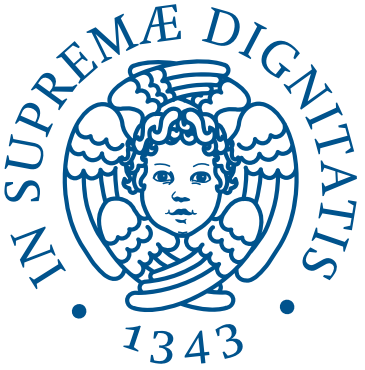

UNIVERSITÀ DI PISA

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.

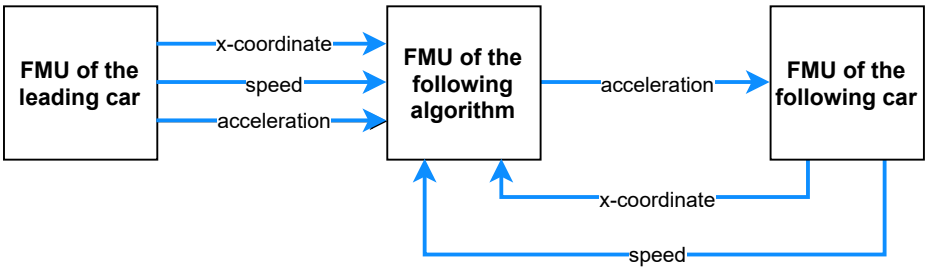

Figure 1: Multi-Model schema del VanillaCase

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.

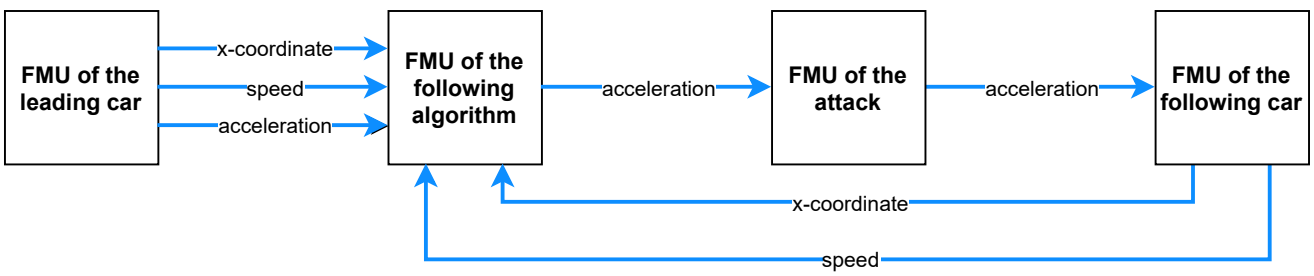

Figure 2: Multi-Model schema dell'Attacco alla Accelerazione

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.

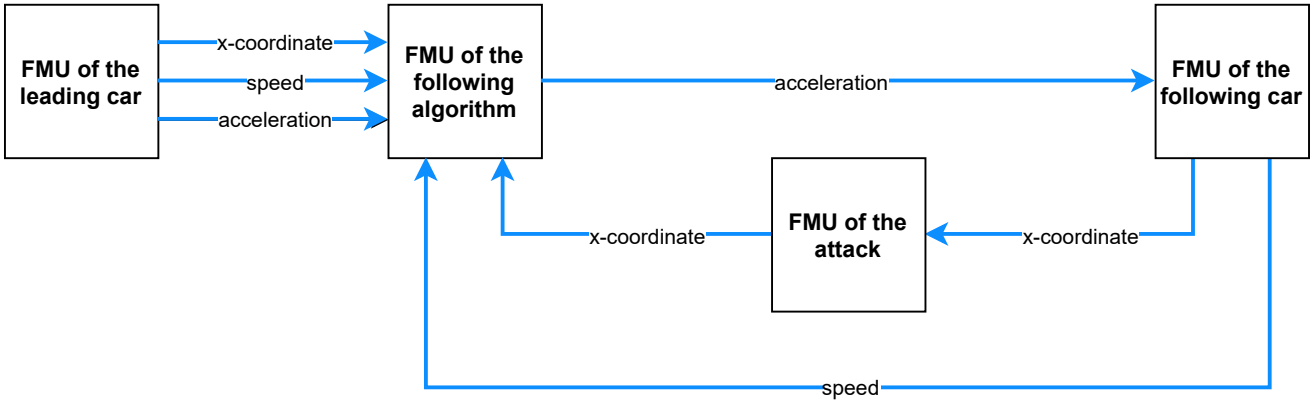

Figure 3: Multi-Model schema dell'Attacco alla Posizione

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 conduce alla convergenza delle due macchine.

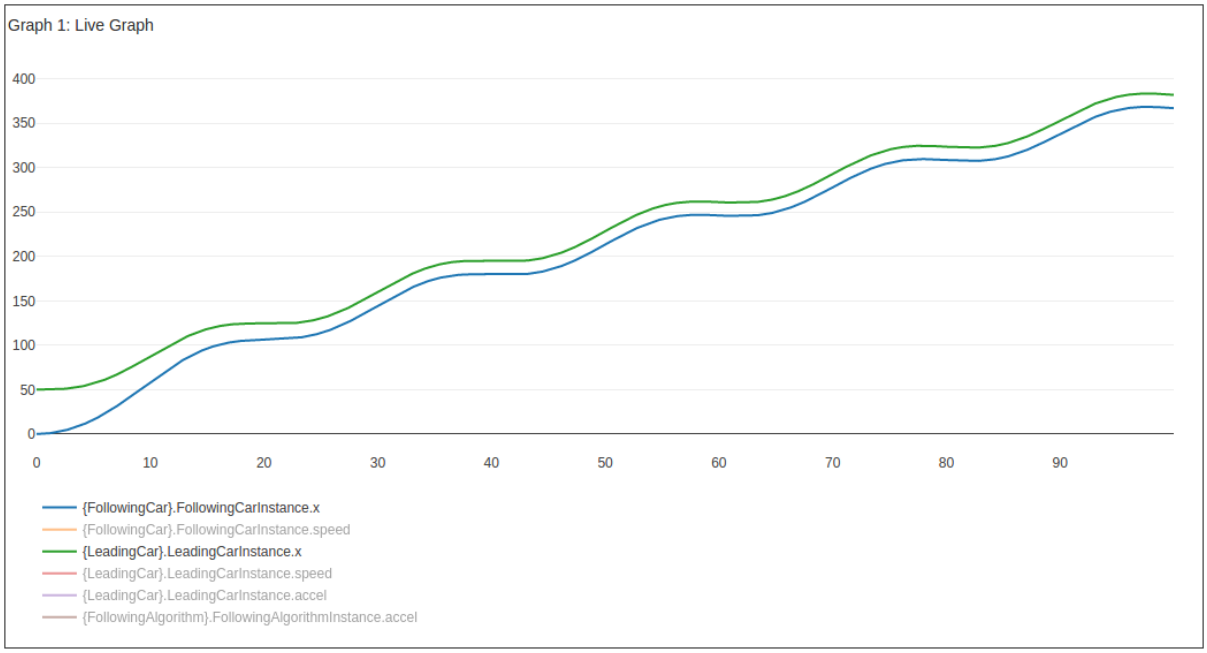

Figure 4: Posizione x della LeadingCar (verde) e FollowingCar (blu)

La distanze media tra le due auto è pari a **18.49m**.

4.2 Attacco all'accelerazione

Attacco Semplice

Attacco Multiplo

4.2.1 Risultati DSE

4.2.2 Risultati Co-Simulazione

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:

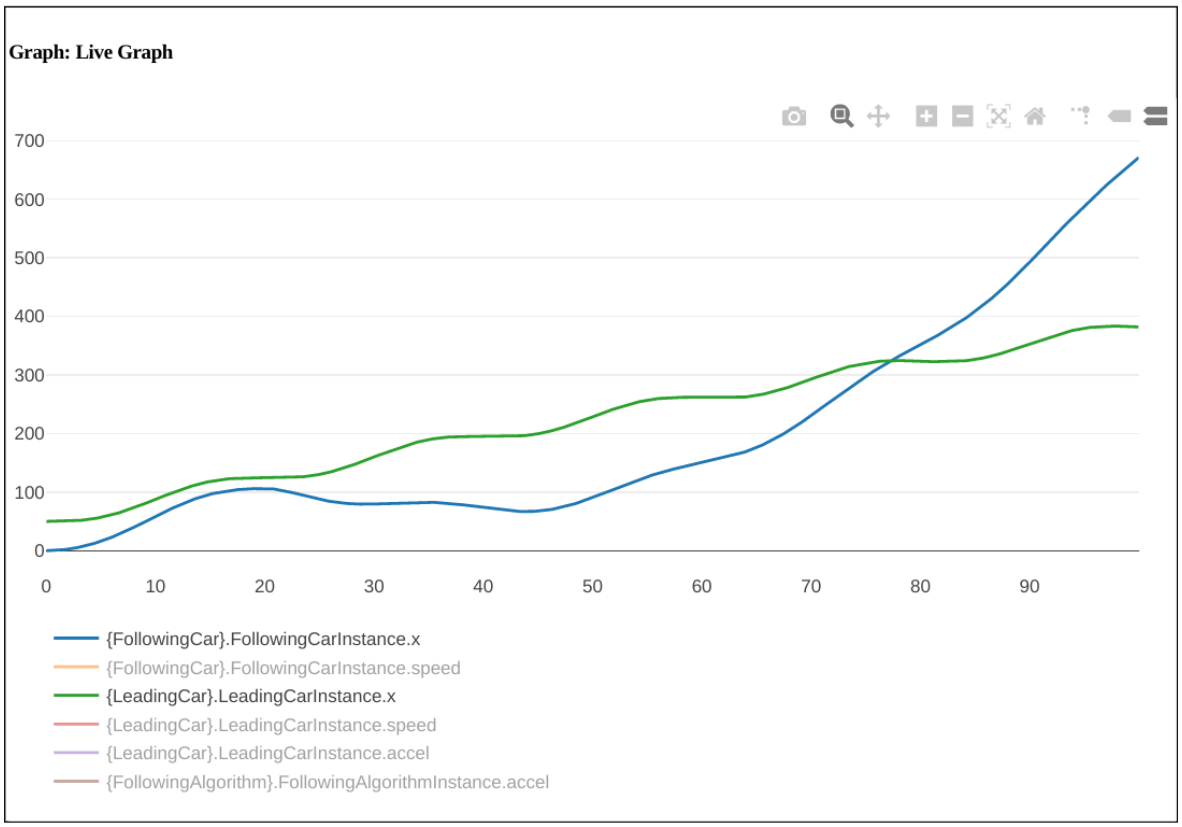

Figure 5: Posizione x della LeadingCar (verde) e FollowingCar (blu)

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 deceleterà; 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] [150, 199]	INCIDENTE NO INCIDENTE
100s	[0, 199] -	INCIDENTE NO INCIDENTE

Da 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

5.1 VanillaCase

5.2 Attacco all'accelerazione

5.3 Attacco alla X