# Security of Distributed Cyber-Physical Systems with Connected Vehicle Applications

PI : Dr. Pierluigi Pisu
Automotive Engineering Department (CUICAR)
Co-PI : Dr. Richard Brooks
Electrical and Computer Engineering Department
Co-PI : Dr. Jim Martin
School of Computing
Clemson University

October 26, 2017

# OUTLINE

□ Overview

□ Motivation & Introduction

□ Problem Statement

□ Scenario I

- Hybrid modeling
- Detection

□ Scenario II

- Game Theory : Attack Resilient Countermeasure

□ Experimental Setup

# Overview

OUTLINE

I. Overview

▷ Overview

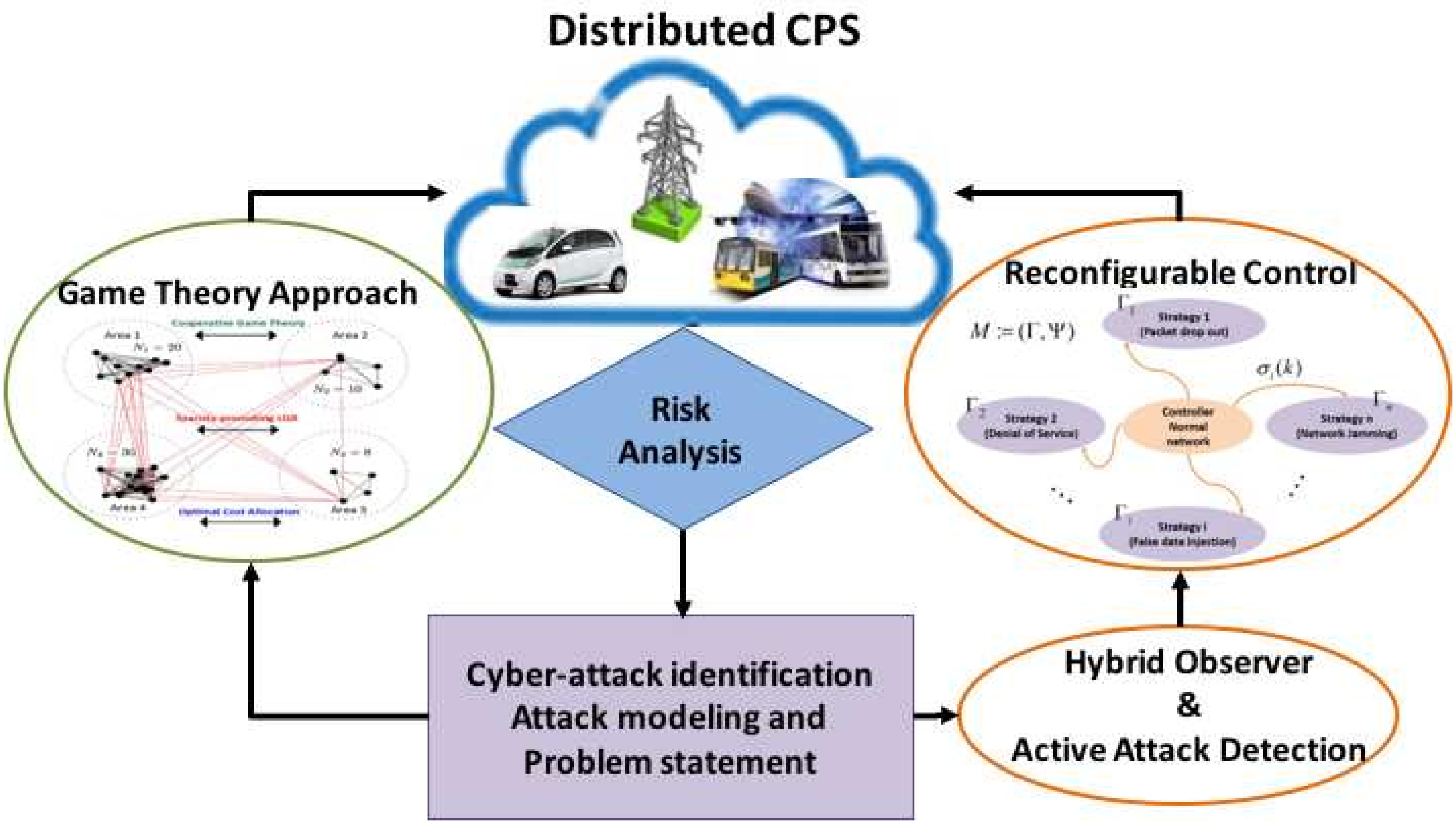
II. Motivation & Introduction

III. Problem Statements

IV. Scenario I

V. Scenario II

VI. Experimental Setup



Distributed CPS

Game Theory Approach

Risk Analysis

Reconfigurable Control

Cyber-attack identification
Attack modeling and
Problem statement

Hybrid Observer
&
Active Attack Detection

# Motivation

- □ Intrusion detection systems (IDS) have shown their inability to detect and distinguish cyber-attacks from failures when CPS is concerned.
- □ Damages to the vehicles in connected vehicles include but not limited to
  - – False data injection to hamper system performance (energy or fuel efficient driving)
  - – Collision between vehicles
- □ The cyber security vulnerabilities that are associated with connected vehicles involve a number of parties: the vehicle users, the vehicle manufacturer, the suppliers, the insurance companies, public agencies and effectively anyone connected in the transportation network.

# Motivation

□ Cyber Physical System (CPS)

- Physical plant
  - ▷ Multi agents/ Interconnected system
  - ▷ Sensors / Actuators
- Communication network
  - ▷ Global
  - ▷ Local

□ Cyber-attacks

- Receiving information
- Sending data
- Control process

□ Physical failure

- Sensors / Actuators

# Cyber attacks on individual subsystem

OUTLINE

I. Overview

II. Motivation & Introduction

III. Problem Statements

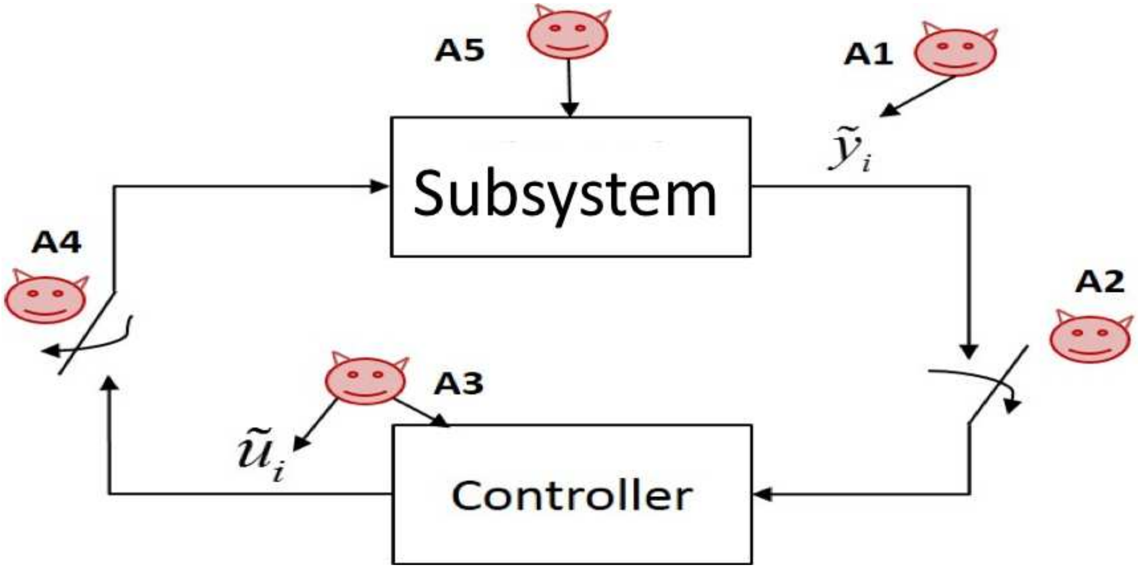
▷ Cyber attacks on individual subsystem

Compromised subsystem in a distributed CPS

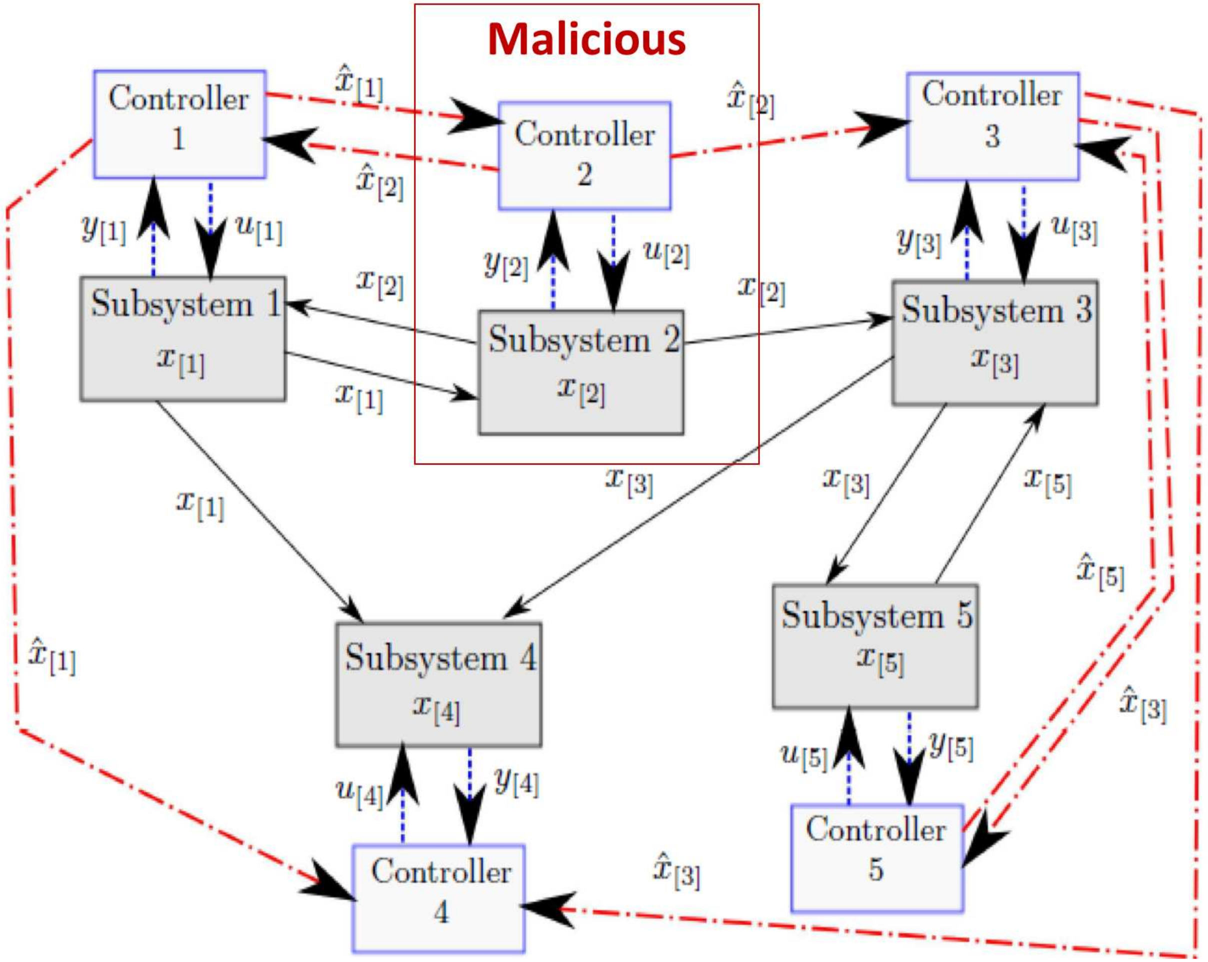
IV. Scenario I

V. Scenario II

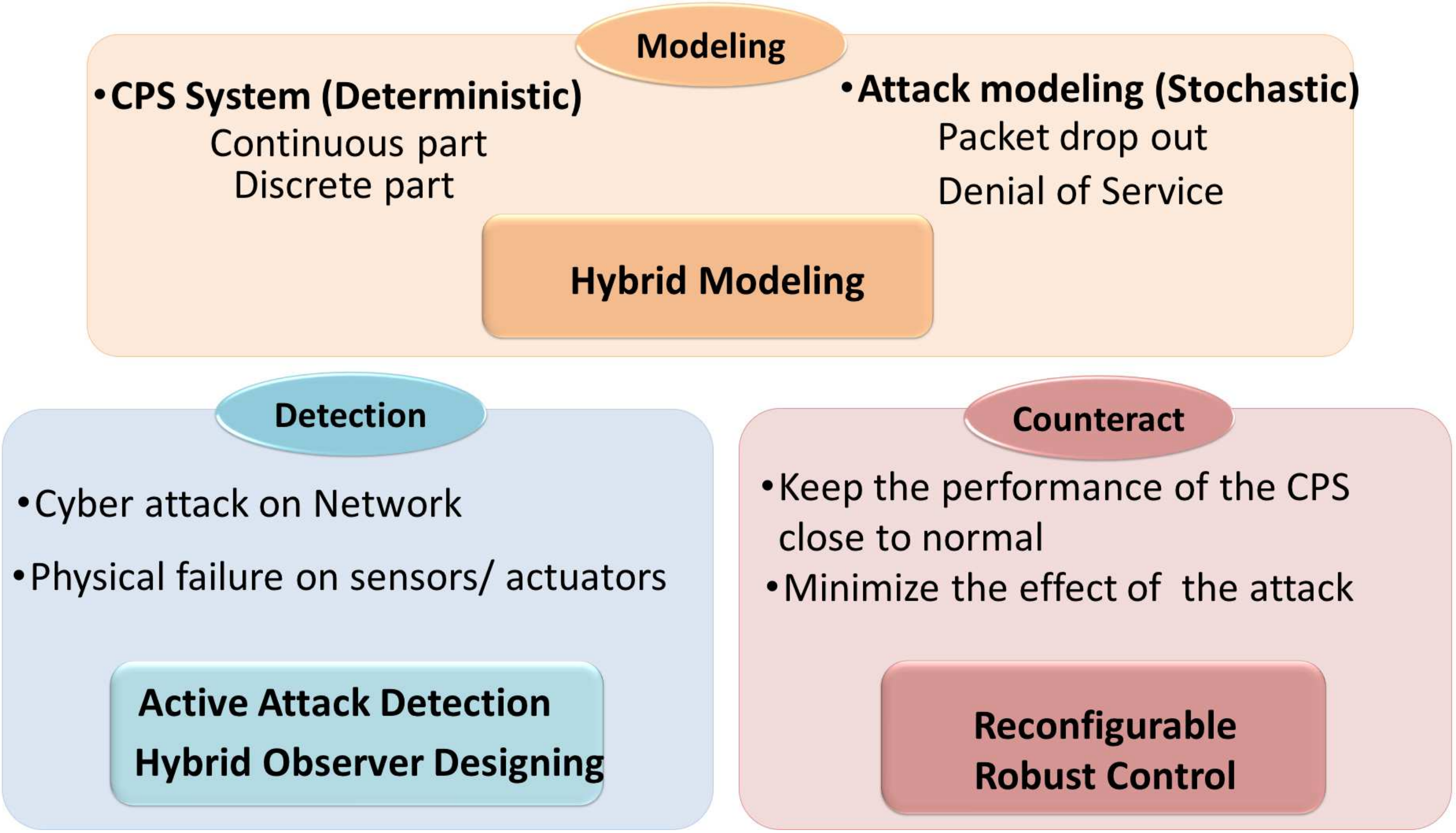
VI. Experimental Setup



# Compromised subsystem in a distributed CPS



# Cyber attacks on individual subsystem



Modeling

- **CPS System (Deterministic)**
  Continuous part
  Discrete part
- **Attack modeling (Stochastic)**
  Packet drop out
  Denial of Service

**Hybrid Modeling**

Detection

- Cyber attack on Network
- Physical failure on sensors/ actuators

**Active Attack Detection**
**Hybrid Observer Designing**

Counteract

- Keep the performance of the CPS close to normal
- Minimize the effect of the attack

**Reconfigurable Robust Control**

# Hybrid Modeling and Control

OUTLINE

I. Overview

II. Motivation & Introduction

III. Problem Statements

IV. Scenario I
Cyber attacks on individual subsystem
▷ Hybrid Modeling and Control
Detection

V. Scenario II

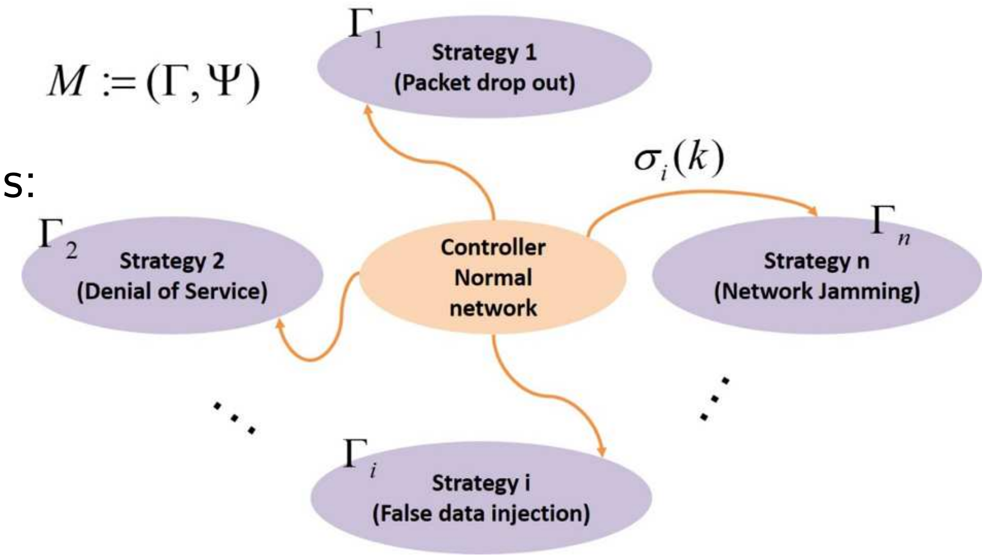
VI. Experimental Setup

□ Hybrid system

- Different strategy for different cyber-attacks
- Switch between strategies based on detection decision
- $M$: Hybrid system
- $\Gamma$: Set of discrete states of M
- $\Psi$: Continuous dynamics of M
- $\sigma(k)$ : Event

□ Assumptions

- Continuous sub-systems: LTI systems



# Detection

□ Hybrid Observer

- Considers the cyber and physical states of the CPS
- Makes decisions on cyber-attack by monitoring the augmented system
- Has the potential to detect a wider range of cyber-attacks that includes common attacks (jamming, false data injection, etc.) as well as intelligent attacks (stealth, covert and replay attacks)

□ Active Attack Detection

- In cases where the reachable output set of different attacks and the normal operating point of a system overlap, due to system uncertainties or control action masking attack effect, mere observer based attack detection would not work well
- n appropriate control signal, over a small duration, would be utilized for the identification of system anomaly

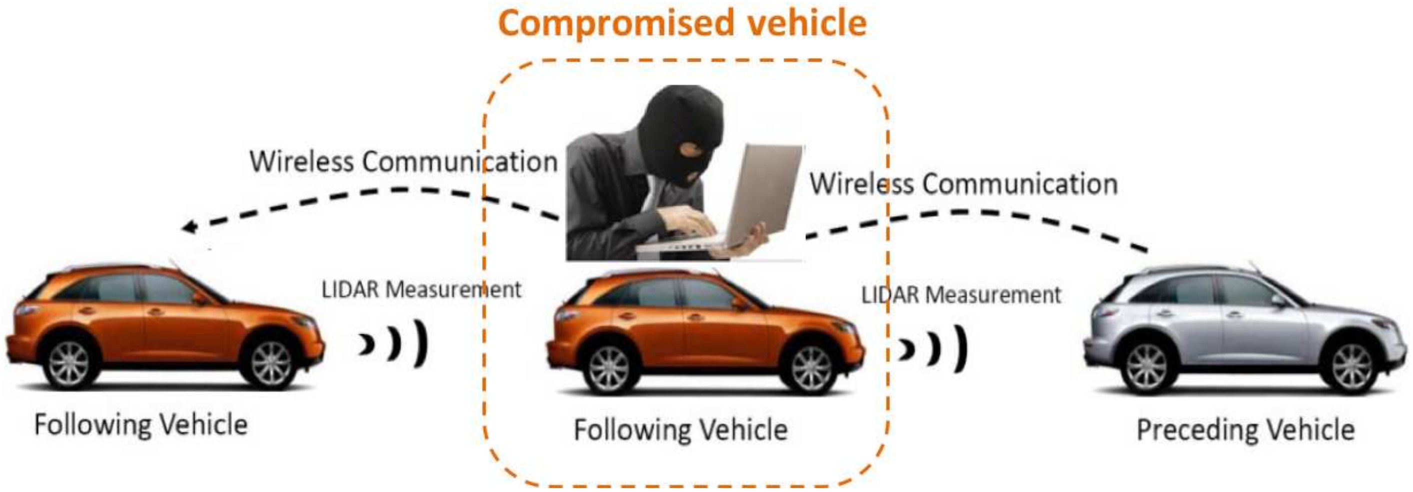
# Compromised subsystem in a distributed CPS

OUTLINE

- I. Overview
- II. Motivation & Introduction
- III. Problem Statements
- IV. Scenario I
- V. Scenario II
  - ▷ Compromised subsystem in a distributed CPS
- VI. Experimental Setup

□ Game Theory : Attack Resilient Countermeasure

- One or more than one of the subsystems in distributed networked CPS are malicious
- Malicious components trying to maximize the global cost function
- The rest of the group want to minimize the cost function
- Win- lose Game theory
- Control countermeasure is performed based on game theory



# Experimental Setup

OUTLINE

I. Overview

II. Motivation & Introduction

III. Problem Statements

IV. Scenario I

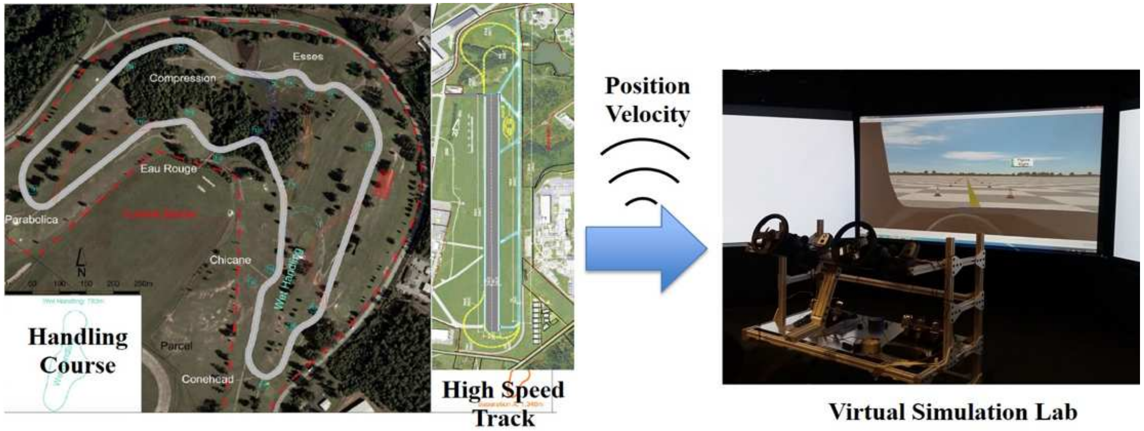
V. Scenario II

VI. Experimental Setup

▷ Experimental Setup

□ Experimental testing and validation has 2 main components

- CV testbed located at South Carolina Technology
  - ▹ More than 2.5-miles of straightaway test track,
  - ▹ 2.5-mile interstate-grade test track (expandable up to 17.5 miles) DSRC-based communication network for V2V and V2I
- Aviation Center (SC-TAC); a CV virtual/simulation lab at CU-ICAR



Virtual Simulation Lab

Connected Vehicle Testbed at SC-TAC

$$L_i(t) = w_1 \int_{\Delta t} \frac{\text{Fuel}}{v_i(t)} \tag{1}$$