Time-Delay Attacks in Network Systems

Gianluca Bianchin and Fabio Pasqualetti

Abstract Modern cyber-physical systems rely on dependable communication channels to accomplish cooperative tasks, such as forming and maintaining a coordinated platooning configuration in groups of interconnected vehicles. We define and study a class of adversary attacks that tamper with the temporal characteristics of the communication channels, thus leading to delays in the signals received by certain network nodes. We show how such attacks may affect the stability of the overall system, even when the number of compromised channels is limited. Our algorithms allow us to identify the links that are inherently less robust to this class of attacks, and to study the resilience of different network topologies when the attacker goal is to minimize number of compromised communication channels. Based on our numerical results, we reveal a relation between the robustness of a certain network to timing attacks and the degree distribution of its nodes.

1 Introduction

Networks of cyber and physical agents are broadly employed across diverse engineering applications to model critical infrastructures such as transportation systems and power grids [1, 2]. The increased coupling between physical components and cyber layers oftentimes comes at the expense of vulnerabilities and security weaknesses. Several real-world incidents and recent research papers have highlighted the vulnerabilities of these infrastructures on both their physical and cyber layers [3, 4, 5, 6]. The available literature on cyber-physical systems security has mainly focused on two categories of attacks: *deception* and *denial of service*. Deception attacks compromise the integrity of the data exchanged across the network, and are

Gianluca Bianchin
University of California, Riverside e-mail: gianluca@engr.ucr.edu

Fabio Pasqualetti
University of California, Riverside e-mail: fabiopas@engr.ucr.edu

cast by altering the behavior of sensors, actuators, and communication channels. On the other hand, denial of service attacks compromise the availability of resources by, for instance, jamming the communication channels.

Yet, an aspect that critically affects the operation of several classes of cyber-physical systems is the indirect effect of non-ideal communication channels, that can introduce timing aberrations in the signals exchanged among their nodes. Timing aberrations can be the indirect result of hardware faults or can be the effect of intentional attacks. For instance, an adversary may temporarily jam communication channels with the goal of delaying the transmitted signal streams, while maintaining unaltered the information enclosed in the packets. Although this action does not prevent information from being delivered correctly, it can disrupt the system operation and performance by impeding the correct synchronization among different system components. In this work, we focus on attacks that target the communication and delay the stream of signals exchanged between cooperative agents. We consider attacks that are sparse in the set of attacked channels, and employ a security metric that captures the stability of the underlying system.

The importance of timing and the effect of time delays in networks of dynamical systems is a well-studied concept (e.g. see [7, 8, 9, 10]). Classical methods to study stability of delayed linear systems can be divided into LMI conditions, which arise from a Lyapunov-Krasovskii quadratic function analysis [11, 12], and techniques based on matrix pencils [13, 14]. However, timing-based security is an inherently different issue from standard communication delay approaches, as an attacker can deliberately select the targeted channels and the specific pattern of time delay. The relation between timing and security in cyber-physical systems has been highlighted in some recent work. In particular, while [15] devises a robust output-feedback controller which is resilient to an attack that changes the order at which packets are delivered, the authors in [16] follow a probabilistic approach and model packet drops through Bernoulli processes representing intentional attacker intrusions. The effect of malicious packet drops has also motivated the study and development of resilient controllers in the context of networked control systems [17].

Differently from this line of previous work, securing cyber-physical systems from timing attacks requires the study and design of a specific, well-designed, set of delayed channels. This work distinguishes from this line of research by (i) considering opportunely-defined attacks that do not follow any specific probabilistic model, and (ii) by relating resilience to network topology and centrality measures such as the degree distribution. We characterize and study the class of delay attacks from a control perspective, and provide a numerical algorithm to identify the set of communication channels that are less robust to timing attacks. Our results suggest that improved robustness can be achieved by network topologies in which nodes exhibit significantly large degrees.

2 Problem Setup

This section describes the models we adopt for the analysis of time delays in dynamical systems. The description first introduces the ideal modeling framework in the absence of external attacks, and then illustrates the attack scenario.

2.1 Network Model

Consider a network modeled by a directed graph $\mathscr{G} = (\mathscr{V}, \mathscr{E})$, where $\mathscr{V} = \{1, \ldots, n\}$ and $\mathscr{E} \subseteq \mathscr{V} \times \mathscr{V}$ are the vertices and edges sets, respectively. Let $a_{ij} \in \mathbb{R}$ denote the weight associated with the edge $(i, j) \in \mathscr{E}$, where $a_{ij} = 0$ whenever $(i, j) \notin \mathscr{E}$. We associate a real value x_i (node state) with each node $i \in \{1, \ldots, n\}$ of the graph , and model the state dynamics as

$$\dot{x}_i(t) = \sum_{j \in \mathscr{N}_i} a_{ij} x_j(t),$$

where $\mathscr{N}_i \subseteq \mathscr{V}, \mathscr{N}_i = \{j : \exists (i, j) \in \mathscr{E}\}$, denotes the set of in-neighbors of node i.

Example 1. ***(Vehicles platooning)*** Consider a group of N vehicles moving along a single lane as in Fig. 1. In a platooning scenario [1], vehicles follow one another and share their state information (e.g. position, velocity, acceleration) with other vehicles by communicating through a V2V communication protocol. The behavior of the i-th vehicle in the platoon, $i \in \{1, \ldots, N\}$, can be described by the two differential equations representing an inertial agent

$$\dot{r}_i(t) = v_i(t), \qquad \dot{v}_i(t) = \frac{1}{m_i} u_i(t),$$

where $r_i : \mathbb{R}_{\geq 0} \to \mathbb{R}$, $v_i : \mathbb{R}_{\geq 0} \to \mathbb{R}$, and $m_i \in \mathbb{R}_{>0}$ denote the i-th vehicle position, velocity, and mass respectively.

The goal of maintaining a desired inter-vehicle spacing can be formulated as the problem of controlling the position and velocities of each vehicle towards the following desired steady state values

$$r_i(t) \to \frac{1}{N} \sum_{j=1}^{N} \left(r_j(t) + d_{ij} \right), \qquad v_i(t) \to \bar{v},$$

where $\bar{v}$ denotes the desired steady-state platoon velocity, and d_{ij} is the desired spacing distance between agent i and j, $i, j \in \{1, \ldots, N\}$. The desired steady-state spacing and velocity can be achieved through a double-integrator consensus protocol [18], of the form

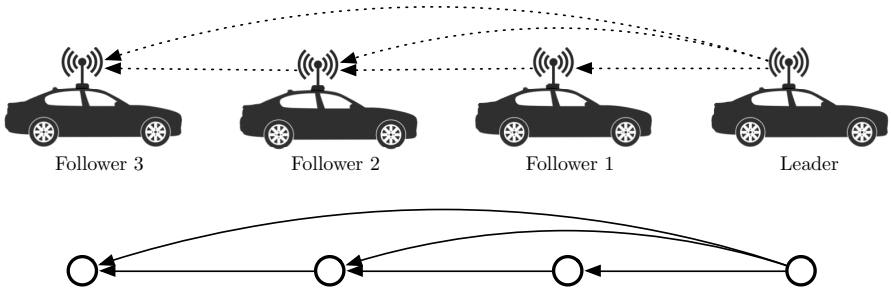


Fig. 1 Vehicles platooning and associated topology. A group of vehicles is moving along a single lane while maintaining a desired inter-vehicle spacing and a certain steady-state speed. To accomplish this task, each vehicle exchanges information with the platoon leader and the vehicle immediately ahead.

$$u_i(t) = \sum_{j=1}^{N} \alpha_{ij}(r_i(t) - r_j(t) - d_{ij}) + \gamma_{ij}(v_i(t) - v_j(t)),$$

where $\sum_{j=1}^{N} \alpha_{ij} = \sum_{j=1}^{N} \gamma_{ij} = 1$ for all $i \in \{1,\dots,N\}$. Therefore, the goal of attaining a platooning configuration can be achieved by modeling each vehicle as a two-node subsystem with states r_i and v_i respectively, and dynamics

$$\begin{aligned} \dot{r}_i(t) &= v_i(t), \\ \dot{v}_i(t) &= \frac{1}{m_i}\left[\alpha_{ij}(r_i(t) - r_j(t) - d_{ij}) + \gamma_{ij}(v_i(t) - v_j(t))\right., \end{aligned}$$

Thus, the above scenario belongs to the more general class of models considered in this work. □

In order to implement the described cooperation protocol, each node is required to transmit the state over a (potentially lossy) communication channel to all its neighbors. For ideal communication channels, the signal transmitted by agent j and received by agent i coincide, therefore, network dynamics can be modeled by a continuous LTI system as

$$\dot{x}(t) = Ax(t), \tag{1}$$

where $x : \mathbb{R}_{\geq 0} \to \mathbb{R}^n$ contains the node states and $A \in \mathbb{R}^{n\times n}$ is the adjacency matrix of the network. We will make the assumption that the adjacency matrix in (1) is (marginally) Hurwitz, that is, for all $z \in \{z \in \mathbb{C} : \ \det(zI - A) = 0\}$, $\Re(z) \leq 0$.

2.2 Attack Model

Common transmission protocols often reframe signals into streams of data packets before transmission. We assume that this underlying process is intangible, and we will equivalently refer to signal streams or to streams of packets in the remainder. We consider attacks that target communication channels and delay the stream of information in the path between transmitter and receiver (Fig. 2). In order to implement the cooperative protocol (1) we assume that every node $j \in \{1,\dots,N\}$ shares the current value of the state $x_j(t)$ with the set of available neighbors; and denote by $r(i,j,t) : \mathscr{V} \times \mathscr{V} \times \mathbb{R}_{\geq 0} \to \mathbb{R}$ the corresponding continuous-time signal received at node i, $i \in \{1,\dots,n\}$. In general, the relation

$$r(i,j,t) = x_j(t),$$

may not be satisfied due to the lossy nature of the communication channels. Notably, these have the effect of altering the content of transmitted data packets and/or introducing time delays in the signal streams. We consider scenarios where attackers can maliciously exploit these features in order to compromise the correct functionality of the system. We make the following assumptions:

1. The attacker does not alter the information contained in transmitted signals;
2. There exists an upper bound $\tau^{\max}$ to the largest packet delay;
3. Data is used as soon as it become available at the receiver.

While scenarios where attackers alter the content of the transmitted signals have been extensively studied in previous works (see e.g. [19]), we argue that attacks delaying communication edges can lead to similar disruptive behaviors.

Remark 1. ***(Compensation mechanisms)*** In the presence of communication delays, two compensation mechanisms are often adopted. Either data that is classified as obsolete (for instance by time-stamping the transmitted packets) is discarded at the receiver, or data is used as soon as it is available at the receiver [20]. We consider scenarios where the latter protocol is used. □

We model received signals in the presence of attacks as

$$r(i,j,t) = x_j(t - \tau_{ij}),$$

where $\tau_{ij} \in \mathbb{R}_{\geq 0}$, $0 \leq \tau_{ij} \leq \tau^{\max}$, for all $i,j \in \{1,\dots,n\}$ represent (deterministic) time delays introduced by the attacker. Then, the dynamics of agent i in the presence of attacks can be written as

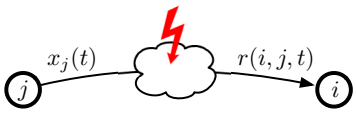


Fig. 2 Attacks to timing can occur in the communication channel between every pair of nodes.

$$\dot{x}_i(t) = \sum_{j \in \mathcal{N}_i} a_{ij} r(i,j,t) = \sum_{j \in \mathcal{N}_i} a_{ij}\, x_j(t - \tau_{ij}).$$

We then denote by $\mathcal{A} \subseteq \mathcal{E}$ the set edges under attack, that is,

$$\mathcal{A} = \{(i,j) : \tau_{ij} > 0\}.$$

Then, the time evolution of the network state can be written as

$$\dot{x}(t) = \bar{A}x(t) + \sum_{(i,j) \in \mathcal{A}} \tilde{A}_{ij}\, x(t - \tau_{ij}), \tag{2}$$

where $\tilde{A}_{ij} \in \mathbb{R}^{n \times n}$,

$$\tilde{A}_{ij}(p,q) = \begin{cases} a_{ij} & \text{if } p = i, q = j, \text{ and } \tau_{ij} > 0, \\ 0 & \text{otherwise,} \end{cases}$$

for all $p,q \in \{1,\dots,n\}$, and $\bar{A} = A - \sum_{i \in \mathcal{A}} \tilde{A}_{ij}$.

Example 2. ***(Transmitter delay and receiver delay attacks)*** Scenarios where an attacker compromises the behavior of a certain network node and deliberately transmit (receive) delayed messages can be modeled as in (2). For instance, consider the circumstance where a compromised node intentionally (i) transmits obsolete information to all its neighbors, or (ii) updates its state with obsolete neighboring data. These two classes of vulnerabilities are reffed to as *transmitter delay attacks* and *receiver delay attacks* respectively and are discussed next.

Transmitter delay attacks, illustrated in Fig. 3(a), model scenarios where a certain time shift is intentionally introduced in all the packets transmitted from an agent to its neighbors. Let $i \in \{1,\dots,n\}$ denote the (single) agent under attack, then

$$r(j,i,t) = x_i(t - \tau)$$

for all j such that $i \in \mathcal{N}_j$. Moreover, the network model under transmission delay attack can be written as

$$\dot{x}(t) = \bar{A}x(t) + \tilde{A}x(t - \tau),$$

where $\tilde{A}$ has only n nonzero entries corresponding to its i-th column, that is,

$$\tilde{A}(p,q) = \begin{cases} a_{pq} & \text{if } q = i \\ 0 & \text{otherwise,} \end{cases}$$

for all $p,q \in \{1,\dots,n\}$, and $\bar{A} = A - \tilde{A}$.

Receiver delay attacks, illustrated in Fig. 3(b), model scenarios where the attacker prevents a timely state-update of a certain node. This, for instance, can be the result of overloading the local processing units of the node. Let $i \in \{1,\dots,n\}$ denote the (single) node under attack, then

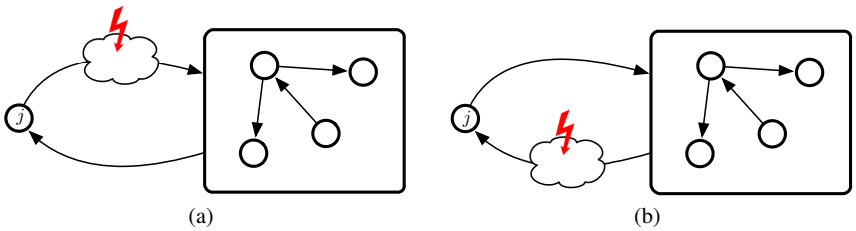


Fig. 3 Illustration of (a) transmitter delay attack, and (b) receiver delay attack. Red patterns represent attacker intrusions.

$$r(i,j,t) = x_j(t-\tau)$$

for all $j \in \mathcal{N}_i$. Moreover, the network model under resources overload attack can be written as

$$\dot{x}(t) = \bar{A}x(t) + \tilde{A}x(t-\tau),$$

where $\tilde{A} \in \mathbb{R}^{n\times n}$ has only n nonzero entries corresponding to its i-th row,

$$\tilde{A}(p,q) = \begin{cases} a_{pq} & \text{if } p = i, \\ 0 & \text{otherwise,} \end{cases}$$

and $\bar{A} = A - \tilde{A}$.

2.3 Problem Formulation

We focus on attacks that aim to compromise the stability properties of (2). To this aim, we next recall a standard definition of convergence.

Definition 1. ***(Convergence criteria)*** The time evolution of system state in (2) is convergent to a limit vector $\bar{x} \in \mathbb{R}^n$ if, for every $\varepsilon > 0$, there exist $\bar{t} \in \mathbb{R}_{\geq 0}$ such that

$$\|x(t) - \bar{x}\| \leq \varepsilon, \quad \text{for all } t \geq \bar{t}.$$

We recall that the convergence of (2), in general, depends on the nominal adjacency matrix A, the attack set $\mathcal{A}$, and on the time delays τ_{ij}. We then restrict our analysis to the uniform delays case, that is, on the model:

$$\dot{x}(t) = \bar{A}x(t) + \tilde{A}x(t-\tau), \tag{3}$$

and focus on the following problem.

Problem 1. Find the minimal cardinality attack set $\mathscr{A}^*$ that makes dynamics (3) non-convergent.

In the remainder of this work we will focus of Problem 1 and propose a method for its solution.

3 Minimum Cardinality Attack Sets

In this section we propose a solution to Problem 1. Recall that the trajectories of (3) are convergent if and only if all the characteristic roots, which are the zeros of[1]

$$\det(sI_n - \bar{A} - \tilde{A}e^{-s\tau}) = 0, \qquad s \in \mathbb{C},$$

where $I_n \in \mathbb{R}^{n\times n}$ denotes the identity matrix, are in the open left half-plane (see e.g. [7]). We then report a well-known result for time-delay dynamical systems that will be needed in the subsequent analysis.

Theorem 1. ([21, Theorem 4.1]) *Consider the delayed dynamical system* (3)*, and define the dual characteristic equation*

$$\det(sI_n - \bar{A} - \tilde{A}e^{-j\theta}) = 0, \tag{4}$$

where $s \in \mathbb{C}$, and $\theta \in [0, 2\pi]$. The time evolution of (3) *is convergent if and only if any solution s to* (4) *satisfies*

$$s \ \in \ \{s = \sigma + j\omega : \sigma \in \mathbb{R}, \omega \in \mathbb{R}, \sigma < 0\} \ \cup \ \{0\},$$

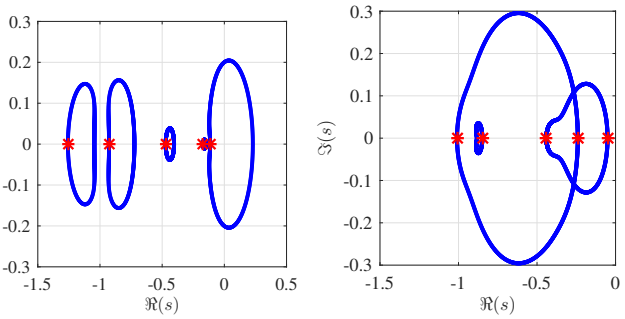
for all $\theta \in [0, 2\pi]$.

The following comments are in order. First, Theorem 1 allows us to separate the double dependency of the primal characteristic equation on the variable s, by introducing the independent variable θ. Second, since θ only affects the coefficients of the polynomial (4), the corresponding roots are continuous functions of θ. Therefore, the roots of (4) form closed curves in the complex plane as θ is varied over the interval $[0, 2\pi]$. It follows that, the convergence of linear dynamical systems in the presence of delayed communication edges can be assessed through the study of the real part of the eigenvalues of the pencil $\bar{A} + \tilde{A}e^{-j\theta}$ as the scalar parameter θ is varied over $[0, 2\pi]$. Third, by comparing the primal and dual characteristic equations, it immediately follows that, if $s = j\omega$ is a root of (4) for a fixed value of θ, then the choice $\tau = \theta/\omega$ will satisfy the primal equation. In the remainder, we will use the compact notation (s, θ) to denote a root s of (4) associated with a fixed θ.

The following result provides a characterization of the roots of (4).

Lemma 1. ***(Hermitian property)*** *Let the pair (s, θ) denote a solution to* (4)*, where $s = \sigma + j\omega$, $\sigma \in \mathbb{R}$, $\omega \in \mathbb{R}$. Then, $(\bar{s}, -\theta)$ is also a solution to* (4)*, with $\bar{s} = \sigma - j\omega$.*

[1] This will be referred to as primal characteristic equation.



(a) (b)

Fig. 4 Numerical study of the roots of (4) for two realizations of a full adjacency matrix A with uniform entries in the interval $[0,1]$. As highlighted in the comparison, the roots (a) may cross the imaginary axis or may not cross the imaginary axis (b). Asterisk represents the roots for $\theta = 0$.

Proof. Recall that $\det\left(sI_n - \bar{A} - \tilde{A}e^{-j\theta}\right) = 0$ if and only if

$$(\bar{A} + \tilde{A}e^{-j\theta})v = (\sigma + j\omega)v,$$

for some $v \in \mathbb{C}^n$. By taking the complex conjugate of the above equation, we obtain

$$(\bar{A} + \tilde{A}e^{j\theta})\bar{v} = (\sigma - j\omega)\bar{v},$$

where $\bar{v}$ denotes the complex conjugate of v, that proves the claimed statement. □

The conjugate property illustrated in the above lemma, combined with the periodic relation $e^{-j\theta} = e^{j(2\pi-\theta)}$, implies that the curves describing the roots of (4) for $\theta \in [0,\pi]$ are the complex conjugate of the curves describing the corresponding roots for $\theta \in (\pi, 2\pi)$. An illustration of the behavior of the roots of the dual characteristic equation (4) as a function of θ is presented in Fig. 4.

We now employ the above characterization of time-delay linear systems for the solution of Problem 1. Let $\Psi = [\psi_{ij}] \in \mathbb{R}^n$, with $\psi_{ij} \in \{0,1\}$, and decompose the network adjacency matrix as

$$A = \underbrace{(\mathbb{1}_{n\times n} - \Psi) \circ A}_{\bar{A}_\Psi} + \underbrace{\Psi \circ A}_{\tilde{A}_\Psi},$$

where $\mathbb{1}_{n\times n} \in \mathbb{R}^{n\times n}$ denotes a n by n matrix of ones, and $\circ$ denotes the Hadamard operator. The notation $\bar{A}_\Psi$ and $\tilde{A}_\Psi$ is employed to emphasize the dependency on Ψ. We then formalize Problem 1 as the following minimization problem: given the network adjacency matrix A and an upper bound to the largest communication delay $\tau^{\max}$, determine the delayed adjacency matrix $\Psi \circ A$ satisfying

$$
\begin{aligned}
\Psi^* = \quad & \underset{\Psi,\theta,v,\omega}{\arg\min} \quad \|\Psi\|_{\ell_1} \\
& \text{subject to} \quad A = \underbrace{(\mathbb{1}_{n\times n} - \Psi)\circ A}_{\bar{A}_\Psi} + \underbrace{\Psi \circ A}_{\tilde{A}_\Psi}, && \text{(5a)} \\
& (\bar{A}_\Psi + \tilde{A}_\Psi e^{-j\theta})v = j\omega v, && \text{(5b)} \\
& \psi_{ij} \in \{0,1\}, && \text{(5c)} \\
& \theta \leq \omega\tau^{\max}, && \text{(5d)}
\end{aligned}
$$

where $i,j \in \{1,\dots,n\}$. It should be observed that (5) is of the form of a mixed-integer optimization problem, where the Boolean variables ψ_{ij}, the real variables θ, ω, and the complex variable v are the optimization parameters. Two major complexities arise in solving (5). First, the optimization variables ψ_{ij} are integers. Second, the variables $\tilde{A}_\Psi$, θ, v, and ω are related by the nonlinear constraint (5b). It is also worth noting that the feasibility of the constraint set depends on the largest allowed time delay $\tau^{\max}$, and it is independent on the nominal adjacency matrix A. To see this, we observe that for any A with eigenvalues $\lambda_1,\dots,\lambda_n$, by letting $\theta = \pi/2$ and $\Psi = \mathbb{1}_{n\times n}$, then $\bar{A} + \tilde{A}e^{-j\theta} = Ae^{-j\theta}$ has eigenvalues $j\lambda_1,\dots,j\lambda_n$. Thus, the feasible set is always nonempty.

3.1 Optimal Delay Attacks

We now manipulate minimization problem (5) to facilitate its solution. We perform the following two simplifying steps.

Rewriting the Hadamard Product

Let $\text{vec}(M) = [m_{11},\dots,m_{m1},m_{12},\dots,m_{mn}]$ denote the vectorization of matrix $M = [m_{ij}] \in \mathbb{R}^{m\times n}$, and let $\text{diag}(v) \in \mathbb{R}^{n\times n}$ denote a diagonal matrix with diagonal entries given by the elements of vector $v \in \mathbb{R}^n$. Then, the Hadamard products in (5a) are linear functions of the entries of Ψ, as formalized in the following result.

Lemma 2. ***(Linearity of Hadamard product)*** *Let $\bar{A}_\Psi = (\mathbb{1}_{n\times n} - \Psi)\circ A$ and $\tilde{A}_\Psi = \Psi \circ A$. Then*

$$
\begin{aligned}
\text{vec}\left(\bar{A}_\Psi\right) &= \text{diag}\left(\text{vec}\left(A\right)\right)\left(\mathbb{1}_{n^2} - \text{vec}\left(\Psi\right)\right), \\
\text{vec}\left(\tilde{A}_\Psi\right) &= \text{diag}\left(\text{vec}\left(A\right)\right)\text{vec}\left(\Psi\right),
\end{aligned}
$$

where $\mathbb{1}_{n^2} \in \mathbb{R}^{n^2}$ denotes the vector of all ones.

Proof. The claimed statement can be verified by inspection. □

Rewriting The Eigenvalue Constraint

We now drop the dependency of constraint (5b) on the complex variable v.

Lemma 3. ***(Rank Constraint)*** *Let $\bar{A}_\Psi + \tilde{A}_\Psi = A$. There exists a solution $v = v_\Re + jv_\Im$, $\omega \in \mathbb{R}_{\geq 0}$ and $\theta \in [0, 2\pi]$ to* (5b) *if and only if*

$$\text{Rank}\,(\Lambda_\Psi) < 2n,$$

where

$$\Lambda_\Psi = \begin{bmatrix} -\tilde{A}_\Psi \sin\theta - \omega I_n & A + \tilde{A}_\Psi(\cos\theta - 1) \\ -A - \tilde{A}_\Psi(\cos\theta - 1) & -\tilde{A}_\Psi \sin\theta - \omega I_n \end{bmatrix}. \tag{6}$$

Proof. By substituting $\bar{A}_\Psi = A - \tilde{A}_\Psi$, $e^{-j\theta} = \cos\theta - j\sin\theta$, and $v = v_\Re + jv_\Im$ into (5b) and by expanding the products we obtain

$$\left(A + \tilde{A}_\Psi(\cos\theta - 1) - j\tilde{A}_\Psi \sin\theta\right)(v_\Re + jv_\Im) = j\omega(v_\Re + jv_\Im),$$

or equivalently, by separating real and imaginary parts,

$$\begin{aligned} (A + \tilde{A}_\Psi(\cos\theta - 1))v_\Re + \tilde{A}_\Psi \sin\theta v_\Im &= -\omega v_\Im, \\ \left(A + \tilde{A}_\Psi(\cos\theta - 1)\right)v_\Im - \tilde{A}_\Psi \sin\theta v_\Re &= \omega v_\Re. \end{aligned}$$

The two equations above can be collected together and rewritten in matrix form as

$$\underbrace{\begin{bmatrix} -\tilde{A}_\Psi \sin\theta & A + \tilde{A}_\Psi(\cos\theta - 1) \\ -A + \tilde{A}_\Psi(\cos\theta - 1) & -\tilde{A}_\Psi \sin\theta \end{bmatrix}}_{\Lambda_\Psi} \begin{bmatrix} v_\Re \\ v_\Im \end{bmatrix} = \omega \begin{bmatrix} v_\Re \\ v_\Im \end{bmatrix},$$

from which the claimed statement follows. □

These simplifications lead to the following result.

Lemma 4. ***(Equivalent minimization problem)*** *Let Λ_Ψ be defined as in* (6) *and let $\bar{A}_\Psi + \tilde{A}_\Psi = A$, where $\tilde{A}_\Psi$ satisfies*

$$\text{vec}\left(\tilde{A}_\Psi\right) = \text{diag}\left(\text{vec}\,(A)\right)\left(\mathbb{1}_{n^2} - \text{vec}\,(\Psi)\right).$$

The following minimization problem is equivalent to (5)*:*

$$\begin{aligned} \Psi^* \;=\; \underset{\Psi,\theta,\omega}{\textit{arg min}} \quad & \|\Psi\|_{\ell_1} \\ \textit{subject to} \quad & \text{Rank}(\Lambda_\Psi) < 2n, \\ & \psi_{ij} \in \{0,1\}, \\ & \theta \leq \omega\tau^{\max}. \end{aligned} \tag{7}$$

It should be noticed that the two simplifying steps performed allow us to (i) write the entries of Λ_Ψ as linear functions of the optimizing variables ψ_{ij}, and (ii) discard the dependency of the optimization problem from the complex variable v. In the next section, we further simplify the optimization problem (7) and propose a numerical method to find an approximate solution.

3.2 Numerical Methods for Finding Optimal Attacks

We observe that the optimization problem (7) is not convex because of (i) the presence of integer optimization variables Ψ, (ii) the nonlinear relation between Λ_Ψ and θ in (6) , and (iii) the rank constraint, that is nonlinear in the entries of Λ_Ψ. We now develop a numerical method to find a delayed set of edges that can be used to gain information about the solution to (7). First, we relax the original integer variables by letting ψ_{ij} vary on the interval $[0,1]$. Second, we emphasize that rank constraints produce challenging nonconvex feasible sets, for which all known finite time algorithms have exponential running times [22]. We will therefore focus on proposing a heuristic that solves a relaxed version of problem (7). A good heuristic is a tractable method that in practice will solve the considered optimization problem, although there is no guarantee on its optimality.

Recent works (see e.g. [22]) propose to relax rank constraints to constraints on the nuclear norm of the considered matrix. Formally, for a (non necessarily square) matrix $M \in \mathbb{R}^{m\times n}$, the nuclear norm is defined as

$$\|M\|_* = \sum_{i=1}^{\min\{m,n\}} \sigma_i(M),$$

where σ_i denotes the i-th singular value of M. The nuclear norm is a convex function that can be optimized efficiently, and is a good convex approximation of the rank function [23]. Loosely speaking, $\|M\|_*$ represents the ℓ_1-norm of the vector of the singular values of M, therefore, constraining the nuclear norm will promote sparsity in such vector [22]. Thus, we consider the relaxed version of the rank constraint (7), that is,

$$\|\Lambda_\Psi\|_* < 2n. \tag{8}$$

Nuclear norm regularization constraints can be reformulated in the form of SDP constraints [23], as formalized in the following result.

Lemma 5. ***(SDP constraint)*** *There exists Λ_Ψ that satisfies* (8) *if and only if there exists symmetric matrices $M \in \mathbb{S}^{n\times n}$ and $N \in \mathbb{S}^{n\times n}$ that satisfy*

$$\begin{bmatrix} M & \Lambda_\Psi \\ \Lambda_\Psi^\intercal & N \end{bmatrix} \succeq 0, \quad \textit{and} \quad \text{Trace}\,(M+N) = n - \frac{1}{2}.$$

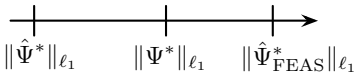


Fig. 5 Relation $\|\Psi^*\|_{\ell_1} \leq \|\hat{\Psi}^*\|_{\ell_1} \leq \|\hat{\Psi}^*_{\mathrm{FEAS}}\|_{\ell_1}$ and optimality gap for the considered problem.

Proof. The proof follows immediately from [23, Lemma 1]. □

These simplifications lead to the following relaxed version of (7):

$$\begin{aligned} \hat{\Psi}^* = \underset{\Psi,\theta,\omega,M,N}{\arg\min} \quad & \|\Psi\|_{\ell_1} \\ \text{subject to} \quad & \begin{bmatrix} M & \Lambda_\Psi \\ \Lambda_\Psi^\top & N \end{bmatrix} \succeq 0, \\ & \mathrm{Trace}\,(M+N) = n - \frac{1}{2}, \\ & \psi_{ij} \in [0,1], \\ & \theta \leq \omega \tau^{\max}, \end{aligned} \tag{9}$$

where $M \in \mathbb{S}^{n\times n}$, $N \in \mathbb{S}^{n\times n}$, and Λ_Ψ is defined in (6). We observe that the feasible set in (9) is a convex set in the optimization variables Ψ, ω, M, and N, as all its constraints are linear functions of these variables. In the next section, we numerically solve (9) for fixed θ and present how the resulting solutions provide an insight on the relation between the smallest cardinality attack sets and network topology.

4 Optimal Attack Sets and Relation with Topology

This section discusses numerical simulations in support to the approximate solution method proposed in Section 3, and includes numerical investigations that provide useful insights regarding the resilience of different network topologies under attack.

We first focus on evaluating numerically the optimality gap between the optimization problem (5) and its relaxation (9). Recall that Ψ^* denotes the true combinatorial optimal solution to (5), and $\hat{\Psi}^*$ denotes the solution of the convex relaxation (9). We observe that, in general, the inequality $\|\hat{\Psi}^*\|_{\ell_1} \leq \|\Psi^*\|_{\ell_1}$ holds as the feasible set of the combinatorial problem is a subset of the feasible set of (9). We employ a rounding algorithm that uses the solution of the convex relaxation with objective value $\hat{\Psi}^*$ to produce a feasible integer solution with (possibly suboptimal) value $\hat{\Psi}^*_{\mathrm{FEAS}}$. The relation between Ψ^*, $\hat{\Psi}^*$, and $\hat{\Psi}^*_{\mathrm{FEAS}}$ is depicted in Fig. 5.

To evaluate the optimality gap, that is the gap between $\|\Psi^*\|_{\ell_1}$ and $\|\hat{\Psi}^*_{\mathrm{FEAS}}\|_{\ell_1}$, we consider graphs constructed by interconnecting nodes randomly [24], where each edge is included in the graph with probability $p = 1/2$, independent from every other edge. Edge weights are chosen randomly in the interval $[0,1]$, and θ is chosen

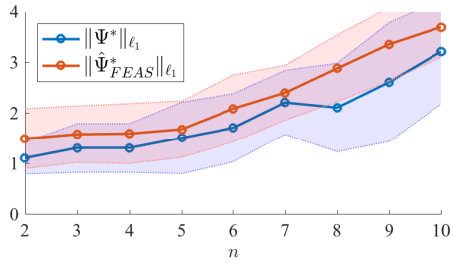


Fig. 6 Monte Carlo simulation illustrating the optimality gap for random graphs where edges between each pairs of nodes have probability $p = 1/2$. Solid lines represent the mean value over the sample and colored bands illustrate standard deviation. Sample size is chosen equal to 10.

equal to $\pi/2$. A Monte Carlo simulation obtained by sampling from the above set of graphs is illustrated in Fig. 6, where a feasible optimal solution is compared with the combinatorial solution Ψ^* for increasing network sizes. The comparison shows that feasible solutions originated from the relaxed problem (9) represent, in this scenario, accurate approximations of the combinatorial optimal solution.

Next, we employ the proposed optimization technique to compare the robustness of different network topologies against timing attacks. We consider (i) the class of random graphs with edge probability $p = 1/2$, (ii) the line topology (Fig. 7(a)), and (iii) the platooning formation (Fig.7(b)). Fig. 8 shows a comparison between the norms $\|\hat{\Psi}^*\|_{\ell_1}$ and $\|\hat{\Psi}^*_{\text{FEAS}}\|_{\ell_1}$ for increasing network sizes. It is worth noting that, while solving the combinatorial problem (5) is prohibitive for significantly large n, $\|\hat{\Psi}^*\|_{\ell_1}$ and $\|\hat{\Psi}^*_{\text{FEAS}}\|_{\ell_1}$ provide a lower bound and an upper bound to this quantity, respectively (Fig. 5). The comparison shows that the line and platoon topologies demonstrate improved resilience for increasing n as opposed to the class of random graphs. We interpret this result by observing that the average degree[2] of the nodes in the random graphs scales with the network size; as opposed to the constant degree of the nodes in the two topologies in Fig. 7. This consideration suggests a relation between attack resilience and the degree distribution of the nodes in the network. To

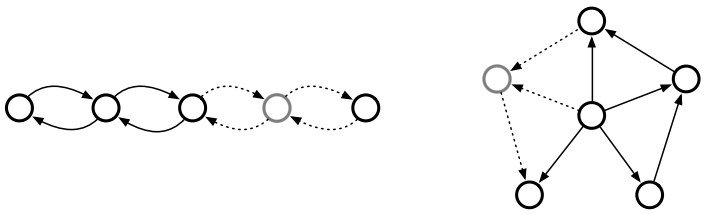


Fig. 7 Considered topologies for variable n, (a) line, (b) platoon.

[2] $|\mathcal{N}_i|$ represents the degree of node i, $i \in \{1,\dots,n\}$

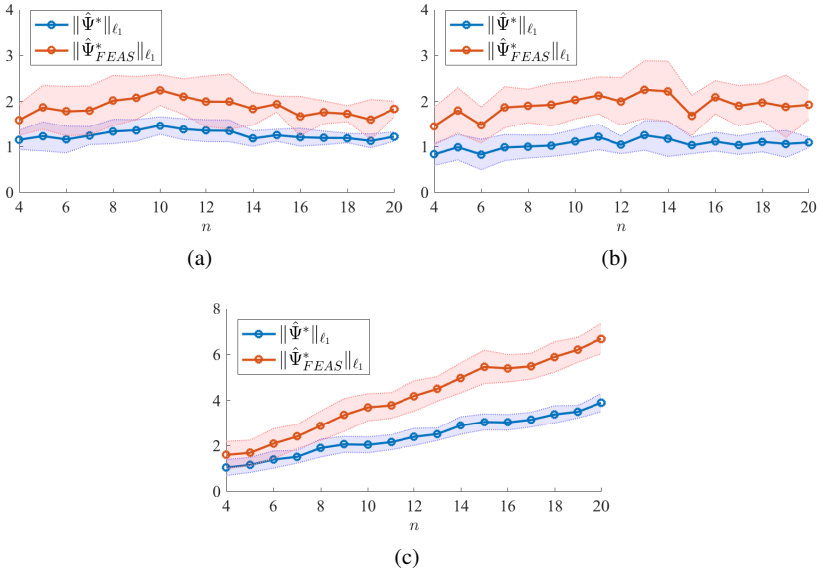


Fig. 8 Norm of optimal attacks for different network topologies. (a) Line topology (b) platooning formation, (c) random graphs with $p = 1/2$. Solid lines represent the mean value over the sample and colored bands illustrate standard deviation. Sample size is chosen equal to 10.

validate this interpretation we consider graphs were all nodes have fixed identical degree, and compare optimal attacks as a function of this parameter. The comparison shown in Fig. 9 numerically validates this claim and suggests that improved robustness can be achieved by designing networks with large node degrees.

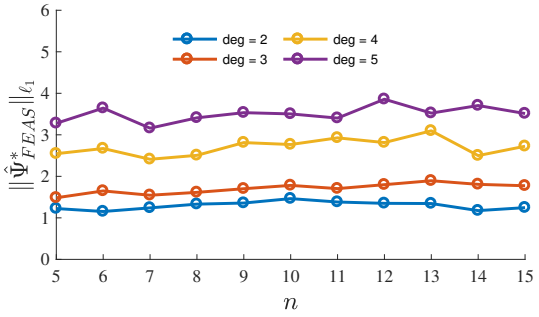


Fig. 9 Mean value of Monte Carlo simulations for optimal attacks to graphs with fixed degree for all nodes. Edge weights are uniform in the interval $[0, 1]$, and sample size is chosen equal to 10.

5 Conclusions

This work defines and studies a class of attacks that tamper with the temporal characteristic of the communication channels, leading to time delays in the signals exchanged between adjacent nodes. Differently from considering conventional channel communication delays, the problem of securing network systems from intentional and specific timing aberrations sets out new security challenges and design goals. In addition to providing a framework to characterize and study timing attacks from a control perspective, this work proposes numerical ways and algorithms to identify links that are inherently less robust to tampering. Our methods suggest that improved robustness can be achieved by designing network topologies in which all nodes have large degree. The numerical nature of the proposed study motivates more rigorous formalization in future works.

References

1. M. di Bernardo, A. Salvi, and S. Santini, "Distributed consensus strategy for platooning of vehicles in the presence of time-varying heterogeneous communication delays," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 1, pp. 102–112, 2015.
2. R. Poovendran, K. Sampigethaya, S. K. S. Gupta, I. Lee, K. V. Prasad, D. Corman, and J. L. Paunicka, "Special issue on cyber-physical systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 6–12, 2012.
3. J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in *International Conference on Critical Infrastructure Protection*. Springer, 2007, pp. 73–82.
4. J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.
5. A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proceedings of the 6th ACM symposium on information, computer and communications security*. ACM, 2011, pp. 355–366.
6. F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.
7. J. K. Hale, E. F. Infante, and F.-S. P. Tsen, "Stability in linear delay equations." DTIC Document, Tech. Rep., 1982.
8. E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," *Sensors*, vol. 15, no. 3, pp. 4837–4869, 2015.
9. R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Transactions on automatic control*, vol. 49, no. 9, pp. 1520–1533, 2004.
10. A. Seuret, D. V. Dimarogonas, and K. H. Johansson, "Consensus under communication delays," in *Decision and Control, 2008. CDC 2008. 47th IEEE Conference on*. IEEE, 2008, pp. 4922–4927.
11. P.-A. Bliman, "Lmi characterization of the strong delay-independent stability of linear delay systems via quadratic lyapunov–krasovskii functionals," *Systems & Control Letters*, vol. 43, no. 4, pp. 263–274, 2001.
12. X. Li and C. E. De Souza, "Delay-dependent robust stability and stabilization of uncertain linear delay systems: a linear matrix inequality approach," *IEEE Transactions on Automatic Control*, vol. 42, no. 8, pp. 1144–1148, 1997.

13. S.-I. Niculescu, "Stability and hyperbolicity of linear systems with delayed state: a matrix-pencil approach," *IMA Journal of Mathematical Control and Information*, vol. 15, no. 4, pp. 331–347, 1998.
14. J. Chen, G. Gu, and C. N. Nett, "A new method for computing delay margins for stability of linear delay systems," in *Decision and Control, 1994., Proceedings of the 33rd IEEE Conference on*, vol. 1. IEEE, 1994, pp. 433–437.
15. Y. Shoukry, J. Araujo, P. Tabuada, M. Srivastava, and K. H. Johansson, "Minimax control for cyber-physical systems under network packet scheduling attacks," in *Proceedings of the 2nd ACM international conference on High confidence networked systems*. ACM, 2013, pp. 93–100.
16. J. Moon and T. Başar, "Minimax control over unreliable communication channels," *Automatica*, vol. 59, pp. 182–193, 2015.
17. G. Fiore, Y. H. Chang, Q. Hu, M. D. Di Benedetto, and C. J. Tomlin, "Secure state estimation for cyber physical systems with sparse malicious packet drops," in *American Control Conference (ACC), 2017*. IEEE, 2017, pp. 1898–1903.
18. W. Ren and R. W. Beard, *Distributed consensus in multi-vehicle cooperative control*. Springer, 2008.
19. F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," vol. 58, no. 11, pp. 2715–2729, 2013.
20. J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, 2007.
21. W. Michiels and S.-I. Niculescu, "Characterization of delay-independent stability and delay interference phenomena," *SIAM Journal on Control and Optimization*, vol. 45, no. 6, pp. 2138–2155, 2007.
22. M. Fazel, "Matrix rank minimization with applications," Ph.D. dissertation, PhD thesis, Stanford University, 2002.
23. M. Jaggi, M. Sulovsk *et al.*, "A simple algorithm for nuclear norm regularized problems," in *Proceedings of the 27th international conference on machine learning (ICML-10)*, 2010, pp. 471–478.
24. P. Erdös and A. Rényi, "On random graphs, i," *Publicationes Mathematicae (Debrecen)*, vol. 6, pp. 290–297, 1959.