\mathcal{G}_s$) from node 2. As can be observed from Fig. 3a, the attack destabilizes the cooperative system. Next, a virtual network baased resilient cooperative control given in (6) is implemented with scalar gain $\beta = 40$. As illustrated in Fig. 3b, the cooperative system interconnected with the virtual network forces the states x_i to converge to the neighborhood around the consensus value of 4 in spite of presence of unknown cyber-attacks.



(a) cooperative control only (b) resilient cooperative control

Fig. 3: State trajectories of Σ_s under attack

Next, using the detection test criterion (10) and results summarized in Lemma 1 each node can distributively and in real-time detect and identify the compromised communication link in Σ_s. For example, node 4 concluded that the



(a) link $(2,4)$ (b) link $(3,4)$

Fig. 4: Attack identification by node 4

communication link $(2,4)$ is compromised while communication link $(3,4)$ is not attacked as illustrated in Fig. 4.

Finally, we simulate resilient control where the virtual network has time-varying weights as shown in (12) and the attacks is also given by (21). Furthermore, we set the gain $\beta = 40$ and matrix $\Gamma(t) = \text{diag}\{[\alpha_1(t), \alpha_2(t), \alpha_3(t), \alpha_4(t)]^T\}$ is chosen as

$$\alpha_1(t) = 2\sin(t) + 3, \quad \alpha_2(t) = \cos(.5t) + 3,$$
$$\alpha_3(t) = 2\cos(t) + 5, \quad \alpha_4(t) = \sin(.5t) + 4.$$

The result is depicted in Fig. 5. As can be observed, the resilient control forces the states x_i to converge to the neighborhood around consensus value of 4 in spite of presence of unknown cyber-attacks.

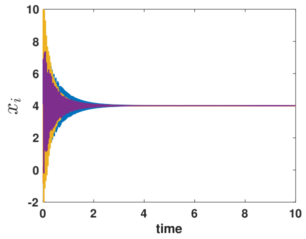


Fig. 5: State Trajectory of Σ_s under resilient control (12)

VII. Conclusion & Future work

This paper presents a unified framework for achieving simultaneously resilient cooperative control against unknown cyber-attacks and real-time attack identification. The framework relies on a new interpretation and insights into the implementation of the virtual network based resilient control originally proposed in [9]. A new virtual network is further proposed which makes it more difficult for the adversary to launch stealthy attacks even though it is also able to manipulate information being exchanged via the virtual network. For future work we aim at extending the results to directed network using the virtual network proposed in [24] and by considering a more general attack than the one in (2). In addition, we also aim to extend the proposed framework by considering noises and uncertainties in the measurements and communication network.

References

[1] Y. Li, Z. Zhang, T. Dragičević, and J. Rodriguez, “A unified distributed cooperative control of dc microgrids using consensus protocol,” *IEEE Transactions on Smart Grid*, vol. 12, no. 3, pp. 1880–1892, 2020.

[2] A. Gusrialdi, Z. Qu, and M. A. Simaan, “Distributed scheduling and cooperative control for charging of electric vehicles at highway service stations,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2713–2727, 2017.

[3] A. Gusrialdi and C. Yu, “Exploiting the use of information to improve coverage performance of robotic sensor networks,” *IET Control Theory & Applications*, vol. 8, no. 13, pp. 1270–1283, 2014.

[4] J. Hu, P. Bhowmick, F. Arvin, A. Lanzon, and B. Lennox, “Cooperative control of heterogeneous connected vehicle platoons: An adaptive leader-following approach,” *IEEE Robotics and Automation Letters*, vol. 5, no. 2, pp. 977–984, 2020.

[5] A. Gusrialdi and Z. Qu, “Smart grid security: Attacks and defenses,” in *Smart Grid Control: An Overview and Research Opportunities* (J. Stoustrup, A. Annaswamy, A. Chakrabortty, and Z. Q. (Eds.), eds.), pp. 199–223, Springer Verlag, 2018.

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

[7] H. Modares, B. Kiumarsi, F. L. Lewis, F. Ferrese, and A. Davoudi, “Resilient and robust synchronization of multiagent systems under attacks on sensors and actuators,” *IEEE Transactions on Cybernetics*, vol. 50, no. 3, pp. 1240–1250, Mar. 2020.

[8] Q. Li, L. Xia, and R. Song, “Novel resilient structure of output formation tracking of heterogeneous systems with unknown leader under contested environments,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2020.

[9] A. Gusrialdi, Z. Qu, and M. Simaan, “Robust design of cooperative systems against attacks,” in *Proceedings of American Control Conference*, pp. 1456–1462, 2014.

[10] G. D. L. Torre and T. Yucelen, “Adaptive architectures for resilient control of networked multiagent systems in the presence of misbehaving agents,” *International Journal of Control*, vol. 91, no. 3, pp. 495–507, 2018.

[11] B. Gharesifard and T. Başar, “Resilience in consensus dynamics via competitive interconnections,” *IFAC Proceedings Volumes*, vol. 45, no. 26, pp. 234–239, 2012.

[12] S. Zuo and D. Yue, “Resilient output formation containment of heterogeneous multigroup systems against unbounded attacks,” *IEEE Transactions on Cybernetics*, 2020.

[13] M. S. Sadabadi and A. Gusrialdi, “On resilient design of cooperative systems in presence of cyber-attacks,” in *Proceedings of European Control Conference*, pp. 946–951, Rotterdam, the Netherlands, 2021.

[14] X. Huang and J. Dong, “Reliable cooperative control and plug-and-play operation for networked heterogeneous systems under cyber–physical attacks,” *ISA transactions*, vol. 104, pp. 62–72, 2020.

[15] A. Gusrialdi, Z. Qu, and M. A. Simaan, “Competitive interaction design of cooperative systems against attacks,” *IEEE Trans. Automatic Control*, vol. 63, no. 9, pp. 3159–3166, Sept. 2018.

[16] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, A. Abusorrah, L. Che, and X. Liu, “Cross-layer distributed control strategy for cyber resilient microgrids,” *IEEE Transactions on Smart Grid*, 2021.

[17] A. Gusrialdi, Y. Xu, Z. Qu, and M. A. Simaan, “Resilient cooperative voltage control for distribution network with high penetration distributed energy resources,” in *Proceedings of European Control Conference*, pp. 1533–1539, 2020.

[18] Y. Liu, Z. Li, and Z. Shen, “Resilient consensus of discrete-time connected vehicle systems with interaction network against cyber-attacks,” *Journal of the Franklin Institute*, vol. 358, no. 5, pp. 2780–2800, 2021.

[19] Z. Qu, *Cooperative Control of Dynamical Systems*. London: Springer Verlag, 2009.

[20] Z. Qu and M. A. Simaan, “Modularized design for cooperative control and plug-and-play operation of networked heterogeneous systems,” *Autmatica*, vol. 50, no. 9, pp. 2405–2414, September 2014.

[21] X. Huang and J. Dong, “Adp-based robust resilient control of partially unknown nonlinear systems via cooperative interaction design,” *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2020.

[22] S. Zhang, “An overview of network slicing for 5g,” *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, 2019.

[23] A. Gusrialdi, Z. Qu, and M. Simaan, “Game theoretical designs of resilient cooperative systems,” in *Proceedings of European Control Conference*, pp. 1699–1705, Linz, Austria, July 15-17, 2015.

[24] M. Iqbal, Z. Qu, and A. Gusrialdi, “Distributed resilient consensus on general digraphs under cyber-attacks,” in *Proceedings of European Control Conference*, 2022, accepted.