sciendo

*Transport and Telecommunication, 2025, volume 26, no. 3, 250-265*
*Transport and Telecommunication Institute, Lauvas 2, Riga, LV-1019, Latvia*
*DOI 10.2478/ttj-2025-0019*

# A VEHICULAR CYBER-PHYSICAL FRAMEWORK FOR STUDYING THE EFFECTS OF MULTIPLE DISTURBANCES WITH APPLICATION TO CONNECTED AUTONOMOUS VEHICLES

***Amir Mohammed, Lincoln Marine, Craig Ramlal, Fasil Muddeen***

*The University of the West Indies, Department of Electrical and Computer Engineering*
*St. Augustine, Trinidad and Tobago*
*STA-Electrical.Engineering@sta.uwi.edu*

Cyber-physical systems (CPSs) are considered a new era of complex systems that harness the integration of computational and physical capabilities to facilitate interactions between humans via different mediums, creating systems that are smarter and more efficient. These systems underpin critical infrastructures (CIs), which require coordination to achieve societal functions. However, the exponential growth of CPSs brings about a new challenge as it relates to the security of such systems and by extension any disturbances which might affect their operation. Inherently, CPSs are sophisticated systems comprising several subsystems, integrated to facilitate functionality. Thus, creating a situation whereby different vulnerabilities may be present, leading to potential cyberattacks. Cyberattacks have become prevalent and complex within society, leading to loss of resources or worse life-threatening events. The authors propose a Vehicular Cyber Physical System (VCPS) framework for studying the effects of Cyberattacks, Communication Impairments, and Sensor Faults with application to Connected Autonomous Vehicles (CAVs). The proposed framework can be used for understanding the effects of multiple disturbances on platooning and by extension serves as a good platform for the development of resilient control strategies.

**Keywords:** Cyberattacks, connected autonomous vehicles, cyber physical systems, sensor faults, transportation system

## 1. Introduction

Cyber-Physical Systems (CPSs) are complex systems integrating computation, communication, and control, collectively known as 3C technology (Liu *et al.,* 2017). Their rapid development and deployment in recent years have led to widespread applications across critical infrastructures such as power grids, oil and gas distribution, telecommunications, and intelligent vehicles (Baheti and Gill, 2011). A popular application is Vehicular Cyber-Physical Systems (VCPS), which support real-time, safe, and dynamic vehicle collaboration, making them an integral part of modern transportation systems. Advancements in sensors, subsystems, and driver assistance technologies enable vehicles to make autonomous decisions, which depends on sensor capabilities, system architecture, and operational context. VCPSs offer solutions to major transportation challenges including congestion, accidents and energy inefficiency.

Therefore, based on the criticality of such systems, one might expect them to operate flawlessly. However, their characteristics introduce vulnerabilities (Duo *et al.,* 2022) resulting in cyberattacks. Several instances have been reported between the years 2010-2021 highlighting the susceptibility of autonomous vehicles (Kukkala *et al.,* 2022). In 2010, the University of Washington and California demonstrated one of the first vehicle vulnerabilities (Koscher *et al.,* 2010). However, since the attack required physical access to the vehicle, it received no significant attention. Then, in 2015, the first major remote attack on a Jeep Cherokee was recorded (Miller and Valasek, 2015), followed by a similar attack on a Nissan Leaf in 2016. That same year, researchers at the University of Birmingham recovered cryptographic keys from the electronic control units (ECUs), affecting Volkswagen (VW) group's vehicles (Garcia *et al.,* 2016). Subsequent attacks include fob cloning of Tesla's Model S (Wouters *et al,* 2019) and Model X in 2019 (Wouters *et al.,* 2021). There have also been attacks targeting Automated Driving Assisted Systems (Eykholt *et al.,* 2018) and onboard sensors used for perception (Petit *et al.,* 2015).

The incidents highlight the severity of cyberattacks, emphasizing the need for improved analysis and mitigation strategies. This creates a clear need for a VCPS framework to model cyberattacks and by extension, any unforeseen disturbances in a controlled simulation environment. The following literature presents an overview of recently developed CPS frameworks and does not serve as a detailed review.

### 1.1. Literature review

Over the years several articles highlighted the effects of cyberattack occurrences affecting Autonomous Vehicles (AVs) (Kumar *et al*, 2018). However, these articles do not address a complete framework for handling multiple disturbances such as cyberattacks, communication impairments and sensor faults which can be seen as an existing gap. To date, multiple frameworks have been proposed for cyberattack evaluation in CAVs. In 2021 a benchmarking framework addressing security issues, vulnerabilities, and attack impacts on CAVs and humans was introduced (Khadka *et al.*, 2021), with capabilities to simulate physical and communication-based attacks. Similarly, a cyber-physical surveillance system was developed to tackle threats in a crowded environment (Singh et al., 2018). A smart digital twin-based framework for cyberattack detection in vehicle to grid CPSs was proposed and tested (Ali *et al.*, 2023). Al Maruf *et al.* (2023) proposed a timing-based framework for resilient architectures and adaptive cruise control policy design. A Cyber Security Evaluation Framework (CSEF) was developed to assess ECUs security, through asset identification, threat analysis and risk assessment (Zhang *et al.*, 2021). Rehman and Gruhn (2018) proposed a security framework for smart parking systems, while Sedjelmaci *et al.* (2019) introduced a cooperative game based cyber defense strategy for detecting and mitigating vehicle attacks. An efficient dual cyber-physical framework was developed to harness trustworthy communication for CV applications, incorporating blockchain technology and physical sensing capabilities (Liu *et al.*, 2021). Lastly, Shirvani *et al.* (2023) developed a comprehensive security risk assessment framework that maps electric vehicles (EVs) vulnerabilities using the STRIDE threat model. Different to the previously mentioned articles. The authors propose a VCPS framework (VCPSF) for studying the effects of multiple disturbances with application to CAVs, developed in the Matlab/Simulink software. This article has been categorized into eight main sections. Section 1 highlights the introduction and literature review. Section 2 describes the CAV and communication system models. Section 3 discusses the disturbance modeling. Section 4 introduces the platoon dynamics subjected to different disturbances. Section 5 presents the control framework. Section 6 analyzes the results of the simulated scenarios. Section 7 outlines the testing of the framework and Section 8 outlines the discussion.

## 2. VCPS framework

The VCPSF describes the simulation modules developed to facilitate the simulation of the entire system. The framework contains five modules which is illustrated in Figure 1. These VCPSF modules are as follows: 1) CAV platoon system; 2) communication system; 3) disturbance system; 4) The VCPSF subjected to disturbances, and, 5) The control framework system.

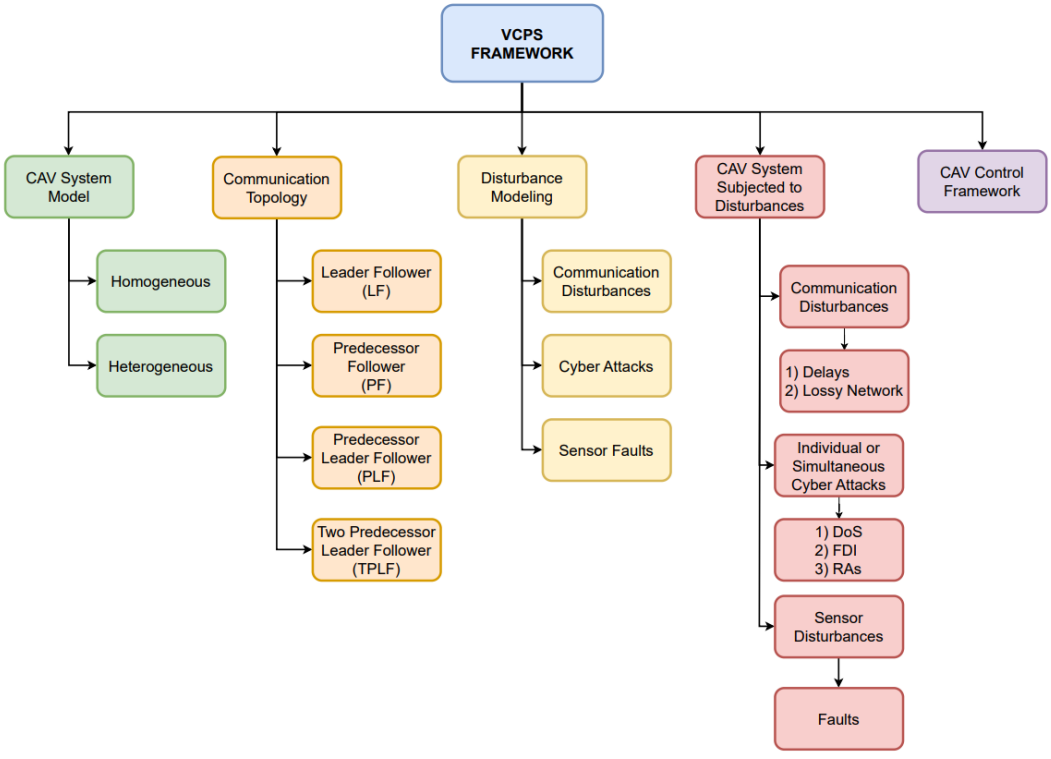



*Figure 1*. A representation of the VCPS simulation modules

### 2.1. Modeling of VCPSF CAV platoon system

The VCPSF's flexible modeling architecture supports the simulation of CAV platoons through an adaptable longitudinal dynamic model. As illustrated in Figure 2, the framework comprises a leader vehicle, six follower vehicles, and a communication medium that transmits state information from the leader. The longitudinal model, as described in Equation 1, was used to simulate the platoon's motion (Ge *et al.*, 2022; Zheng *et al.*, 2017). In this model, $A$ denotes the state transition matrix, $x(t)$ represents the system states, $B$ the input vector, $u(t)$ is the vehicle's velocity as well as the control input, and the parameter $\tau$ represents the powertrain lag constant (Petrillo *et al.*, 2020). The system states, $x(t)$ consists of: $p(t)$ (position), $v(t)$ (velocity), and $a(t)$ (acceleration). The associated matrices and vector sizes are defined in Equations 2 and 3. The VCPSF allows simulation of heterogeneous platoons by adjusting key parameters such as powertrain lag constant $\tau$, vehicle length $V_L$ and inter-vehicular spacing policies. This modeling versatility allows the framework to accurately represent real world configurations from the longitudinal perspective where vehicles may differ in performance and behavior. While the framework focuses on longitudinal dynamics, lateral dynamics and environmental factors (road curvature, slope, etc.) are excluded. As such, the VCPS framework is best suited for highway like platooning studies. In this scenario, the leader generates a reference trajectory, which the platoon safely tracks, while adhering to the spacing policy.

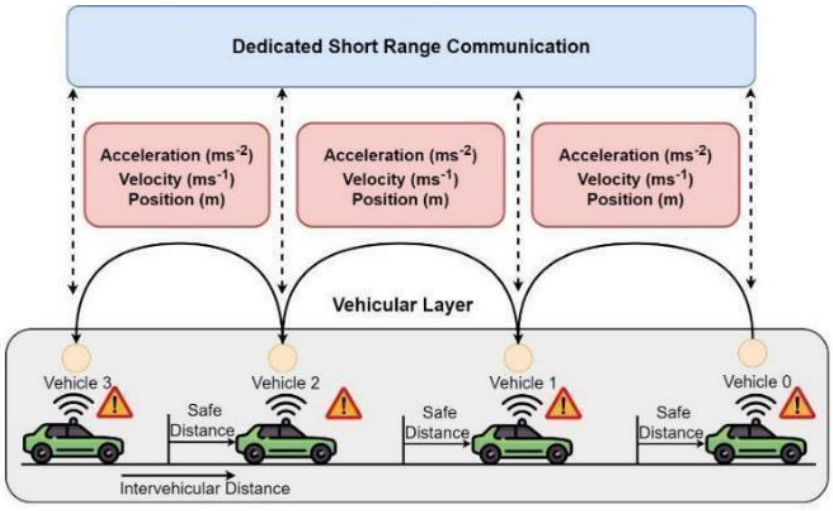



*Figure 2.* A representation of the Vehicle Cyber Physical System

$$\dot{x}(t) = Ax(t) + Bu(t). \tag{1}$$

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & \frac{-1}{\tau} \end{bmatrix}, x(t) = \begin{bmatrix} p(t) \\ v(t) \\ a(t) \end{bmatrix}, B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{\tau} \end{bmatrix}. \tag{2}$$

$$A \in \mathbb{R}^{3\times3}, B \in \mathbb{R}^{3\times1}, x(t) \in \mathbb{R}^{3\times1}. \tag{3}$$

### 2.2. VCPSF communication system

The communication topology defines the structure and direction of information flow among vehicles, directly influencing aspects such as stability, responsiveness, and coordination. The VCPSF distinguishes itself by offering the flexibility to simulate a wide range of communication topologies including Leader-Follower (LF), Predecessor-Follower (PF), Predecessor-Leader-Follower (PLF), and Two-Predecessor-Leader-Follower (TLPF) (Zhai *et al.*, 2018). The framework also allows comparison of topologies tailored to answer specific questions, experimental setups or deployment conditions.

Each vehicle shares state information such as position, velocity and acceleration, measured via onboard sensors, through an assumed IEEE 802.11p communication layer, alongside the leader's reference behavior. In this study, the PF topology was implemented due to its simple structure, where each vehicle receives information from its immediate predecessor. Figure 3 illustrates configurable topologies that the framework supports. Importantly the VCPS facilitates the study of topology switching, where the communication structure can be altered based on changes within the platoon environment. Despite these strengths, several limitations should be acknowledged. The current implementation treats topology selection as static within simulation execution, where

true dynamic reconfiguration remains an area for development. Additionally, while the framework captures structural differences in information flow, it does not simulate aspects such as message queuing and channel contention, that occur in communication systems. These aspects, while simplifying the simulation environment, may underrepresent the communication layer or congestion under high vehicle density.

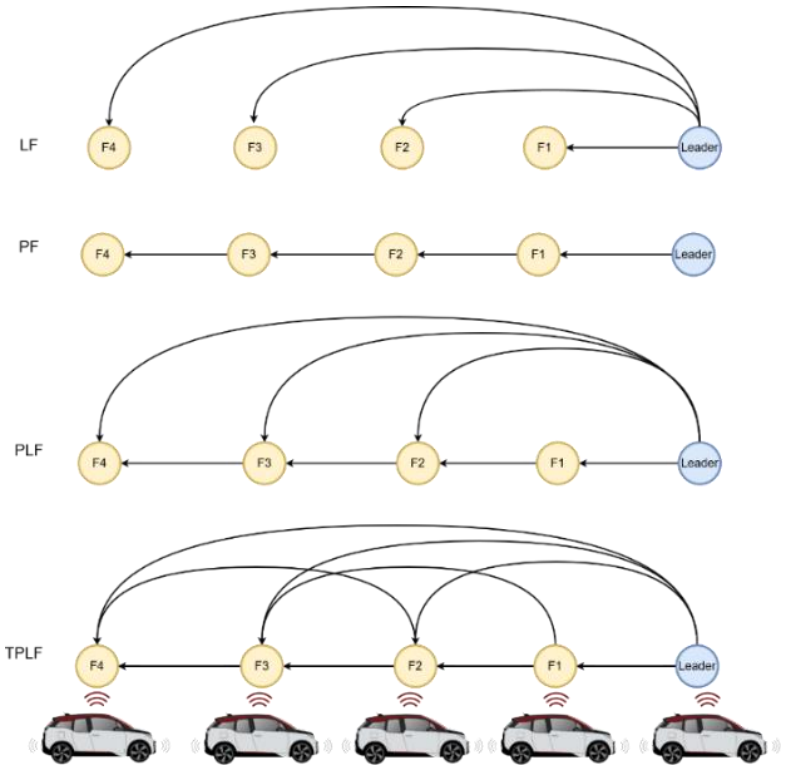



*Figure 3.* Communication topologies for the VCPSF

## 3. VCPS disturbance modeling

The VCPSF integrates a unified disturbance modeling framework to simulate realistic conditions affecting CAV platoons. It supports a wide range of disturbances such as communication impairments, cyberattacks, and sensor faults. Each disturbance type is governed by a configurable set of parameters that define its timing, magnitude, and target vehicle, allowing precise control over the experimental setup. This flexibility enables the creation of specialized test scenarios that can be used for benchmarking algorithms and exploring system vulnerabilities in a controlled environment. An additional novelty lies in the framework's ability to simulate disturbances both independently and in a combinatorial manner, which is often overlooked in prior works. The aspect of spatial targeting within the platoon can be harnessed to assess how disturbance impact varies based on vehicle position. By supporting both spatial and temporal variation in disturbance applications, the framework facilitates scalable and systematic analysis of complex disturbance scenarios. This capability holds significant implications for cyber physical security and control research, as it allows new avenues for stress testing, detection, estimation and control algorithms. Additionally, the platform serves as an experimental foundation for exploring how redundancy and resilience structures can mitigate cascading failures resulting from concurrent disturbances.

However, certain limitations exist such as idealized models of disturbance injection. While it covers a broad spectrum of disturbances, it does not consider attacker intelligence or adaptive adversarial behaviour. Similarly, physical layer communication impairments such as signal interference or bandwidth contention are not modelled in full detail. Moreover, while the system supports deterministic and randomized scheduling, the absence of environment-triggered disturbance logic may limit scenario realism.

### 3.1. Communication impairments

Two common disturbances during wireless communication are modeled as: (1) Probabilistic Loss of Information (Zhang *et al.*, 2013), and (2) Heterogeneous Communication Delays. The communication module allows for simulation of three conditions: (i) packet loss, (ii) network delays, and (iii) a combination of both.

*Probabilistic loss model*

Let $\theta_k \in [0,1]$ represent the transmission indicator at time step $k$, where $\theta_k = 1$ indicates a successful transmission and $\theta_k = 0$ indicates a packet drop. Let $\theta = \{\theta_0, \theta_1, \dots\}$ denote a scheduling scheme that determines the value of $\theta_k$ at each time step. When transmission takes place, the data packet can be successfully delivered or dropped due to communication channel interference. We assume that each $\theta_k$ is modelled as an independent and identically distributed Bernoulli random variable with $\mathbb{P}(\theta_k = 1) = 1 - \rho$ and $P(\theta_k = 0) = \rho$, where $\rho \in [0,1]$ is the probability of packet drop Hence, $\theta_k$ acts as an indicator of transmission success. For the sake of this section, the packet is defined as $x(t)$.

$$x(t) = \theta_k[x(t)]. \tag{4}$$

*Communication delay model*

Delays are modeled using a time-varying, bounded delay parameter $\eta \in [0, 50]$. When a delay is present, the data received at time $t$ is from an earlier time $t - \eta$ (Yamamoto *et al*., 2021):

$$x(t) = \begin{cases} x(t) & No\ Delay \\ x(t-\eta), & Delay\ Present \end{cases}. \tag{5}$$

### 3.2. Cyberattacks

*DoS and FDI*

The following highlights the mathematical models used for each of the cyberattacks implemented within the framework. These include: 1) Denial of Service (DoS), 2) False Data Injection (FDI), and 3) Replay Attacks (RAs). DoS attacks were assumed to block communication, where information was unable to be received (Ding *et al.*, 2018). In such a case $\alpha = 0$ and $\beta = 0$. A DoS attack is dependent on the time-period which the attacker determines which is referred to as the attack window. Given the attack window, the attacker can set the loss rate percentage which ranges between $0\% \leq\ loss\ rate \leq\ 100\%$. This loss rate defines how frequently data is lost during the attack window. FDI attacks were assumed to modify sensor data before transmission. In such situations, stored data values were modified and transmitted to the receiving vehicles within the platoon. In the case of a FDI attack $\alpha =\ 1\ and\ \beta \in \mathbb{Z},\ |\beta| > 0$, represents the magnitude of the attacks.

In this section, the mathematical model for the DoS and FDI attacks are described (Noei *et al.*, 2016) and can be seen in Equation 6.

$$x(t) = \begin{cases} x(t) & No\ Attack \\ \alpha x(t) + \beta, & Attack\ Present \end{cases}. \tag{6}$$

*Replay Attack (RA)*

A RA can be described as an attack that takes place in two stages: 1) the attacker records past information at different points in time, 2) re-injects this information during an attack window (Sanchez *et al.*, 2021). The framework facilitates the execution of three independent replay attacks which can affect any states within the system. Equation 7 highlights the replay behaviour mathematically, where $x(t)$ represents a state variable within the system such that $0 < \vartheta \leq 20$ when the replay attack occurs. $\vartheta$ denotes the age of the recorded information.

$$x(t) = \begin{cases} x(t) & No\ Attack \\ x(t-\vartheta), & Attack\ Present \end{cases}. \tag{7}$$

### 3.3. Sensor faults

Sensor faults are modeled as deviations from expected sensor outputs. The VCPSF includes the following fault types (Amin and Hasan, 2019), each of which is described below.

*Bias (Offset)*

Bias can be defined as a consistent offset in the sensor's output, which may exist due to improper calibration or physical deterioration, as described in Equation 8. $\delta \in \mathbb{Z}, |\delta| > 0$, represents the magnitude of the bias being applied.

$$x(t) = \begin{cases} x(t) & No\ Fault \\ x(t) + \delta, & Fault\ Present \end{cases}. \tag{8}$$

*Scaling (Gain)*

Gain can be seen as a proportional deviation in the sensor output. This type of fault can be described as an error in the scaling of the sensor value as seen in Equation 9. $\mathcal{E}(t)$ is a time-varying scaling factor within the range: $0 \leq \mathcal{E}(t) \leq \infty$.

$$x(t) = \begin{cases} x(t) & No\ Fault \\ x(t)\mathcal{E}, & Fault\ Present \end{cases}. \tag{9}$$

*Noise*

Noise can be considered random variations in the sensor values possibly due to ambient, hardware or wire conditions. The noise can be represented in Equation 10 where $\zeta \in \mathbb{Z}$, $|\zeta| > 0$ represents the magnitude of the random noise signal affecting the states of the system $x(t)$.

$$x(t) = \begin{cases} x(t) & No\ Fault \\ x(t) + \zeta, & Fault\ Present \end{cases}. \tag{10}$$

*Hard Fault*

A Hard Fault is defined as a stuck sensor value which can represent a complete loss of the sensor in terms of operation (Amin and Hasan, 2019). C is a value that spans between $0 \leq C \leq \infty$ as shown in Equation 11.

$$x(t) = C. \tag{11}$$

## 4. VCPSF subjected to disturbances

This section outlines the interaction between the disturbance model and the CAV platoon system as illustrated in Figure 4. The system is structured into two primary layers: 1) the Cyber Layer and 2) the Vehicular Layer. These layers continuously exchange information to ensure the platoon maintains its control objective. The model operates on three major assumptions.

- An attacker exists that can compromise any of the following vehicles, with the sole intention of disrupting the platoon dynamics.
- Sensors on the vehicles are affected by intermittent faults.
- The communication network is subject to common impairments that may affect the data transmission.

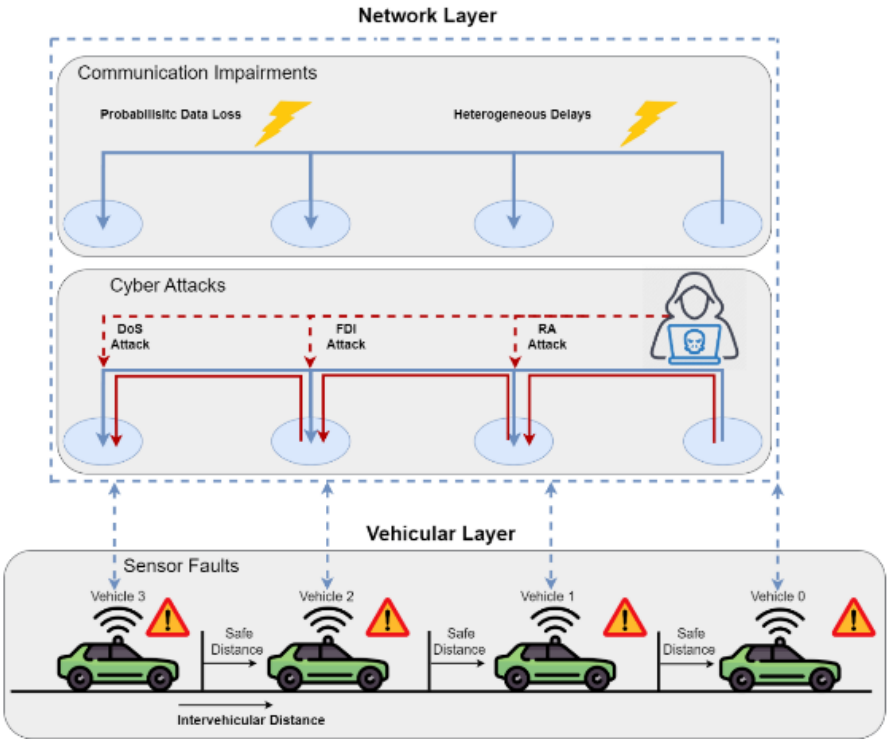



*Figure 4.* CAV platoon subjected to disturbances

The CAV platoon system can be affected by: 1) communication impairments; 2) cyberattacks; 3) sensor faults. All disturbances are highlighted in Figure 4. These disturbances specifically impact the communication and application layers within the framework. Disturbances can target transmitted states individually or simultaneously, as well as target individual or multiple vehicles within the platoon. These disturbances may occur periodically, sporadically, on a defined schedule, or randomly. In the case of cyberattacks, multiple scenarios can be explored, including individual vehicles subjected to: 1) DoS with varying loss rates; 2) FDI with varying magnitudes; 3) RAs, and, 4) combined scenarios. The VCPSF can simulate the effects of Communication Impairments by modeling: i) heterogeneous communication delays; ii) packet loss to represent a lossy network, and, iii) a combination of both, applied to either individual or multiple vehicles within the platoon. In the same way, sensor faults can also be simulated to demonstrate their influence on platoon performance. The complete details of the simulated scenarios are provided in Section 6.

This architecture allows decoupling of cyber-physical interaction mechanisms for clearer disturbance attribution and diagnostic traceability. However, there are some limitations to consider. While the layered abstraction improves modularity, the framework currently assumes ideal interfaces between layers and may not yet capture aspects such as jitter, or synchronization issues that occur in real-time embedded systems.

## 5. Control module framework

The control framework outlines the control method used to ensure platoon stability. In platooning applications, spacing policies are employed as part of the control strategy to ensure safe distances between vehicles. There are several policies that can be adopted, such as Constant Time Headway (CTH) policy, Constant Distance (CD) policy, and Nonlinear Distance (NLD) policy (Liu *et al.*, 2020), (Fan *et al.*, 2021), (Zhao *et al.*, 2021), as illustrated in Figure 4. Within this framework, the CTH policy was selected, which is dependent on the velocity of the preceding vehicle. The distance required is calculated using Equation 12 which include the parameters, inter-vehicular spacing, $d_{cth}$, vehicle's length, $L$, leader's velocity, $v$ , and the time headway constant, $t_{cth}$.

$$d_{cth} = L + (v + t_{cth}). \tag{12}$$

### 5.1. Sliding mode controller

This section outlines the Sliding Mode Control (SMC) strategy which was employed to attain the stability of the entire platoon under disturbance-free conditions. The design of the controller can be seen in Equations 13-15. The order of the system is represented by $n$, as specified in Equation 2. The error, $\mathcal{E}_{rr}$, between the current state, $x_{\mathrm{m}}$, and the desired state, $\gamma$, is calculated as follows,

$$\mathcal{E}_{rr}\begin{cases} e = \gamma - x_1 & e_1 = e \\ \frac{d}{dx}e = \frac{d}{dx}\gamma - \frac{d}{dx}x_1 & e_2 = \frac{d}{dx}e_1 \\ \vdots & \vdots \\ \frac{d^n}{dx^n}e = \frac{d^n}{dx^n}\gamma - \frac{d^n}{dx^n}x_1 & e_{n+1} = \frac{d^n}{dx^n}e_n \end{cases}, \tag{13}$$

where $\gamma$ is defined by $\gamma = x^{i-1} - d_{cth}$, $x^{i-1}$ is the $i^{th}$ car's predecessor's states. The sliding surface, $S$, and its derivatives can be designed as:

$$\begin{cases} S = e_1 + e_2 + \cdots + e_{n+1} \\ \frac{d}{dx}S = \frac{d}{dx}e_1 + \frac{d}{dx}e_2 + \cdots + \frac{d}{dx}e_{n+1} \\ \quad = e_2 + e_3 + \cdots + \frac{d^n}{dx^n}\gamma - \frac{d^n}{dx^n}x_1 \\ \quad = e_2 + e_3 + \cdots + \frac{d^n}{dx^n}\gamma + (x_n - u) \end{cases}. \tag{14}$$

Finally, the control law, $u$, is defined as:

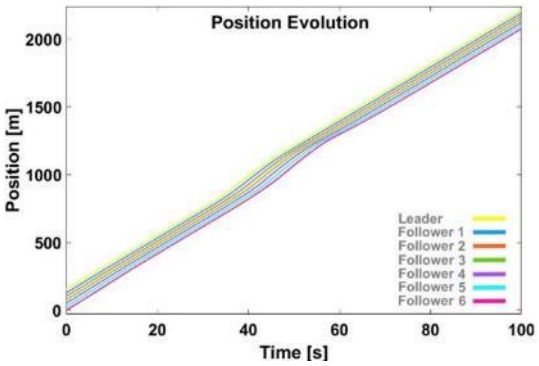
$$u = e2 + e3 + \ldots + e_n + x_n + Ksgn(S), \tag{15}$$

where $K$ is a positive gain, and $sgn(S)$ is the signum function of $S$ which is 1 if $S > 0$, -1 if $S < 0$ or 0 if $S = 0$.

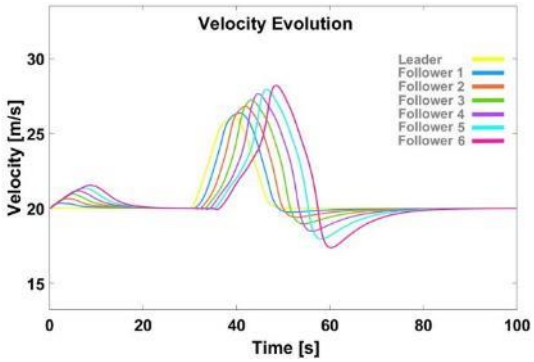
One of the key advantages of the control framework lies in its modularity and extensibility, where the control logic is decoupled from the disturbance modeling layer, allowing the testing and implementation of new controllers without needing to restructure the entire simulation environment. This promotes flexibility and accelerates the iterative development of resilient control strategies. Additionally, the repeatable setting simplifies the performance validation of various controllers under well-defined disturbance conditions. However, the current implementation focuses exclusively on longitudinal control, which limits its application as it relates to controller transferability and hardware-in-the-loop systems. Despite these constraints, the control framework offers a strong platform for both academic inquiry and practical development.

## 6. Results

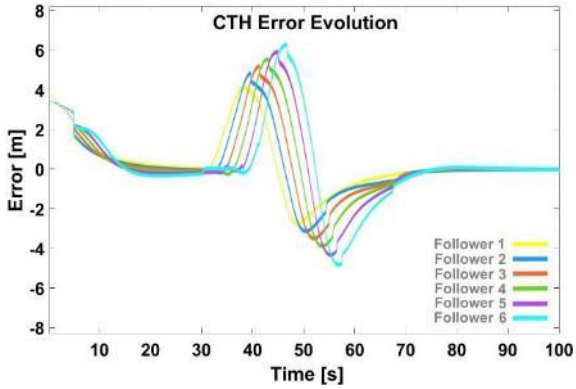
This section highlights the simulated scenarios involving various disturbances and their effects on the platoon, in contrast to the disturbance-free behaviour shown in Figure 5. This baseline behaviour was maintained due to the Sliding Mode Control (SMC) approach along with the CTH policy. These results emphasize the flexibility of the VCPSF when simulating different operating conditions, allowing analysis of both individual and multiple disturbances. The following four main scenarios have been presented: (1) the effects of Communication Impairments on the VCPSF; (2) the effects of Cyberattack on the VCPSF; (3) the effects of Sensor Faults on the VCPSF, and, (4) the combined effects of all disturbances.




*b) Position Evolution*




*a) Velocity Evolution*




***c)** CTH Error Evolution*

*Figure 5.* A representation of the Vehicle Platoon System without disturbances

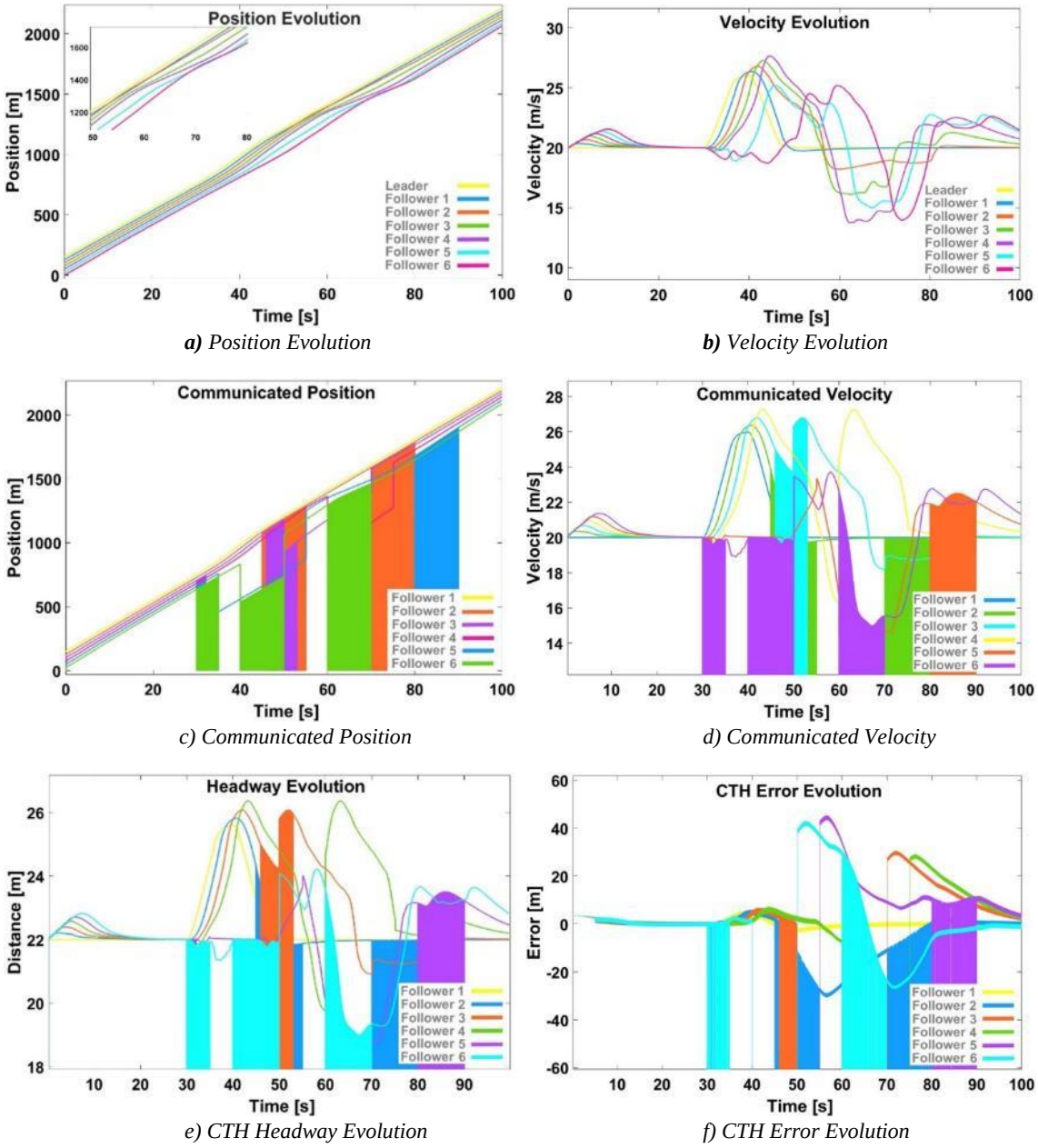
Table 1 highlights the details of each of the simulated cases from Section 6.1 – 6.4. The "-" means the disturbance is experienced throughout the entire simulation.

**Table 1.** Simulated cases for section 6.1 – 6.4

| Disturbance Modeling | | | |
|---|---|---|---|
| **Section** | **Affected Vehicle** | **Disturbance Type** | **Disturbance Time** |
| 6.1 | F2 | Lossy Comm (50%) | [45 - 55], [70 - 80] |
| | F3 | Delay (-10 s) | [50 - 70] |
| | F4 | Delay (-20s) | [60 – 75] |
| | F5 | Lossy Comm (32%) | [30 – 32], [80 – 90] |
| | | Delay (-15s) | [35 – 55] |
| | F6 | Lossy Comm (25%) | [30 – 35], [40 – 50], [60 -70] |
| | | Delay (-15s) | [40 – 50] |
| 6.2 | F2 | DoS (50%) | [30 - 32], [45 - 55] |
| | F3 | FDI (velocity $\pm 10ms^{-1}\ error$) | [8 - 10], [18 - 20], [28 - 30], [88- 90] |
| | | FDI (position $\pm 15m\ error$) | [30 - 40], [50 - 55], [70 - 73], [80- 90] |
| | F4 | FDI (velocity $\pm 5ms^{-1}\ error$) | [12 - 15], [25 - 30], [40 - 46], [60- 80] |
| | | FDI $position \pm 25\ m\ error$ | [50 - 53], [60 - 63], [70 - 73], |
| | F5 | RA (- 10 sec) | [50 - 70] |
| | F6 | DoS (100 %) | [8 - 15], [30 - 35], [40 - 45], [60- 70] |
| 6.3 | F2 | RBAU on RaDar $(50\%\ Dev \pm\ 5ms^{-1})$ | - |
| | | RBAU on LiDar $(50\%\ Dev\ \pm\ 10m)$ | - |
| | F3 | RBAU on RaDar $(50\%\ Dev \pm\ 3ms^{-1})$ | - |
| | | Noise on LiDar $(50\%\ Dev \pm\ 10m)$ | - |
| | F4 | RaDar Bias $(+\ 5ms^{-1})$ | - |
| | | LiDar Bias $(+\ 15m)$ | - |
| | F5 | RaDar Scaling $(80\%)$ | - |
| | | LiDar Bias $(80\%)$ | - |
| | | Radar Scaling (80%) | - |
| | | LidaR Bias (80%) | - |
| | F6 | RaDar Hard Fault $(5ms^{-1})$ | - |
| | | LiDar Hard Fault $(10m)$ | - |
| 6.4 | F2 | Lossy Comm (20%) | - |
| | | RA (-20s) | [60-70] |
| | F3 | RA(-20s) | [60-70] |
| | | Noise on RaDar $(10\%\ Dev \pm 0.5\ ms^{-1})$ | - |
| | | Noise on LiDar $(10\%\ Dev \pm 3m)$ | - |
| | | RaDar Scaling (85%) | - |
| | | LiDar Scaling (90%) | - |
| | F4 | FDI $(velocity \pm 5\ ms^{-1}\ error)$ | [12-15], [25-30], [40-46], [60-80] |
| | | FDI $(position \pm 25\ m\ error)$ | [50-53], [60-63], [70-73] |
| | | RaDar Bias (+5m/s) | - |
| | | LiDar Bias (+15m) | - |
| | | Delay (-10sec) | [40-50] |
| | F5 | DoS (32%) | [30-32], [80-90] |
| | | RaDar Bias (+10m/s) | - |
| | | LiDar Bias (+15m) | - |
| | F6 | RaDar Hard Fault (20 m/s) | - |
| | | LiDaR Hard Fault (20m) | - |

### 6.1. Communication Impairments effects on the VCPS

This section presents the effects of communication disturbances affecting the information received by followers (F) F2 to F6. Refer to Table 1 for details of the disturbances experienced within the platoon system. This scenario involves heterogeneous delays and information loss over different time-periods. The graphs in Figure 6 highlight the general behaviour under these conditions.




***a)*** *Position Evolution* ***b)*** *Velocity Evolution*

*c) Communicated Position* *d) Communicated Velocity*

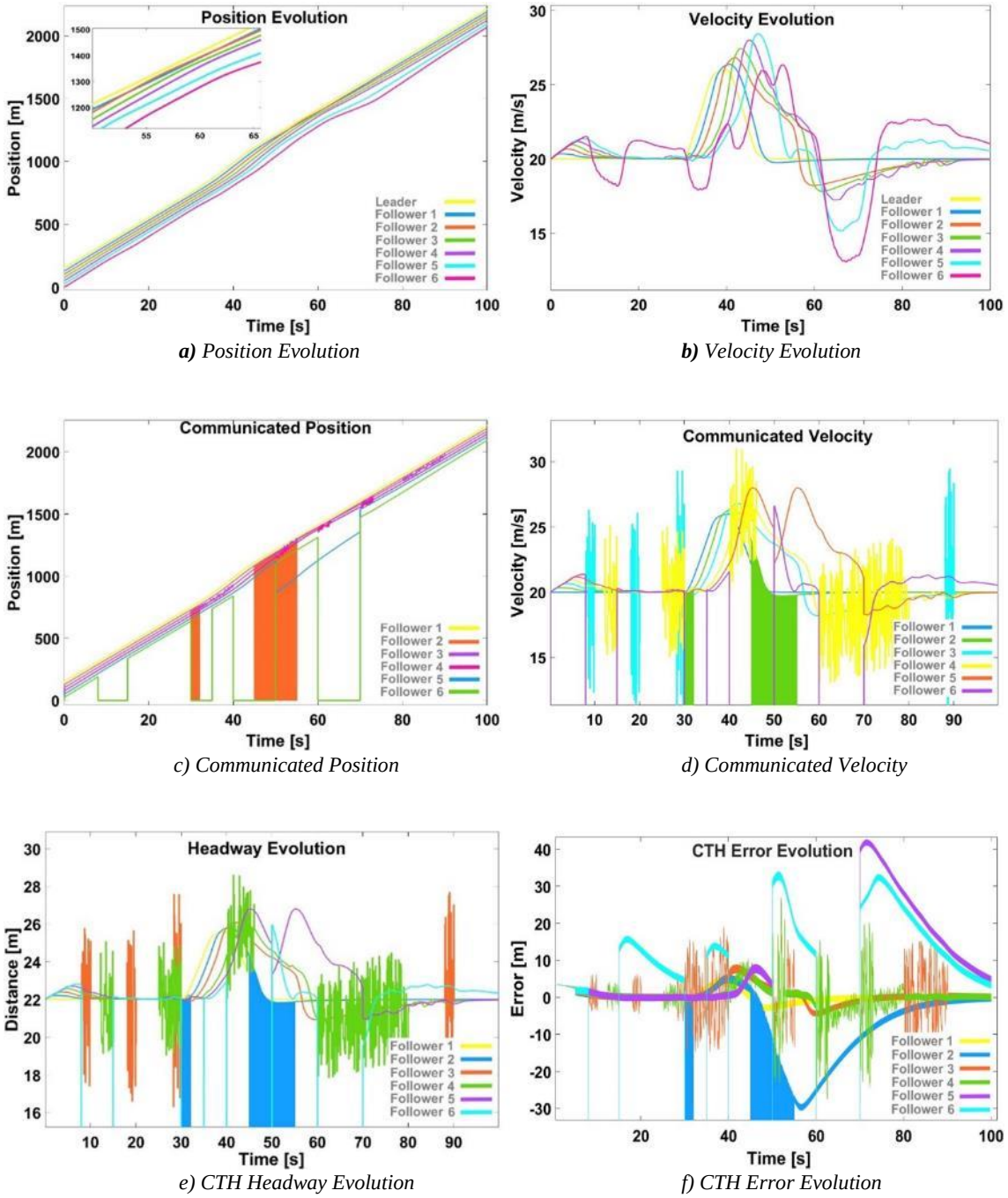
*e) CTH Headway Evolution* *f) CTH Error Evolution*

*Figure 6.* VCPS under effects of Communication Disturbances

Figures 6(a) – 6(b) highlight the position and velocity profiles for the platoon. The implemented delays, and information loss, caused the platoon to crash between 65s - 80s respectively in Figure 6(a). Figure 6(b) shows the evolution of the velocity profile and the associated erratic behaviour due to communication disturbances which can be compared to Figure 5. Figures 6(c) – 6(f) highlight the communicated position, communicated velocity, CTH headway, and CTH error evolutions.

### 6.2. Cyberattack effects on the VCPS

The section presents the effects of cyberattacks affecting the information received by F2 to F6 respectively. This scenario considers the occurrence of DoS, FDI and RAs over different time periods as shown in Table 1. The graphs in Figure 7 highlight the general behaviour under these conditions. Figure 7(a) – 7(b) highlight the position and velocity profiles for the platoon under different cyberattack situations. This scenario resulted in the platoon crashing between the time 55s - 65s respectively in Figure 7(a). Figure 7(b) shows the evolution of the velocity profile. Figures 7(c) – 7(f) highlight the communicated position, communicated velocity, CTH headway, and CTH error.




***a)*** *Position Evolution* ***b)*** *Velocity Evolution*

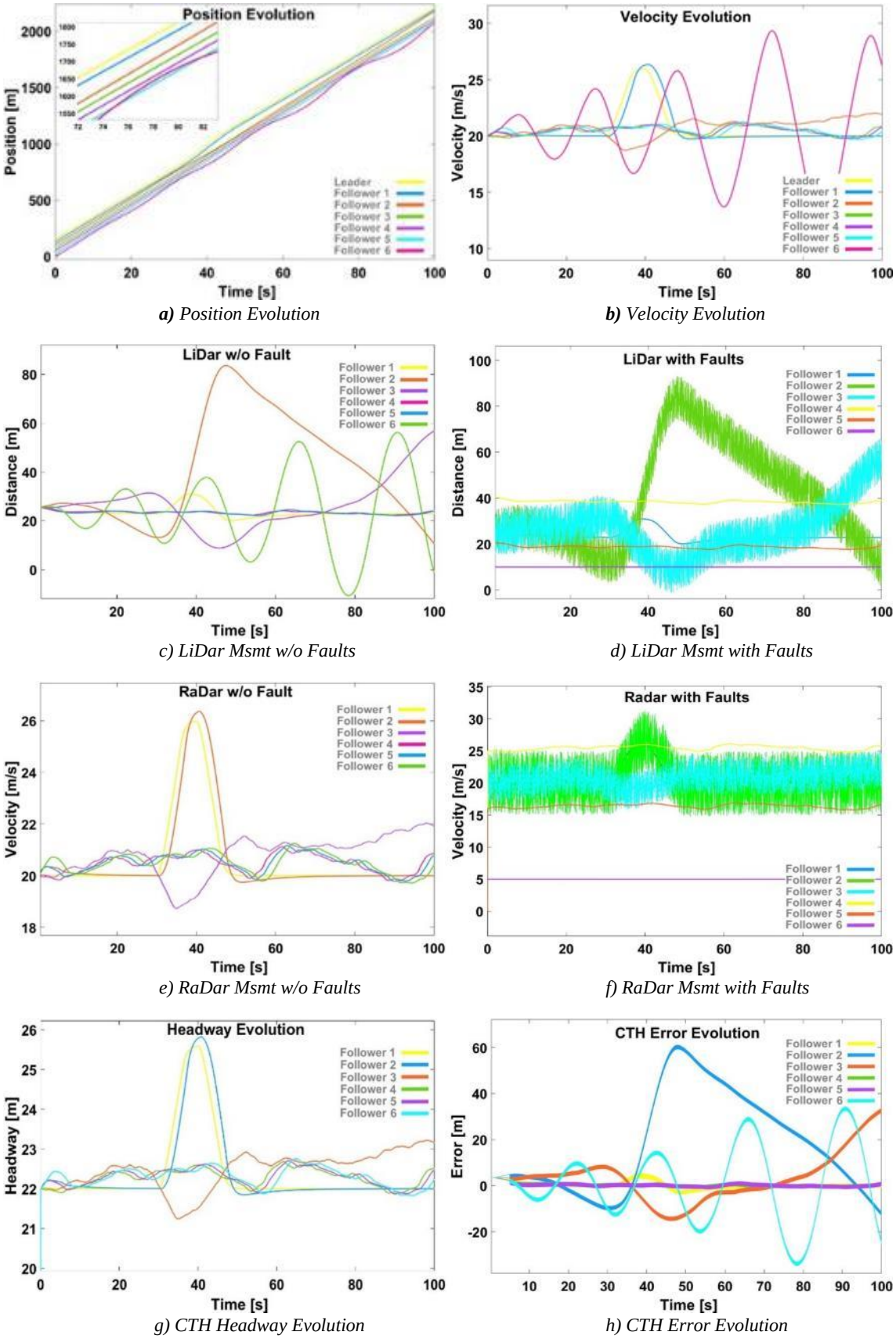
*c) Communicated Position* *d) Communicated Velocity*

*e) CTH Headway Evolution* *f) CTH Error Evolution*

*Figure 7*. VCPS under effects of Cyberattacks

### 6.3. Sensor Fault effects on the VCPS

This section highlights the effects of Sensor faults affecting the information received by F2 to F6 respectively. This scenario considers the occurrence of Sensor faults over different time periods as specified in Table 1. The graphs in Figure 8 highlight the general behaviour under these conditions. Figures 8(a) – 8(b) highlight the position and velocity profiles for the platoon under different Sensor fault situations. The scenario resulted in the platoon crashing between the time 72s - 82s respectively in Figure 8(a). Figure 8(b) shows the evolution of the velocity profile. Figures 8(c) – 8(f) show the comparisons between the sensor measurements of LiDar and RaDar with and without (w/o) the effects of faults. Note that the measurements with the effects of faults were sent to the controller which caused the effects seen. Figures 8(g) – 8(h) highlight the CTH headway, and CTH error evolution respectively.




***a)*** *Position Evolution*

***b)*** *Velocity Evolution*

*c) LiDar Msmt w/o Faults*

*d) LiDar Msmt with Faults*

*e) RaDar Msmt w/o Faults*

*f) RaDar Msmt with Faults*

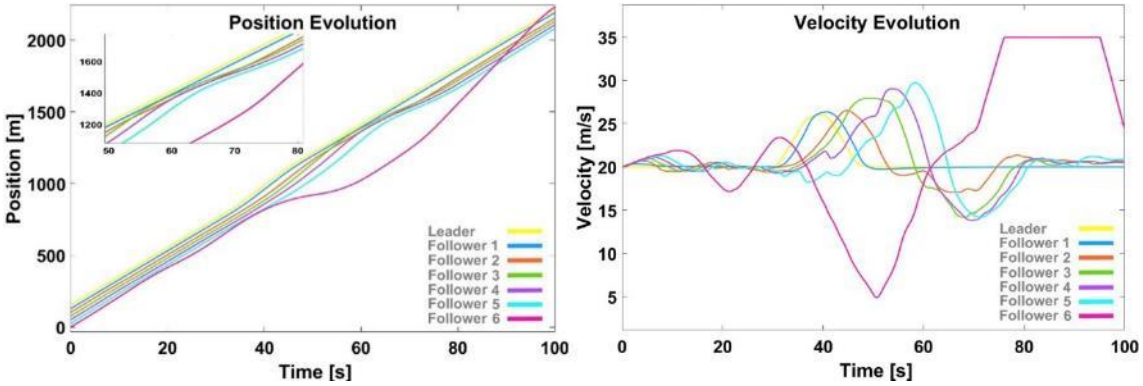
*g) CTH Headway Evolution*

*h) CTH Error Evolution*

*Figure 8.* VCPS under effects of Sensor Faults

### 6.4. The effects of all disturbances on the VCPS

This section shows the effects of all disturbances affecting the information received by F2 to F6 respectively. This scenario considers the occurrence of Communication Impairments, Cyberattacks, and Sensor faults over different time periods as specified in Table 1. The graphs in Figure 9 highlight the general behaviour under these conditions. Figures 9(a) – 9(b) highlight the position and velocity profiles for the platoon and highlight the occurrence of crashes taking place. As expected, the combination of all disturbances produces a more pronounced disruption of the expected behaviour of the platoon.




***a)*** *Position Evolution* ***b)*** *Velocity Evolution*

*Figure 9*. VCPS under effects of all disturbances

## 7. Testing and validation of framework

The proposed VCPSF was developed with an emphasis on conceptual rigor and internal coherence, making use of simulation-based reasoning as the means of validation. As a result of complexity and the inherent risk involved in real word experimentation with application to CAVs, a set of detailed simulated scenarios was created within the MATLAB\Simulink environment to investigate the framework's behaviour when subjected to varying disturbance conditions. Internal consistency was prioritized throughout the developmental process, as all modules within the framework were constructed ensuring well defined input and output relationships which ensured modular integrity. Inter-module dependencies were also reviewed to confirm that the flow and processing of data were coherent with the intended design. This establishes a strong foundation for empirical validation. Additionally, to further strengthen the framework's credibility, the development was done by using established best practices and related methodologies used within literature. Key concepts were drawn from validated systems in cyber-physical infrastructure, secure control theory, and vehicular network simulations as discussed within the literature review. Indirect benchmarking ensures that the developed VCPSF can be extended into ongoing studies and includes proof-of-concept validation via simulated multi-disturbance experiments. Looking ahead, a more rigorous empirical evaluation is planned, involving integration of real-time data streams, deployment in hardware-in-the-loop (HIL) environments, and quantitative benchmarking against performance metrics.

## 8. Discussion

The discussion focuses on the effects of each disturbance in a combinatorial manner as highlighted in Section 6. In the case of cyberattacks, platoon stability is disrupted by corrupting state information. These attacks lead to erratic behavior, especially in velocity tracking and inter-vehicular spacing, which are crucial under the CTH policy. The simulation results showed crashes particularly when FDI and DoS were applied simultaneously. Disturbances applied to vehicles near the front of the platoon induced cascading instability downstream, leading to amplified tracking errors and safety violations. Communication impairments degraded the transmission channel itself causing infringement of safety distances and misaligned control actions across vehicles. Notably, when comparing the velocity tracking profiles, disturbances caused by cyberattacks produced more erratic behaviors than those caused by communication impairments. Sensor faults affected the enforcement of inter-vehicular spacing. The effects were severe when multiple sensor faults occurred simultaneously across different vehicles, with some vehicles showing abrupt trajectory shifts. Notably, compared to cyberattacks and communication impairments, sensor faults resulted in

significantly more pronounced destabilization. The simulation results also showed that faulty measurements in even a single vehicle could disrupt the entire platoon. In the case of all three disturbances, crashes occurred earlier and with greater severity, resulting in total loss of control. Notably, those further away often suffered from delayed yet intensified responses.

Therefore, by comparing the effects of each disturbance type on the platoon system, a relative ranking can be established based on the severity observed in position evolution, velocity profiles, CTH error tracking, and headway maintenance. For this simulation, sensor faults had the most severe impact, followed by cyberattacks, and then communication impairments. One significant insight is that the location of the disturbance application plays a critical role. Vehicles affected at the front of the platoon induced cascading errors downstream, amplifying the instability more than if the same disturbance occurred at the rear. Similarly, increasing the number of attacked vehicles magnified these effects, which was observed when attacks were progressively layered across scenarios. These findings emphasize the need for the development of robust detection, isolation, and estimation mechanisms, and by extension, resilient control strategies capable of addressing these types of disturbances individually or in combination and regardless of its spatial target.

## References


1. Al Maruf, A., Niu, L., Clark, A., Mertoguno, J.S., Poovendran, R. (2023) A timing-based framework for designing resilient cyber-physical systems under safety constraint. *ACM Transactions on Cyber-Physical Systems*, 7(3), 1-25. DOI:10.1145/3594638.
2. Ali, M., Kaddoum, G., Li, W.T., Yuen, C., Tariq, M., Poor, H.V. (2023) A smart digital twin enabled security framework for vehicle-to-grid cyber-physical systems. *IEEE Transactions on Information Forensics and Security*, 18, 5258 – 5271. DOI: 10.1109/TIFS.2023.3305916.
3. Amin, A.A., and Hasan, K.M. (2019) A review of fault tolerant control systems: advancements and applications. *Measurement*, 143, 58–68. DOI: 10.1016/j.measurement.2019.04.083.
4. Baheti, R. and Gill, H. (2011) Cyber-physical systems. *The Impact of Control Technology*, 12(1), 161-166. Available at: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=ae1154337cdb44b69c1efbf3d9d9b52d76732be2.
5. Ding, D., Han, Q.L., Xiang, Y., Ge, X., and Zhang, X.M. (2018) A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 275, 1674–1683, DOI:10.1016/j.neucom.2017.10.009.
6. Duo, W., Zhou, M. and Abusorrah, A. (2022) A survey of cyberattacks on cyber physical systems: Recent advances and challenges. *IEEE/CAA Journal of Automatica Sinica*, 9(5), 784-800. DOI:10.1109/JAS.2022.105548.
7. Eykholt, K., Evtimov, I., Fernandes, E., Li, B., Rahmati, A., Xiao, C., Prakash, A., Kohno, T. and Song, D. (2018) Robust physical-world attacks on deep learning visual classification. In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, Salt Lake City, June 2018. IEEE, 1625-1634. DOI: 10.1109/CVPR.2018.00175.
8. Fan, J., Li, Y., Zhu, H., and Yu, S. (2021) Longitudinal control of connected truck platoon based on prescan. In: *Proceedings of the 33rd Chinese Control and Decision Conference (CCDC)*, Kunming, May 2021. IEEE, 1110– 1115. DOI: 10.1109/CCDC52312.2021.9602602.
9. Garcia, F.D., Oswald, D., Kasper, T., and Pavlidès P. (2016) Lock it and still lose it—on the (in) security of automotive remote keyless entry systems. In: *Proceedings of the 25th USENIX Security Symposium*, Austin, August 2016. Available at: https://kasper-oswald.de/wp-content/uploads/2013/03/paper.pdf.
10. Ge, X., Han, Q.L., Wu, Q. and Zhang, X.M. (2022) Resilient and safe platooning control of connected automated vehicles against intermittent denial-of-service attacks. *IEEE/CAA Journal of Automatica Sinica, 10*(5), 1234-1251. DOI: 10.1109/JAS.2022.105845.
11. Khadka, A., Karypidis, P., Lytos, A. and Efstathopoulos, G. (2021) A benchmarking framework for cyber-attacks on autonomous vehicles. *Transportation Research Procedia*, 52, 323-330. DOI:10.1016/j.trpro.2021.01.038.
12. Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. and Savage, S. (2010) Experimental security analysis of a modern automobile. In: *IEEE Symposium on Security and Privacy*, Oakland, May 2010. IEEE, 447-462. DOI:10.1109/SP.2010.34.
13. Kukkala, V.K., Thiruloga, S.V. and Pasricha, S. (2022) Roadmap for cybersecurity in autonomous vehicles. *IEEE Consumer Electronics Magazine*, 11(6), 13-23. DOI:10.1109/MCE.2022.3154346.

14. Kumar, A.D., Chebrolu, K.N.R., Vinayakumar R. and KP, S. (2018) A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities. *arXiv preprint arXiv:1810.04144*.
15. Liu, X., Luo, B., Abdo, A., Abu-Ghazaleh, N. and Zhu, Q. (2021) Securing connected vehicle applications with an efficient dual cyber-physical blockchain framework. In: *Proceedings of IEEE Intelligent Vehicles Symposium (IV)*, Nagoya, July 2021. IEEE Press, 393-400. DOI:10.1109/IV48863.2021.9575869.
16. Liu, Y., Peng, Y., Wang, B., Yao, S. and Liu, Z. (2017) Review on cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica*, *4*(1), 27-40. DOI: 10.1109/JAS.2017.7510349.
17. Liu, Y., Zong, C., Han, X., Zhang, D., Zheng, H. and Shi, C. (2020) Spacing allocation method for vehicular platoon: A cooperative game theory approach. *Applied Sciences*, 10(16), 5589. DOI:10.3390/app10165589.
18. Miller, C. and Valasek, C. (2015) Remote exploitation of an unaltered passenger vehicle. Black Hat USA. Available at: https://ioactive.com/wp-content/uploads/pdfs/IOActive_Remote_Car_Hacking.pdf.
19. Noei, S., Sargolzaei, A., Abbaspour, A. and Yen, K. (2016) A decision support system for improving resiliency of cooperative adaptive cruise control systems. *Procedia Computer Science*, 95, 489-496. DOI: 10.1016/j.procs.2016.09.326.
20. Petit, J., Stottelaar, B., Feiri, M., and Kargl, F. (2015) Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR. In: *Proceedings of Black Hat Europe Conference.* Available at: https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf.
21. Petrillo, A., Pescape, A., and Santini, S. (2020) A secure adaptive control for cooperative driving of autonomous connected vehicles in the presence of heterogeneous communication delays and cyberattacks. *IEEE Transactions on Cybernetics*, 51(3). DOI: 10.1109/TCYB.2019.2962601.
22. Rehman, S.U. and Gruhn, V. (2018) An effective security requirements engineering framework for cyber-physical systems. *Technologies*, 6(3), 65. DOI:10.3390/technologies6030065.
23. Sánchez, H.S., Rotondo, D., Puig, V., Escobet, T., and Quevedo, J. (2021) Detection of replay attacks in autonomous vehicles using a bank of qpv observers. In: *Proceedings of the 29th Mediterranean Conference on Control and Automation (MED)*, Puglia, June 2021. IEEE, 1149–1154. DOI:10.1109/MED51440.2021.9480330.
24. Sedjelmaci, H., Brahmi, I.H., Ansari, N. and Rehmani, M.H. (2019) Cyber security framework for vehicular network based on a hierarchical game. *IEEE Transactions on Emerging Topics in Computing*, 9(1), 429-440. DOI:10.1109/TETC.2018.2890476.
25. Shirvani, S., Baseri, Y. and Ghorbani, A. (2023) Evaluation framework for electric vehicle security risk assessment. *IEEE Transactions on Intelligent Transportation Systems*, 25(1), 33-56. DOI:10.1109/TITS.2023.3307660.
26. Singh, D., Tripathi, G., Shah, S.C. and da Rosa Righi, R. (2018) Cyber physical surveillance system for Internet of Vehicles. In: *Proceedings of the 4th World Forum on Internet of Things (WF-IoT)*, Singapore, February 2018. IEEE, 546-551. DOI: 10.1109/WF-IoT.2018.8355218.
27. Wouters, L., Gierlichs, B. and Preneel, B. (2021) My other car is your car: Compromising the Tesla Model X keyless entry system. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2021(4), 149-172. DOI:10.46586/tches.v2021.i4.149-172.
28. Wouters, L., Marin, E., Ashur, T., Gierlichs, B. and Preneel, B. (2019) Fast, furious and insecure: Passive keyless entry and start systems in modern supercars. *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 2019(3), 66-85. DOI:10.46586/tches.v2019.i3.66-85.
29. Yamamoto, Y., Kuze, N. and Ushio, T. (2021) Attack detection and defense system using an unknown input observer for cooperative adaptive cruise control systems. *IEEE Access*, 9, 148810-148820. DOI:10.1109/ACCESS.2021.3124547.
30. Zhai, C., Liu, Y., and Luo, F. (2018) A switched control strategy of heterogeneous vehicle platoon for multiple objectives with state constraints. *IEEE Transactions on Intelligent Transportation Systems*, 20(5), 1883–1896. DOI:10.1109/TITS.2018.2841980.
31. Zhang, H., Cheng, P., Shi, L., and Chen, J. (2013) Optimal dos attack policy against remote state estimation. In: *Proceedings of the 52nd IEEE Conference on Decision and Control*, Firenze, December 2013. IEEE, 5444–5449. DOI: 10.1109/CDC.2013.6760746.
32. Zhang, H., Pan, Y., Lu, Z., Wang, J. and Liu, Z. (2021) A cyber security evaluation framework for in-vehicle electrical control units. *IEEE Access*, 9, 149690-149706. DOI:10.1109/ACCESS.2021.3124565.

33. Zhao, X., Ju, J., Dong, F., Chen, Y.H., Zhang, L. and Zhang, B. (2021) An exponential type control design for autonomous vehicle platoon systems. *Asian Journal of Control*, 23(2), 1025-1039. DOI:10.1002/asjc.2279.
34. Zheng, Y., Li, S.E., Li, K. and Ren, W. (2017) Platooning of connected vehicles with undirected topologies: Robustness analysis and distributed H-infinity controller synthesis. *IEEE Transactions on Intelligent Transportation Systems*, 19(5), 1353-1364. DOI:10.1109/TITS.2017.2726038.