



# UNIVERSITÀ DI PISA

Computer Engineering

Formal Methods for Secure Systems

## *Project Report*

---

*MEMBRI DEL TEAM:*

Matteo Biondi

Olgerti Xhanej

Anno Accademico: 2020/2021

# Contents

<b>1</b>	<b>Introduzione</b>	<b>2</b>
1.1	Descrizione del problema . . . . .	2
<b>2</b>	<b>Scelte di Sviluppo</b>	<b>3</b>
2.1	Strategia Attacco . . . . .	3
2.2	Scelta dei parametri . . . . .	3
<b>3</b>	<b>Implementazione</b>	<b>4</b>
3.1	VanillaCase . . . . .	4
3.2	Attacco all'accelerazione . . . . .	5
3.3	Attacco alla Posizione . . . . .	7
3.4	Configurazione in Comune . . . . .	8
3.5	Comportamento degli Attacchi . . . . .	8
<b>4</b>	<b>Analisi dei Risultati</b>	<b>10</b>
4.1	VanillaCase . . . . .	10
4.1.1	Risultati Co-Simulazione . . . . .	10
4.2	Attacco all'accelerazione . . . . .	11
4.2.1	Attacco Semplice . . . . .	11
4.2.2	Attacco Multiplo . . . . .	18
4.3	Attacco alla X . . . . .	23
4.3.1	Attacco Semplice . . . . .	23
4.4	Attacco Multiplo . . . . .	24
<b>5</b>	<b>Conclusioni</b>	<b>25</b>

# 1 — Introduzione

## 1.1 Descrizione del problema

Tramite il software Into-CPS viene richiesto di modellare degli scenari con una following car che insegue una leading Car ad una distanza desiderata di 15m. L'unica dimensione presa in oggetto l'asse x.

L'obiettivo del progetto il seguente: analizzare possibili attacchi al suddetto sistema che possono causare uno scontro tra i due veicoli. In particolar modo implementare attacchi "Data Alteration" contro la posizione e l'accelerazione della following car.

## 2 — Scelte di Sviluppo

### 2.1 Strategia Attacco

Gli attacchi verranno implementati utilizzando la tecnica del *Man-in-the-Middle*: verrà introdotta una FMU semplificata tra un punto di comunicazione di due FMU. Questo consentirà di semplificare la modifica dell'implementazione dell'attacco in quanto non necessario conoscere i dettagli implementativi delle (altre) FMU in gioco. Questo comporta per un maggior overhead del sistema per effettuare la comunicazione dei parametri tra le varie FMU.

### 2.2 Scelta dei parametri

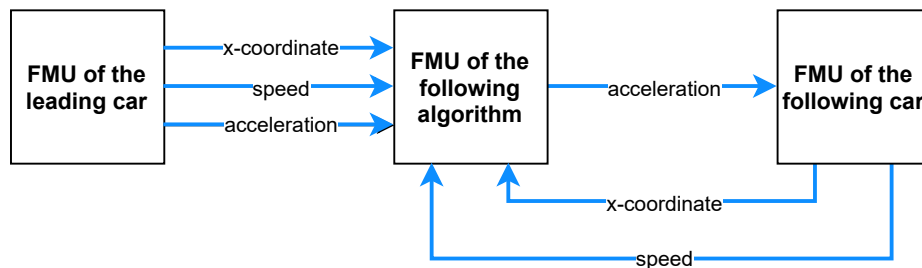
- **Step-size: 0.01s.** E' un buon trade-off tra un sensing più preciso ed una durata di simulazione accettabile.
- **Tempo di Simulazione: 100s.** Abbiamo valutato questo tempo come un ragionevole trade-off tra la capacità di computazione delle nostre macchine ed i risultati che possiamo mettere in luce.

## 3 — Implementazione

### 3.1 VanillaCase

Nella seguente figura è possibile osservare le connessioni logiche tra tre FMU principali:

- **FMU of the leading car:** questa FMU implementa il comportamento della leading car. Per funzionare non ha bisogno di alcun input da altre FMU e produce in output la posizione della macchina, la velocità e la sua accelerazione.
- **FMU of the following algorithm:** questa FMU implementa l'algoritmo di inseguimento. Presi in ingresso i parametri di posizione, velocità e accelerazione della leading car ed i parametri di posizione e velocità della following car produce in output l'accelerazione per la following car.
- **FMU of the following car:** questa FMU implementa il comportamento della following car. Per funzionare prende in ingresso l'accelerazione dalla precedente FMU e produce in output la sua posizione e velocità.



**Figure 1:** Multi-Model schema del VanillaCase

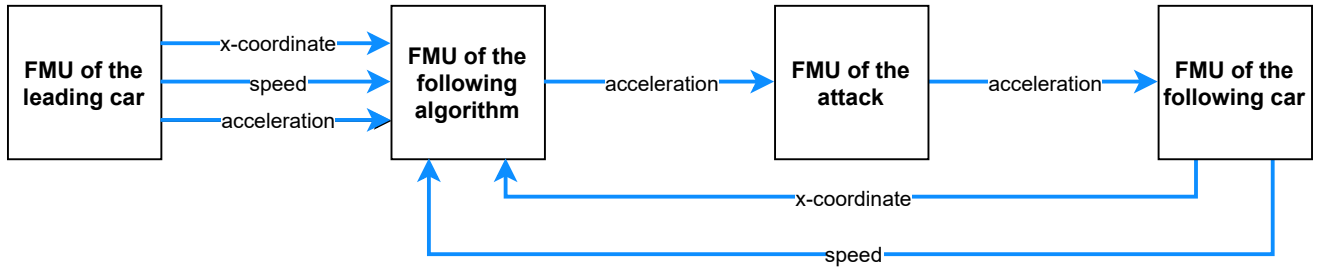
In figura 2 viene rappresentata l'overview del relativo Multi-Model sviluppato con il tool INTO-CPS.

Overview	
Outputs	Inputs
{FollowingAlgorithm}.FollowingAlgorithmInstance.accel	{FollowingCar}.FollowingCarInstance.accel
{FollowingCar}.FollowingCarInstance.x	{FollowingAlgorithm}.FollowingAlgorithmInstance.ego_x
{FollowingCar}.FollowingCarInstance.speed	{FollowingAlgorithm}.FollowingAlgorithmInstance.ego_speed
{LeadingCar}.LeadingCarInstance.x	{FollowingAlgorithm}.FollowingAlgorithmInstance.lead_x
{LeadingCar}.LeadingCarInstance.speed	{FollowingAlgorithm}.FollowingAlgorithmInstance.lead_speed
{LeadingCar}.LeadingCarInstance.accel	{FollowingAlgorithm}.FollowingAlgorithmInstance.accel_in

**Figure 2:** Multi-Model Overview del Vanilla Case

### 3.2 Attacco all'accelerazione

A differenza dello schema presentato nel VanillaCase, viene ora aggiunta una ulteriore FMU situata fra "FMU of the following algorithm" e "FMU of the following car" gi presenti. La nuova FMU implementa con strategia *Man-in-the-Middle* un attacco di tipo data alteration sull'accelerazione passata tra il Following Algorithm e la Following Car. Fare riferimento alla sezione 3.5 per dettagli sul comportamento dell'attacco.



**Figure 3:** Multi-Model schema dell'Attacco alla Accelerazione

In figura 4 e 5 viene rappresentata l'overview del relativo Multi-Model sviluppato con il tool INTO-CPS.

Overview	
Outputs	Inputs
{FollowingAlgorithm}.FollowingAlgorithmInstance.accel	{MitmAttackFmu}.MitmAttackFmuInstance.input
{MitmAttackFmu}.MitmAttackFmuInstance.output	{FollowingCar}.FollowingCarInstance.accel
{FollowingCar}.FollowingCarInstance.x	{FollowingAlgorithm}.FollowingAlgorithmInstance.ego_x
{FollowingCar}.FollowingCarInstance.speed	{FollowingAlgorithm}.FollowingAlgorithmInstance.ego_speed
{LeadingCar}.LeadingCarInstance.x	{FollowingAlgorithm}.FollowingAlgorithmInstance.lead_x
{LeadingCar}.LeadingCarInstance.speed	{FollowingAlgorithm}.FollowingAlgorithmInstance.lead_speed
{LeadingCar}.LeadingCarInstance.accel	{FollowingAlgorithm}.FollowingAlgorithmInstance.accel_in

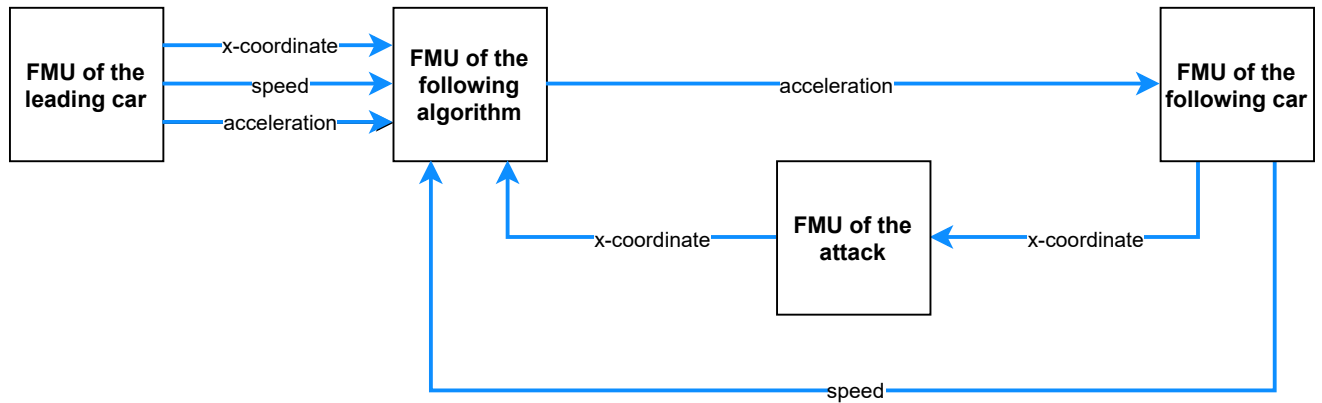
**Figure 4:** Multi-Model Overview dell'attacco all'accelerazione (caso attacco semplice)

Overview	
Outputs	Inputs
{FollowingAlgorithm}.FollowingAlgorithmInstance.accel	{MitmAttackFmu}.MitmAttackFmuInstance.input
{MitmAttackFmu}.MitmAttackFmuInstance.output	{FollowingCar}.FollowingCarInstance.accel
{FollowingCar}.FollowingCarInstance.x	{FollowingAlgorithm}.FollowingAlgorithmInstance.ego_x
{FollowingCar}.FollowingCarInstance.speed	{FollowingAlgorithm}.FollowingAlgorithmInstance.ego_speed
{LeadingCar}.LeadingCarInstance.x	{FollowingAlgorithm}.FollowingAlgorithmInstance.lead_x
{LeadingCar}.LeadingCarInstance.speed	{FollowingAlgorithm}.FollowingAlgorithmInstance.lead_speed
{LeadingCar}.LeadingCarInstance.accel	{FollowingAlgorithm}.FollowingAlgorithmInstance.accel_in

**Figure 5:** Multi-Model Overview dell'attacco all'accelerazione (caso attacco multiplo)

### 3.3 Attacco alla Posizione

A differenza dello schema presentato nel VanillaCase, viene ora aggiunta una ulteriore FMU situata fra "FMU of the following car" e "FMU of the following algorithm" gi presenti. La nuova FMU implementa con strategia *Man-in-the-Middle* un attacco di tipo data alteration sulla posizione passata tra la Following Car e il Following Algorithm. Fare riferimento alla sezione 3.5 per dettagli sul comportamento dell'attacco.



**Figure 6:** Multi-Model schema dell'Attacco alla Posizione

In figura 7 e 8 viene rappresentata l'overview del relativo Multi-Model sviluppato con il tool INTO-CPS.

Overview	
Outputs	Inputs
{FollowingAlgorithm}.FollowingAlgorithmInstance.accel	{FollowingCar}.FollowingCarInstance.accel
{FollowingCar}.FollowingCarInstance.x	{Attack}.AttackInstance.input
{FollowingCar}.FollowingCarInstance.speed	{FollowingAlgorithm}.FollowingAlgorithmInstance.ego_speed
{Attack}.AttackInstance.output	{FollowingAlgorithm}.FollowingAlgorithmInstance.ego_x
{LeadingCar}.LeadingCarInstance.x	{FollowingAlgorithm}.FollowingAlgorithmInstance.lead_x
{LeadingCar}.LeadingCarInstance.speed	{FollowingAlgorithm}.FollowingAlgorithmInstance.lead_speed
{LeadingCar}.LeadingCarInstance.accel	{FollowingAlgorithm}.FollowingAlgorithmInstance.accel_in

**Figure 7:** Multi-Model Overview dell'attacco alla posizione (caso attacco semplice)



Overview	
Outputs	Inputs
{LeadingCar}.LeadingCarInstance.x	{FollowingAlgorithm}.FollowingAlgorithmInstance.lead_x
{LeadingCar}.LeadingCarInstance.speed	{FollowingAlgorithm}.FollowingAlgorithmInstance.lead_speed
{LeadingCar}.LeadingCarInstance.accel	{FollowingAlgorithm}.FollowingAlgorithmInstance.accel_in
{FollowingAlgorithm}.FollowingAlgorithmInstance.accel	{FollowingCar}.FollowingCarInstance.accel
{FollowingCar}.FollowingCarInstance.speed	{FollowingAlgorithm}.FollowingAlgorithmInstance.ego_speed
{FollowingCar}.FollowingCarInstance.x	{MultiAttack}.MultiAttackInstance.input
{MultiAttack}.MultiAttackInstance.output	{FollowingAlgorithm}.FollowingAlgorithmInstance.ego_x

**Figure 8:** Multi-Model Overview dell'attacco alla posizione (caso attacco multiplo)

### 3.4 Configurazione in Comune

La configurazione delle seguenti FMU verr applicata per tutte le simulazioni che verranno effettuate.

- **LeadingCar:**
  - Posizione iniziale **x0**: 50m
  - Velocit iniziale **v0**: 0m/s
- **FollowingAlgorithm:**
  - **c1**: 0.5
  - **eps**: 1
  - **omega\_n**: 0.2
- **FollowingCar:**
  - Posizione iniziale **x0**: 0m
  - Velocit iniziale **v0**: 0m/s

### 3.5 Comportamento degli Attacchi

L'FMU che verr utilizzata negli attacchi MITM presenter due implementazioni diverse:

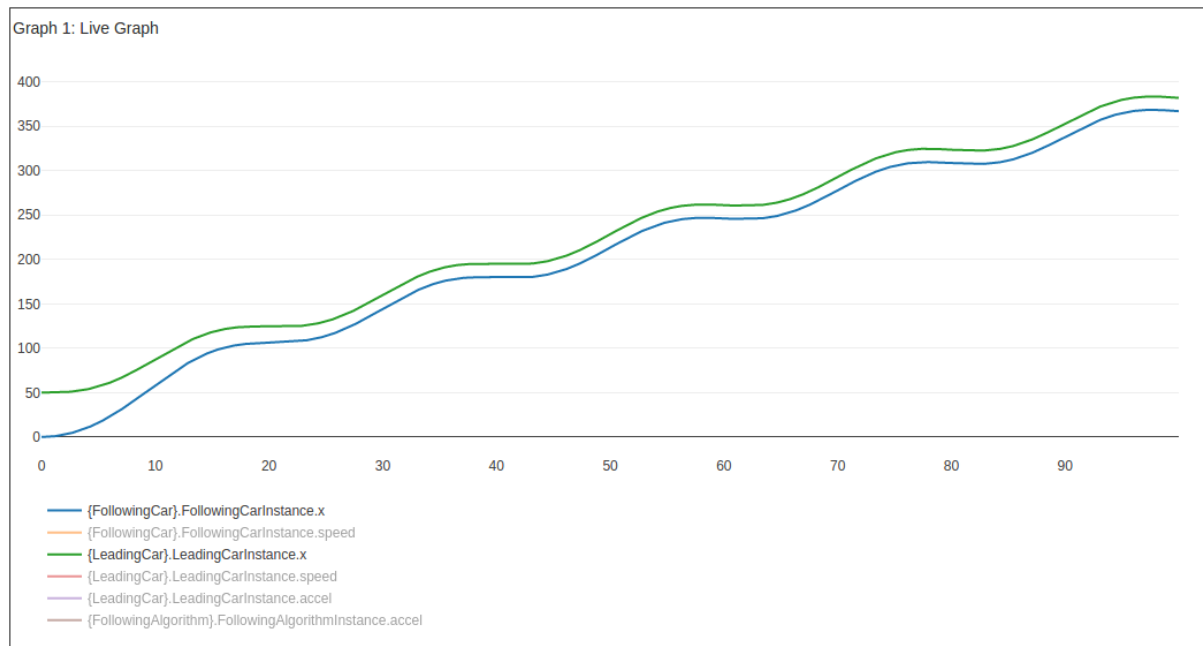
- **Attacco Semplice:** l'attacco consiste nel modificare l'input dell'FMU di attacco con il valore del parametro **attack\_value** dall'istante temporale **attack\_time** fino al termine della simulazione. Tale valore viene restituito in output dall'FMU di attacco. Tale FMU implementata tramite il file `Attack_fmu.fmu`.
- **Attacco Multi-step:** l'attacco consiste nel modificare l'input dell'FMU di attacco con il valore del parametro **attack\_value** per un tempo pari a **attack\_duration**, ripetuto **attack\_occurencies** volte e separato nel tempo da **attack\_distance** secondi. Tale valore viene restituito in output dall'FMU di attacco. L'attacco inizier dall'istante temporale **attack\_time**. Tale FMU implementata tramite il file `MultiStep_MultiAttacks_Fmu.fmu`.

## 4 — Analisi dei Risultati

### 4.1 VanillaCase

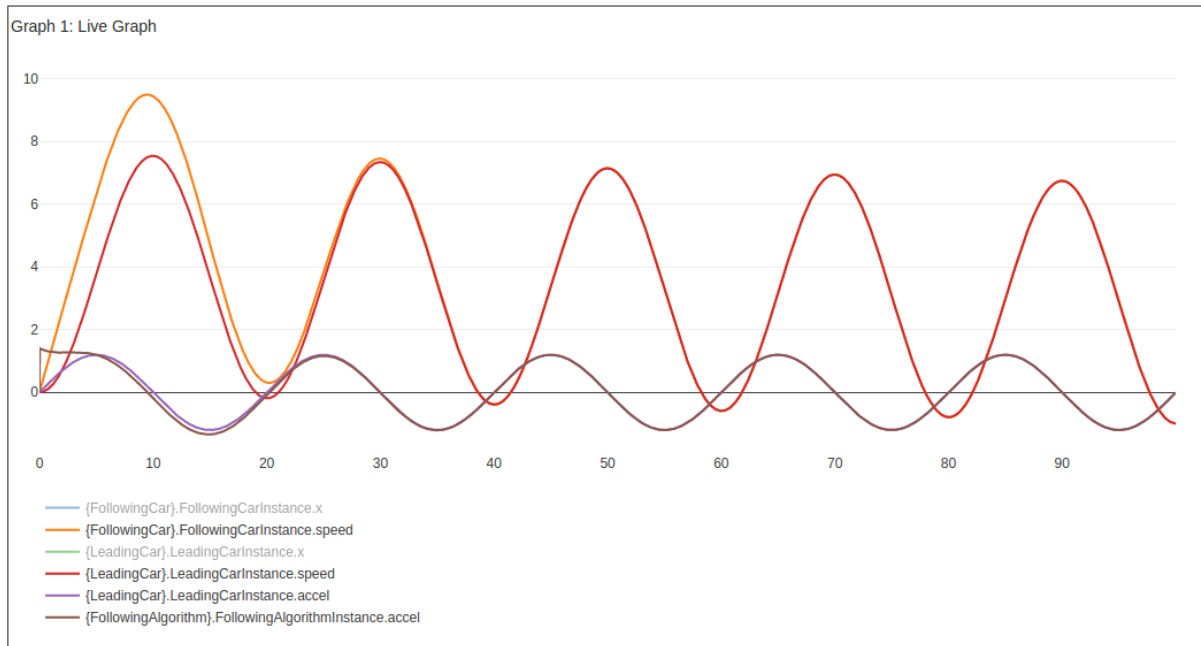
#### 4.1.1 Risultati Co-Simulazione

E' stata effettuata una simulazione nel caso base per accertarsi che il comportamento del sistema conduca alla convergenza delle due macchine.



**Figure 9:** Posizione x della LeadingCar (verde) e FollowingCar (blu)

La distanza media tra le due auto pari a **18.49m**. Dopo un iniziale periodo di transizione di circa 20s il sistema raggiunge la convergenza attesa e i due veicoli proseguono il percorso ad una distanza approssimativa di 15m fino a fine simulazione.



**Figure 10:** Velocit  e accelerazione della LeadingCar (rispettivamente rossa e viola) e FollowingCar (rispettivamente gialla e marrone)

Dalla figura sopra riportata   inoltre osservabile come negli istanti iniziali la Following Car abbia una accelerazione positiva maggiore di quella della Leading Car. Questo si riflette inoltre sulle relative velocit . Il motivo di questo comportamento   dovuto all’iniziale periodo di transizione in cui la Following Car recupera la distanza iniziale (molto maggiore di 15m) dalla Leading Car.

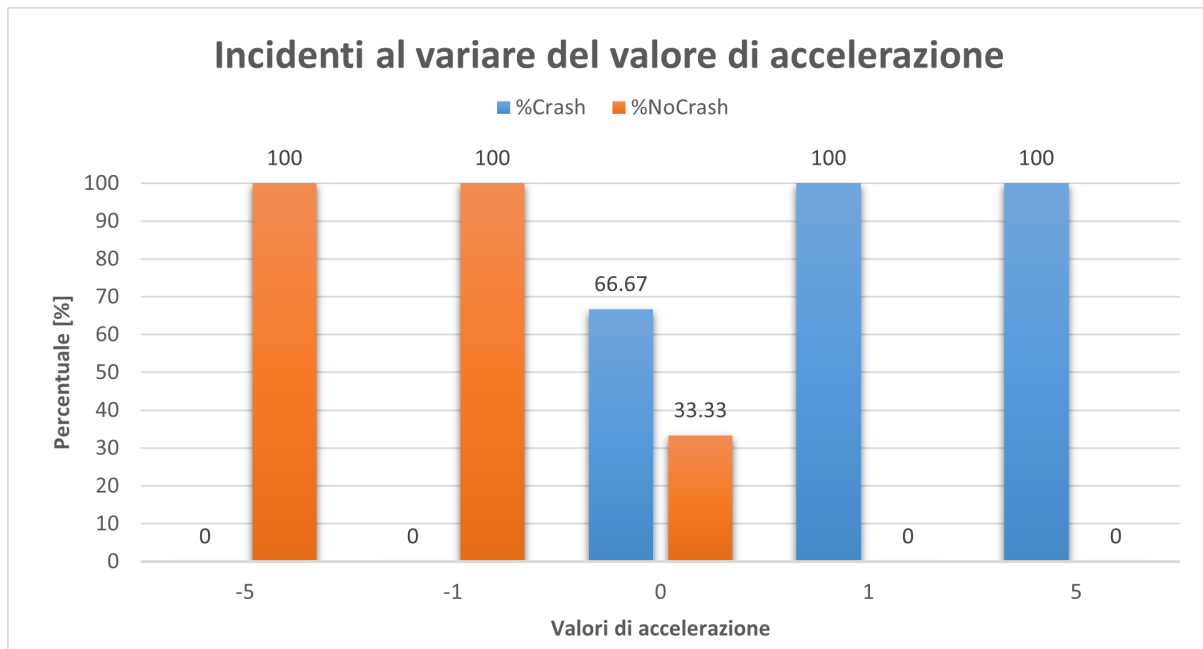
## 4.2 Attacco all’accelerazione

### 4.2.1 Attacco Semplice

**Risultati DSE** Come primo approccio all’analisi al sistema   stato scelto di fare uso del DSE, configurato andando a variare l’**attack\_value** e l’**attack\_time** con i seguenti parametri::

- **Attack\_value:** [-5, -1, 0, 1, 5]
- **Attack\_time:** [0s, .., 40s] con step a 5

I risultati ottenuti sono stati successivamente elaborati cos  da estrapolare il seguente grafico che mostra la percentuale degli incidenti per ogni **attack\_value** al variare di **attack\_time**. Per individuare le condizioni di attacco   stato necessario estrapolare la distanza minima delle due macchine sull’intero tempo di simulazione.



**Figure 11:** Rappresentazione delle percentuali di incidenti nei casi testati con studio DSE

Come si pu notare, possibile individuare tre casi ben distinti:

- **Attacchi con accelerazione negativa:** La Following Car portata a rallentare con andamento lineare fino a cambiare la propria direzione di marcia. In questo caso le macchine tendono ad allontanarsi e l'incidente non avr luogo. Inoltre doveroso sottolineare che la Following Car perde completamente la capacit di inseguimento della Leading Car. Non ci sar quindi convergenza fra le due vetture.
- **Attacchi con accelerazione pari a 0:** Dal grafico emerge una chiara necessit di uno studio pi approfondito di questa casistica in quanto non si delinea alcun risultato conclusivo. Essendo che l'accelerazione resta costante e pari a 0, la velocit della Following Car rimane costante al valore nel momento **Attack.time**. La presenza o meno di incidenti dipende quindi proprio dal valore della velocit e quindi da **Attack.time**
- **Attacchi con accelerazione positiva:** La Following Car portata ad aumentare la propria velocit con andamento lineare . In questo caso le macchine tendono ad avvicinarsi e l'incidente avr luogo.

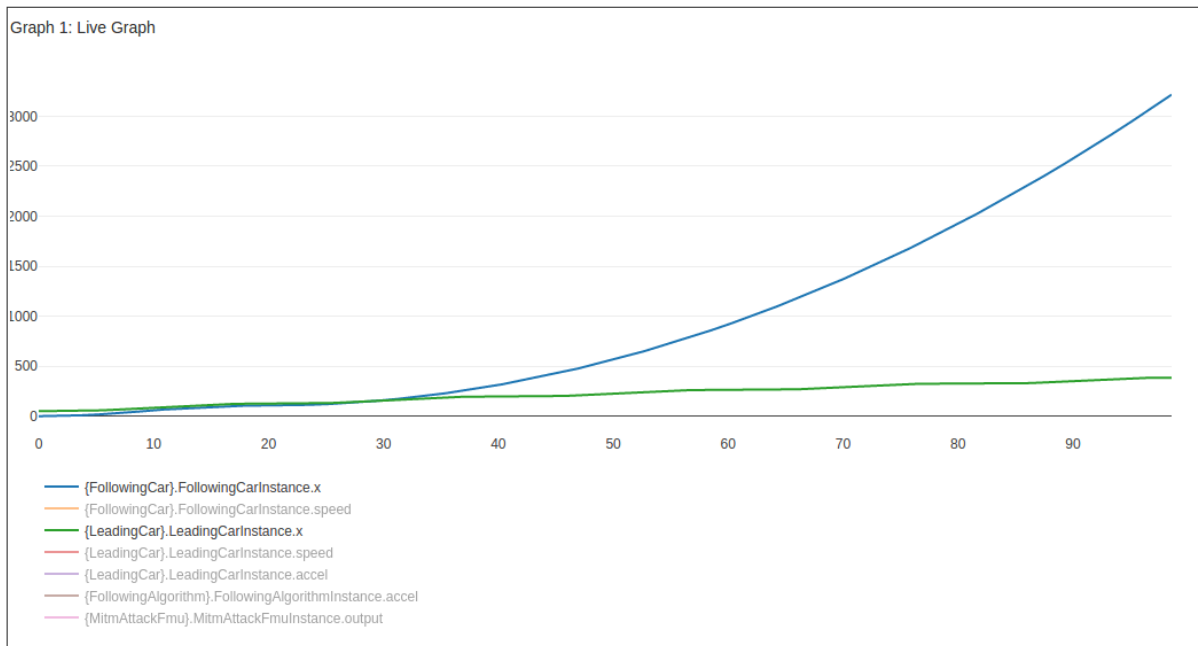
Esistono tuttavia condizioni speciali che doveroso sottolineare:

- **Attacchi con accelerazione negativa:** Se la Leading Car decellerasse con continuit (per un intervallo di tempo sufficientemente ampio ) pi di quanto non faccia la Following Car sotto attacco, allora in tal caso l'incidente avverrebbe
- **Attacchi con accelerazione positiva:** Se la Leading Car accelerasse con continuit (per un intervallo di tempo sufficientemente ampio ) pi di quanto non faccia la Following Car sotto attacco, allora in tal caso l'incidente non avverrebbe

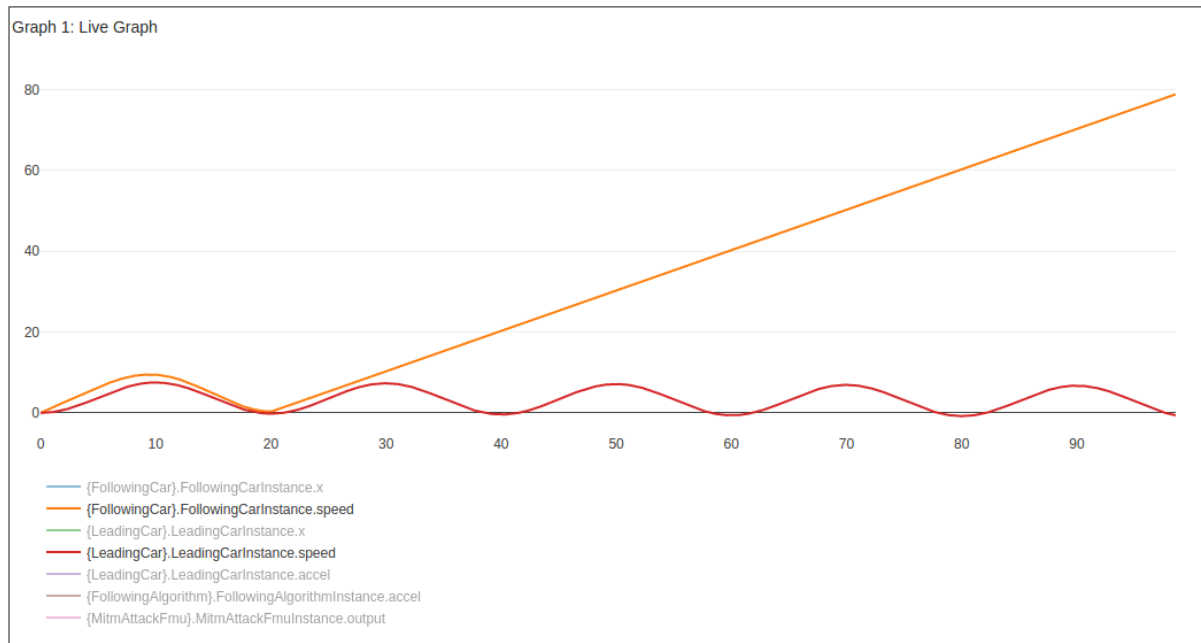
**Risultati Co-Simulazione** Con l'obiettivo di rafforzare quanto appena descritto e individuato tramite l'analisi dei risultati del DSE, vengono qui riportati tre casi fondamentali.

**Attacchi con accelerazione positiva pari a 1** Di seguito sono riportati i grafici in cui sono raffigurati le posizioni (Fig. 12), le velocità (Fig. 13) le accelerazioni (Fig. 14) delle macchine e l'accelerazione dell'algoritmo di inseguimento (Fig. 15). L'attacco è stato eseguito con:

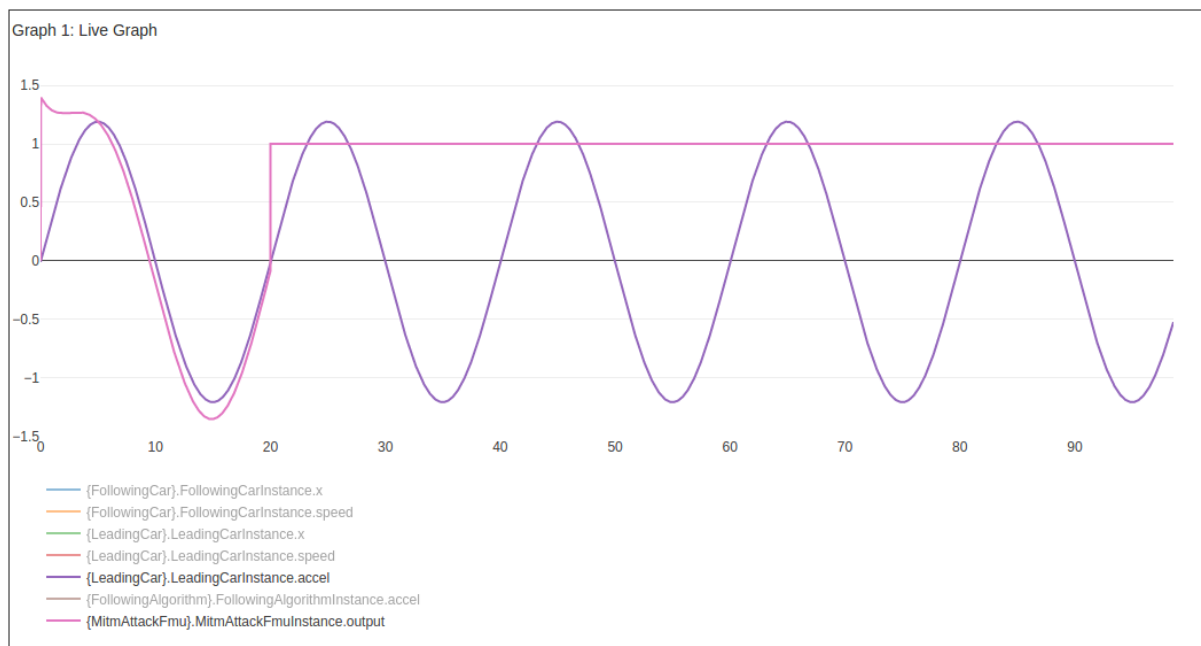
- **attack\_value:** 1
- **attack\_time:** 20s



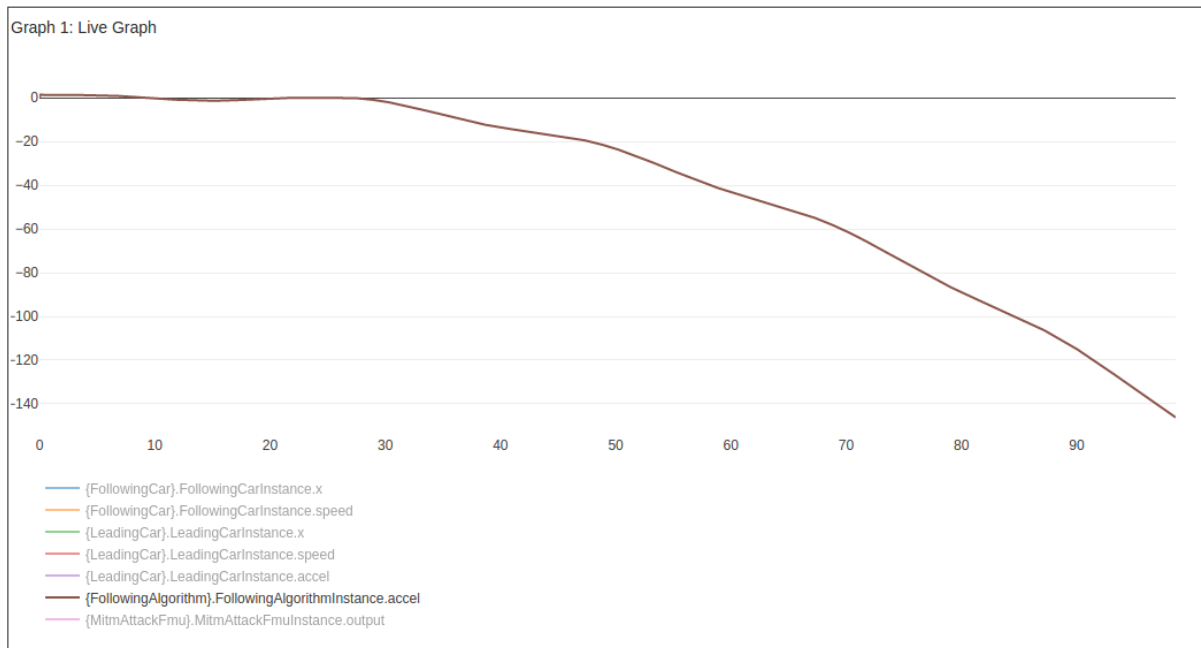
**Figure 12:** Grafico raffigurante le posizioni dei due veicoli in questo caso di attacco semplice



**Figure 13:** Grafico raffigurante le velocità dei due veicoli in questo caso di attacco semplice



**Figure 14:** Grafico raffigurante le accelerazioni dei due veicoli in questo caso di attacco semplice



**Figure 15:** Grafico raffigurante l'accelerazione suggerita da Following Algorithm in questo caso di attacco semplice

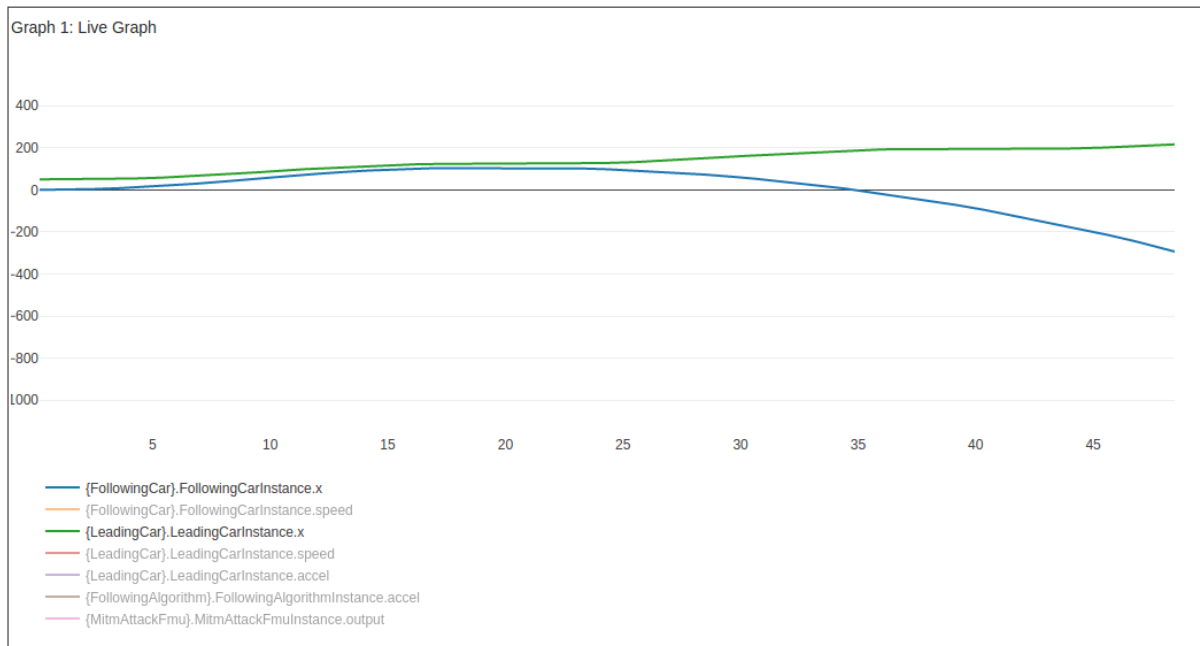
Dalle osservazioni fatte si pu evincere quanto segue:

- La Following Car e la Leading Car fanno un incidente. Essendo che l'accelerazione costante e tale che  $|Attack\_value| > 0$ , allora la velocit tende ad aumentare linearmente. L'allontanamento da Leading Car avverr in modo quadratico nel tempo
- L'accelerazione che Following Algorithm pensa di dire a Following Car sempre minore con andamento non lineare. Avr sicuramente delle micro-oscillazioni ma sono quasi impercettibili a causa dell'elevata distanza dalla Leading Car. Quindi una decelerazione/accelerazione della Leading Car ha un effetto quasi trascurabile su Following Algorithm

**Attacchi con accelerazione negativa pari a -1** Di seguito viene riportato il grafico raffigurante le posizioni dei due veicoli (Fig. 16). I grafici di velocit e accelerazione sono deducibili dal lettore osservando quelli dell'attacco precedente. L'attacco stato eseguito con:

- **attack\_value:** -1
- **attack\_time:** 20s





**Figure 16:** Ingrandimento del grafico delle posizioni dei due veicoli in questo caso di attacco semplice

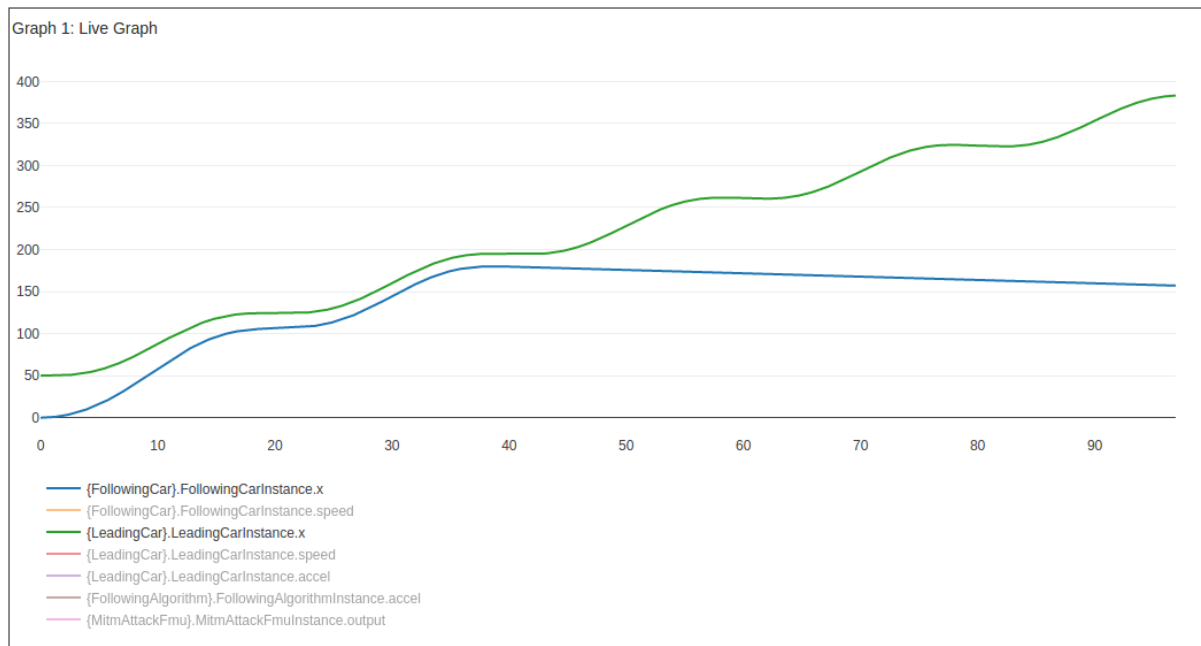
Dalle osservazioni fatte si pu evincere quanto segue:

- La Following Car non fa un incidente e continua la sua corsa in senso opposto rispetto alla Leading Car. Ogni considerazione fatta per il caso precedente rispetto a accelerazione e velocit sono ancora valide ma speculari.
- La velocit di Following Car decresce linearmente fino ad annullarsi e poi a cambiare segno (facendo muovere la macchina in retromarcia)
- Ogni considerazione fatta nel caso precedente rispetto all'accelerazione che Following Algorithm pensa di dire a Following Car tutt'ora valida e speculare al caso precedente.

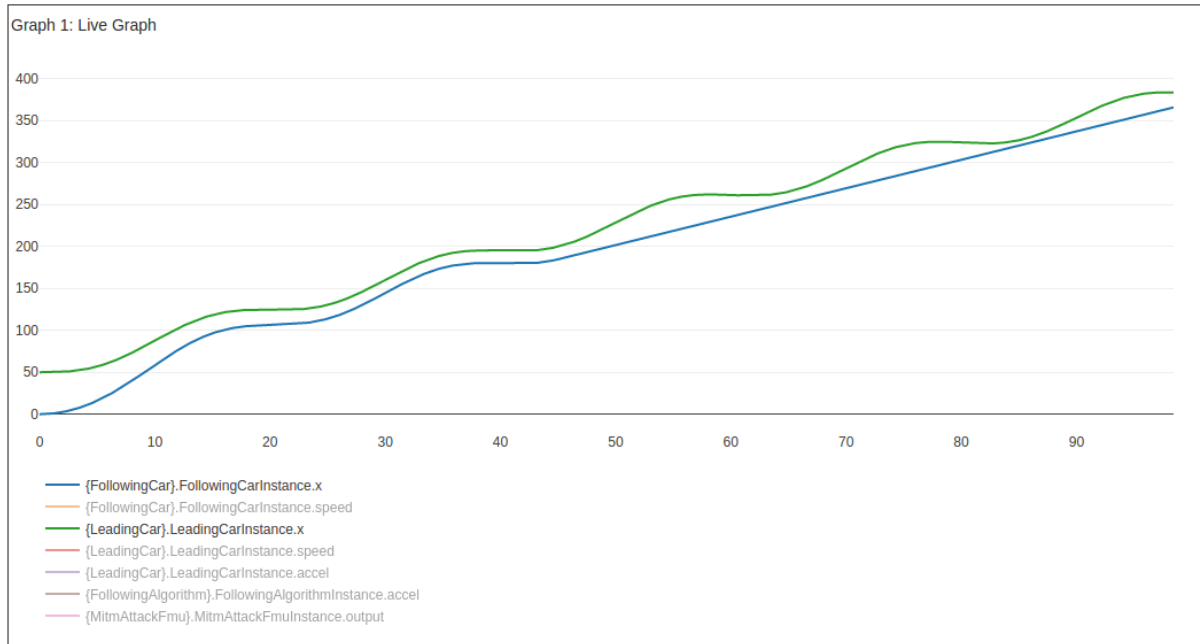
**Attacchi con accelerazione pari a 0** Nella tabella seguente sono riportati le diverse simulazioni effettuate per il caso **attack\_value = 0**. Per ogni casistica viene indicato il diverso tempo di attacco, una idea approssimativa della velocit a cui la Following Car si stabilizza ed infine una breve descrizione di alcune osservazioni fatto sul risultato ottenuto.

A dimostrazione dell'elevata variabilit del risultato vengono ora proposti tre grafici raffiguranti le posizioni dei due veicoli nei tre casi a convergenza sopra descritti.

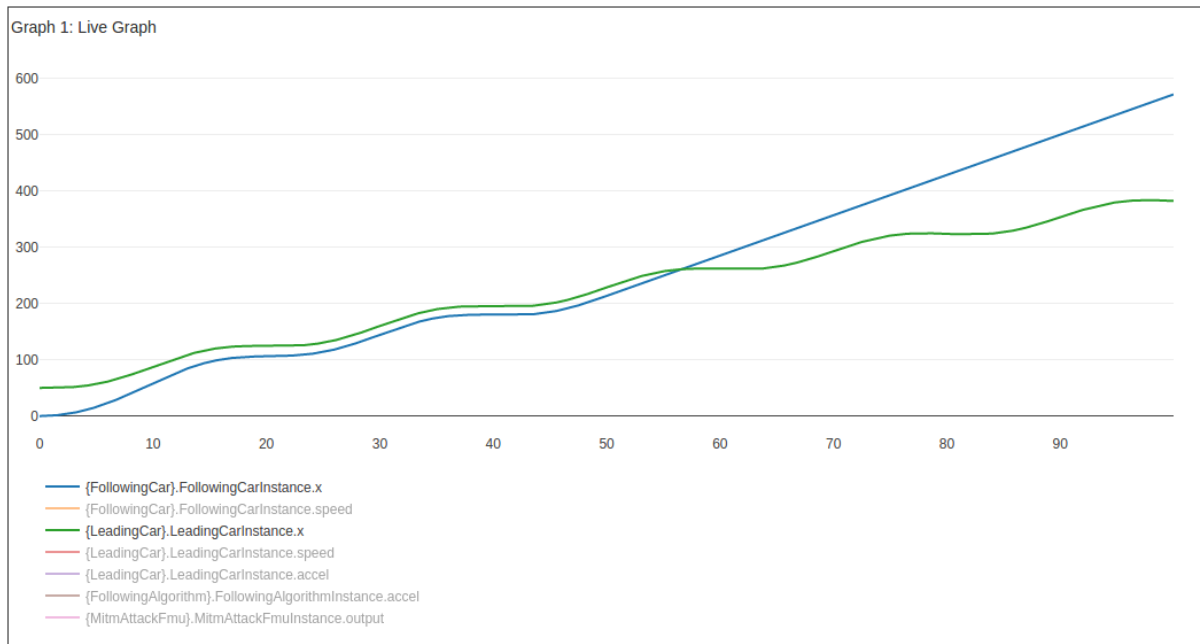
Stato Convergenza	Tempo di Attacco	Valore Velocit Following Car dopo Attacco	Risultato
Prima della Convergenza	10	Circa Valore Massimo	La following car fa un incidente. Accelerazione risultato di Following Algorithm ha andamento sinusoidale decrescente, posizione leading car non trascurabile
	15	Circa Valore Medio	Si verifica un incidente tra i veicoli. Accelerazione di Following Algorithm decrescente con andamento sinusoidale
	20	Circa Valore Minimo	Following car non fa un incidente e continua la sua corsa distanziandosi dalla leading car. L'accelerazione risultato di Following Algorithm per following car ha un andamento sinusoidale e crescente
Dopo la Convergenza	40	Circa Valore Minimo	Accelerazione risultato di Following Algorithm crescente con andamento sinusoidale. Nessun incidente ma allontanamento con movimento di Following Car in senso opposto.
	45	Circa Valore Medio	Susseguirsi di avvicinamenti e allontanamenti fra i due veicoli. Se progredita nel tempo pu portare ad un lento avvicinamento e ad incidente. Accelerazione di Following Algorithm ha un andamento sinusoidale decrescente.
	50	Circa Valore Massimo	Following Car fa un incidente con leading car. Accelerazione di Following Algorithm sinusoidale decrescente



**Figure 17:** Grafico della posizione dei veicoli nel caso Tempo di Attacco a 40s



**Figure 18:** Grafico della posizione dei veicoli nel caso Tempo di Attacco a 45s



**Figure 19:** Grafico della posizione dei veicoli nel caso Tempo di Attacco a 50s

I grafici in Fig. 17 e 18, ad esempio, mostrano come, nonostante vengano simulati attacchi con **attack\_time** molto simili, il risultato sia completamente diverso.

#### 4.2.2 Attacco Multiplo

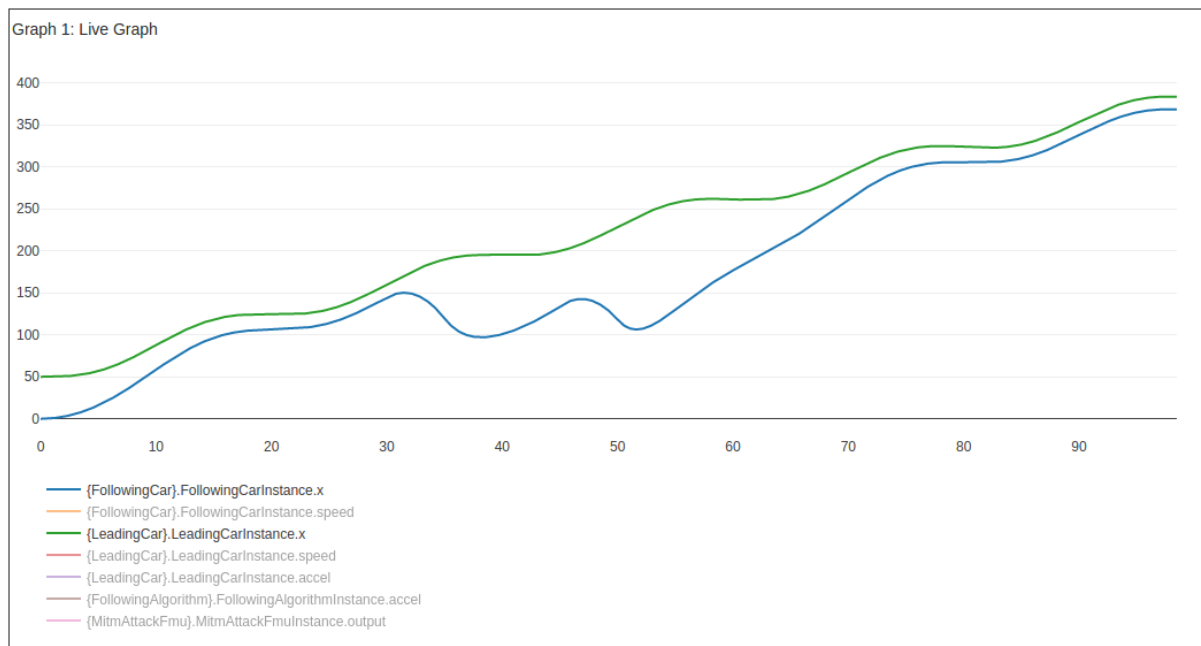
In questa sezione vengono riportate due diverse condizioni di attacco in cui quest'ultimo ha una durata di un certo numero di step e si ripete pi volte nel tempo. L'obiettivo quello di individuare una condizione in cui, nonostante gli attacchi ripetuti, il sistema risulta tollerante e uno invece in cui l'attacco porta ad un incidente fra i due veicoli

## Risultati Co-Simulazione

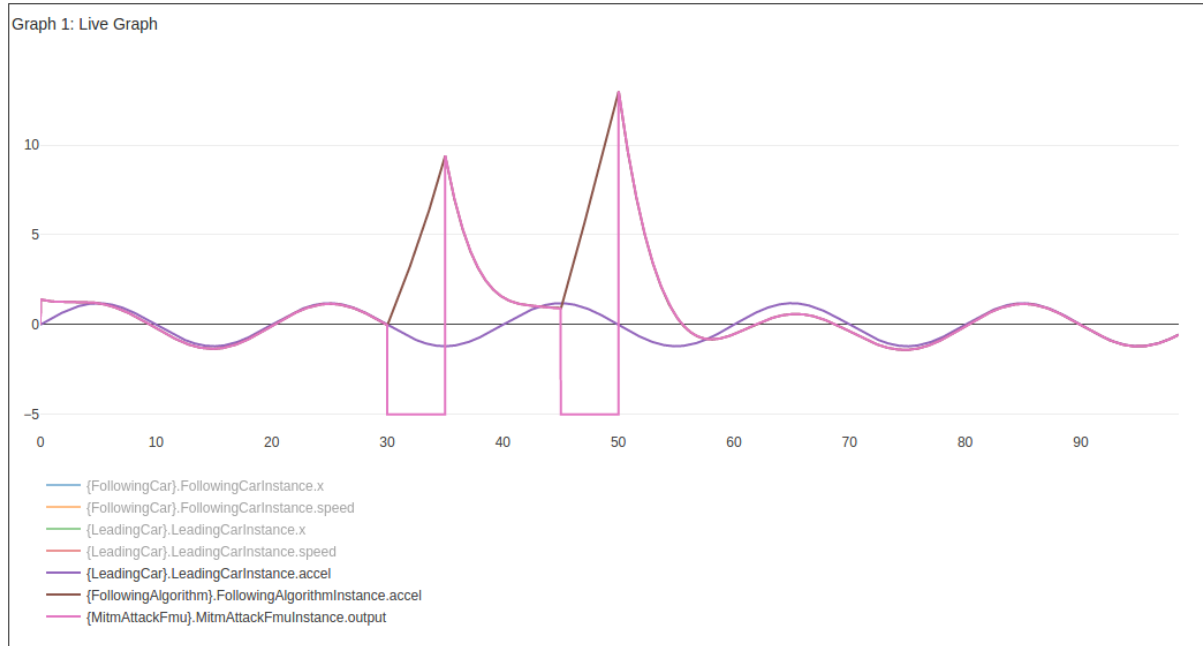
**Attacco senza incidente** L'obiettivo della presente co-simulazione è quello di andare ad individuare un attacco in cui la presenza di più occorrenze risulta essere un elemento non chiave nel verificarsi di un incidente fra i due veicoli. In particolare viene posto come obiettivo quello di studiare il comportamento della Following Car al termine dell'attacco multiplo. Di seguito sono riportate le configurazioni dell'attacco in esame.

- **Attack\_occurrences:** 2
- **Attack\_duration:** 5s
- **Attack\_time:** 30s
- **Attack\_value:** -5
- **Attack\_distance:** 10s
- **Step\_size:** 0.01s

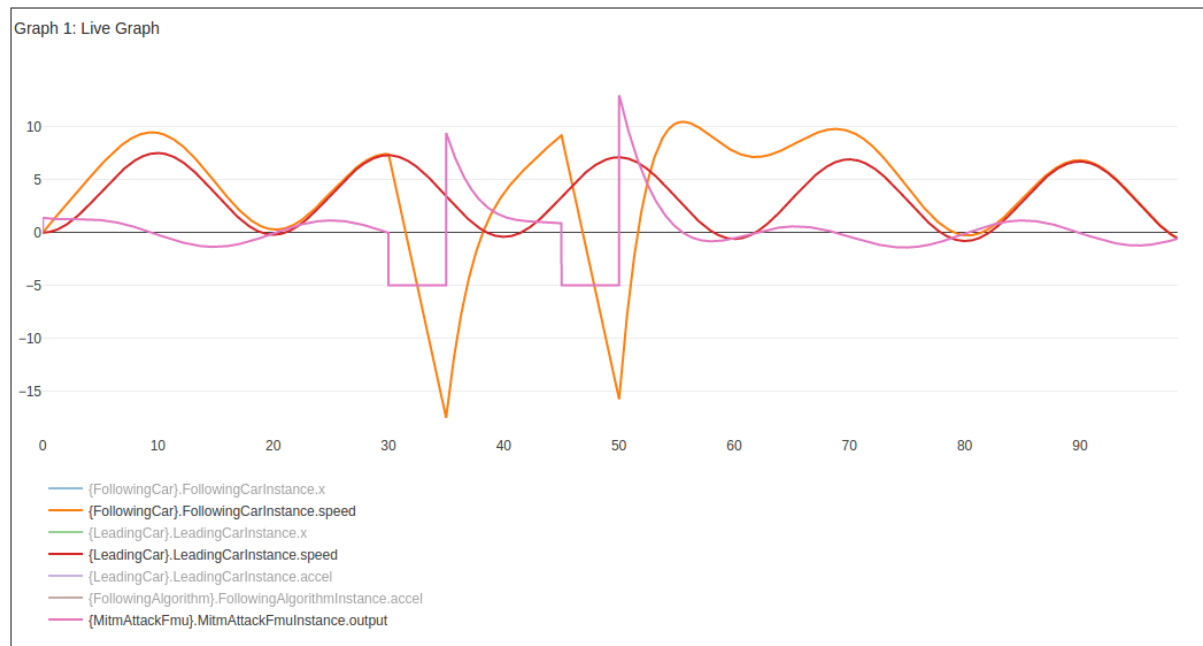
Vengono ora riportati i risultati della co-simulazione nelle immagini seguenti.



**Figure 20:** Grafico di posizione dei due veicoli nel caso di attacco multiplo in esame. Notare il non verificarsi di un incidente e il ritorno a convergenza.



**Figure 21:** Grafico delle accelerazioni nel caso di attacco multiplo in esame.



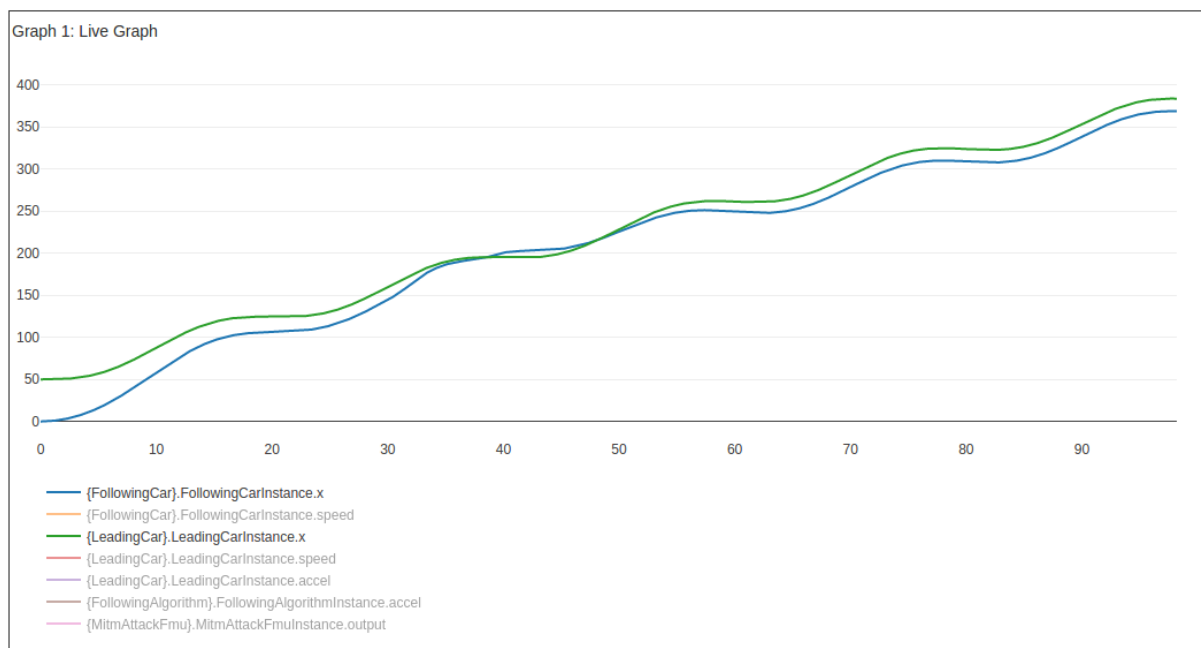
**Figure 22:** Grafico di velocit dei due veicoli nel caso di attacco multiplo in esame.

Osservando i grafici sopra descritti possibile osservare come, nonostante il verificarsi di molteplici attacchi, la Following Car non crei alcun incidente. Inoltre doveroso soffermare l'attenzione sulla tolleranza del sistema a questo tipo di attacco, al termine del quale la Following Car si avvicina nuovamente portandosi alla distanza di 15m dalla Leading Car.

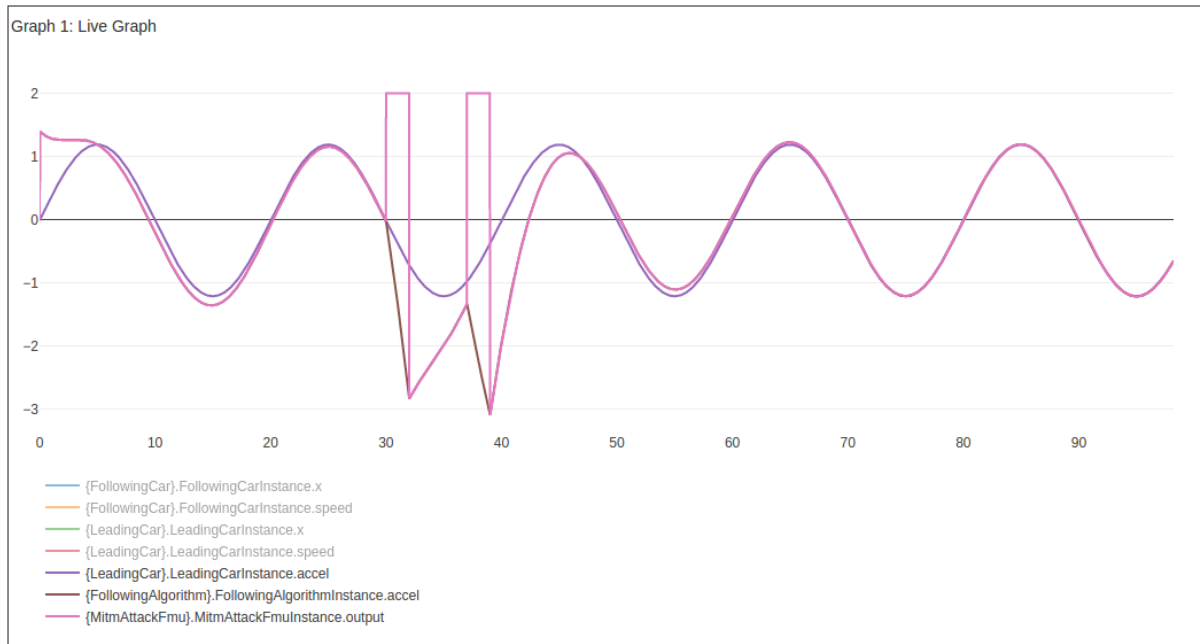
**Attacco con incidente** L'obiettivo della presente co-simulazione quello di andare ad individuare un attacco in cui la presenza di pi occorrenze risulta essere un elemento chiave nel verificarsi di un incidente fra i due veicoli. Di seguito sono riportate le configurazioni dell'attacco in esame.

- **Attack\_occurrences:** 2
- **Attack\_duration:** 2s
- **Attack\_time:** 30s
- **Attack\_value:** +2
- **Attack\_distance:** 5s
- **Step\_size:** 0.01s

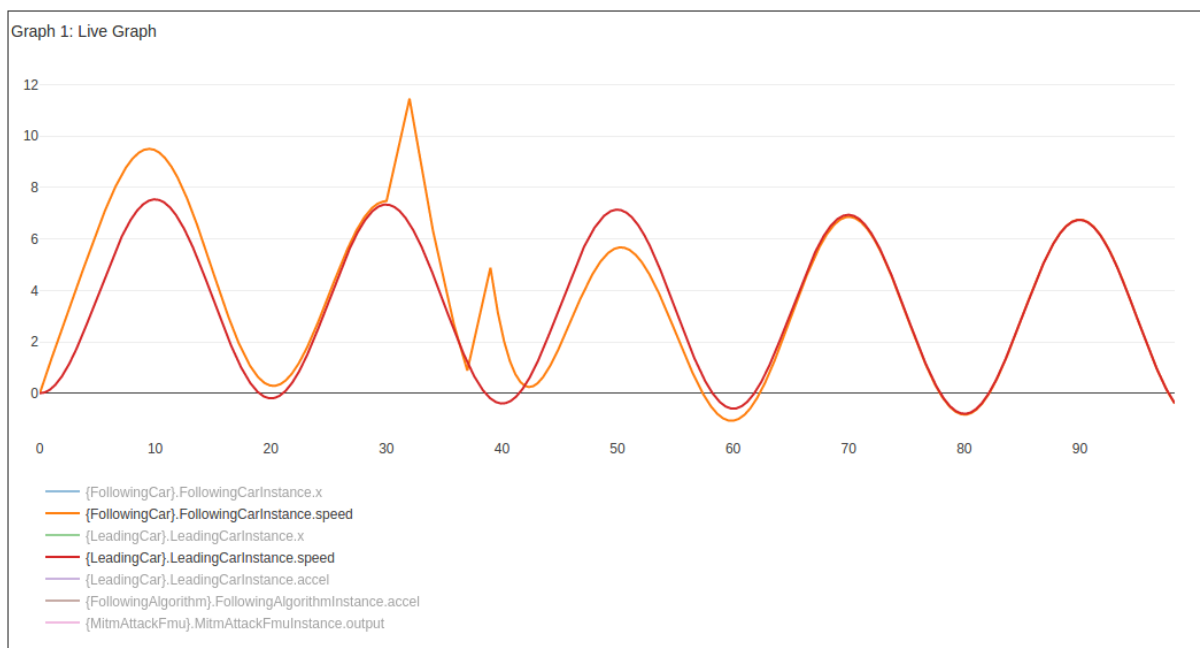
Vengono ora riportati i risultati della co-simulazione nelle immagini seguenti.



**Figure 23:** Grafico di posizione dei due veicoli nel caso di attacco multiplo in esame. Notare il verificarsi di un incidente.



**Figure 24:** Grafico delle accelerazioni nel caso di attacco multiplo in esame.



**Figure 25:** Grafico di velocit dei due veicoli nel caso di attacco multiplo in esame.

Osservando i grafici sopra descritti possibile osservare come il secondo evento di attacco risulta fondamentale nel verificarsi dell'incidente. Senza questo secondo evento infatti la Following Car si sarebbe nuovamente distanziata dalla Leading Car cos da raggiungere la distanza richiesta di 15m.

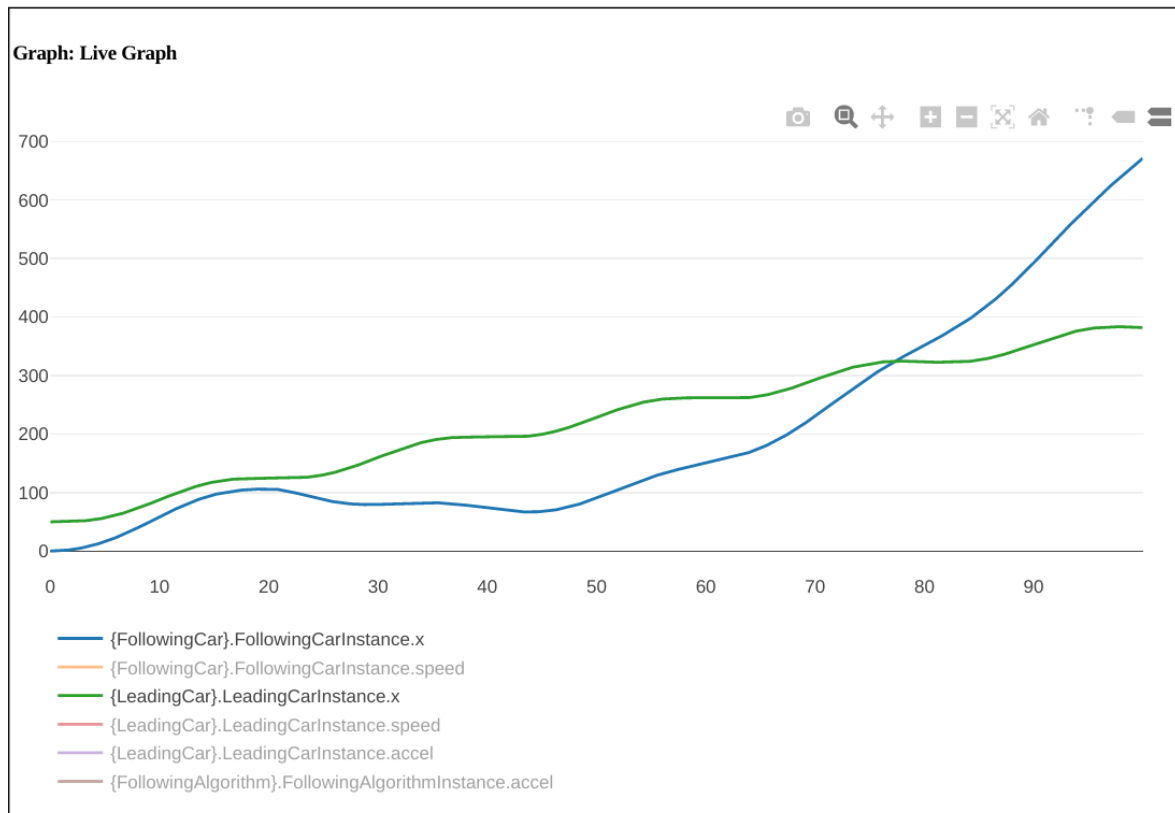
## 4.3 Attacco alla X

### 4.3.1 Attacco Semplice

**Risultati Co-Simulazione** Per cercare di dare un'interpretazione ai risultati del successivo studio verr prima analizzato un caso d'esempio con i seguenti parametri:

- **attack\_value:** 200
- **attack\_time:** 20s

Si ottiene il seguente grafico:



**Figure 26:** Posizione x della Leading Car (verde) e Following Car (blu)

Dal seguente risultato è possibile evincere tre differenti zone di comportamento della Following Car: nel **primo caso** nel quale l'attacco non viene ancora effettuato, la Following Car tende ad avvicinarsi alla Leading Car alla distanza configurata; nel **secondo caso**, da un tempo di 20s ad uno di circa 40s, l'attacco inizia ma la Leading Car non ha ancora superato l'**attack\_value** impostato, che rappresenta la (alterata) posizione della Following Car: quest'ultima pensa di trovarsi davanti e decelererà; il **terzo caso**, dopo 40s, nel quale la Leading Car ha superato l'attack value e perciò la Following Car inizia a riavvicinarsi fino all'impatto tra le due auto. Per come è configurata la Leading Car, ovvero che tende sempre ad andare "in avanti" con qualche oscillazione nella velocità, è facile intuire che **un incidente con questo tipo di attacco per un tempo sufficiente avrà sempre luogo**, in quanto esisterà sempre un tempo nella quale la Leading Car supererà l'attack\_value, per quanto elevato possa essere quest'ultimo.



**Risultati DSE** E' stato studiato l'esito dell'attacco (INCIDENTE/NON INCIDENTE) andando a variare l'**attack\_value** e l'**attack\_time** con i seguenti parametri:

- **Attack\_value:** [0 .. 200] con step a 1
- **Simulation\_time:** [50s, 100s]

I risultati ottenuti possono essere riassunti nella seguente tabella

Tempo di Simulazione	Attack Value	Risultato
50s	[0, 149]	INCIDENTE
	[150, 199]	NO INCIDENTE
100s	[0, 199]	INCIDENTE
	-	NO INCIDENTE

Come si pu notare il tempo una variabile importante per questo tipo di attacco, con un tempo sufficientemente alto l'attacco ha sempre luogo come detto in precedenza.

#### 4.4 Attacco Multiplo

Sono state individuate quattro diverse configurazioni che danno luogo a quattro classi di risultati diversi:

- **Attack\_occurencies:** 3
- **Attack\_duration:** 2s
- **Attack\_time:** [30s, 50s, 70s]
- **Attack\_value:** 200
- **Attack\_distance:** 5s
- **Step\_size:** 0.01s

L'attacco pertanto avr un pattern simile a livello temporale, la variabile l'inizio dell'attacco stesso. I risultati degli esperimenti sono riassunti nella seguente tabella

Attack Time	Distanza Minima	Risultato
30s	14.9368	NO INCIDENTE
50s	0.639284	NO INCIDENTE
70s	-20.38	INCIDENTE

Una semplice interpretazione di questi risultati si basa sul fatto che il Following Algorithm produce un'accelerazione maggiore in caso la distanza tra le due auto sia maggiore: considerato che la distanza della Following Car vista dal Following Algorithm fissa (per via dell'attacco in corso), nel caso il tempo di inizio dell'attacco sia maggiore, maggiore sar la posizione della Leading Car e perci maggiore sar l'accelerazione in input. Questo ci che porta ad una collisione nel caso di Attack time pari a 70s.

## 5 — Conclusioni

A fronte dello studio riportato in questo documento risulta evidente come i casi di attacchi (tra Following Algorithm e Following Car) alla posizione e quelli all'accelerazione (con valore positivo) possano essere identificati come i casi più critici in quanto portano con estrema probabilità ad un incidente tra i veicoli.

Ad opinione degli autori di questo documento sarebbe opportuno investire risorse per contrastare queste casistiche rendendo il sistema più tollerante: ad esempio aggiungere ridondanza tra i collegamenti per individuare condizioni di attacco.

Attacchi all'accelerazione con valore pari a 0 risultano scaturire in comportamenti variabili a seconda del tempo di attacco.

Attacchi all'accelerazione con valori negativi risultano invece meno critici dal punto di vista degli incidenti, i quali risultano essere altamente improbabili.