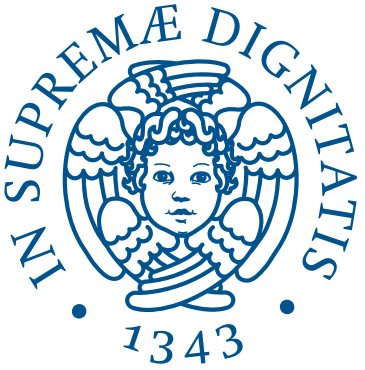


# UNIVERSITÀ DI PISA

Computer Engineering

Formal Methods for Secure Systems

## *Project Report*

---

*TEAM MEMBERS*:
Matteo Biondi
Olgerti Xhanej

Academic Year: 2020/2021

# Contents

# 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 è l'asse x.

L'obiettivo del progetto è il seguente: analizzare possibili attacchi al suddetto sistema che possono causare uno scontro tra i due veicoli.

# 2 — Scelte di Sviluppo

## 2.1 Strategia Attacco

Gli attacchi verrano 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 è necessario conoscere i dettagli implementativi delle FMU in gioco. Questo a patto di 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 sensoring 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 carò Per funzionare prende in ingresso l'accelerazione dalla precedente FMU e produce in output la sua posizione e velocità.

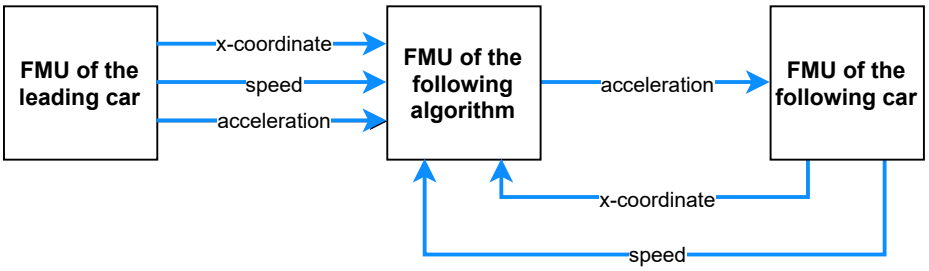


**Figure 1:** Multi-Model schema del VanillaCase

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

... Overview Vanilla Case ...

## 3.2 Attacco all'accelerazione

A differenza dello schema presentato nel VanillaCase, viene ora aggiunto un ulteriore FMU situato fra "FMU of the following algorithm" e "FMU of the following car" già presenti. Il nuovo 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.

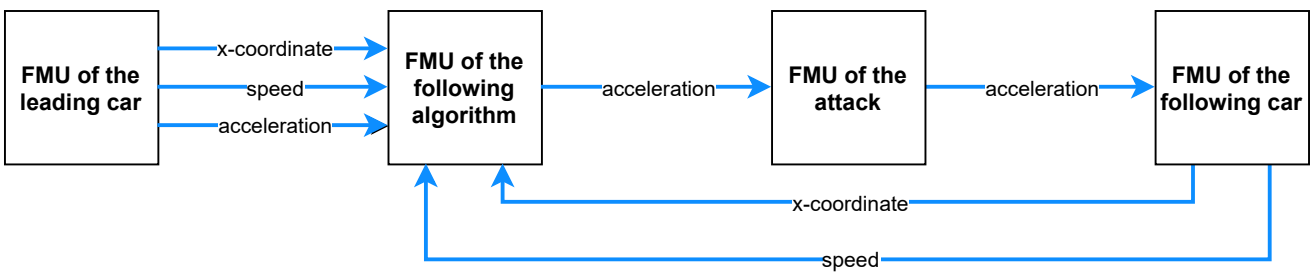


**Figure 2:** Multi-Model schema dell'Attacco alla Accelerazione

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

... Overview Caso Singolo ... ... Overview Caso Multiplo ...

## 3.3 Attacco alla Posizione

A differenza dello schema presentato nel VanillaCase, viene ora aggiunto un ulteriore FMU situato fra "FMU of the following car" e "FMU of the following algorithm" già presenti. Il nuovo 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.

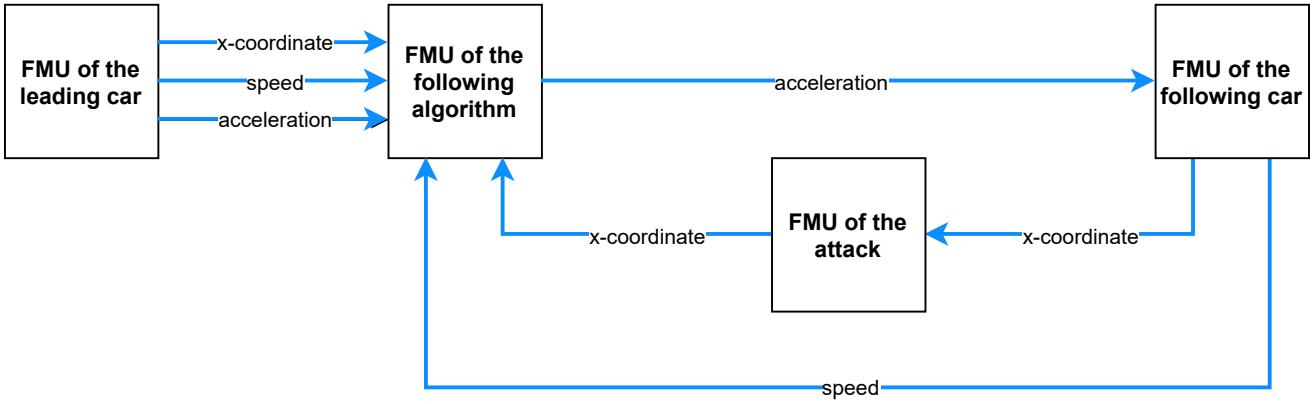


**Figure 3:** Multi-Model schema dell'Attacco alla Posizione

In figura 6 viene rappresentata l'overview del relativo Multi-Model sviluppato con il tool INTO-CPS.

... Overview Caso Singolo ... ... Overview Caso Multiplo ...

## 3.4 Configurazione in Comune

La configurazione dei seguenti FMU verrà applicata per tutte le simulazioni che verranno effettuate.

- **LeadingCar**:
  - Posizione iniziale **x0**: 50m
  - Velocità iniziale **v0**: 0m/s
- **FollowingAlgorithm**:
  - **c1**: 0.5
  - **eps**: 1
  - **omega_n**: 0.2
- **FollowingCar**:
  - Posizione iniziale **x0**: 0m
  - Velocità iniziale **v0**: 0m/s

## 3.5 Comportamento degli Attacchi

L'FMU che verrà utilizzata negli attacchi MITM presenterà due implementazioni diverse:

- **Attacco Semplice**: l'attacco consiste nel modificare l'input dell'AttackFMU con il valore del parametro **attack_value** dall'istante temporale **attack_time** fino al termine della simulazione. Tale valore viene restituito in output dall'AttackFMU. Tale FMU è implementata tramite il file Attack_fmu.fmu.

- **Attacco Multi-step**: l'attacco consiste nel modificare l'input dell'AttackFMU con il valore del parametro **attack_value** per un tempo pari a **attack_duration**, ripetuto **attack_occurrencies** volte e separato nel tempo da **attack_distance** secondi. Tale valore viene restituito in output dall'AttackFMU. L'attacco inizierà dall'istante temporale **attack_time**. Tale FMU è 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.

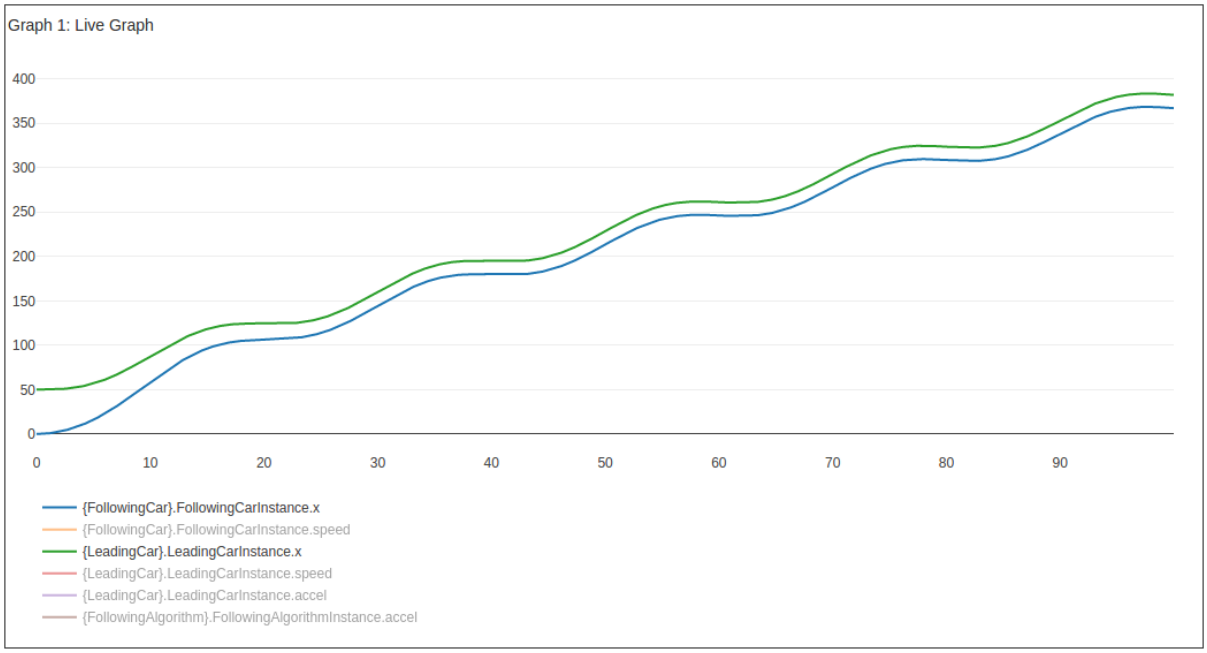


**Figure 4:** Posizione x della LeadingCar (verde) e FollowingCar (blu)

La distanze media tra le due auto è 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.

... immagine accel_speed ...

Dalla figura sopra riportata è inoltre osservabile come negli istanti iniziali la following car abbia una accelerazione positiva maggiore di quella della leading. Questo si riflette inoltre sulle relative velocità. Il motivo di questo comportamento è 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 è 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]
- **Simulation_time**: [0s, .., 40s] con step a 5

I risultati ottenuti sono stati successivamente eleborati così 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 è stato necessario estrapolare la distanza minima delle due macchine sull'intero tempo di simulazione.

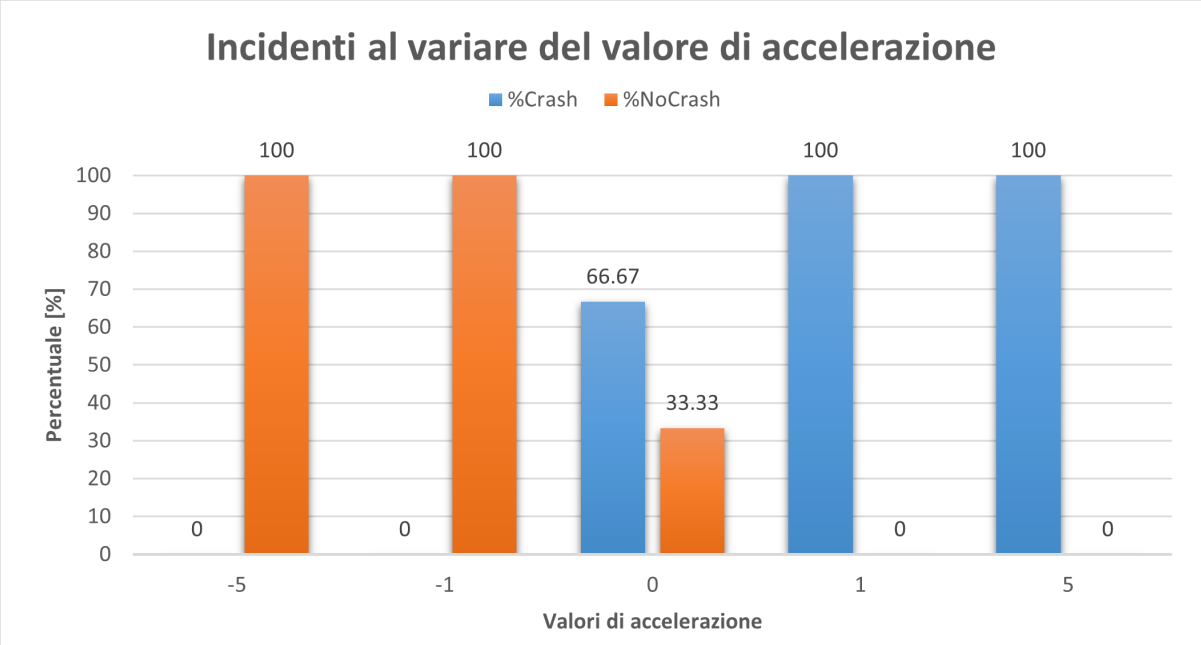


**Figure 5:** Rappresentazione delle percentuali di incidenti nei casi testati con studio DSE

Come si può notare, è possibile individuare tre casi ben distinti:

- **Attacchi con accelerazione negativa**: La following car è 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 avrà luogo. Inoltre è doveroso sottolineare che la following car perde completamente la capacità di inseguimento della leading car. Non ci sarà quindi convergenza fra following e leading car.

- **Attacchi con accelerazione pari a 0**: dal grafico emerge una chiara necessità di uno studio più approfondito di questa casistica in quanto non si delinea alcun risultato conclusivo. Essendo che l'accelerazione resta costante e pari a 0, la velocità della following car rimane costante al valore nel momento **Attack_time**. La presenza o meno di incidenti dipende quindi proprio dal valore della velocità e quindi da **Attack_time**

- **Attacchi con accelerazione positiva**: La following car è portata ad aumentare la propria velocità con andamento lineare . In questo caso le macchine tendono ad avvicinarsi e l'incidente avrà luogo.

Esistono tuttavia condizioni speciali che è doveroso sottolineare:

- **Attacchi con accelerazione negativa**: Se la leading car decellerasse con continuità (per un intervallo di tempo sufficientemente ampio ) più 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 continuità (per un intervallo di tempo sufficientemente ampio ) più 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** Diseguito sono riportati i grafici in cui sono raffigurati l'attacco alle accelerazioni (Fig ...) e le posizioni dei due veicoli (Fig ...) L'attacco è stato eseguito con:

- **attack_value**: 1
- **attack_time**: 20s

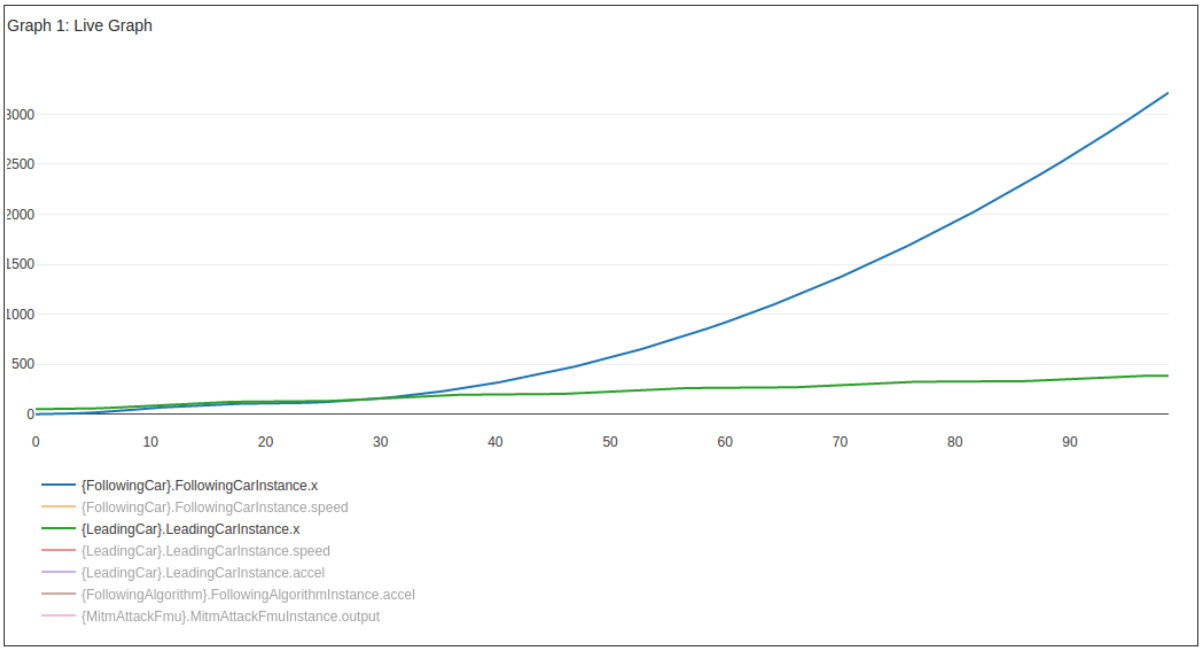


**Figure 6**

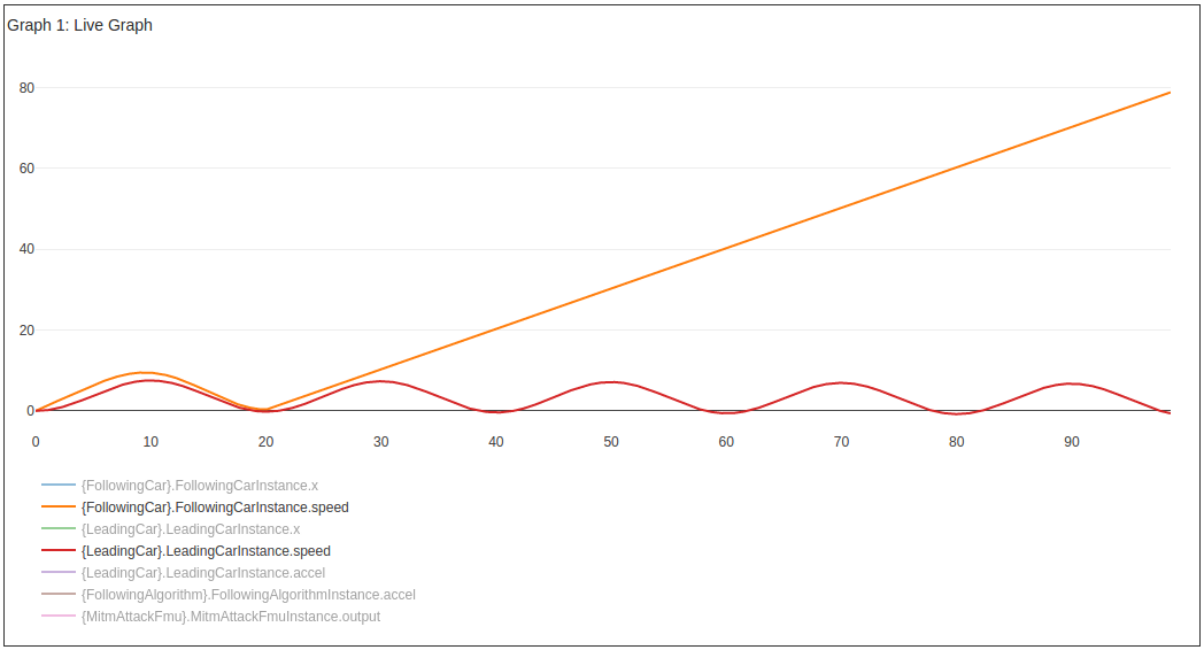


**Figure 7**

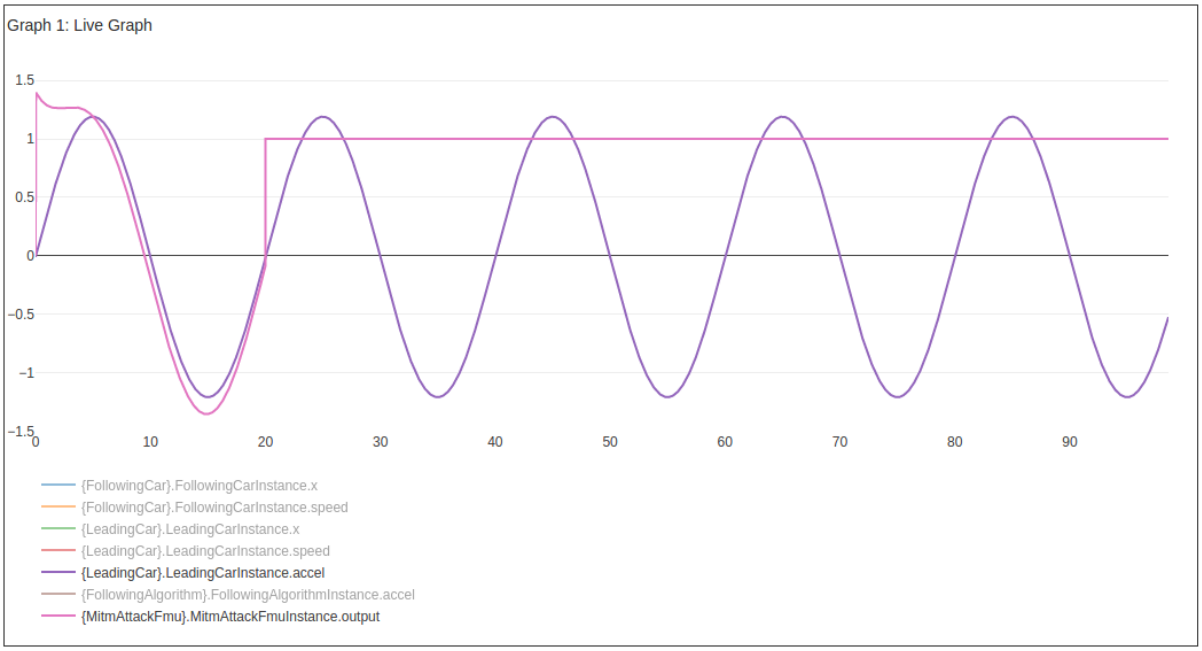


**Figure 8**

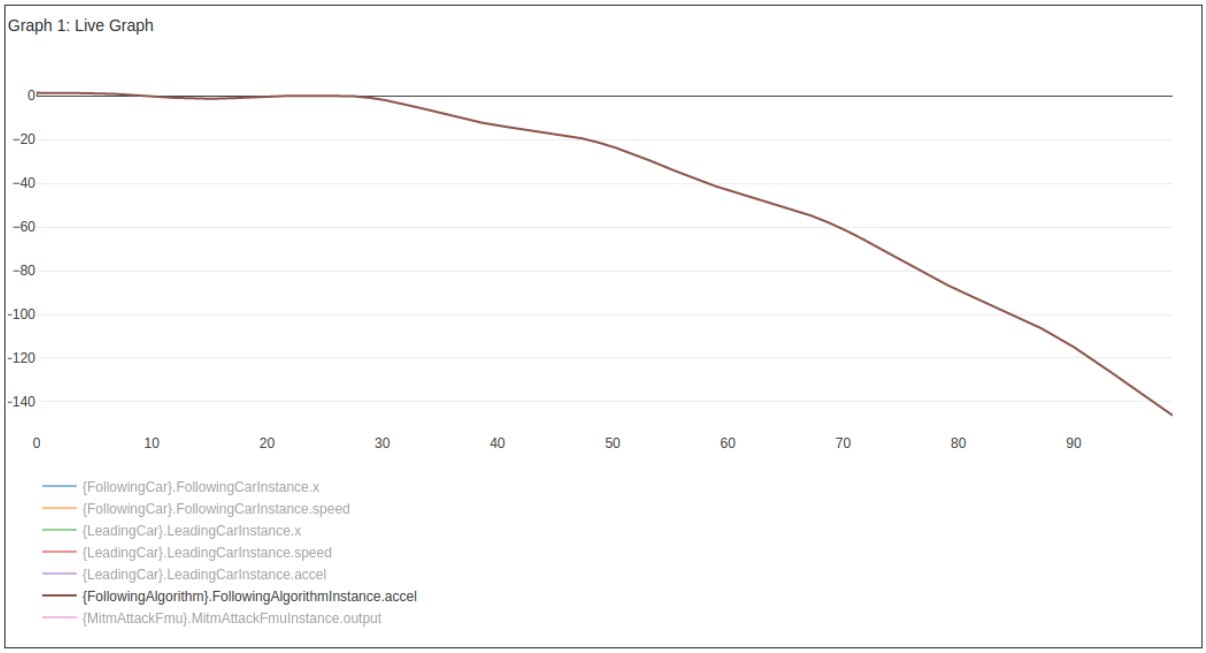


**Figure 9**

Dalle osservazioni fatte si può evincere quanto segue:

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

**Attacchi con accelerazione negativa pari a -1** Diseguito sono riportati i grafici in cui sono raffigurati l'attacco alle accelerazioni (Fig ...) e le posizioni dei due veicoli (Fig ...) L'attacco è stato eseguito con:

- **attack_value**: -1
- **attack_time**: 20s

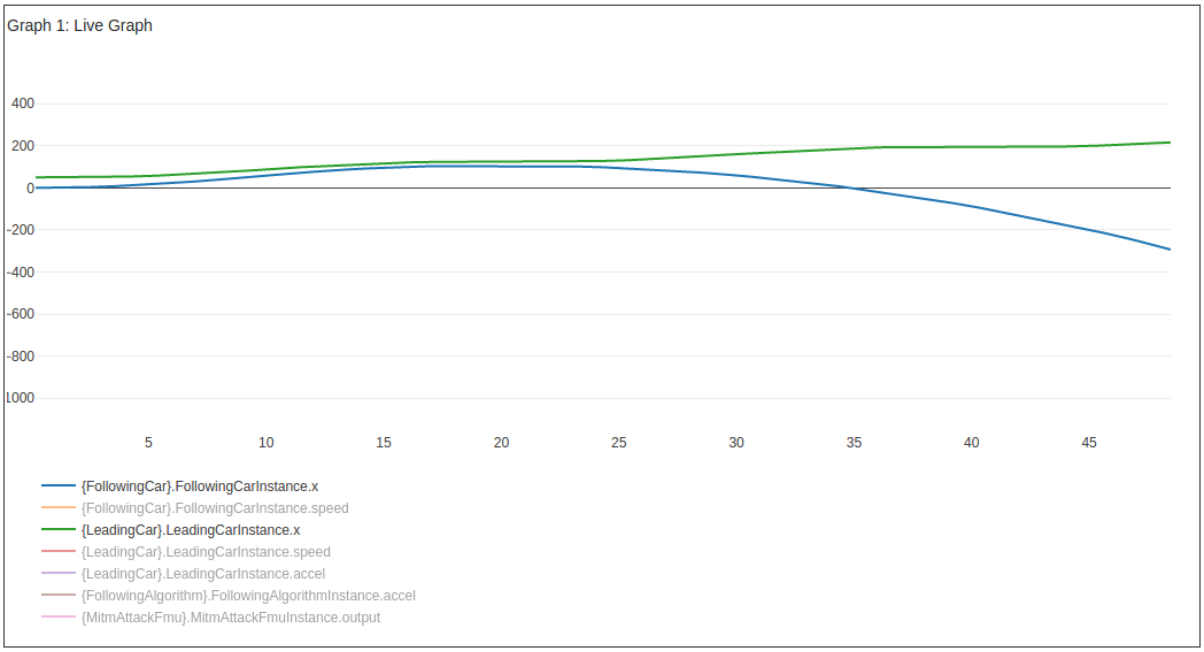


**Figure 10:** Ingrandimento del grafico delle posizioni dei due veicoli

Dalle osservazioni fatte si può 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 velocità sono ancora valide ma speculari.
- La velocità 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 è tutt'ora valida e speculare al caso precedente.

### Attacchi con accelerazione pari a 0

| Stato Convergenza | Tempo di Attacco | Valore Velocità dopo Attacco | Risultato |
|---|---|---|---|
| Prima della Convergenza | 10 | Circa Valore Massimo | La following car fa un incidente. Accelerazione di following Algorithm sinusoidale decrescente, posizione leading car non trascurabile |
| | 15 | Circa Valore Medio | Incidenti multipli ma la macchina non si allontana troppo dalla leading Car. Accelerazione decrescente con andamento sinusoidale |
| | 20 | Circa Valore Minino | Following car non fa un incidente e continua la sua corsa distanziandosi sempre più dalla leading car. l'accelerazione che il following algorithm pensa di dire a followingcar ha un andamento sinusoidale e crescente |
| Dopo la Convergenza | 40 | Circa Valore Minimo | Accelerazione 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 può portare ad un lento avvicinamento e ad incidente. Accelerazione di Following Algorithm ha un andamento sinusoidale che presenta un valore di picco ed un valore minimo sempre minore. |
| | 50 | Circa Valore Massimo | Following Car fa incidente. Accelerazione di following algorithm sinusoidale decrescente |

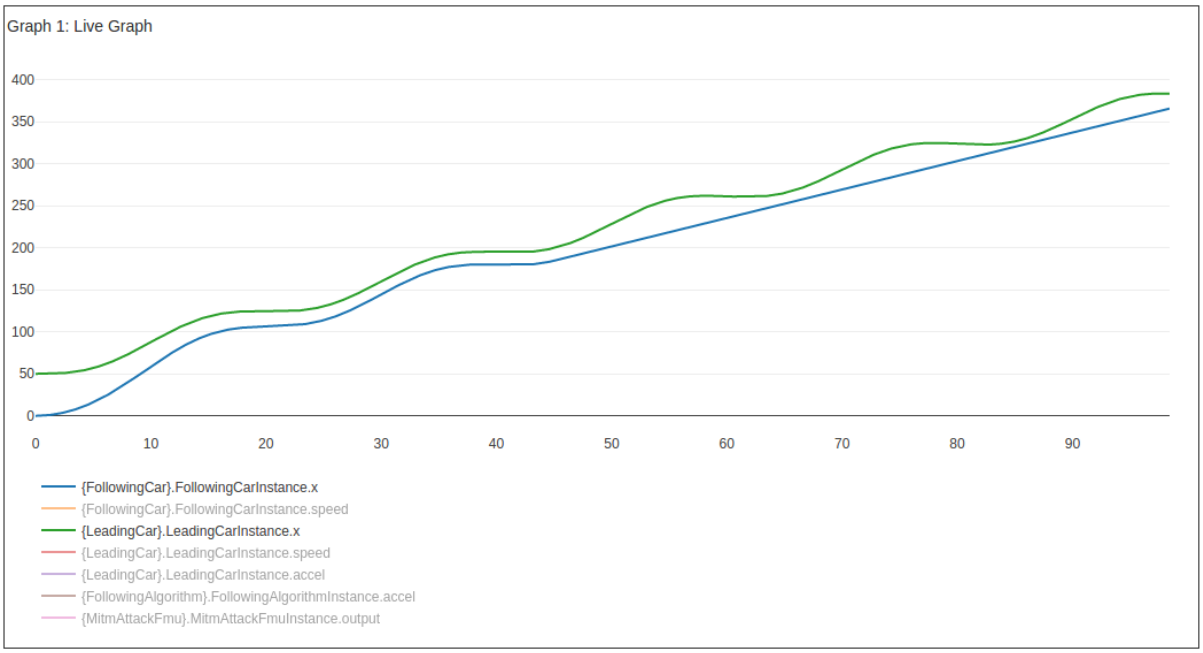


**Figure 11:** Grafico posizione veicoli nel caso Tempo di Attacco a 45s

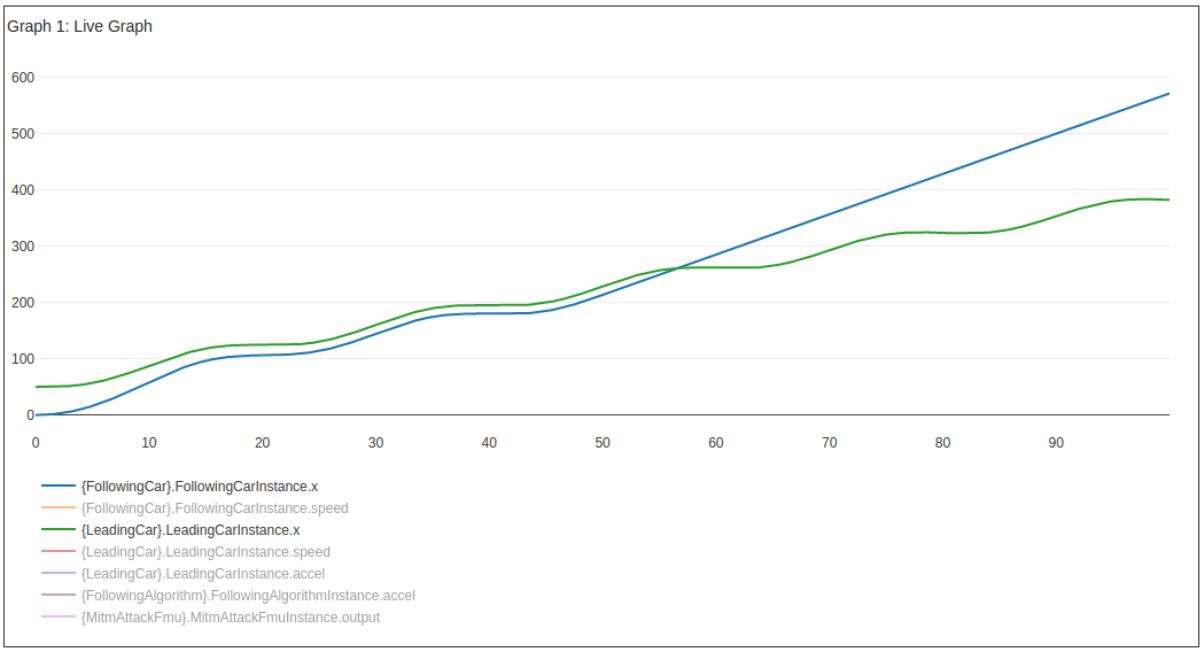


**Figure 12:** Grafico posizione veicoli nel caso Tempo di Attacco a 50s

### 4.2.2 Attacco Multiplo

In questa sezione vengono riportati due diverse condizioni di attacco in cui quest'ultimo ha una durata di un certo numero di step e si ripete più volte nel tempo. L'obiettivo è quello di individuare una condizione in cui,nonostante gli attacchi ripetuti, il sistema risulta tollerante e uno invece in cui l'attacco porta a 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 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_occurencies**: 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.

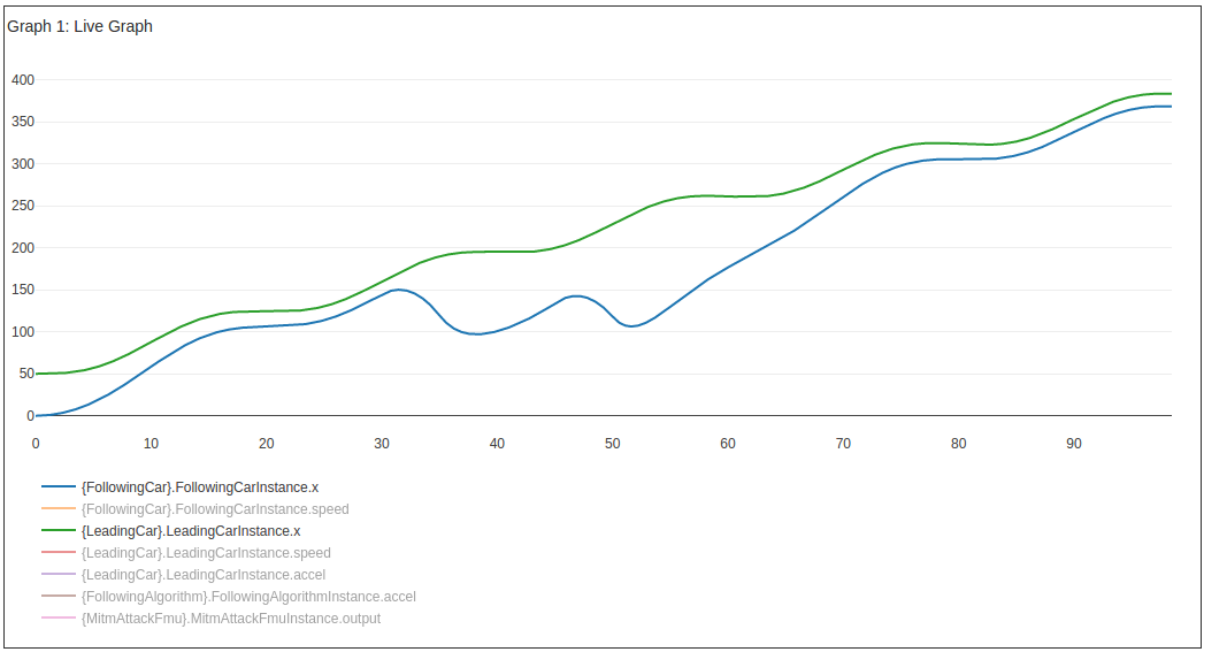


**Figure 13:** Grafico di posizione dei due veicoli nel caso di attacco multiplo. Notare il non verificarsi di un incidente e il ritorno a convergenza.

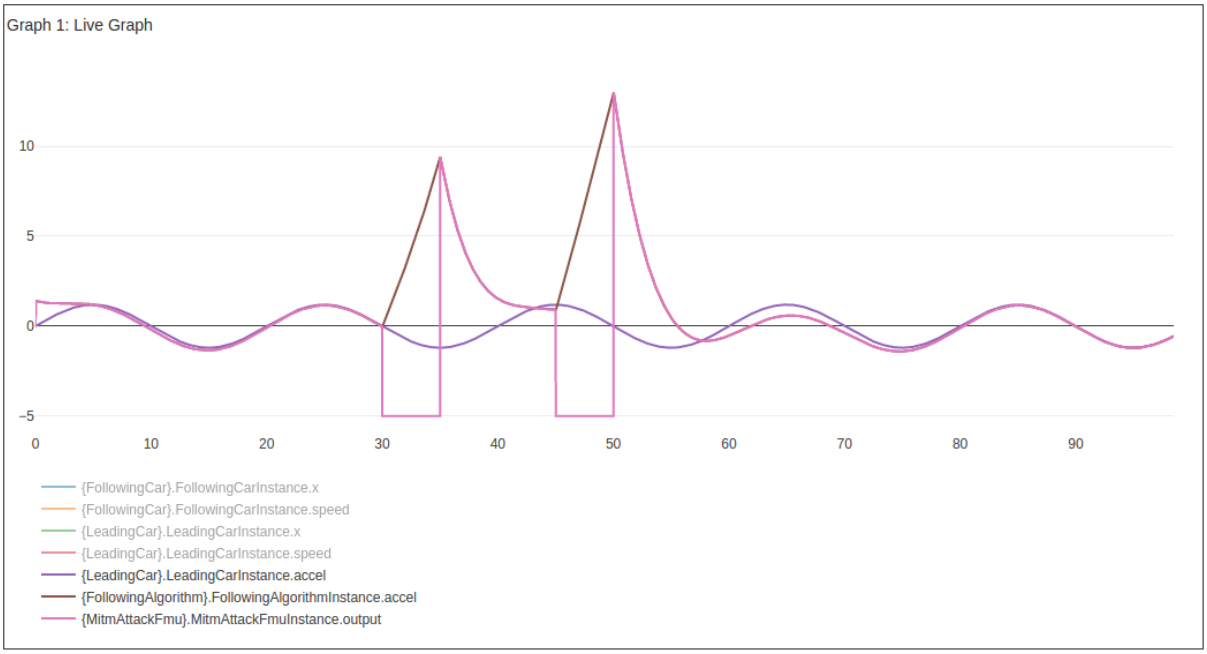


**Figure 14:** Grafico delle accelerazioni nel caso di attacco multiplo.

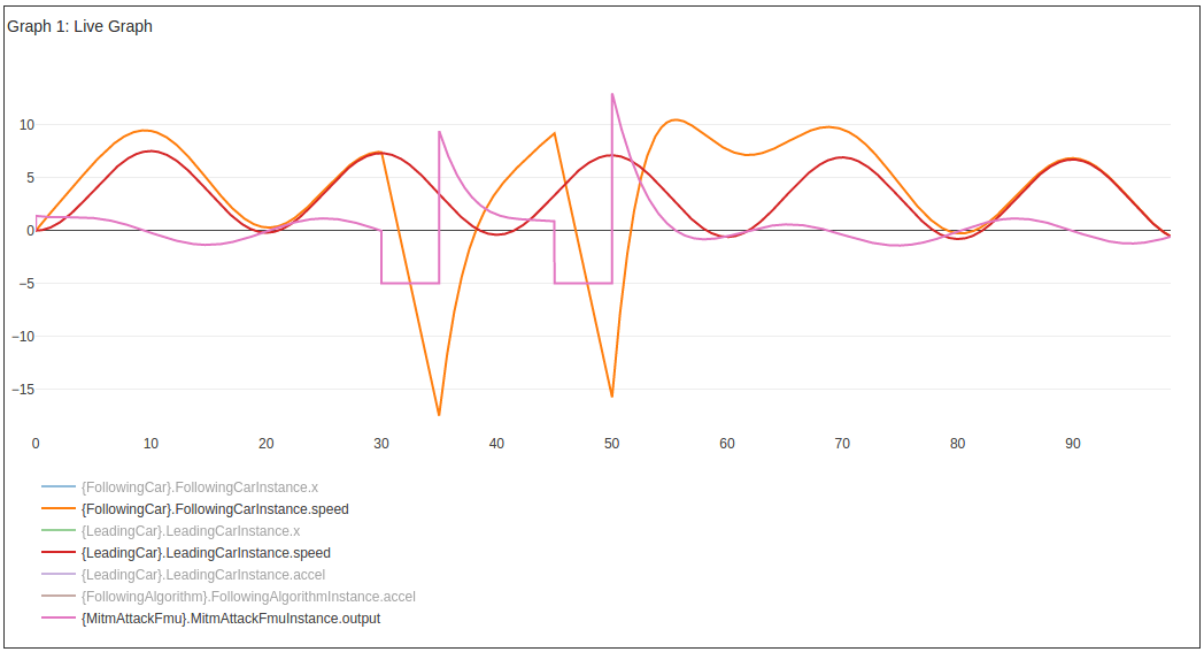


**Figure 15:** Grafico di velocità dei due veicoli nel caso di attacco multiplo.

Osservando i grafici sopra descritti è possibile osservare come, nonostante il verificarsi di molteplici attacchi, la following car non crei alcun incidente. Inoltre è 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 è quello di andare ad individuare un attacco in cui la presenza di più occorrenze risulta chiave nel verificarsi di un incidente fra i due veicoli. Di seguito sono riportate le configurazioni dell'attacco in esame.

- **Attack_occurencies**: 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.

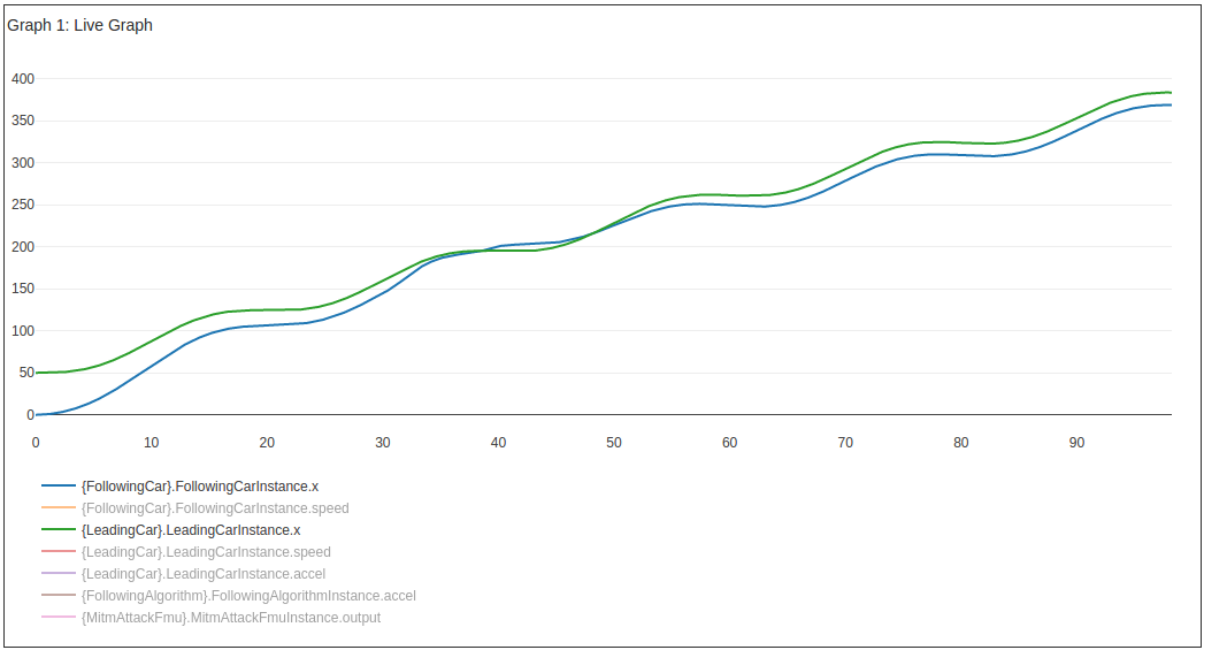


**Figure 16:** Grafico di posizione dei due veicoli nel caso di attacco multiplo. Notare il verificarsi di un incidente.

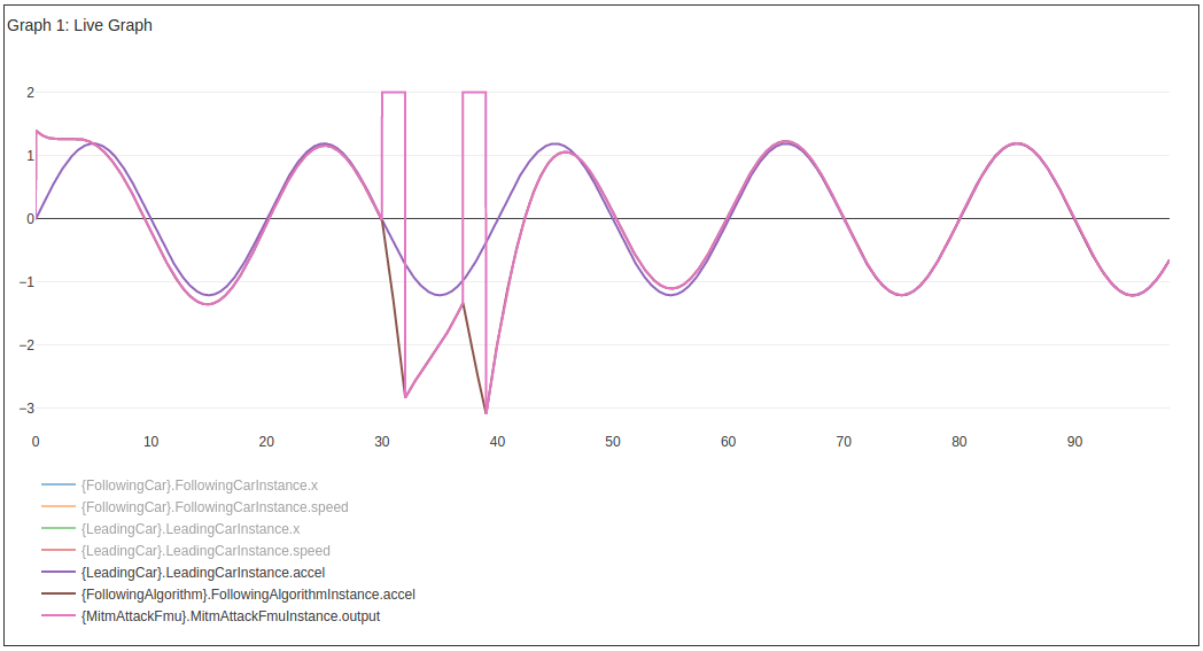


**Figure 17:** Grafico delle accelerazioni nel caso di attacco multiplo.

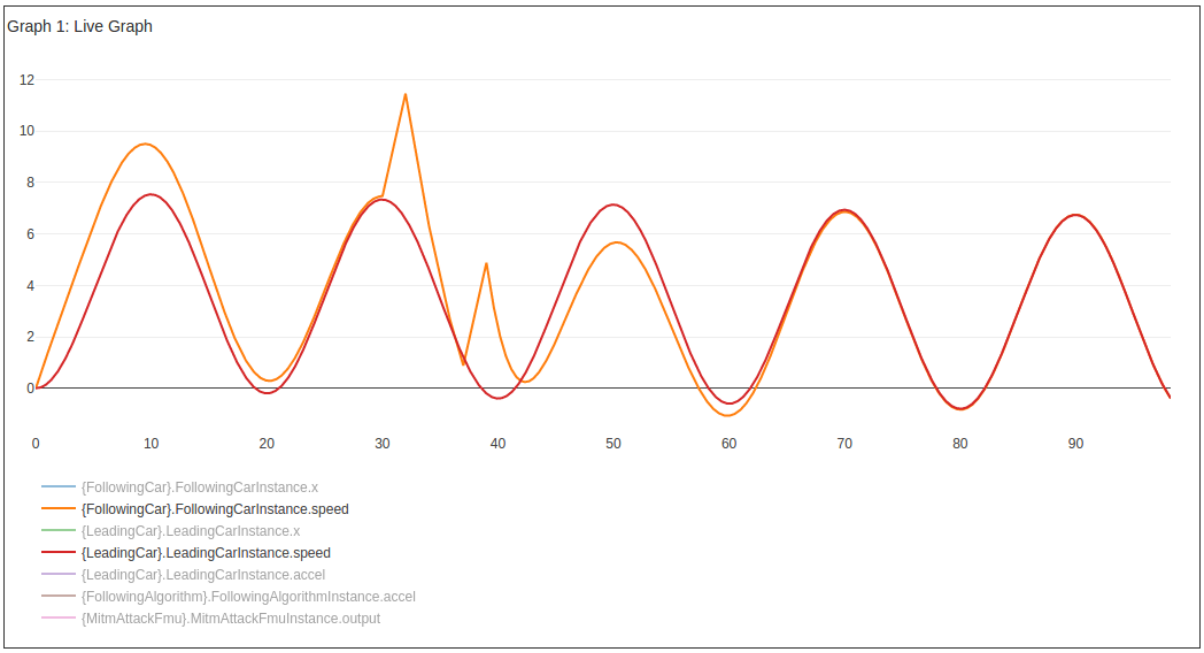


**Figure 18:** Grafico di velocità dei due veicoli nel caso di attacco multiplo.

Osservando i grafici sopra descritti è 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 così da raggiungere la distanza richiesta di 15m.

## 4.3 Attacco alla X

**Attacco Semplice**

### 4.3.1 Risultati Co-Simulazione

Per cercare di dare un'interpretazione ai risultati del successivo studio verrà prima analizzato un caso d'esempio con i seguenti parametri:

- **attack_value**: 200
- **attack_time**: 20s

Si ottiene il seguente plot:

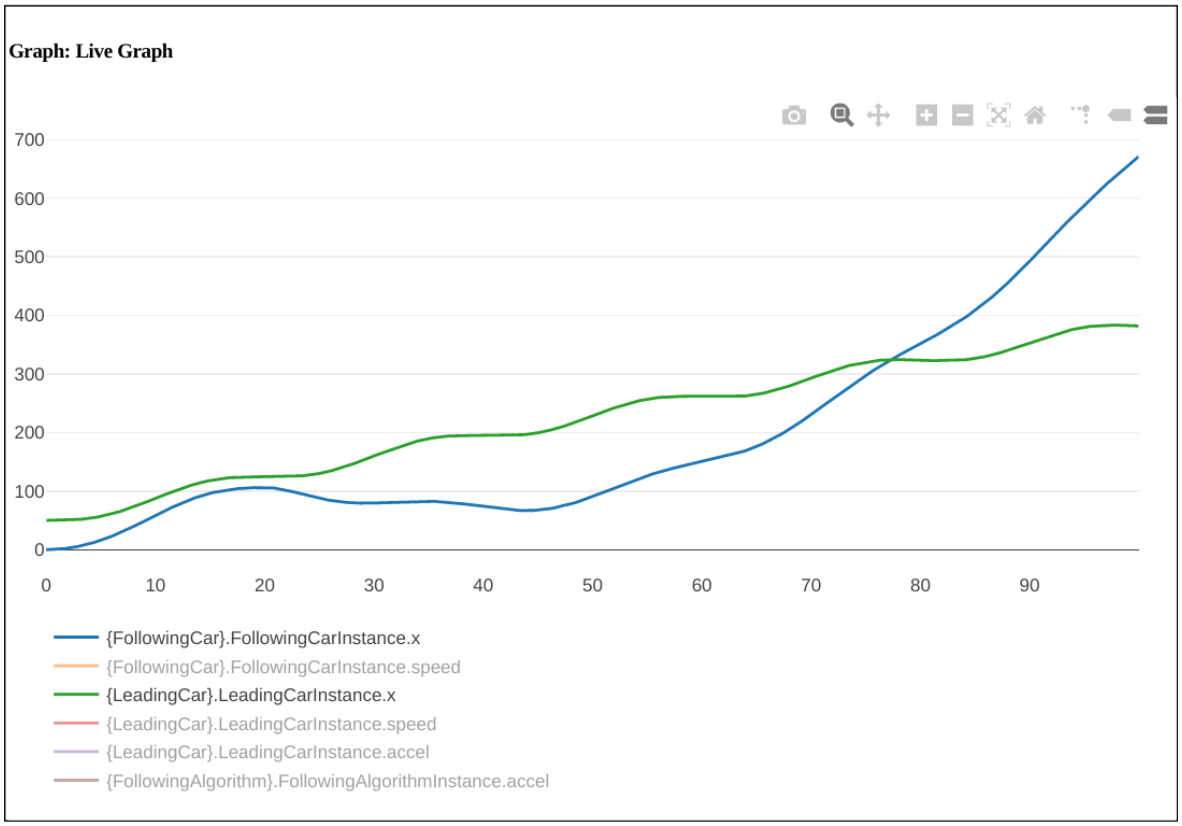


**Figure 19:** Posizione x della LeadingCar (verde) e FollowingCar (blu)

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**, dal un tempo di 20s ad uno di circa 40s, l'attacco inizierà ma la leading car non avrà superato ancora l'**attack_value** impostato, che rappresenta la (alterata) posizione della following car: quest'ultima penserà 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 inizierà a riavvicinarsi fino all'impatto tra le due auto. Per come è configurata la leading car, ovvero che tenderà 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.

### 4.3.2 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 può notare il tempo è una variabile importante per questo tipo di attacco, con un tempo sufficientemente alto l'attacco ha sempre luogo come detto in precedenza.

**Attacco Multiplo** Sono stati individuati quattro diverse configurazioni che portano 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 avrà un pattern simile a livello temporale, la variabile è 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 è fissa (per via dell'attacco in corso), nel caso il tempo di inizio sia maggiore, maggiore sarà la posizione della leading car e perciò maggiore sarà l'accelerazione in input che porterà 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 alla X (tra following algorithm e following car) 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 che risultano essere altamente improbabili.