You Make Me Tremble: A First Look at Attacks Against Structural Control Systems

Abel Zambrano [*] Alejandro Palacio-Betancur [+] Luis Burbano [†] Andres Felipe Niño [*]
Luis Felipe Giraldo [*] Mariantonieta Gutierrez Soto [+] Jairo Giraldo [‡] Alvaro A. Cardenas [†]
[*] Universidad de Los Andes [+] The Pennsylvania State University
[‡] University of Utah [†] University of California, Santa Cruz

ABSTRACT

This paper takes a first look at the potential consequences of cyber-attacks against structural control systems. We design algorithms and implement them in a testbed and on well-known benchmark models for buildings and bridges. Our results show that attacks to structures equipped with semi-active and active vibration control systems can let the attacker oscillate the building or bridge at the resonance frequency, effectively generating threats to the structure and the people using it. We also implement and test the effectiveness of attack-detection systems.

CCS CONCEPTS

• **Computer systems organization** → **Embedded and cyber-physical systems**; • **Applied computing** → *Engineering*.

KEYWORDS

Structural control, attacks, smart structures, security, building, bridges

ACM Reference Format:
Abel Zambrano, Alejandro Palacio-Betancur, Luis Burbano, Andres Felipe Niño, Luis Felipe Giraldo, Mariantonieta Gutierrez Soto, Jairo Giraldo, & Alvaro A. Cardenas. 2021. You Make Me Tremble: A First Look at Attacks Against Structural Control Systems. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS '21), Nov. 15–19, 2021, Virtual Event, Republic of Korea.* ACM, NY, NY, USA, 18 pages. https://doi.org/10.1145/3460120.3485386

1 INTRODUCTION

Since 1980, 258 weather and climate-related natural hazards in the United States (US) have resulted in $1.75 trillion cumulative costs of damage to cities [80]. To reduce these costs, civil infrastructures are being equipped with various sensors for health monitoring and structural control [65]. Sensors can measure physical quantities related to the building motion, such as strain, acceleration, velocity, displacement, pressure, temperature, and ground motion [21, 102]. Structures equipped with control devices can adapt in real-time to counteract extreme dynamic loads such as earthquakes or wind storms.

Among 525 buildings of 250 meters or greater height worldwide, 18% (97) are equipped with dynamic modification devices [56]. This statistic increases to 39% if we consider buildings constructed in the last decade. Without considering their height, in Japan alone, more than 50 buildings have Active Mass Dampers (AMD) to control building vibrations [102], and more than 30 high-rise buildings have been instrumented with semi-active variable oil dampers [35, 50].

Structural vibration control systems are particularly useful for tall buildings, often affected by wind-induced vibrations. Wind-induced vibrations in tall buildings have proven to cause *building motion sickness* to the occupants during normal operations [57, 58] and supplemental damping can mitigate these vibrations. Life-cycle cost analysis about the investment in control devices, including semi-active friction devices, has shown that structural control provides significant economic benefits on tall buildings subjected to wind loading [29, 64], among other natural hazards.

While structural control provides many benefits, as far as we are aware, these systems have not been studied from a security perspective. As the popularity of structural control increases, we need to start assessing and improving the security posture. This paper presents the first study of attacks against control systems in civil engineering structures. We consider two types of attacks: Denial of Service (DoS) attacks, where the attacker disables the activation of specific actuators, and False Data Injection (FDI) attacks, where the attacker forces the actuators to follow an attack command.

Our contributions include the following: (1) we are the first research paper to study the impact of attacks to structural control systems, (2) we provide the first algorithm for optimal DoS attacks trying to maximize the impact of external vibrations, (3) We identify metrics, testbeds, and benchmark models of buildings and bridges to evaluate the effectiveness of our methods, (4) We design and test the first effective attack-detection method in structural control, (5) We make all our algorithms and models open to the community https://github.com/BuildingResearch/security.

2 RELATED WORK

Attacks to CPS Attacks to Cyber-Physical Systems (CPS) can happen in a variety of components, including sensors, controllers, and actuators: (1) an attacker can inject false data into the system by faking sensor data (e.g., if the sensor data is unauthenticated or if the attacker has the key material for the sensors) and cause the control logic of the system to act on malicious data [59]. (2) The attacker can delay or even completely block the information from the sensors to the controller, causing it to operate with *stale data* [54].

CCS '21, November 15–19, 2021, Virtual Event, Republic of Korea

ACM ISBN 978-1-4503-8454-4/21/11…$15.00
https://doi.org/10.1145/3460120.3485386

(3) The attacker may be able to compromise the controller and send incorrect control signals to the actuators [63]. (4) The attacker can delay or block any control command, thus causing a denial of control to the system [4]. (5) The attacker can compromise the actuators and execute a control action that is different to what the controller intended [88]. And, (6) the attacker may be able to physically attack the system (e.g.. physically destroying part of the infrastructure and combine this with a cyber attack) [5].

All these attacks can be classified as either a **False Data Injection** FDI or a **Denial of Service** DoS attack. FDI [49, 59] and DoS attacks [4] have been discussed in the context of cyber-physical systems since 2009. In a **Denial-of-Service (DoS)** attack [4], the adversary prevents the controller from receiving sensor measurements, or the physical system from receiving a proper actuation command. To launch a denial of service, the adversary can jam the communication channels, compromise devices and prevent them from sending data, attack the routing protocols, or even turn off the lights (without electricity, control systems won't work). Similarly physical side channel attacks can inject false signals into a system, they can also be used to cause DoS attacks [71]. Attackers in close proximity of a target device can also damage them physically.

In a **False Data Injection (FDI)** attack [49, 59], the adversary sends false information where a malicious value (at time t) $a(t)$ will be different than the non-attacked value $u(t)$ ($a(t) \neq u(t)$). The adversary can launch these attacks by obtaining the *secret key* of some sensors, controllers, or actuators (if the communications are authenticated). Several control systems are air-gaped, and assume a trusted environment once a device is inside this air-gaped network, so a malicious insider doesn't need to worry about authentication. CPS can be compromised even without a computer-based exploit in what has been referred to as *transduction attacks* [34]. By targeting the way sensors capture real-world data, the attacker can inject a false sensor reading or even a false actuation action, by manipulating the physical environment around the sensor [34, 36]. For example attackers can use speakers to affect the gyroscope of a drone [82], exploit unintentional receiving antennas in the wires connecting sensors to controllers [76], or use intentional electromagnetic interference to cause a servo (an actuator) to follow the attacker's commands [76].

Popular examples of FDI attacks include scaling attacks $a(t) = \alpha u(t)$ [86], bias attacks $a(t) = u(t) + b$ [13, 16], delay attacks $a(t) = u(t - d)$ [86], and random attacks (where $a(t)$ is a random value at each time) [26, 98]. These attacks were successfully applied to power systems [86], a power plant boiler [98], water plants [13], robotic vehicles [16], and autonomous vehicles [26]. These simple attacks, however, do not succeed when targeting a structural control system.

One critical difference between structural control systems and most other cyber-physical systems is that attacks against structural control are not obvious. In a power grid, you know that opening circuit breakers will disconnect systems. In a vehicle, you know that you can crash another vehicle by accelerating to top speed. In a water system, you know that if you inject liquid into a tank and do not let it out, it will cause an overflow, etc. In contrast, in structural control systems it is not obvious how to attack the system in a way that it causes any significant effect. In particular, because each actuator's energy is small compared to the whole structure, most random attacks or heuristics will not have any significant effect. An attack against structural control systems needs to be strategic in the way frequencies, magnitudes, and phases are injected at each of the compromised endpoints.

To target structural control systems, we need to focus on analyzing the response of the structure to various types of vibrations. This is called frequency analysis. This paper is related to previous work that exploits when physical systems are sensitive to oscillations at specific frequencies. For example, an external acoustic signal tuned at a specific frequency can deteriorate the accuracy of Micro-Electro-Mechanical Systems (MEMS) gyroscopes [89]. The power grid might also be vulnerable to small oscillations being amplified by the system [46, 100]. Our proposed FDI attacks are closest to the work of Dadras et al. [22], where the authors study how malicious vehicles in a platoon can make small oscillations in their speed, be amplified by their neighbors, making the system unstable.

Our FDI attacks extend previous work by designing a new algorithm that finds a (local) optimal amplitude, phase, and frequency of attacks (rather than just finding a parameter of a predefined control). In addition, work on DoS attacks is (as far as we are aware) completely novel. To design our DoS attacks we need to evaluate the potential frequency response of the structure to a future unknown perturbation. We are not aware of anything similar in previous work on CPS attacks. Our final novelty when compared to previous work, is the use-case of structural control, which hasn't been previously explored.

Building Automation Security In terms of applications, our study is related to the security of Building Automation Systems (BAS) [18, 70]. BAS can monitor and control Heating, Ventilation, and Air Conditioning (HVAC), lighting, energy consumption and physical security (cameras, key cards, etc.). Previous research focused on proposing new security for the Building Automation and Control Network (BACnet) protocol [11, 31, 32], as well as for improving the security of endpoint devices in BAS [95, 96].

Despite these research efforts, ethical hackers as well as attackers, have found several ways to attack these systems. For example, ethical hackers took control of the building control system of a Google office in Australia [104], a ransomware gang attacked a hotel in Austria four times, disabling their electronic keys [8], a DDoS attack cut heat to apartments in Finland [62], and vulnerabilities found in one of the most popular software frameworks to create building automation controls (the Niagara framework) had vulnerabilities that could have allowed attackers from taking remote control to access systems, elevators, HVAC systems, alarms, and other critical operations [105]. The interest of attackers in structural control (wherever available) is the logical next step and this paper is the first proposal for understanding the potential impacts of sophisticated structural control attacks, as well the first study to propose new countermeasures.

3 STRUCTURAL CONTROL

Vibration control of structures can adapt in real-time to minimize the movements of a building, bridge, or wind turbine during extreme events [44]. Structural control systems have three major components: (i) sensors to capture the state of the environment, (ii) a computer to process the information from the sensors and make

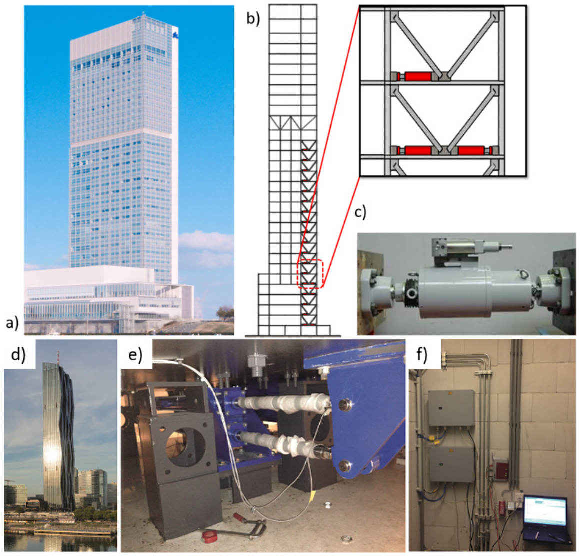


Figure 1: Top: (a)-(c) The Bandaijima 31-story building in Niigata, Japan, equipped with 72 hydraulic oil dampers (HiDAX-s) by Kajima Corporation. Bottom: (d)-(f) The Danube City Tower in Vienna, Austria, instrumented with two semi-active vibration absorbers based on Maurer MR dampers and two independent real-time controllers (Courtesy of Felix Weber [99]).

decisions based on the information, and (iii) actuators to perform the actions determined by the computer system [20].

Standard sensors for structural monitoring include Linear variable differential transformers (LVDTs), velocity transducers, accelerometers, and load cells, which measure displacement, velocity, acceleration, and force, respectively. These sensors can work as linear proportional devices in the frequency range of 0.1–100 Hz, covering the frequency band of structural vibration under seismic or wind excitation.

Actuators are the set of physical devices that execute the instructions from the controller [20]. There are four main types of structural control actuators: passive, semi-active, active, and hybrid (which combine active and passive actuators). Passive actuators dissipate the power of external perturbations and do not receive any control [30]. Passive control devices include linear viscous dampers, friction dampers, tuned mass dampers, and tuned liquid column dampers [42, 48]. Active and semi-active systems have an external energy source to activate hydraulic, electromechanical, or electromagnetic systems. Active control actuators include HiDAX-s, linear pistons, and mass dampers. Semi-active control actuators include magneto-rheological (MR) dampers [17] and friction dampers [23, 24, 39]. Active and semi-active dampers improve energy dissipation capacity, and create a safer structure when compared to passive devices [1, 55, 102]. Examples of active and semi-active dampers can be found on bridges and buildings worldwide, as shown in Fig. 1 and Fig. 2.

In this paper we focus on the following three actuators: Magneto-Rheological **MR Dampers**, Active Mass Dampers **AMDs**, and Active Tuned Mass Dampers **ATMDs**. An MR damper has a fluid controlled by a magnetic field. By varying the power of an electromagnet, we can control the damping characteristics of the shock absorber. Active mass damping approaches consist of applying a dynamic modification system in a few locations in the structure. An AMD controls the movement of a mass to counteract vibrations in the structure. An ATMD consists of an actuator placed between the structure and a tuned mass damper, a system composed of a mass, spring, and damper (adequately tuned) attached to a structure to reduce its dynamic response.

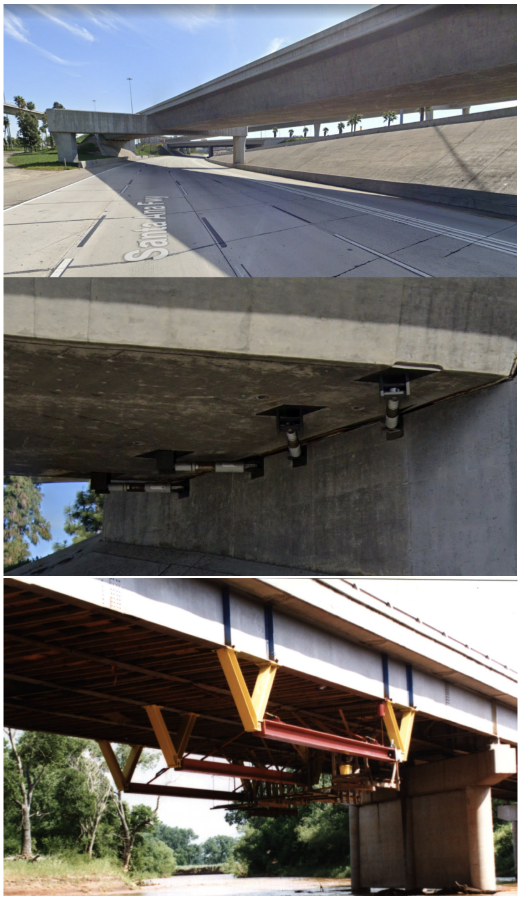


Figure 2: Top: Perspective view of a highway bridge equipped with dampers in Orange County, California, and close-up to the installed dampers (Source: Google Street View 33°51’27.5"N 117°58’46.9"W). Bottom: Highway bridge in Oklahoma, US, instrumented with semi-active variable friction control devices (Source: DoT [69]).

In our simulations we use bridge and building benchmarks proposed by the Committee on Structural Control of the American Society of Civil Engineers (ASCE) [27, 67, 78].

3.1 Vulnerabilities and Adversary Model

Structural control systems integrate various operational technologies such as Industrial PCs (Regular Windows PCs that pass safety standards because of their enclosures), Ethernet networks (e.g., EtherCAT) or in legacy implementations serial lines (e.g., RS422),

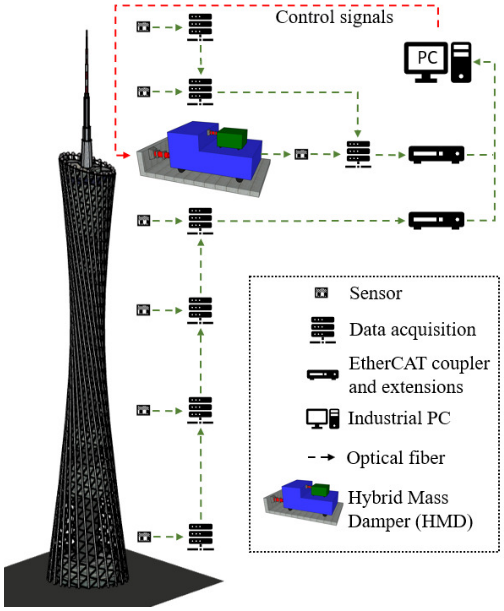


Figure 3: Operational Technology for structural control of the Guangzhou TV Tower (adapted from a diagram in [66]).

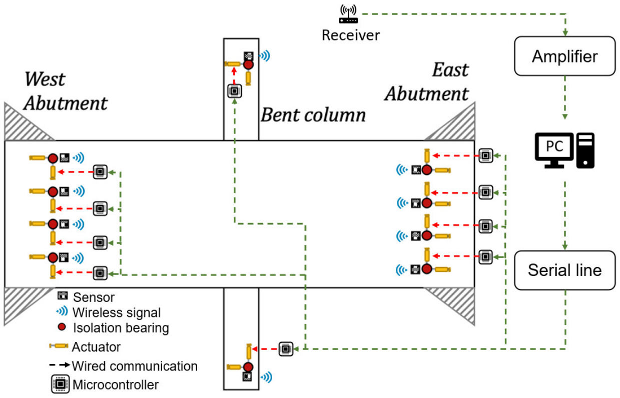


Figure 4: Operational technology for structural control of the Walnut Bridge (adapted from a diagram in [68]).

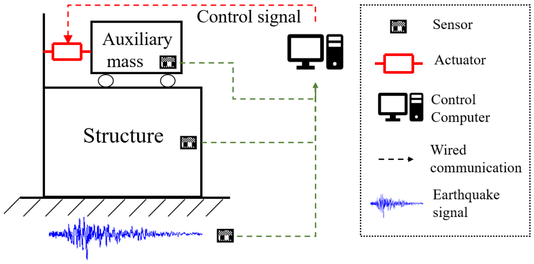


Figure 5: AMD instrumentation (adapted from [60]).

embedded computers near sensors and actuators to capture and convert physical signals to computer information [10, 61, 81, 101]. Fig. 3 illustrates how computers and networks are integrated in the control of the Guangzhou tower, Fig. 4 shows the technology in the Walnut Creek Bridge, and Fig. 5 illustrates how an AMD actuator is instrumented within the Kyobashi Seiwa Building.

As we can see, these systems use computers and networks that can be attacked with methods that worked for similar technologies [6, 15, 40, 52, 79, 106]. In general, these networks are air-gapped and assume a trusted insider setting, but as the Stuxnet attack showed, air-gapped networks are not immune to attacks (especially not against state-sponsored attacks). A malicious insider, an untrusted contractor, a supply-chain attack, or malware on a device crossing the air-gapped network (such as USB drives) can defeat this isolation.

Attacks	Passive	Semi-active	Active	Hybrid
DoS	Y	X	X	X
FDI		X	X	X

Table 1: Possible Attacks for Each Type of Actuator. Y denotes physical attacks. X denotes that the attack can be launched through a cyber-attack.

Once inside the system, the attacker can launch a variety of DoS or FDI attacks. DoS attacks can be launched by blocking (or not even sending) the control signal to active or semi-active actuators. DoS attacks can also occur by shutting down the electric power to the building: without power, active and semi-active actuators cannot be controlled. Finally, an insider can launch DoS attacks against passive actuators (the attacker can physically destroy the damper). FDI attacks can be launched by an attacker that compromised the industrial PC. The industrial PC can then send malicious control signals to the active or semi-active actuators. A malicious supply chain attack providing a compromised microcontroller can also be used to launch FDI attacks. Table 1 shows a summary of this discussion.

In this paper, we assume an attacker that can disrupt the communication link to the actuators (DoS attack), and another one who has partial (or total) access to the control system and can send false control commands to the actuators (FDI attack). We also assume the attacker has some knowledge about the operation and design of the structural control system.

3.2 Damage Metrics

To understand the impact of attacks, we need to look at how structural engineers evaluate risks to buildings and bridges. The standard ASCE 7-16 [51] is an integral part of building codes in the US and is adopted by the International Building Code, the International Existing Building Code, the International Residential Code, and the NFPA 5000 Building Construction and Safety Code. In ASCE 7-16, the primary metric to evaluate the effects of wind and seismic events is the **Inter-Story Drift (ISD)** (lateral deflection of a building) as drifts damage cladding, nonstructural walls, and partitions [87]. The allowable drift limits placed by ASCE 7-16 are functions of the risk category and type of seismic forces. ASCE 7-16 Section 12.12 states the allowable drift for any floor in most structures is $0.020h_{sx}$, $0.015h_{sx}$, $0.010h_{sx}$, for Risk Category I or II,

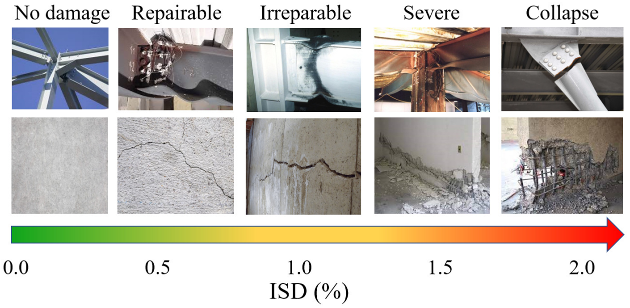


Figure 6: ISD vs. damage. Top: Steel. Bottom: Concrete.

III, and IV, respectively, where h_{sx} is the story height below level x. The Risk Category is based on the risk to human life, health, and welfare associated with structural damage or by the nature of their occupancy or use. For example, buildings designated as essential facilities such as hospitals have a Risk Category IV and will require a drift limit of 1% of the height of all floors. Buildings that create a substantial risk to human life have a Risk Category III, and buildings that pose a low risk to human life are Risk Category I. Similarly, the National Building Code of Canada limits ISD to 1% of the height of the floors for post-disaster buildings that must remain in operation immediately after an earthquake [33].

Fig. 6 illustrates the ISD-damage relationship for concrete and steel buildings, adapted from the NEHRP Guidelines for the Seismic Rehabilitation of Buildings [77]. If a building has an ISD above its elastic range, a few places start presenting some permanent distortion; however they are repairable by replacing the affected components. A more severe ISD can create visible deformation in beams and columns. Damage in concrete structures is evident with the propagation of cracks instead of distortion of components. If the displacements in the structure are higher, there is extensive cracking and severe damage in the structure that can bring the structure near collapse [77]. We can see that a 1% ISD is at the boundary between reparable and irreparable damages. We highlight this value in our simulations to show when attacks can cause significant damages.

Since bridges do not have several stories, we need to use a different metric. The most common metrics for predicting bridge damages are the lateral displacement and the lateral force [41]. We will use them to analyze the impact of attacks on bridges.

4 DESIGNING OPTIMAL ATTACKS

Buildings, bridges, and soil/rock formations have several vibration frequencies at which they tend to oscillate more strongly, as illustrated in Fig. 7. When these peaks are large enough, they are called resonant frequencies. An attacker trying to damage an infrastructure can launch DoS or FDI attacks to change the frequency response of the building and maximize the magnitude and the number of amplifying frequencies. In addition, if a building vibrates at the same frequency as the input seismic wave, the vibrations may double in amplitude, causing devastating consequences [3].

Launching attacks to drive a building or a bridge to oscillate at a resonant frequency is not obvious. This section studies the risk that sophisticated attackers may pose when they design a strategic attack. We assume that the adversary has gained (full or partial) access to the building's control system. We consider DoS attacks (interrupting communications to actuators) and FDI attacks (sending false commands to actuators) and demonstrate their effects on real and simulated scenarios based on well-known benchmarks from structural engineering societies. We first define a dynamical system model that characterizes the controlled structure and later propose strategies to design attacks that maximize their impact over the building.

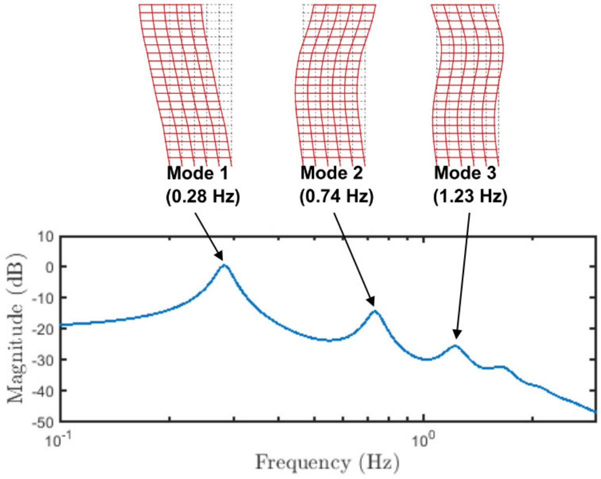


Figure 7: Frequency response associated with the vibration modes of the 20-story benchmark steel building.

4.1 Mathematical Description of a Structure

The design of active and semi-active vibration controllers uses well-known equations of motion for a building or bridge (see Appendix A) that describe how the lumped masses, stiffness, and damping properties of the elements of a structure interact to change their position, velocity, and acceleration [43]. The model has three main variables: i) the structure's state variables $\mathbf{x}$, which typically include displacements and their velocities at different points in the structure; ii) the forces that are exerted by the actuators trying to stabilize the structure $\mathbf{u}$; and iii) forces that are exerted by external disturbances such as earthquakes and wind $\mathbf{w}$. If we denote the variations of the structure's state variables by $\mathbf{x}$ (the derivative of $\mathbf{x}$ with respect to time), the mathematical model of the structure is

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{A}\mathbf{x} + \mathbf{B}\mathbf{u} + \mathbf{E}\mathbf{w} \\ \mathbf{z} &= \mathbf{F}\mathbf{x} \end{aligned} \tag{1}$$

where $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{E}$ are matrix elements that are used to represent the combined action of variables $\mathbf{x}$, $\mathbf{u}$, and $\mathbf{w}$. The matrix $\mathbf{F}$ is a mask that selects only those state variables that we want to attack. Therefore, $\mathbf{z}$ contains such variables. A popular vibration control system consists of a feedback control strategy represented by $\mathbf{u} = -\mathbf{R}\mathbf{x}$, where $\mathbf{R}$ is a matrix gain [107]. Structural engineers design this control matrix to reduce the displacement of the structure caused by external disturbances.

4.2 Denial of Service (DoS) Attack

A DoS attack is opportunistic, and therefore it will only be damaging if it is launched during an occurring natural event (earthquake or high winds). Since attackers cannot predict the type of vibrations this natural hazard will create in the structure, they need to maximize the damage over the maximum number of potential perturbations. To capture this criterion, we study the H_2 norm of a system [107], which can be seen as the power of the response of the dynamical system to external disturbances for a wide range of frequencies. A large H_2 norm indicates that the response of the structure to external disturbances will be large as well for a wide range of frequencies. If the DoS attack is designed in a way to maximize the H_2 norm, then it has a high chance of damaging the system.

The H_2 norm of Eq. (1) is defined as:

$$||\mathbf{H}_{zw}||_2 = \left(\frac{1}{2\pi}\int_{-\infty}^{+\infty} \text{Trace}\big(\mathbf{H}_{zw}(j\omega)\mathbf{H}^*_{zw}(j\omega)\big)d\omega\right)^{1/2}.$$

Now, let $\mathbf{x}_s$ be a n-dimensional binary vector that indicates what actuators the adversary will disconnect: entry i is 1 if the i-th is not attacked, and 0 otherwise. The H_2 norm of the controlled system with the feedback matrix gain $\mathbf{R}$ is defined as $h_2(\mathbf{x_s}) = ||\mathbf{H}_{zw}||_2$, where $\mathbf{H}_{zw}(j\omega) = \mathbf{F}(j\omega\mathbf{I} - \mathbf{A}_{cl})^{-1}\mathbf{E}$, $\mathbf{A}_{cl} = \mathbf{A} + \mathbf{B}\mathbf{R}_{new}$, and $\mathbf{R}_{new} = \text{diag}(1 - \mathbf{x}_s)\mathbf{R}$. Then, the actuators to be affected by the DoS attack can be chosen by the following optimization process:

$$\begin{aligned} \underset{\mathbf{x}_s \in \mathbb{Z}^n}{\text{maximize}} \quad & h_2(\mathbf{x_s}) \\ \text{subject to:} \quad & \sum_{i=1}^{n} x_s^i = k \\ & x_s^i \in \{0, 1\} \quad \forall i = 1, \ldots, n. \end{aligned} \tag{2}$$

4.3 False Data Injection (FDI) Attack

An adversary launching an FDI attack on the control system changes the system's frequency response (e.g., it changes the curve in Fig. 7). Therefore we need a process based on two steps: i) finding those k actuators such that, if their control is blocked, then the response of the system controlled by the remaining $n - k$ actuators is maximized at a particular frequency of the force exerted by the blocked actuators; and ii) designing the control signals at the frequency with the maximum response of the system to be injected to the attacked actuator.

In contrast to DoS attacks, an FDI attack will attempt to maximize the frequency response of an individual frequency of attack. Therefore in this case we use the H_∞ norm of a system [107], which is the maximum gain of the system for a given control input at a specific frequency. This norm can be seen as the maximum response of the system for a given set of inputs that oscillate at a specific frequency. The H_∞ norm is computed using the representation of the structure in Eq. (1) and the control policy that defines the stabilizing forces $\mathbf{u}$ as follows. Let $\mathbf{H}_{zu}(j\omega)$ be the transfer function matrix of the structure, representing the response of the stable system with outputs $\mathbf{z}$ for the input control signals $\mathbf{u}$. These input signals are the ones that inject energy into the system to try to control the vibrations of the structure. Let $\bar{\sigma}_H(\omega)$ be the largest singular value of matrix $\mathbf{H}_{zu}(j\omega)$. Then, the H_∞ norm of a system with transfer function $\mathbf{H}_{zu}(j\omega)$ is

$$||\mathbf{H}_{zu}||_\infty = \sup_{\omega} \bar{\sigma}_H(\omega) = \sup_{||\mathbf{u}||_2 \neq 0} \frac{||\mathbf{z}||_2}{||\mathbf{u}||_2}. \tag{3}$$

Let $\mathbf{x}_s$ be a n-dimensional binary vector that indicates what actuators are not attacked by the adversary: entry i is 1 if the i-th is not attacked, and 0 otherwise. The H_∞ norm of the controlled system with the feedback matrix gain $\mathbf{R}$ is defined as $h_\infty(\mathbf{x}_s) = ||\mathbf{H}_{zu}||_\infty$, where $\mathbf{H}_{zu}(j\omega) = \mathbf{F}(j\omega\mathbf{I} - \mathbf{A}_{cl})^{-1}\mathbf{B}$, $\mathbf{A}_{cl} = \mathbf{A} + \mathbf{B}\mathbf{R}_{new}$, and $\mathbf{R}_{new} = \text{diag}(1 - \mathbf{x}_s)\mathbf{R}$. Here, $\mathbf{H}_{zu}$ is the transfer function matrix that captures the response of the outputs of the controlled system $\mathbf{z}$ with the control inputs $\mathbf{u}$. The attack is designed in two steps:

Step 1: The adversary determines which actuators will be disconnected from the central control system such that the peak of the frequency response of the system is maximized, via the following optimization process:

$$\begin{aligned} \underset{\mathbf{x}_s \in \mathbb{Z}^n}{\text{maximize}} \quad & h_\infty(\mathbf{x}_s) \\ \text{subject to:} \quad & \sum_{i=1}^{n} x_s^i = k \\ & x_s^i \in \{0, 1\} \quad \forall i = 1, \ldots, n. \end{aligned} \tag{4}$$

Step 2: The adversary needs to determine the magnitude and phase of the signals that will be injected into the actuators. From Eq. (3), the H_∞ norm corresponds to the largest singular value of matrix $\mathbf{H}_{zu}(j\omega)$, that is, $\bar{\sigma}_H(\omega)$. We know that the input vector that produces this maximum gain corresponds to the right-singular vector associated with the largest singular value $\bar{\sigma}_H(\omega)$ [38]. This right-singular vector contains the amplitude and phases that the sinusoidal signals to be injected into the actuators. This vector is known as the direction of the input signal. This is a unitary vector, meaning that amplitudes of the sinusoidal signals are such that the Euclidean norm of this vector is 1. The magnitude of this vector can be amplified by any constant that keeps the signals inside the range of operation of the actuators.

5 QUANSER TESTBED

Our first experiment is conducted using Quanser's bench-scale model that emulates a building equipped with active mass dampers (AMDs) subjected to earthquake loading, as shown in Fig. 8. The plant is a two-story building-like structure with two active masses[1] and a shake table that generates an external earthquake-like disturbance[2]. Two accelerometers are used to estimate the position and velocity of two different points of the structure relative to the ground. The frame of the structure is made of steel and has a flexible facade. The computer program sending commands to the actuators (AMDs) is a Linear Quadratic Regulator (LQR), an algorithm commonly used to suppress vibrations in tall buildings [73]. The parameters of the mathematical model of the structure as in Eq. (1) and the control parameters of the LQR are given in Appendix B.

The state variables from the vector $\mathbf{x}$ in Eq. (1) are (i) the position of the moving cart at floor 1 x_{c1}, (ii) the position of the moving cart of floor 2 x_{c2}, (iii) displacement at floor 1 x_{f1}, (iv) displacement at floor 2 x_{f2}, (v) velocity of cart 1 $\dot{x}_{c1}$, (vi) velocity of cart 2 $\dot{x}_{f2}$, (vii)

[1] https://www.quanser.com/products/active-mass-damper

[2] https://www.quanser.com/products/shake-table-ii/

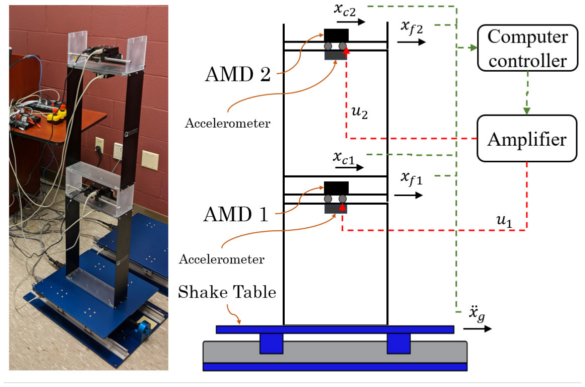


Figure 8: Experimental setup: Quanser's shake table with two-floor plants equipped with two active mass dampers (AMDs) and accelerometers to estimate position and velocity. Variables x_{c1} and x_{c2} indicate the position of carts 1 and 2; variables x_{f1} and x_{f2} indicate the position of stories 1 and 2, variables u_1 and u_2 are the control signals of carts 1 and 2, and variable $\ddot{x}_g$ indicate the acceleration produced by the earthquake-like disturbance produced by the shake table.

Table 2: H_2 norm for different configurations of the system in Fig. 8 under DoS attacks.

Attack configuration	H_2 norm (dB)
Uncontrolled	-16.26
Controlled	-19.53
DoS on u_1	-16.57
DoS on u_2	-19.46

velocity of floor 1 relative to the ground $\dot{x}_{f1}$, and (viii) velocity of floor 2 relative to the ground $\dot{x}_{f2}$. The vector $\mathbf{z}$ defines the variables that we want to attack, namely the ISD at floors 1 and 2, and their velocities.

5.1 DoS Attack

We used the optimization process in Eq. (2) to design a DoS attack on the two-story building, based on the physical equations of the testbed (see Appendix B). In this process, the H_2 norm is computed from the response of the system for external disturbances at frequencies ranging from 0Hz to 10Hz, which is the maximum allowed vibration frequency of the structure. In this case study, the attacker evaluates the response of the system for four different scenarios: the controlled system (no disconnections), disconnecting actuator 1 (u_1), disconnecting actuator 2 (u_2), or disconnecting both actuators. Fig. 9 shows the frequency response, and Table 2 shows the H_2 norm in these scenarios.

From Fig. 9 and Table 2, we can see that an adversary that conducts the optimization process in Eq. (2) to deliver a DoS attack on this building will disconnect all actuators if possible. If the adversary can only disconnect one actuator, it will choose actuator 1.

To illustrate this result, we tested two external disturbances. First, we used the Kanai-Tajimi model [53, 85], which is commonly used to artificially generate earthquake-like disturbances, to create 200 time-series of artificial ground motions with different frequencies ranging from 1 Hz to 11 Hz. This range of frequencies is commonly seen in earthquakes[43]. In these experiments, 70.5% of the time, disconnecting actuator 1 produced a larger ISD than disconnecting actuator 2, confirming the prediction of our theory and optimization problem.

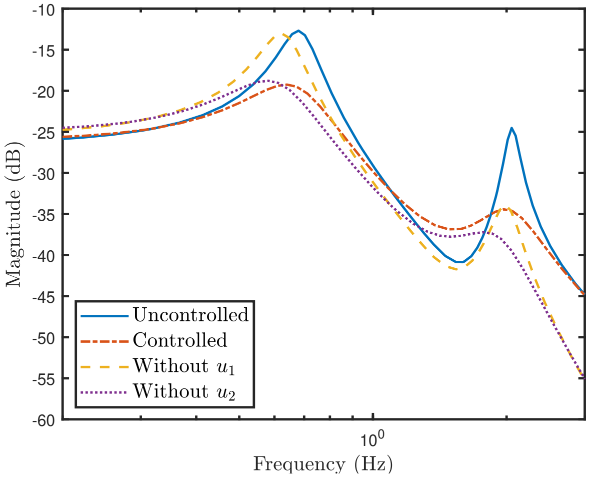


Figure 9: Response of the system in Fig. 8 for different frequencies when the two actuators are disconnected (uncontrolled), only actuator 1 (u_1) is disconnected, only actuator 2 (u_2) is disconnected, and when the control system of the bench-scale structure is completely functional (controlled).

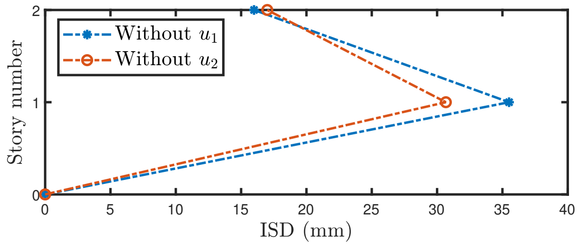


Figure 10: Our experimental results in the testbed match our prediction that disconnecting u_1 will cause a larger maximum ISD than disconnecting u_2.

Second, we tested the laboratory bench-scale model by disconnecting one actuator when the disturbance is the time series corresponding to the recording of the famous Kobe earthquake that occurred in Japan in 1995 [74]. This recording is widely used as a reference to test vibration attenuation systems due to its impact on civil structures. Fig. 11 shows the response of the system when the DoS attack disconnects actuator 1 and when the attack disconnects actuator 2. The maximum ISD per story is shown in Fig. 10. The behavior of this real bench-scale model shows that a DoS attack that blocks actuator 1, as it was designed, has a bigger impact than the one that blocks actuator 2 (confirming our prediction again).

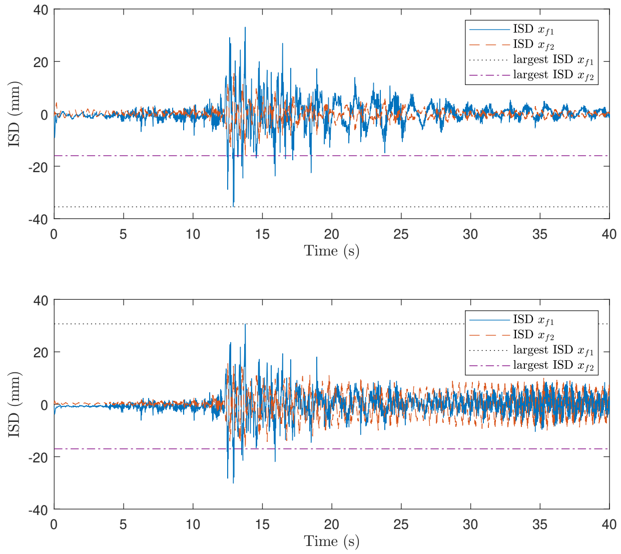


Figure 11: ISD vs. time of the bench-scale structure for two different DoS attacks (above: blocking actuator 1, and below: blocking actuator 2), when the Kobe earthquake-like disturbance is exerted on the system.

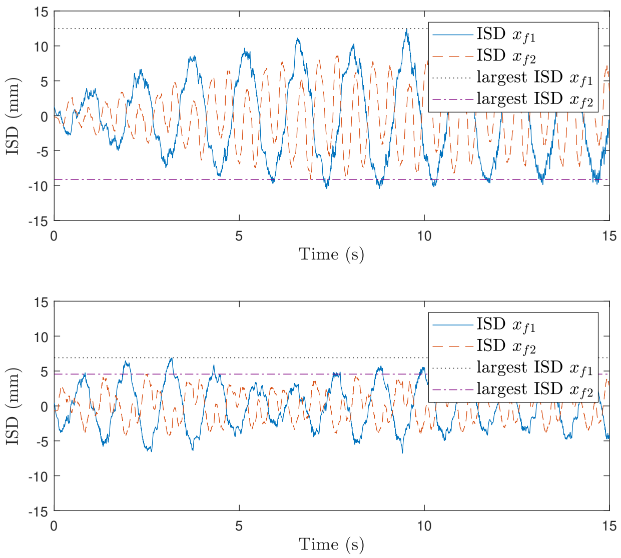


Figure 12: ISD vs. time for each FDI attack on the bench-scale structure.

5.2 FDI Attack

We now use the design process in Section 4.3 to design an FDI attack for the testbed based on the model in Appendix B. Fig. 13 shows the frequency response of the building with respect to the action of u_1 (signal of actuator 1) on the system and the response of the building with respect to the action of u_2 (actuator 2) on the system.

From these plots, the highest peak occurs when u_1 is manipulated. Since these responses are shown on a logarithmic scale (decibels), the difference between these two responses is significant. Here, the highest peak occurs at 0.68Hz. Using this information, the adversary injects a control command with a frequency of 0.68Hz. In the second step of the FDI attack design process, the adversary determines the magnitude and phase of the attacks sent to actuators.

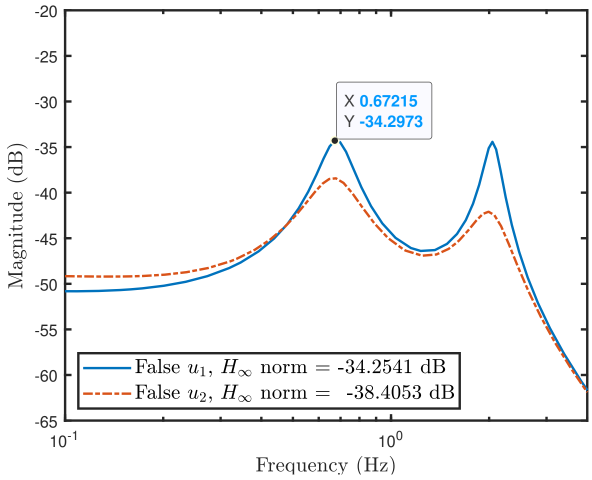


Figure 13: Frequency response of the system with respect to $u1$ (actuator 1) and with respect to u_2 (actuator 2). Note that the system's response with respect to u_1 has its highest peak when actuator 1 is manipulated at 0.68 Hz; the response of the system with respect to u_2 has its highest peak when actuator 2 is manipulated at 0.70Hz.

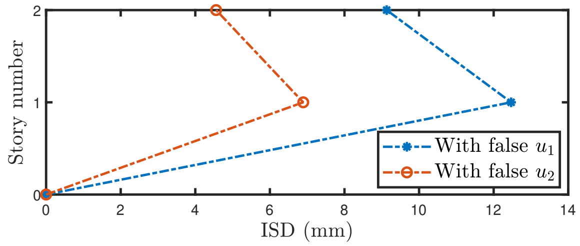


Figure 14: Our experimental results confirm our theoretical prediction that the attack with u_1 would cause larger damages (a larger maximum ISD).

For comparison purposes, we also studied the scenario when only actuator 2 is attacked using a signal at a frequency where the maximum peak occurs, that is, 0.70Hz (see Fig. 13). The ISD vs. time in the real plant for both attacks is shown in Fig. 12. Fig. 14 shows the maximum ISD for both attacks. From these experimental results, it is clear that attacking signal u_1 is the best decision that an attacker should take based on the model to generate the worst damage in the structure. This is consistent with the result in Fig. 13 obtained from the mathematical model of the building. Fig. 15

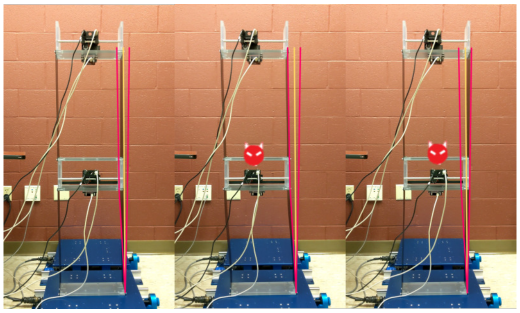


Figure 15: A video can be seen at https://youtu.be/vM_n1t92NJg.

shows the maximum displacement of the real plant when the attack on one of the actuators is deployed.

To show that our designed attack using Eq. (4) is the one that will generate the largest impact on the structure, we injected signals on actuator 1 at different frequencies but with the same amplitude. We injected sinusoidal actuation signals at frequencies 1.11 Hz, 1.27 Hz, and 1.43 Hz for comparison purposes and compared them to our predicted optimal attack at 0.68Hz Fig. 16 shows the results using these test signals. An anonymized video of this comparison can be seen at https://youtu.be/vM_n1t92NJg. We confirm that these higher-frequency attacks result in smaller ISDs than our optimal design.

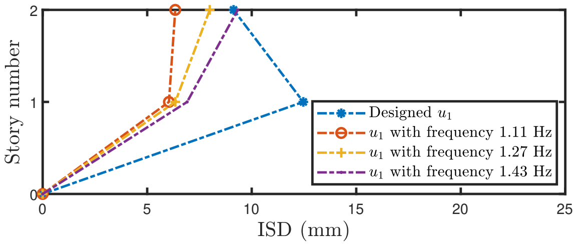


Figure 16: Maximum ISD for each story of the bench-scale structure for u_1 at different frequencies. Our predicted optimal attack oscillates at 0.68Hz.

6 ATTACKING A BUILDING WITH SEMI-ACTIVE DAMPERS

To study more realistic scenarios, we start using standard models of large scale structures. This case study consists in a benchmark 20-story building shown in Fig. 17 supplied by the Structural Engineer Association of California (SAC) [84]. The structure has magnetorheological (MR) fluid dampers at every story that work as semi-active control devices, and it is modeled as an in-plane lumped-mass shear structure.

The mass of story 1 is 1.126×10^6 kg, masses from story 2 to story 19 are 1.100×10^6 kg, and the mass of story 20 is 1.170×10^6 kg. The inter-story stiffness are the following: from story 1 to story 5 are 862.07×10^3 kN/m, from story 6 to story 11 are 554.17×10^3 kN/m, from story 12 to story 14 are 453.51×10^3 kN/m, from story 15 to story 17 are 291.23×10^3 kN/m, for story 18 and story 19 are 256.46×10^3 kN/m, and for story 20 is equals to 171.70×10^3 kN/m per [97].

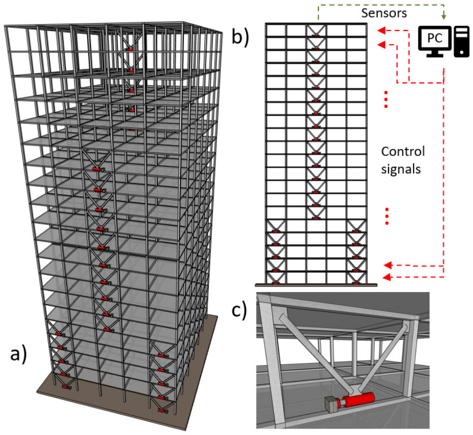


Figure 17: a) Benchmark 20-story high-rise building, b) its layout of actuators, and c) a close-up of the MR damper.

The state variables of the vector $\mathbf{x}$ are the displacement and velocity of each of the 20 stories of the building. Similarly, since the adversary wants to maximize the ISD, $\mathbf{z}$ in Equation (1) is defined as a vector of the ISD at each floor. The ASCE 7-16 standard states that ISD ratios above 1% can compromise the integrity of the structure.

The dynamic behavior of the MR damper is based on the Bouc-Wen hysteretic model in parallel with a dashpot added for a nonlinear "roll-off" effect. The force produced by this model is a function of the velocity of the device, an evolutionary variable, a set of parameters controlling the behavior of the hysteresis, and the command voltage applied to the current driver. The values of the parameters used in this study have a capacity of 1000kN [103] and scaled to have this capacity with a maximum voltage of 10 V.

The control algorithm for this system consists of an LQR algorithm as the primary controller that determines the command force (f_c), and a clipped-optimal controller that defines the input voltage to the MR dampers (v). The latter can be expressed as [28]:$v = V_{max}H((f_c - f)f)$, where f is the force of the MR damper, V_{max} is the maximum voltage, and $H(.)$ is the Heaviside step function.

We used the optimization process in Equation (2) to design a DoS attack on the 20-story building. Fig. 18 shows the H_2 norm and the maximum ISD ratio for all stories when the DoS attack is deployed on k actuators, from $k = 1$ to $k = 20$, when the building is under a 0.7 "El Centro" earthquake [90].

Note that when you only disconnect 12 actuators you get a better attack (higher ISD) than when you disconnect all 16 of them. Furthermore, the ISD ratio surpasses the safety limit of 1% after disabling only 5 actuators! This information is important, because an attacker might not be able to attack every actuator. With the proposed algorithm, an optimal attack can be designed for whatever number of actuators an attacker can affect.

Fig. 19 shows which actuators are disabled by the genetic algorithm for each designed attack. It can be seen that the algorithm

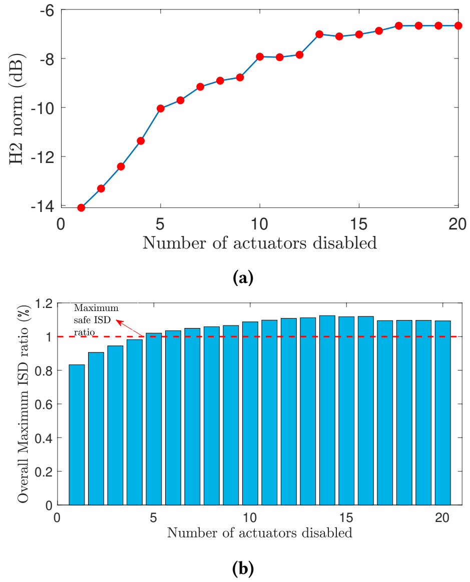


Figure 18: (a) H_2 norm of the system for each k attacked actuators. (b) maximum ISD ratio for all stories when the attacker has blocked k signals from the designed DoS attack. The horizontal line indicates the 1% safety level, any ISD above that is dangerous for the building.

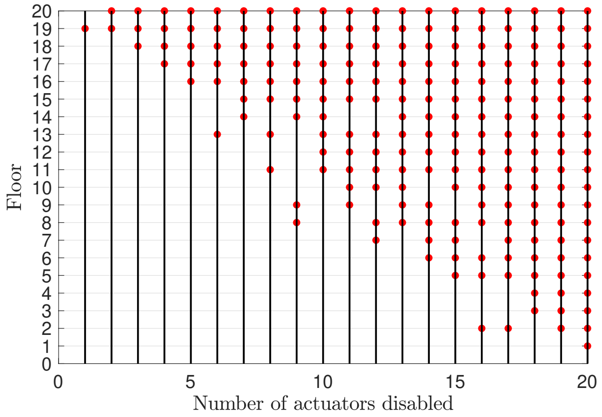


Figure 19: Actuators disabled for every k.

tends to disable the actuators located in the top floors. This is intuitive as actuators in the top floors can compensate better the vibrations in the building.

To show that our attacks are optimal, we compare our results with random disconnections of actuators. Fig. 20 shows that our optimal attack is considerably more effective.

7 ATTACKING A BUILDING WITH ACTIVE DAMPERS

We use the same 20-story benchmark building but the control system is replaced by two different mass damper systems as shown in Fig. 21. The first one is an Active Mass Damper (AMD) where an auxiliary mass is connected to the structure through an actuator, and the second is an Active Tuned Mass Damper (ATMD) where the mass is connected to the structure through an actuator, a spring, and a damping device [73]. The latter is known as Hybrid control because it is a combination of an active component (actuator) and a passive component (spring and damping) that increase the reliability of the system if there is a malfunction of the actuator, an energy outage, or, in this case, a cyberattack.

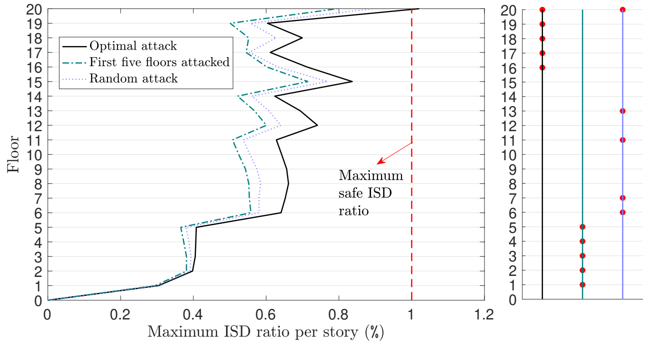


Figure 20: Comparison between the optimal attack and other different selections for k=5, with the actuators disabled in each attack.

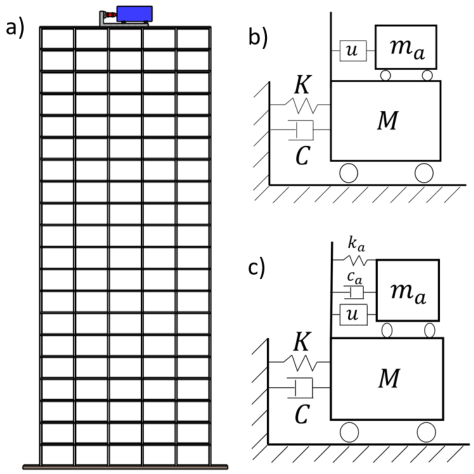


Figure 21: a) Benchmark 20-story high-rise building with a mass damper, b) AMD model, c) and ATMD model.

The state variables of the vector **x** for this case are the displacement and velocity of each of the 20 stories, as well as the displacement and velocity of the auxiliary mass. Similar to the previous case study, the output vector **z** in Eq. (1) is a vector of the ISD for each floor.

First the AMD is considered with a mass ratio of 2% of the first modal mass, corresponding to 332 tons, an actuator with maximum capacity of 2MN, a maximum stroke of 50 cm, and an LQR control algorithm [47]. The LQR is designed with the identity matrix and a control force weight as $R = 10^{-14}$. The ATMD is considered with the same mass ratio, actuator and LQR controller as the AMD, and the optimal tuning of the spring and damping is evaluated using the Sadek criterion [75]. Since the movement of the mass is limited by the stroke of the actuator, this state is bounded during the simulation by generating a stopping force [19].

Our study shows that i) a DoS attack to the single actuator can compromise the integrity of the structure, and additionally, the attacks are more successful on the AMD than the ATMD thanks to the additional reduction of vibrations provided by the passive component of the ATMD; and ii) FDI attacks that are able to inject energy to the system causing similar or worse damages than those caused by natural hazards. Contrarily to the DoS results, the FDI is more effective on the ATMD than the AMD because the passive component assists the oscillation of the attacking signal.

7.1 DoS Attack

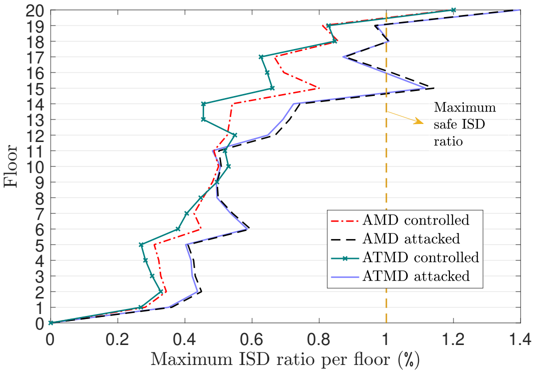
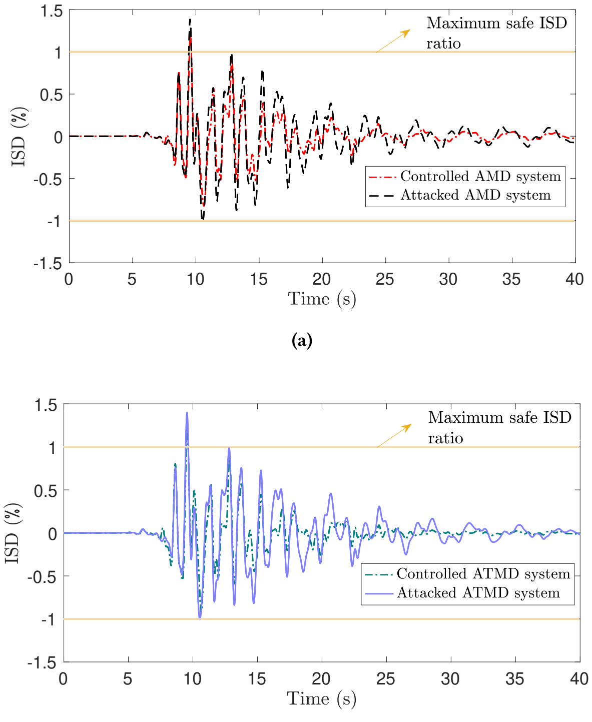


Figure 22: Maximum ISD ratio per floor for the AMD and ATMD systems controlled and under a DoS attack

The system was subjected to a Kobe earthquake disturbance, with a scaling factor of 0.4. In Fig. 22, the maximum ISD per floor can be seen when the Kobe disturbance was applied to the ATMD and AMD systems, both controlled and attacked. Note that the DoS attack generates higher ISD ratios for the AMD system. This can be explained by the passive dynamics involved in the ATMD model. When the AMD actuator is disconnected, the system is essentially left as if no preventive measure was installed. On the contrary, when the ATMD actuator is disconnected, there still is a passive component mitigating the effect of the disturbance by a small margin. However, the DoS attack is highly effective in both cases, where floors 15 and 18 surpass de 1% limit even when they were within safe ranges on the controlled system

A more detailed effect of the DoS attack can be seen in Fig. 23. Even though the maximum ISD ratio of the roof is higher than 1% for the four simulated systems, it is still considerably higher when the DoS attack is performed. It is also notable how other ISD ratio values are mitigated in other instants of the time response by the control system, which reduce the oscillations performed by the system, diminishing the overall damage to the structure during the earthquake. All of this proves the effectiveness of the DoS attack, and while it may be slightly more effective in the AMD system, disabling the actuator causes high damage in both systems.



(a)

(b)

Figure 23: (a) Time response of the ISD ratio for the roof for the AMD system. (b) Time response of the ISD ratio for the roof for the ATMD system.

7.2 FDI Attack

The FDI attack was designed by using the two step process from section 4.3. We obtained the frequency response in Fig. 24 from the singular value decomposition of the systems. The specified H_∞ norm is the maximum value seen in the plot. The frequencies for both systems are very similar: $H\omega_{FDI} = 0.2847$Hz for the AMD and $H\omega_{FDI} = 0.2787$Hz for the ATMD. Despite this similarity, we can predict that the FDI attack will be more effective on the ATMD system, since the H_∞ norm is higher for this case.

Figures 25 and 26 present the Maximum ISD ratios per floor and the ISD ratio of the roof during the attack for the injected signal. As predicted by the SVD analysis, the attack has a significantly higher impact for the ATMD system, where the ISD ratios are over 1% for every floor, and as high as 3% on the roof. This means that a critical damage is achieved for the entire building structure. As for the FDI attack on the AMD system, it has less significant effects. In spite of this, permanent damage is achieved on the structure on floors 15 and 20, which shows that this attack still can have devastating consequences on both systems.

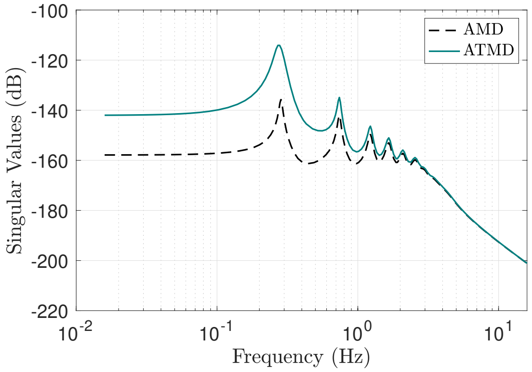


Figure 24: SVD for the AMD and ATMD models with the actuator force as input.

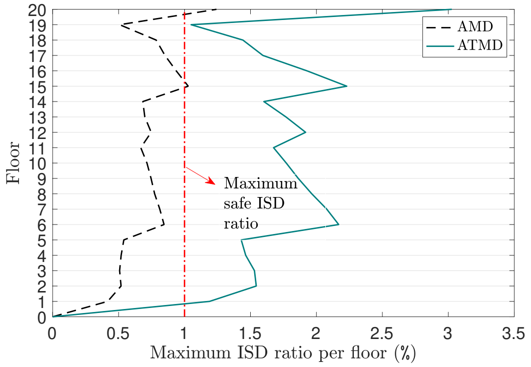


Figure 25: Maximum ISD per floor for the FDI attack.

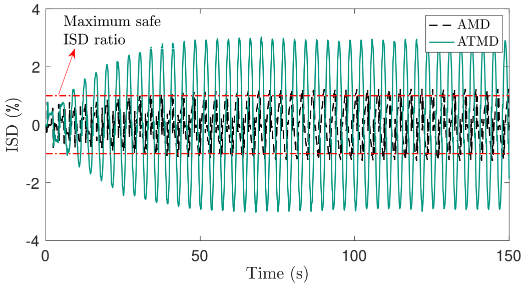
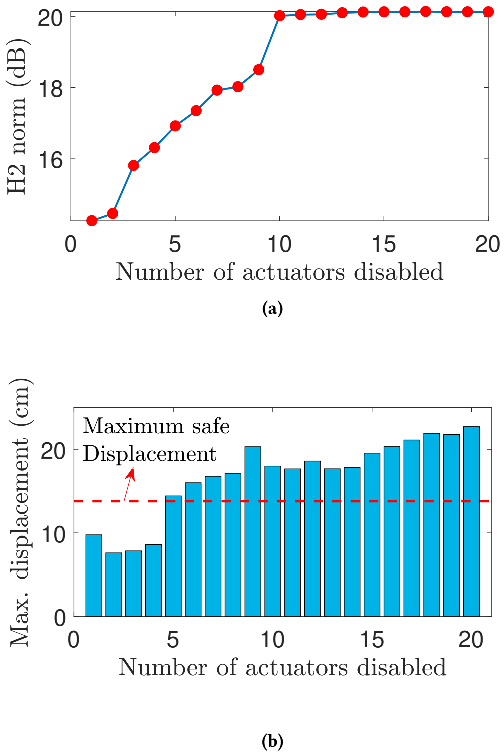


Figure 26: Time response of the roof ISD ratio during the FDI attack.

Fig. 26 reveals that the system has repeated oscillations over the maximum ISD ratio. This means that every additional oscillation will be even more damaging. While ISD ratios above 1% are achieved for only a few instants during an earthquake (even when a DoS attack is performed), values above 1% are achieved repeatedly during the FDI attack. Furthermore, this attack requires no external disturbance to generate damage to the structures. Consequently, for active dampers, an FDI attack poses a greater danger than a DoS attack.



(a)

(b)

Figure 27: (a) H_2 norm of the system for each k attacked actuators. (b) maximum displacement at mid-span when the attacker has blocked k signals from the designed DoS attack. The horizontal line indicates the 2% safety level, any higher displacement is dangerous for the bridge.

8 CASE STUDY: ATTACKING A BRIDGE WITH SEMI-ACTIVE DAMPERS

Our final case study investigates the effect of DoS attacks on a benchmark model from the ASCE community [2] to study the structural performance of a bridge with semi-active dampers subjected to historical earthquakes. Researchers have used this benchmark problem to test the performance of control algorithms in reducing vibrations and mitigate damage caused by seismic events [12, 45, 94]. The bridge is equipped with 20 MR fluid dampers with a maximum capacity of 1MN, nonlinear isolation bearings, and a sensor network capturing acceleration and displacement at the abutments and bent columns. Fig. 4 shows a plan view of this smart bridge. The control algorithm consists of an LQR algorithm as the primary controller that determines the command force and a clipped-optimal controller that defines the input voltages to the MR dampers.

Since bridges do not have different floors, we cannot use ISD to measure the impact of attacks. Instead, we use the maximum displacement at mid-span to evaluate safety [2]. In particular, we study the maximum displacement at mid-span for DoS during the Kobe earthquake [74]. We want to see if the attack exceeds the maximum safe displacement of 2% of the height of the bridge where potential spalling, a non-reparable damage on the columns of the bridge, starts to appear [93]

We use the optimization process in Eq. (2) again to design a DoS attack on the highway bridge, based on the linear mathematical model from [2]. Fig. 27 shows the H_2 norm of the system and the maximum displacement at mid-span for the DoS attack on the most damaging k actuators, from $k = 1$ to $k = 20$.

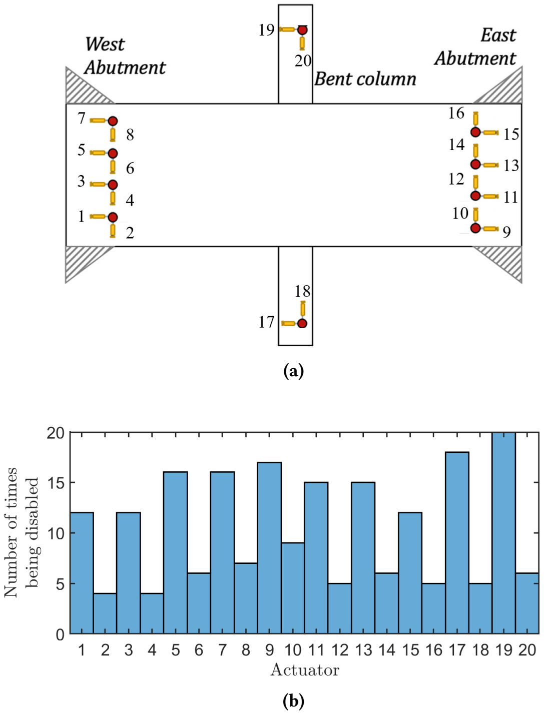


Figure 28: (a) Layout of the actuators on the bridge. (b) Actuators disabled for every designed attack with k ranging from 1 to 20.

Notice that only 5 disabled actuators are required to surpass the maximum safe displacement for this bridge. This information is important, because an attacker might not be able to attack every actuator. Fig. 28 shows the histogram of the number of times each actuator is disabled for the 20 DoS attacks. This shows that the mid-span displacement is heavily dependant on the horizontal actuators, more specifically actuators 17 and 19 located in the bent column of the bridge. This is another intuitive result, because the displacements in the horizontal direction are usually double the magnitude of the vertical direction on this particular bridge model and the design of the attacks identified this characteristic through the H_2 norm. Also, the actuators in the bent column are the most crucial because they support the mid-span of the bridge.

We again show that our attacks are optimal, with a comparison to other attacks that deactivate k=6 actuators at random, as shown in Fig. 29.

9 CONCLUSIONS

A structural control system is designed to reduce vibrations and tolerate uncertainties caused by variations in the structure, dynamic loads, or disturbances in the measurements and actuation signals [7, 25, 83]. However, to our knowledge, there are no studies that design and evaluate structural control systems in scenarios where the structure is subject to attacks. In this paper, we showed that simple disconnections of some of the actuators, or the injection of signals on the actuators at specific frequencies, magnitudes, and phases, may cause critical damage to the structure. This first look at attacks against structural control systems is a crucial step to define criteria for the design and evaluation of structural control systems that consider not only *robustness* in its common use, but also *resilience* to attacks.

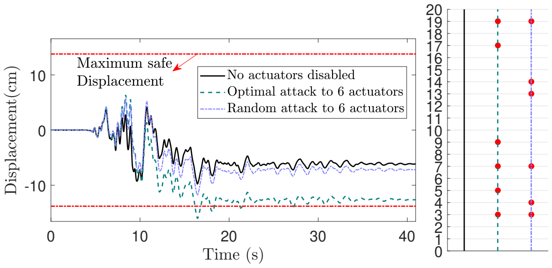


Figure 29: Comparison of response in time between the controlled bridge structure, the optimal attack, and a random selection for k=6.

As part of our contributions to this new area of inquiry, we (1) Propose a set of benchmarks to evaluate the security of structural control systems. Not only did we find and argue for the use of high-fidelity industry-approved simulations of buildings and bridges, but we also propose a set of standard earthquake models to consider in these studies. (2) Propose a set of metrics to measure the impact of attacks on buildings (ISD) and on bridges (maximum displacement and acceleration at mid-span). (3) Design two types of attacks (DoS and FDI) and show how their effects are better than other heuristic attacks (e.g., in the Quanser testbed, we showed how our proposed attack is better than others). (4) We start the discussion on unique defenses for these types of attacks. Based on our previous work on physics-based attack detection [9, 37, 72, 91], in Appendix C we design and test a new model-based attack detection tool that can identify both DoS and FDI attacks on actuators (or sensors). To detect attacks from the controller itself, we need an additional model of the control system.

This paper is the first type of research in this direction, and we hope it can motivate more work in this safety-critical system. Future work includes studying mitigation strategies such as redesigning the system when it is found vulnerable to our attacks and proposing attack-resilient-control algorithms.

ACKNOWLEDGEMENTS

This material is based on research sponsored by NSF CNS-1929410, 1929406, 1931573, and by the Air Force Research Laboratory under agreement number FA8750-19-2-0010. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

REFERENCES

[1] Ahmad Abdelrazaq. 2012. Validating the structural behavior and response of Burj Khalifa: Synopsis of the full scale structural health monitoring programs. *International Journal of High-Rise Buildings* 1, 1 (2012), 37–51.

[2] Anil Agrawal, Ping Tan, Satish Nagarajaiah, and Jian Zhang. 2009. Benchmark structural control problem for a seismically excited highway bridge—Part I: Phase I problem definition. *Structural Control and Health Monitoring: The Official Journal of the International Association for Structural Control and Monitoring and of the European Association for the Control of Structures* 16, 5 (2009), 509–529.

[3] David Alexander. 2018. *Natural disasters.* Routledge.

[4] Saurabh Amin, Alvaro A Cárdenas, and S Shankar Sastry. 2009. Safe and secure networked control systems under denial-of-service attacks. In *International Workshop on Hybrid Systems: Computation and Control.* Springer, 31–45.

[5] Saurabh Amin, Xavier Litrico, Shankar Sastry, and Alexandre M Bayen. 2013. Cyber security of water SCADA systems–part I: analysis and experimentation of stealthy deception attacks. *Control Systems Technology, IEEE Transactions on* 21, 5 (2013), 1963–1970.

[6] AP. 2017. Revenge Hacker: 34 Months, Must Repay Georgia-Pacific $1M. https://www.usnews.com/news/louisiana/articles/2017-02-16/revenge-hacker-34-months-must-repay-georgia-pacific-1m.

[7] Gary J Balas and John C Doyle. 1994. Robustness and performance trade-offs in control design for flexible structures. *IEEE Transactions on control systems technology* 2, 4 (1994), 352–361.

[8] Matt Burgess. 2017. Could hackers really take over a hotel? WIRED explains. *WIRED* (2017).

[9] Alvaro A Cárdenas, Saurabh Amin, Zong-Syun Lin, Yu-Lun Huang, Chi-Yen Huang, and Shankar Sastry. 2011. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM symposium on information, computer and communications security.* 355–366.

[10] S. Casciati and Z. Chen. 2012. An active mass damper system for structural control using real-time wireless sensors. *Structural Control and Health Monitoring* 19, 8 (2012), 758–767.

[11] Marco Caselli, Emmanuele Zambon, Johanna Amann, Robin Sommer, and Frank Kargl. 2016. Specification mining for intrusion detection in networked control systems. In *25th {USENIX} Security Symposium ({USENIX} Security 16).* 791–806.

[12] Young-Jin Cha and Anil K Agrawal. 2013. Decentralized output feedback polynomial control of seismically excited structures using genetic algorithm. *Structural Control and Health Monitoring* 20, 3 (2013), 241–258.

[13] Yuqi Chen, Christopher M Poskitt, and Jun Sun. 2018. Learning from mutants: Using code mutation to learn and monitor invariants of a cyber-physical system. In *2018 IEEE Symposium on Security and Privacy (SP).* IEEE, 648–660.

[14] Franklin Y Cheng, Hongping Jiang, and Kangyu Lou. 2008. *Smart structures: innovative systems for seismic response control.* CRC press.

[15] Anton Cherepanov. 2017. Win32/Industroyer, A new threat for industrial control systems. *White Paper. ESET* (2017).

[16] Hongjun Choi, Wen-Chuan Lee, Yousra Aafer, Fan Fei, Zhan Tu, Xiangyu Zhang, Dongyan Xu, and Xinyan Deng. 2018. Detecting Attacks Against Robotic Vehicles: A Control Invariant Approach. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security* (Toronto, Canada) *(CCS '18).* ACM, New York, NY, USA, 801–816.

[17] Richard Christenson, Yi Zhong Lin, Andrew Emmons, and Brent Bass. 2008. Large-scale experimental verification of semiactive control through real-time hybrid simulation. *Journal of Structural Engineering* 134, 4 (2008), 522–534.

[18] Pierre Ciholas, Aidan Lennie, Parvin Sadigova, and Jose M Such. 2019. The security of smart buildings: a systematic literature review. *arXiv preprint arXiv:1901.05837* (2019).

[19] Cong Cong. 2019. Using active tuned mass dampers with constrained stroke to simultaneously control vibrations in wind turbine blades and tower. *Advances in Structural Engineering* 22, 7 (2019), 1544–1553.

[20] Jerome Connor and Simon Laflamme. 2014. *Applications of Active Control.* Springer International Publishing, Cham, 347–386. https://doi.org/10.1007/978-3-319-06281-5_7

[21] Jerome Connor and Simon Laflamme. 2014. *Structural motion engineering.* Springer.

[22] Soodeh Dadras, Ryan M Gerdes, and Rajnikant Sharma. 2015. Vehicular platooning in an adversarial environment. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security.* ACM, 167–178.

[23] Austin Downey, Liang Cao, Simon Laflamme, Douglas Taylor, and James Ricles. 2016. High capacity variable friction damper based on band brake technology. *Engineering Structures* 113 (apr 2016), 287–298. https://doi.org/10.1016/j.engstruct.2016.01.035

[24] Austin Downey, Connor Theisen, Heather Murphy, Nicholas Anastasi, and Simon Laflamme. 2019. Cam-based passive variable friction device for structural control. *Engineering Structures* 188 (jun 2019), 430–439. https://doi.org/10.1016/j.engstruct.2019.03.032

[25] John Doyle and Gunter Stein. 1981. Multivariable feedback design: Concepts for a classical/modern synthesis. *IEEE transactions on Automatic Control* 26, 1 (1981), 4–16.

[26] Raj Gautam Dutta, Feng Yu, Teng Zhang, Yaodan Hu, and Yier Jin. 2018. Security for safety: a path toward building trusted autonomous vehicles. In *Proceedings of the International Conference on Computer-Aided Design.* ACM, 92.

[27] Shirley J Dyke, Juan Martin Caicedo, Gursoy Turan, Lawrence A Bergman, and Steven Hague. 2003. Phase I benchmark control problem for seismic response of cable-stayed bridges. *Journal of Structural Engineering* 129, 7 (2003), 857–872.

[28] Shirley J Dyke, BF Spencer Jr, MK Sain, and JD Carlson. 1996. Modeling and control of magnetorheological dampers for seismic response reduction. *Smart materials and structures* 5, 5 (1996), 565.

[29] Omar El-Khoury, Abdollah Shafieezadeh, and Ehsan Fereshtehnejad. 2018. A risk-based life cycle cost strategy for optimal design and evaluation of control methods for nonlinear structures. *Earthquake Engineering & Structural Dynamics* 47, 11 (2018), 2297–2314.

[30] Josué Enríquez-Zárate, Hugo Francisco Abundis-Fong, Ramiro Velázquez, and Sebastián Gutiérrez. 2019. Passive vibration control in a civil structure: Experimental results. *Measurement and Control* 52, 7-8 (2019), 938–946. https://doi.org/10.1177/0020294019847715 arXiv:https://doi.org/10.1177/0020294019847715

[31] Herson Esquivel-Vargas, Marco Caselli, and Andreas Peter. 2017. Automatic deployment of specification-based intrusion detection in the BACnet protocol. In *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy.* 25–36.

[32] Davide Fauri, Michail Kapsalakis, Daniel Ricardo dos Santos, Elisa Costante, Jerry den Hartog, and Sandro Etalle. 2018. Leveraging semantics for actionable intrusion detection in building automation systems. In *International Conference on Critical Information Infrastructures Security.* Springer, 113–125.

[33] André Filiatrault. 2013. *Elements of earthquake engineering and structural dynamics.* Presses inter Polytechnique.

[34] Kevin Fu and Wenyuan Xu. 2018. Risks of trusting the physics of sensors. *Commun. ACM* 61, 2 (2018), 20–23.

[35] R Fukuda and H Kurino. 2017. Highly efficient semi-active oil damper for structural control with energy recovery system. In *Proceedings of the 16th World Conference on Earthquake Engineering.*

[36] Ilias Giechaskiel and Kasper Bonne Rasmussen. 2019. Sok: Taxonomy and challenges of out-of-band signal injection attacks and defenses. *arXiv preprint arXiv:1901.06935* (2019).

[37] Jairo Giraldo, David Urbina, Alvaro Cardenas, Junia Valente, Mustafa Faisal, Justin Ruths, Nils Ole Tippenhauer, Henrik Sandberg, and Richard Candell. 2018. A survey of physics-based attack detection in cyber-physical systems. *ACM Computing Surveys (CSUR)* 51, 4 (2018), 1–36.

[38] Gene H Golub and Christian Reinsch. 1971. Singular value decomposition and least squares solutions. In *Linear Algebra.* Springer, 134–151.

[39] Yongqiang Gong, Liang Cao, Simon Laflamme, Spencer Quiel, James Ricles, and Douglas Taylor. 2018. Characterization of a novel variable friction connection for semiactive cladding system. *Structural Control and Health Monitoring* 25, 6 (2018), e2157.

[40] Andy Greenberg. 2020. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers.* Anchor.

[41] Michael A Grubb, Kenneth E Wilson, Christopher D White, William N Nickas, et al. 2015. *Load and resistance factor design (lrfd) for highway bridge superstructures-reference manual.* Technical Report. National Highway Institute (US).

[42] Mariantonieta Gutierrez Soto and Hojjat Adeli. 2013. Tuned mass dampers. *Archives of Computational Methods in Engineering* 20, 4 (2013), 419–431.

[43] Mariantonieta Gutierrez Soto and Hojjat Adeli. 2017. Multi-agent replicator controller for sustainable vibration control of smart structures. *Journal of Vibroengineering* 19 (2017), 4300–4322.

[44] Mariantonieta Gutierrez Soto and Hojjat Adeli. 2017. Recent advances in control algorithms for smart structures and machines. *Expert Systems* 34, 2 (2017), e12205.

[45] Mariantonieta Gutierrez Soto and Hojjat Adeli. 2019. Semi-active vibration control of smart isolated highway bridge structures using replicator dynamics. *Engineering Structures* 186 (2019), 536–552.

[46] Eman Hammad, Ahmed M. Khalil, Abdallah Farraj, Deepa Kundur, and Reza Iravani. 2015. Tuning out of phase: Resonance attacks. In *2015 IEEE International Conference on Smart Grid Communications (SmartGridComm).* 491–496. https://doi.org/10.1109/SmartGridComm.2015.7436348

[47] Masahiko Higashino, Satoru Aizawa, Masashi Yamamoto, and Kotaro Toyama. 1998. Application of active mass damper (AMD) system, and earthquake and wind observation results. In *Proceedings of the 2nd World Conference on Structural Control*, Vol. 1. 783–794.

[48] GWea Housner, Lawrence A Bergman, T Kf Caughey, Anastassios G Chassiakos, Richard O Claus, Sami F Masri, Robert E Skelton, TT Soong, BF Spencer, and James TP Yao. 1997. Structural control: past, present, and future. *Journal of engineering mechanics* 123, 9 (1997), 897–971.

[49] Yu-Lun Huang, Alvaro A Cárdenas, Saurabh Amin, Zong-Syun Lin, Hsin-Yi Tsai, and Shankar Sastry. 2009. Understanding the physical and economic consequences of attacks on control systems. *International Journal of Critical Infrastructure Protection* 2, 3 (2009), 73–83.

[50] Yoshiki Ikeda, Masashi Yamamoto, Takeshi Furuhashi, and Haruhiko Kurino. 2019. Recent research and development of structural control in Japan. *JAPAN ARCHITECTURAL REVIEW* 2, 3 (2019), 219–225. https://doi.org/10.1002/2475-8876.12081 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/2475-8876.12081

[51] Structural Engineering Institute. 2016. *Minimum design loads for buildings and other structures*. American Society of Civil Engineers.

[52] Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker, and Christopher Glyer. 2017. Attackers Deploy New ICS Attack Framework" TRITON" and Cause Operational Disruption to Critical Infrastructure. *Threat Research Blog* (2017).

[53] Kiyoshi Kanai. 1957. Semi-empirical formula for the seismic characteristics of the ground. *Bulletin of the Earthquake Research Institute, University of Tokyo* 35, 2 (1957), 309–325.

[54] Marina Krotofil, Alvaro Cardenas, Jason Larsen, and Dieter Gollmann. 2014. Vulnerabilities of cyber-physical systems to stale data?Determining the optimal time to launch attacks. *International journal of critical infrastructure protection* 7, 4 (2014), 213–232.

[55] Haruhiko Kurino, Jun Tagami, Kan Shimizu, and Takuji Kobori. 2003. Switching oil damper with built-in controller for structural control. *Journal of Structural Engineering* 129, 7 (2003), 895–904.

[56] Alberto Lago, Hadi Moghadasi Faridani, and Dario Trabucco. 2018. Damping Technologies for Tall Buildings. *CTBUH Journal* 3 (2018).

[57] S. Lamb and K.C.S. Kwok. 2019. The effects of motion sickness and sopite syndrome on office workers in an 18-month field study of tall buildings. *Journal of Wind Engineering and Industrial Aerodynamics* 186 (2019), 105 – 122. https://doi.org/10.1016/j.jweia.2019.01.004

[58] S. Lamb, K.C.S. Kwok, and D. Walton. 2013. Occupant comfort in wind-excited tall buildings: Motion sickness, compensatory behaviours and complaint. *Journal of Wind Engineering and Industrial Aerodynamics* 119 (2013), 1 – 12. https://doi.org/10.1016/j.jweia.2013.05.004

[59] Yao Liu, Peng Ning, and Michael K Reiter. 2009. False data injection attacks against state estimation in electric power grids. In *Proceedings of the conference on Computer and communications security (CCS)*. ACM, 21–32.

[60] Jerome Peter Lynch. 1998. Active structural control research at Kajima Corporation. *The National Science Foundation's Summer Institute in Japan Program, Research Project* 17 (1998), 11.

[61] J. P. Lynch, Y. Wang, R. A. Swartz, K. C. Lu, and C. H Loh. 2008. Implementation of a closed-loop structural control system using wireless sensor networks. *Structural Control and Health Monitoring* 15, 4 (2008), 518–539.

[62] Lee Mathews. 2016. Hackers use DDoS attack to cut heat to apartments. *Forbes* (2016).

[63] Stephen McLaughlin. 2013. CPS: Stateful Policy Enforcement for Control System Device Usage. In *Proceedings of the 29th Annual Computer Security Applications Conference* (New Orleans, Louisiana, USA) *(ACSAC '13)*. ACM, New York, NY, USA, 109–118.

[64] Laura Micheli, Alice Alipour, Simon Laflamme, and Partha Sarkar. 2019. Performance-based design with life-cycle cost assessment for damping systems integrated in wind excited tall buildings. *Engineering Structures* 195 (2019), 438–451.

[65] Satomi Nakanishi and K. Taira. 2010. Study on cost reduction by seismic isolation bearing and vibration control device for the bridge. In *Proceedings of the IABSE-JSCE Joint Conference on Advances in Bridge Engineering-II*.

[66] Y. Q. Ni and H. F. Zhou. 2010. Guangzhou new TV tower: Integrated structural health monitoring and vibration control. In *Structures Congress 2010*. https://doi.org/10.1061/41130(369)283

[67] Y Ohtori, RE Christenson, BF Spencer Jr, and SJ Dyke. 2004. Benchmark control problems for seismically excited nonlinear buildings. *Journal of engineering mechanics* 130, 4 (2004), 366–385.

[68] William N Patten. 1997. *Semiactive vibration absorbers (SAVA) at the I-35 Walnut Creek bridge (FHWA-OK-97-08) 2125*. Technical Report.

[69] William Neff Patten, Jinghui Sun, and Gang Song. 1998. Prototype Testing of Intelligent Stiffener for Bridges at I-35 Walnut Creek Bridge. *Transportation Research Record* 1624, 1 (1998), 160–165. https://doi.org/10.3141/1624-19 arXiv:https://doi.org/10.3141/1624-19

[70] Matthew Peacock, Michael N Johnstone, and Craig Valli. 2017. An exploration of some security issues within the BACnet protocol. In *International Conference on Information Systems Security and Privacy*. Springer, 252–272.

[71] Jonathan Petit, Bas Stottelaar, Michael Feiri, and Frank Kargl. 2015. Remote attacks on automated vehicles sensors: Experiments on camera and lidar. (2015).

[72] Raul Quinonez, Jairo Giraldo, Luis Salazar, Erick Bauman, Alvaro Cardenas, and Zhiqiang Lin. 2020. {SAVIOR}: Securing Autonomous Vehicles with Robust Physical Invariants. In *29th {USENIX} Security Symposium ({USENIX} Security 20)*. 895–912.

[73] Francesco Ricciardelli, A David Pizzimenti, and Massimiliano Mattei. 2003. Passive and active mass damper control of the response of tall buildings to wind gustiness. *Engineering structures* 25, 9 (2003), 1199–1209.

[74] Andreas Rietbrock. 2001. P wave attenuation structure in the fault area of the 1995 Kobe earthquake. *Journal of Geophysical Research: Solid Earth* 106, B3 (2001), 4141–4154.

[75] Fahim Sadek, Bijan Mohraz, Andrew W Taylor, and Richard M Chung. 1997. A method of estimating the parameters of tuned mass dampers for seismic applications. *Earthquake Engineering & Structural Dynamics* 26, 6 (1997), 617–635.

[76] Jayaprakash Selvaraj, Gökçen Y Dayanıklı, Neelam Prabhu Gaunkar, David Ware, Ryan M Gerdes, Mani Mina, et al. 2018. Electromagnetic induction attacks against embedded systems. In *Proceedings of the 2018 on Asia Conference on Computer and Communications Security*. ACM, 499–510.

[77] CHARLESTON SEMINAR. 1997. NEHRP Guidelines for the Seismic Rehabilitation of Buildings (FEMA 273). (1997).

[78] Christian E Silva, Daniel Gomez, Amin Maghareh, Shirley J Dyke, and Billie F Spencer Jr. 2020. Benchmark control problem for real-time hybrid simulation. *Mechanical Systems and Signal Processing* 135 (2020), 106381.

[79] Jill Slay and Michael Miller. 2007. Lessons Learned from the Maroochy Water Breach. In *Critical Infrastructure Protection*, Vol. 253/2007. Springer Boston, 73–82.

[80] Adam Smith. 2020. 2010-2019: A Landmark Decade of US Billion-Dollar Weather and Climate Disasters| NOAA Climate. Gov. *Climate. Gov* 9 (2020).

[81] I. Solomon, J. Cunnane, and P. Stevenson. 2000. Large-scale structural monitoring systems. *Nondestructive Evaluation of Highways, Utilities, and Pipelines IV* 3995 (2000), 281–303.

[82] Yun Mok Son, Ho Cheol Shin, Dong Kwan Kim, Young Seok Park, Ju Hwan Noh, Ki Bum Choi, Jung Woo Choi, and Yong Dae Kim. 2015. Rocking drones with intentional sound noise on gyroscopic sensors. In *24th USENIX Security symposium*. USENIX Association.

[83] BF Spencer Jr, MK Sain, C-H Won, DC Kaspari, and PM Sain. 1994. Reliability-based measures of structural control robustness. *Structural safety* 15, 1-2 (1994), 111–129.

[84] B. F. Spencer Jr., R. E. Christenson, and S. J. Dyke. 1998. Next generation benchmark control problem for seismically excited buildings. *Second World Conference on Structural Control* (1998), 1135–1360.

[85] H Tajimi. 1960. A statistical method of determining the maximum response of a building structure during an earthquake. 2nd WCEE. *Tokyo, Japan* (1960).

[86] Rui Tan, Varun Badrinath Krishna, David KY Yau, and Zbigniew Kalbarczyk. 2013. Impact of integrity attacks on real-time pricing in smart grids. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 439–450.

[87] Bungale S Taranath. 2016. *Structural analysis and design of tall buildings: Steel and composite construction*. CRC press.

[88] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. 2012. Revealing stealthy attacks in control systems. In *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*. 1806–1813. https://doi.org/10.1109/Allerton.2012.6483441

[89] Yazhou Tu, Zhiqiang Lin, Insup Lee, and Xiali Hei. 2018. Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors. In *27th {USENIX} Security Symposium ({USENIX} Security 18)*. 1545–1562.

[90] FE Udwadia and MD Trifunac. 1973. Comparison of earthquake and microtremor ground motions in El Centro, California. *Bulletin of the Seismological Society of America* 63, 4 (1973), 1227–1253.

[91] David Urbina, Jairo Giraldo, Alvaro A. Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, and Henrik Sandberg. 2016. Limiting The Impact of Stealthy Attacks on Industrial Control Systems. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*. https://doi.org/10.1145/2976749.2978388

[92] David I Urbina, Jairo A Giraldo, Alvaro A Cardenas, Nils Ole Tippenhauer, Junia Valente, Mustafa Faisal, Justin Ruths, Richard Candell, and Henrik Sandberg. 2016. Limiting the impact of stealthy attacks on industrial control systems. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1092–1105.

[93] Marc Veletzos, Mario Panagiutou, Jose Restrepo, Stephen Sahs, et al. 2008. *Visual inspection & capacity assessment of earthquake damaged reinforced concrete bridge elements*. Technical Report. California. Dept. of Transportation. Division of Research and Innovation.

[94] Nengmou Wang and Hojjat Adeli. 2015. Self-constructing wavelet neural network algorithm for nonlinear control of large structures. *Engineering Applications of Artificial Intelligence* 41 (2015), 249–258.

[95] Xiaolong Wang, Richard Habeeb, Xinming Ou, Siddharth Amaravadi, John Hatcliff, Masaaki Mizuno, Mitchell Neilsen, S Raj Rajagopalan, and Srivatsan Varadarajan. 2017. Enhanced security of building automation systems through microkernel-based controller platforms. In *2017 IEEE 37th International Conference on Distributed Computing Systems Workshops (ICDCSW)*. IEEE, 37–44.

[96] Xiaolong Wang, Masaaki Mizuno, Mitch Neilsen, Xinming Ou, S Raj Rajagopalan, Will G Boldwin, and Bryan Phillips. 2015. Secure rtos architecture for building

automation. In *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy*. 79–90.

[97] Yang Wang, Jerome P. Lynch, and Kincho H. Law. 2009. Decentralized H_∞ controller design for large-scale civil structures. *Earthquake Engineering and Structural Dynamics* (2009). https://doi.org/10.1002/eqe.862

[98] Yong Wang, Zhaoyan Xu, Jialong Zhang, Lei Xu, Haopei Wang, and Guofei Gu. 2014. Srid: State relation based intrusion detection for false data injection attacks in scada. In *European Symposium on Research in Computer Security*. Springer, 401–418.

[99] Felix Weber, Hans Distl, Sebastian Fischer, and Christian Braun. 2016. MR damper controlled vibration absorber for enhanced mitigation of harmonic vibrations. *Actuators* 5, 4 (2016), 27.

[100] Yongdong Wu, Zhuo Wei, Jian Weng, Xin Li, and Robert H. Deng. 2018. Resonance Attacks on Load Frequency Control of Smart Grids. *IEEE Transactions on Smart Grid* 9, 5 (2018), 4490–4502. https://doi.org/10.1109/TSG.2017.2661307

[101] H. B. Xu, C. W. Zhang, H. Li, P. Tan, J. P. Ou, and F. L. Zhou. 2014. Wind induced vibration characteristics and model updating of Canton Tower structure. *Smart Structures and Systems* 13, 2 (2014), 281–303.

[102] Masashi Yamamoto and Takayuki Sone. 2014. Behavior of active mass damper (AMD) installed in high-rise building during 2011 earthquake off Pacific coast of Tohoku and verification of regenerating system of AMD based on monitoring. *Structural Control and Health Monitoring* 21, 4 (2014), 634–647.

[103] Fu Yi, Shirley J Dyke, Juan M Caicedo, and J David Carlson. 2001. Experimental verification of multiinput seismic control strategies for smart dampers. *Journal of Engineering Mechanics* 127, 11 (2001), 1152–1164.

[104] Kim Zetter. 2013. Researchers hack building control system at google australia office. *Wired. com, available at https://www. wired. com/2013/05/googles-control-system-hacked (accessed 9th June, 2017)* (2013).

[105] K Zetter. 2013. Vulnerability lets hackers control building locks, electricity, elevators and more. *WIRED, Boone, IA, USA, Feb* 6 (2013).

[106] Kim Zetter. 2014. *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon.* Broadway books.

[107] Kemin Zhou, John Comstock Doyle, Keith Glover, et al. 1996. *Robust and optimal control.* Vol. 40. Prentice hall New Jersey.

A STRUCTURE'S EQUATION OF MOTION

We can model the frame shown in Fig.30a as the simple, dynamically equivalent model shown in Fig. 30b. In this model, the lateral stiffness of the columns is modeled by the spring (k), the damping is modeled by the shock absorber (c) and the mass of the floor is modeled by the mass (m). Figure 30c shows the free body diagram of the structure. The forces include the spring force $f_s(t)$, the damping force $f_d(t)$, the external dynamic load on the structure $p(t)$, and the inertial force $f_i(t)$. These forces are defined as:

$$f_s = kq(t) \qquad f_d = c\dot{q}(t) \qquad f_i = m\ddot{q}(t) \tag{5}$$

where $\dot{q}(t)$ is the first derivative of the displacement with respect to time (velocity) and $\ddot{q}(t)$ is the second derivative of the displacement with respect to time (acceleration). Summing the forces shown in Figs. 30b and c, we obtain the following:

$$\sum F = m\ddot{q}(t) = p(t) - c\dot{q}(t) - kq(t) \tag{6}$$

Translating this concept to a multiple degree of freedom and its equivalent dynamic model is shown in Fig. 31, with n-degrees of freedom subjected to m_1 external excitation and m_2 controlling devices, we obtain the following expression:

$$\mathbf{M}\mathbf{q}(t) + \mathbf{C}\mathbf{q}(t) + \mathbf{K}\mathbf{q}(t) = \mathbf{T_u}\mathbf{u}(t) + \mathbf{T_p}\mathbf{p(t)} \tag{7}$$

where $\mathbf{q}(t) \in \mathbb{R}^{n\times 1}$ is the displacement vector relative to the ground, $\mathbf{M}, \mathbf{C}, \mathbf{K} \in \mathbb{R}^{n\times n}$ are the mass, damping, and stiffness matrices, respectively; $\mathbf{u}(t) \in \mathbb{R}^{m_2\times 1}$ is the control force vector; $\mathbf{T_u} \in \mathbb{R}^{n\times m_2}$ and $\mathbf{T_w} \in \mathbb{R}^{n\times m_1}$ are the control and excitation location matrices, respectively. In terms of calculating the inter-story drift (ISD), the displacement is shown Fig. 31 and the calculated inter-story drift is determined by $\Delta_2 = (q_2 - q_1)$ with the inter-story drift ratio computed as, $\Delta_{r2} = (q_2 - q_1)/h_2$ and $\Delta_{r1} = q_1/h_1$. In the case of the building subjected to seismic loading, the spatial load pattern vector $\mathbf{T_p}$ is equal to $-\mathbf{M}\left\{\bar{\mathbf{I}}\right\}_{n\times 1}\ddot{q}_g(t)$ where the external excitation $\ddot{q}_g(t)$ is the ground acceleration time history. Chen et al. [14] and Connor and Laflamme[21] provide additional information of the mathematical derivation of buildings equipped with control devices.

B MODEL OF QUANSER'S BENCH-SCALE TESTBED

The state variables that define the mathematical representation of the structure according to Equation (1) are chosen to be: (i) the position of the moving cart at story 1 x_{c1}, (ii) the position of the moving cart of floor 2 x_{c2}, (iii) displacement at story 1 x_{f1}, (iv) displacement at story 2 x_{f2}, (v) velocity of cart 1 $\dot{x}_{c1}$, (vi) velocity of cart 2 $\dot{x}_{f2}$, (vii) velocity of story 1 relative to the ground $\dot{x}_{f1}$, and (viii) velocity of story 2 relative to the ground $\dot{x}_{f2}$. These are the variables that are considered to provide information about the state of the structure. The output vector $\mathbf{z}$ corresponds to the inter-story drifts $\Delta x_{f1} = x_{f1}$ and $\Delta x_{f2} = x_{f2} - x_{f1}$. The state-space vector of the plant is given by

$$\mathbf{x} = \begin{bmatrix} x_{c1} & x_{c2} & x_{f1} & x_{f2} & \dot{x}_{c1} & \dot{x}_{c2} & \dot{x}_{f1} & \dot{x}_{f2} \end{bmatrix}^T .$$

The parameters of the state-space representation of the structure in Equation (1) are:

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 87.61 & -43.73 & 30.09 & 0 & 0 \\ 0 & 0 & 0 & 87.60 & 30.09 & -43.73 & 0 & 0 \\ 0 & 0 & -66.41 & 66.41 & 0 & 0 & 0 & 0 \\ 0 & 0 & 66.41 & -140.89 & 2.64 & 2.64 & 0 & 0 \end{bmatrix},$$

$$\mathbf{B} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 7.2714 & -5.6968 \\ -5.6968 & 7.2714 \\ 0 & 0 \\ -0.4078 & -0.4078 \end{bmatrix}, \quad \mathbf{E} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 0 \\ -1 \\ 0 \end{bmatrix}.$$

Matrix $\mathbf{F}$ is chosen to compute the inter-story drift for each floor:

$$\mathbf{F} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

The feedback control gain used to define the control strategy is computed using the LQR method and is given by $\mathbf{R}$ as follows:

$$\mathbf{R} = \begin{bmatrix} 7.0244 & -0.8110 & 42.2172 & -80.4384 \\ 0.3627 & 3.1414 & 8.8323 & -14.0781 \end{bmatrix.$$
$$\begin{matrix} -0.1108 & -0.2989 & -1.1316 & -11.8019 \\ 0.0319 & 0.0874 & 0.0148 & -2.2558 \end{matrix}\Bigg]$$

Here, the control action is defined by the feedback gain $\mathbf{u} = -\mathbf{R}\mathbf{x}$ to reduce the effect vibrations on the structure.

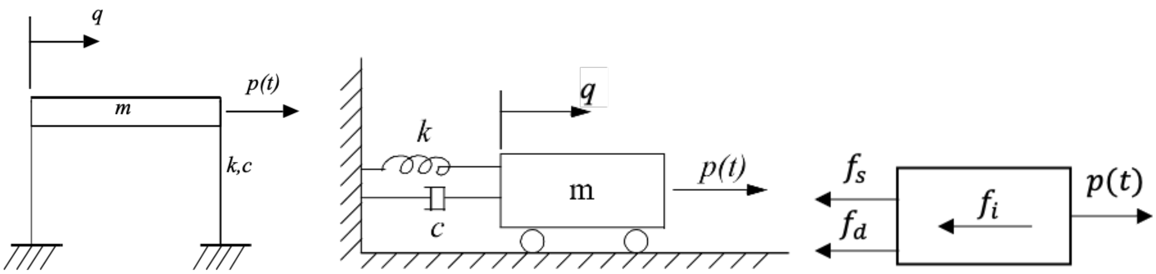


Figure 30: a) Single degree of freedom structure, b) Mass with spring and damper, c) Free Body Diagram

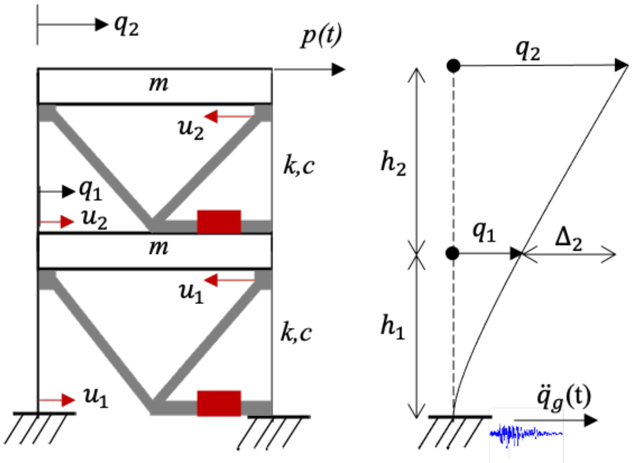


Figure 31: Two-degree of freedom structure with an active bracing system equipped with 2 hydraulic actuators

C DEFENSES

We have seen that attacks against structural control systems can pose significant damages. Therefore in this section we start the discussion on potential defenses to attacks against structural control systems. In particular, we focus on how to detect these attacks.

Taking advantage of the physical model of the system, it is possible to construct an independent reference monitor that uses existing or redundant sensor measurements (e.g., place additional vibration sensors in an independent network) to estimate the sensor measurements $\hat{y}$ and compute a residual $r = y^a - \hat{y}$ comparing how the system should be behaving with what we measure. This type of approach has been widely studied in the literature, [37, 92] and we can adapt these defenses to civil structures.

These detectors can determine if sensors or actuators are under attack. To detect the attack, the measurements obtained with the sensors are compared with our expected estimate of the behavior of the system. When a historical difference between those values is large, we raise an alert.

It is easier to keep track of anomalies in discrete time [37], therefore we use a discrete version of the Luenberger observer to estimate the system states. The state estimation $\hat{\mathbf{x}}$ and the output estimation $\hat{\mathbf{z}}$ are given by,

$$\hat{\mathbf{x}}[k+1] = \mathbf{A}^d\hat{\mathbf{x}}[k] + \mathbf{B}^d\mathbf{u}[k] + \mathbf{L}(\mathbf{z}[k] - \mathbf{F}^d\hat{\mathbf{x}}[k])$$
$$\hat{\mathbf{z}}[k] = \mathbf{F}^d\hat{\mathbf{x}}[k],$$

where $\mathbf{A}^d$, $\mathbf{B}^d$, and $\mathbf{F}^d$ are a discrete version of the system in Eq. (1), $\mathbf{L}$ is matrix selected such that the eigenvalues of $\mathbf{A}^d - \mathbf{L}\mathbf{F}^d$ are inside the unit circle, and $\hat{\mathbf{x}}[0]$ is the initial condition of the estimator.

The difference between what we expect and what we measure is called a residue $\mathbf{r}[k]$:

$$r_i[k] = |z_i[k] - \hat{z}_i[k]|,$$

where z_i refers to the measurement obtained with the i^{th} sensor, and $\hat{z}_i$ refers to the estimation of the i^{th} output.

When the system is under attack, the residues $\mathbf{r}$ are large. To determine if such difference is large enough to raise an alarm, we use the non-parametric cumulative sum (CUSUM). Unlike other tests, the CUSUM considers not only the current residue but also the historical behavior of the residues. We select this detector because it outperforms other statistics [92]. For the CUSUM, we define a new statistic for each sensor $S_i[k]$, which is given by,

$$S_i[k+1] = \max\{0, S_i[k] + r_i[k] - b_i\},$$

where $S_i[0] = 0$, and $b_i > 0$ is selected to prevent that statistic increases without attack. The parameter is tuned such that, in a scenario without attack,

$$\mathbb{E}[r_i[k] - b_i] < 0,$$

where $\mathbb{E}[\cdot]$ is the expected value. An alarm is raised for the i^{th} sensor when the statistic exceeds a threshold $S_i[k] > \tau_i$, $\tau_i > 0$. Commonly, the statistic is reset to zero $S_i[k+1] = 0$ once an alarm is raised. However, for illustration purposes, we will not reset the CUSUM in the results of this section. The selection of the parameter τ_i is a trade-off between the time taken to detect an attack and the false alarm rate: a large threshold will give us low false alarms, but then, the time to detect an attack will increase. A block diagram that summarizes the anomaly detection strategy is presented in Fig. 32.

We study the performance of this defense in the 20-story building with an ATMD.

One of our unanticipated challenges of using a model-based anomaly detection in structural control, is that the system generates false alarms whenever there is an earthquake, as seen in Fig. 33a. So if a DoS attack is launched during an earthquake, it would be

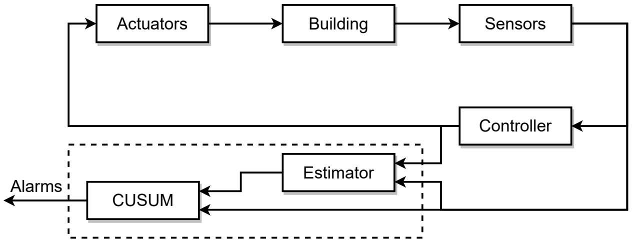
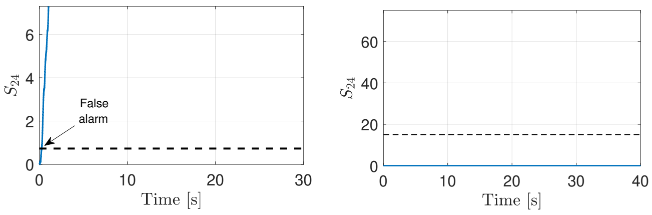


Figure 32: Model-based anomaly detection.

impossible to determine if the alert is the result of an attack or the earthquake.

To address this problem, we need to measure ground seismic signals. Fortunately, seismic waves can be recorded with seismographs and their size or intensity can be estimated using the Moment magnitude or the Richter scale. Most structural health monitoring systems include an accelerometer installed in the ground to capture earthquake signals in real time and trigger the control system. These accelerometers can be digital seismographs or the same type of sensors used inside the structure [20].



(a)

(b)

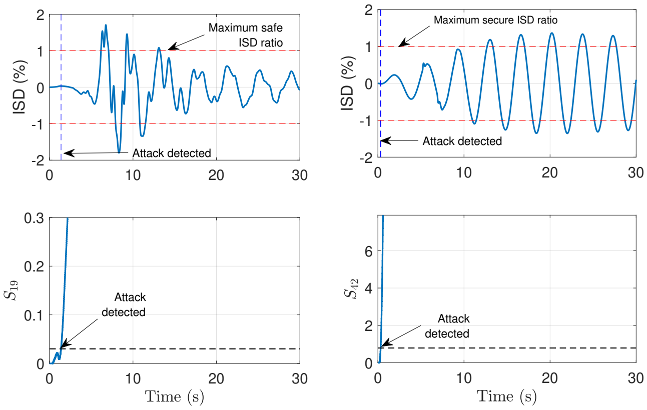
Figure 33: Anomaly detection statistic when there is no attack but during an earthquake for a) a detector that does not consider the earthquake and b) a detector that considers the earthquake.

With earthquake measurements, we need to select the discretization time to ensure that the earthquake is properly sampled. Since the maximum frequency of an earthquake is 10 Hz, we select a sampling time of $T_s = 0.01\,s$.

With this new system, the estimator receives a noisy version of the earthquake instead of the actual signal. For this new detector, the CUSUM parameters are tuned by generating different earthquakes using the Kanai-Tajimi model for each of the one thousand simulations used to tune the CUSUM.Fig. 33b shows the CUSUM for this new detector during El Centro earthquake.

We now consider the performance of this attack-detector when facing a DoS attack during an earthquake, and an FDI attack without an earthquake. The results of those scenarios are presented in Figs. 34a and 34b, respectively. Our system detects the DoS attack at time 4.78 s before the ISD ratio reaches 1% (that is, the attack is detected before they damage the structure). We detect an FDI attack even faster and well before any damage to the system.

To sum up, model-based anomaly detection algorithms can be used to detect both, DoS and FDI attacks to structural control systems; however, we need to measure the earthquake during a DoS attack (in addition to measuring the control and sensor signals from all other floors).



(a)

(b)

Figure 34: Detection of the a) DoS and b) FDI attacks using a detector that considers the disturbances.