Platoon Security

Vehicle Platooning;
Communication Attack;
Collision Attack;
String Stability

Lecture outline

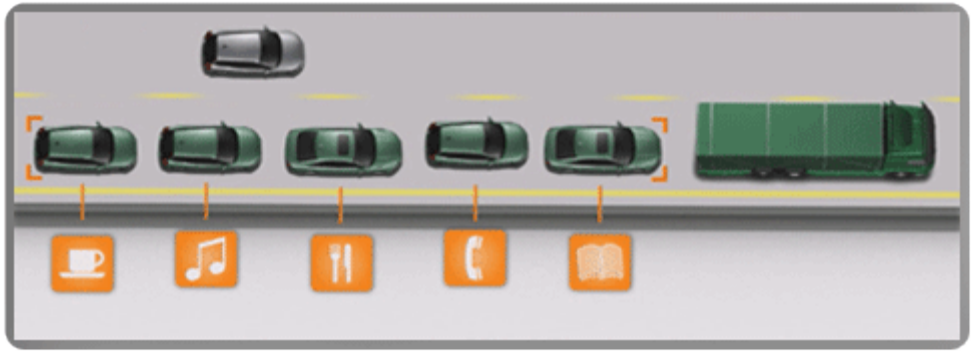
1. Fundamental Concepts of Platooning
2. Current Platooning Projects
3. Vehicle Communication Attack
4. Vehicle Collision Attack
5. String Stability Attack

Lecture outline

1. Fundamental Concepts of Platooning
2. Current Platooning Projects
3. Vehicle Communication Attack
4. Vehicle Collision Attack
5. String Stability Attack

Vehicle platooning

- Also referred as Cooperative Adaptive Cruise Control (CACC)
- A method allowing a group of vehicles, following one another, acts as a single unit through coordinated movements
- Benefits
  - Highway capacity
  - Fuel economy
  - User comfort
  - Safety
  - ….



Platoon in real: SATRE Project

- SATRE: Safe Road Trains for the Environment
- Demonstrated successfully in public highway in May 2012

- Led by a truck
- Driver is a trained professional

- Following vehicles in the platoon drive autonomously
- Drivers can relax and do other things

Enabling technologies

- Sensing
  - Cameras and radar systems for relative position sensing
  - GPS for absolute positioning

- Wireless communication
  - Automotive standard 802.11p DSRC modules for inter-vehicle communications

Cybersecurity of Vehicle Platooning

- Complexity of automated vehicle platooning
  - Inter-vehicle communications
  - Vehicle's internal networking
  - Connection to external networks
  - Distributed platooning algorithms
- Open doors to malicious attacks

Lecture outline

1. Fundamental Concepts of Platooning
2. Current Platooning Projects
3. Vehicle Communication Attack
4. Vehicle Collision Attack
5. String Stability Attack

Current Platooning Projects

- SARTRE an European platooning project
- PATH a California traffic automation program
- GCDC a cooperative driving initiative
- Energy ITS a Japanese truck platooning

SARTRE

- Aim to allow vehicles to drive in platoons on public motorways without modification to the infrastructure
- Define a platoon as a collection of vehicles led by a manually driven heavy lead vehicle
- Expected advantages: increased fuel and traffic efficiency, safety and driver comfort

PATH

- Motivated by the need to produce a significant increase in the capacity of a highway lane
- Developed the eight-car automated platoon for the National Automated Highway System Consortium in 1997
- Experiments on truck platoons achieved twice the capacity with trucks driven individually

GCDC

- Grand Cooperative Driving Challenge (GCDC)
- Increase the road throughput by reducing the spacing between vehicles
- GCDC not only uses multi-vender vehicles but also a mix of both heavy and passenger vehicles

Energy ITS

- Aims at energy saving and global warming prevention, also mitigating the lack of skilled drivers

- Platooning of 10 m gap at 80 km/h can reduce energy by about 15% (measurement)

Lecture outline

1. Fundamental Concepts of Platooning
2. Current Platooning Projects
3. Vehicle Communication Attack
4. Vehicle Collision Attack
5. String Stability Attack

Abstract

- Autonomous vehicle systems rely heavily on onboard sensors such as cameras, radar/LIDAR, and GPS as well as capabilities such as 3G/4G connectivity and V2V/V2I communication to make real-time maneuvering decisions

- This study [1] presents a first look at the effects of security attacks on the communication channel as well as sensor tampering of a connected vehicle stream

[1] Amoozadeh, Mani, et al. "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving." *IEEE Communications Magazine* 53.6 (2015): 126-132.

Platoon Wireless Communication

- Each CACC vehicle listens to beacon messages sent wirelessly using IEEE 802.11p from its immediately preceding vehicle

- The vehicles then utilize the speed, position, acceleration and other information embedded in these beacon messages to achieve distributed longitudinal control

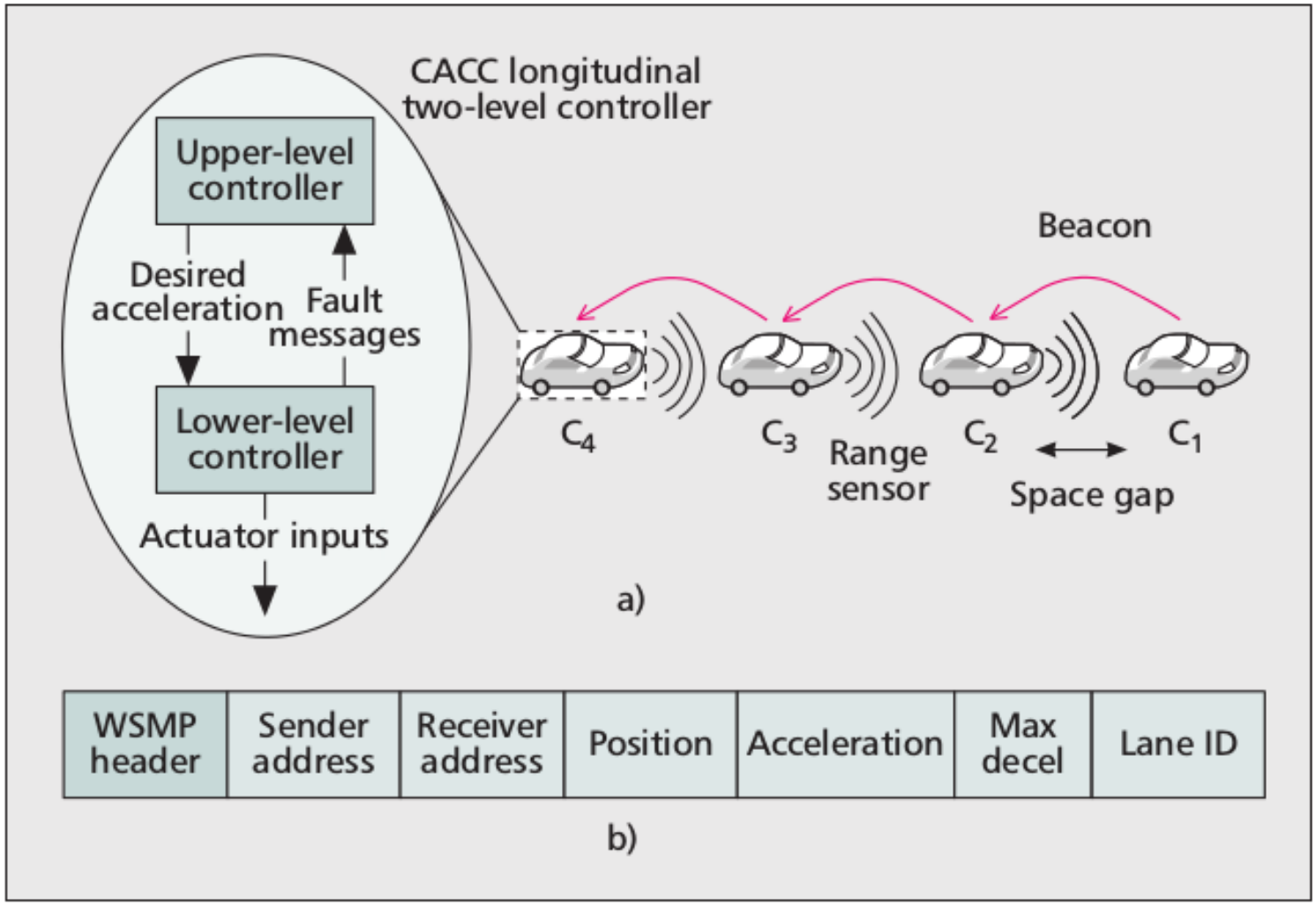


Figure 1. One-vehicle look-ahead communication in a CACC vehicle stream. The *i*th vehicle receives information embedded in beacon messages from the $(i - 1)$th vehicle using V2V wireless communication, and feeds it into the longitudinal control system to maintain a safe gap from the preceding vehicle. The longitudinal control system in each vehicle is typically designed as a hierarchical two-level controller [2]: a) V2V communications; b) beacon format.

Attack Model

- We assume that the platoon of vehicles is already formed and is traveling on a straight single-lane highway

- The only active communication between CACC vehicles is beaconing used to exchange necessary parameters for a longitudinal controller

Security Attacks on a CACC Vehicle Stream

- We group the security attacks on a CACC vehicle stream as application layer, network layer, system layer and privacy leakage attacks
- Such attacks can be launched by either an outsider or insider adversary
- While leveraging state-of-the-art security architectures can potentially limit the capabilities of outsider attacks, there can still be disruptive insider attacks

Application Layer Attacks

- Application layer attacks affect the functionality of a particular application such as CACC beaconing or message exchange in the platoon management protocol

- The adversary can use message falsification, spoofing or replay attacks to maliciously affect the vehicle stream

Message Falsification Attack

- Adversary starts listening to the wireless medium and, upon receiving each beacon, manipulates the content meaningfully and rebroadcasts it

- For instance, change the acceleration field

Spoofing Attack

- Adversary impersonates another vehicle in the stream in order to inject fraudulent information into a specific vehicle

- In one-vehicle look-ahead communication, adversary can impersonate the vehicle preceding the target vehicle even when the vehicle is distant from the target vehicle

Replay Attack

- Adversary receives and stores a beacon sent by a member of the stream and tries to replay it at a later time with malicious intent

- State-of-the-art security architecture employing a strong cryptographic system have the potential to effectively thwart application layer attacks in the case where the adversary is an untrusted outsider

Countermeasures for Application Layer Attacks

- Digital signatures provide data integrity for beacon messages and protect them from unauthorized change

- Using nonce in the messages, which is an arbitrary number used only once in communication, is a technique to prevent replay attacks

Network Layer Attacks

- Unlike application layer attacks, network layer attacks have the potential to affect the functioning of multiple user applications

- For instance, the adversary can attempt a denial-of-service(DoS) or distributed DoS(DDoS) attack to overwhelm the communication capability of a vehicle

- Radio jamming to deliberately disrupt communications over small or wide geographic areas is another possible network layer DoS attack

System Level Attacks

- All presented attacks so far have been centered around exploiting V2V communication

- Another type of attack is tampering with vehicle hardware or software, which can be done by malicious insider at the manufacturing level or by an outsider in an unattended vehicle

Privacy Leakage Attacks

- CACC vehicles periodically broadcast beacons that contain various types of information such as vehicle identity, current vehicle position, speed and acceleration

- The adversary can carry out an eavesdropping attack to extract valuable information about the vehicle stream

Simulation Study

- VENTOS is an integrated simulator and is made up of many different modules, including SUMO and OMNET++/Veins

- The traffic control interface (TraCI) which is responsible for data/command exchange between SUMO and OMNET++, is extended with a new set of commands to gain necessary control over parameters exchange for ACC/CACC vehicle

Simulation Setting

- The insider adversary is on the side of the road with fixed position and is equipped with a radio to communicate with other vehicles in the network
- In application level attack, we consider message falsification
- In network layer attack, we consider radio jamming through which all wireless communications are disrupted

Simulation Results

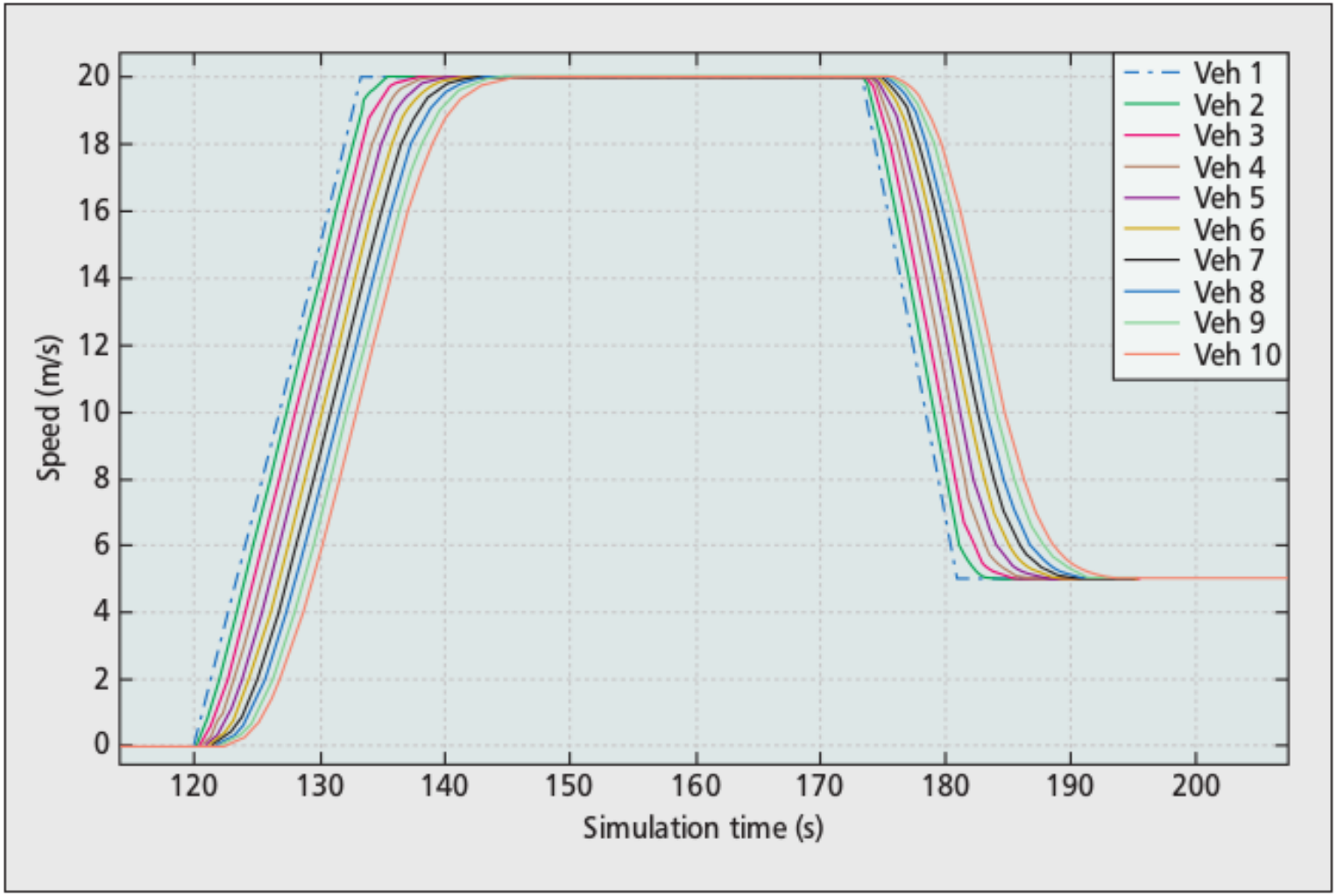


Figure 3. Speed profile of CACC vehicle stream with no adversary. The system is stable, and as "Veh 1" speeds up and slows down, all vehicles follow each other smoothly.

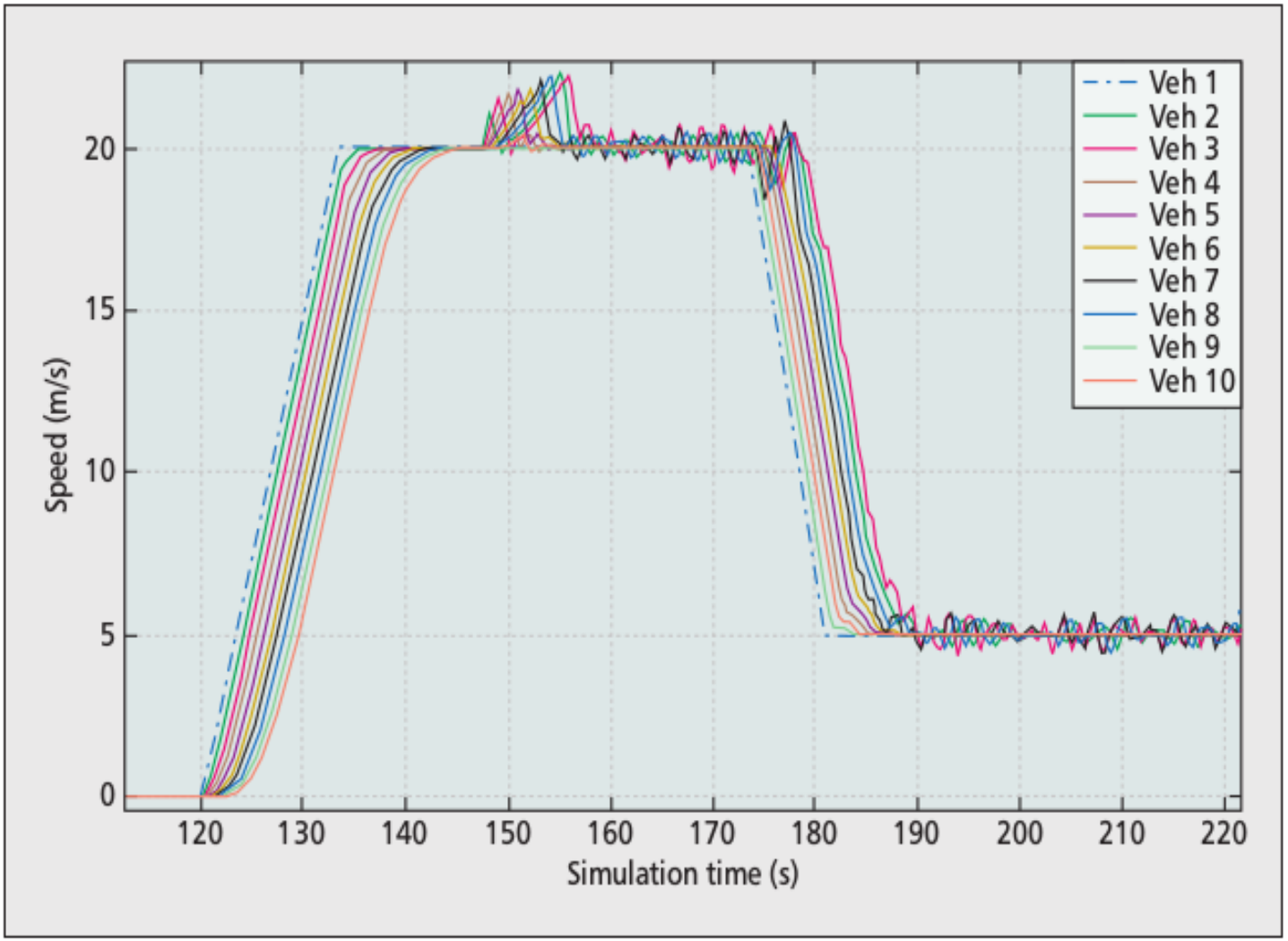


Figure 4. The effect of a message falsification attack on a CACC vehicle stream. String stability is not maintained, and the disturbance magnifies through the stream.

Concept of String Stability

- Local stability is that magnitude of disturbance decrease with time
- String stability concerns the propagation of disturbance in a string of vehicles
- String stable means disturbance damps out when propagating to upstream vehicles

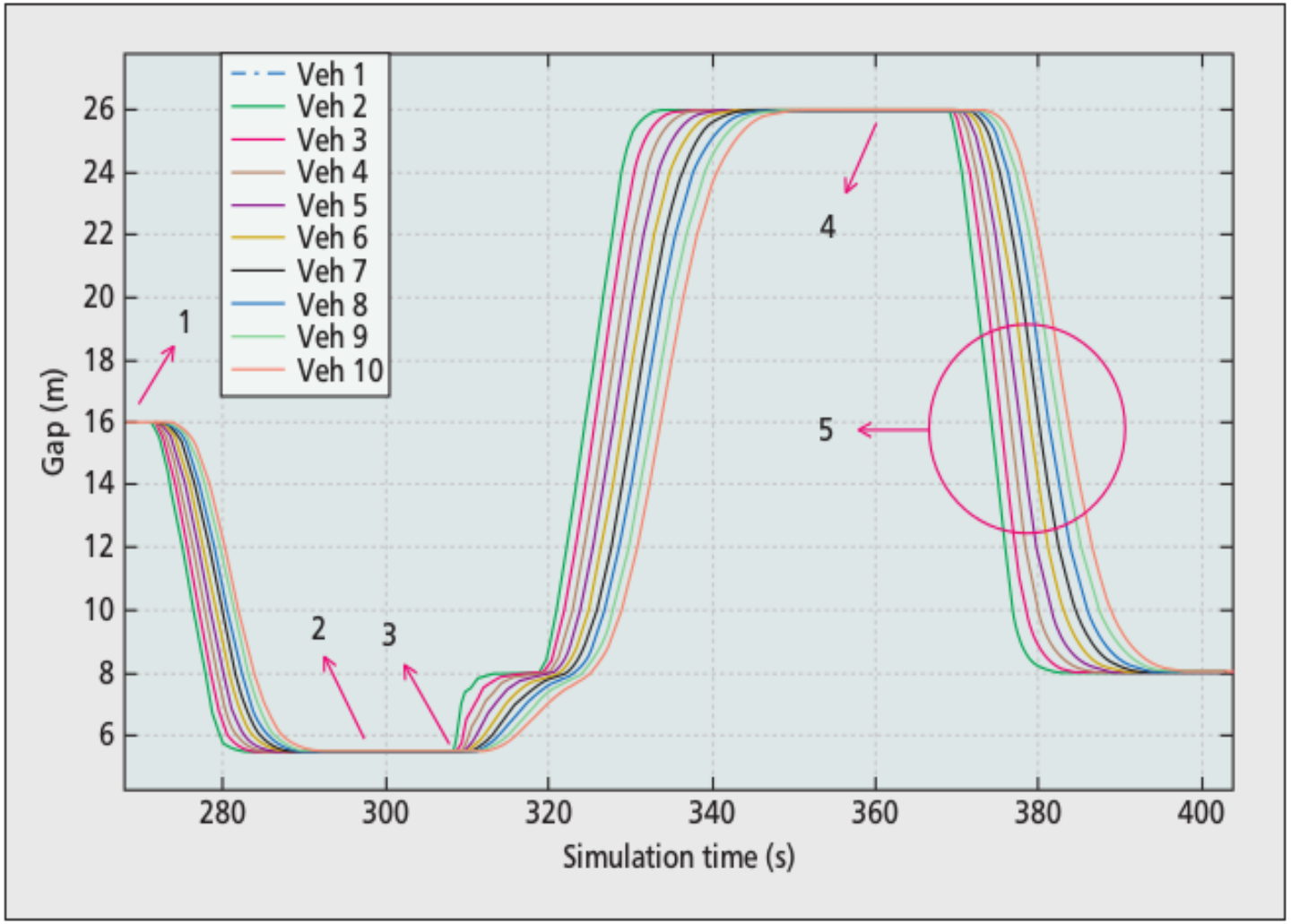


Figure 5. The effect of a radio jamming attack on the CACC vehicle stream. The CACC controller detects communication loss at $t = 308$ s and downgrades to ACC mode.

Countermeasures for Detecting Malicious Behavior

- Local Plausibility Check
- Wearables and Mobile Devices
- Voting

Local Plausibility Check

- A simple approach to detecting a faulty sensor is to check whether the incoming information is plausible

- For instance, if a sensor is not reading within its normal range, the sensor may be faulty or tampered with

Wearables and Mobile Devices

- Wearable and mobile devices carry a wide array of sensors such as cameras, accelerometers and GPS units.

- The wearable device can construct a belief from its sensor data about the position of the vehicle, velocity or acceleration and cross check this with the belief compute by the vehicle

Voting

- Voting is the most effective in scenarios where there are multiple vehicles in a group that are coordinating with one another

Lecture outline

1. Fundamental Concepts of Platooning
2. Current Platooning Projects
3. Vehicle Communication Attack
4. Vehicle Collision Attack
5. String Stability Attack

Abstract

- This study [2] Proposed a set of insider attacks that can cause unexpected behavior in platoons
- Developed a platoon detection method to detect misbehavior
- Simulated above attacks, detection and mitigation schemes

[2] DeBruhl, Bruce, et al. "Is your commute driving you crazy?: a study of misbehavior in vehicular platoons. " *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2015.

System Model

We model the cars using a double integrator model with a lag constant of η_i for each car. Given a desired acceleration of u_i, car i has the following continuous time differential equations.

$$\dot{a}_i = -\eta_i^{-1} a_i + \eta_i^{-1} u_i \tag{2}$$

$$\dot{v}_i = a_i \tag{3}$$

$$\dot{q} = v_i \tag{4}$$

$$\dot{e}_i = v_{i-1} - v_i - h_{d,i} a_i. \tag{5}$$

Controller

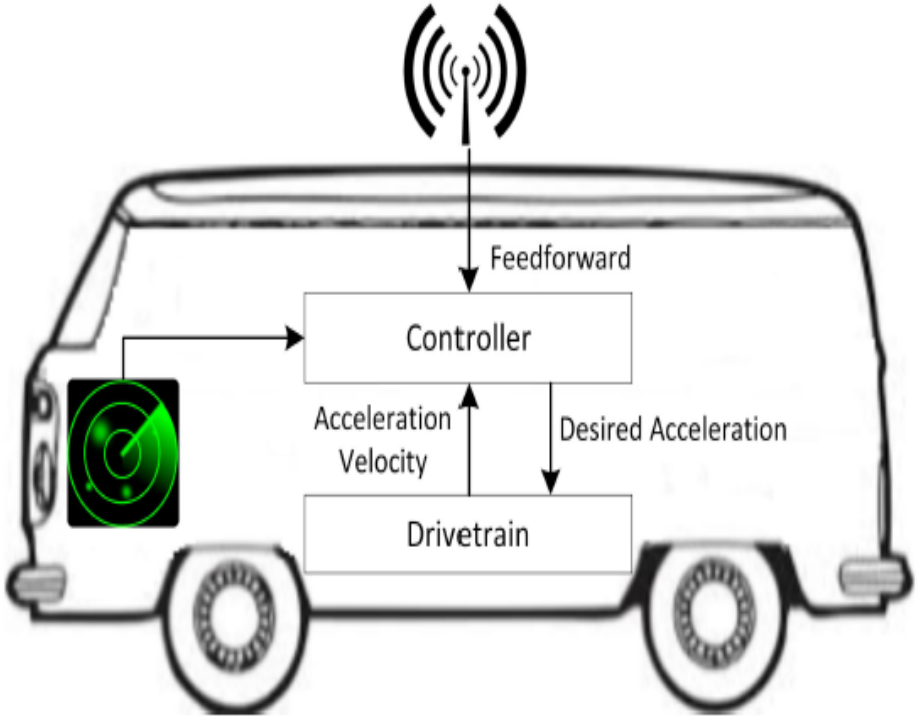


Figure 2: In this figure, we show our controller structure for a platooned vehicle. The vehicle uses radar to determine distance and error from the car in front of it, DSRC to get feedforward information from other cars, and powertrain measurements to determine its current state.

System Description

We define the vector $x_i^T = [e_i, v_i, a_i, u_{ff,i}]$ for the state of car i. The update equation for a vehicle can be written as a linear system such that

$$\dot{x_i} = A_{i,i}x_i + A_{i,i-1}x_{i-1} + B_{s,i}u_i + B_{c,i}\hat{u}_{i-1}, \forall\, i > 0 \quad (9)$$

and

$$\dot{x_0} = A_0 x_0 + B_{s,i}u_r \quad (10)$$

$$A_{i,i} = \begin{pmatrix} 0 & -1 & -h_{d,i} & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -\eta_i^{-1} & 0 \\ 0 & 0 & 0 & -h_{d,i}^{-1} \end{pmatrix}, \quad (11)$$

$$A_{i,i-1} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad (12)$$

$$B_{s,i}^T = \begin{pmatrix} 0 & 0 & \eta_i^{-1} & 0 \end{pmatrix}, \quad (13)$$

$$B_{c,i}^T = \begin{pmatrix} 0 & 0 & 0 & h_{d,i}^{-1} \end{pmatrix}, \quad (14)$$

and

$$A_0 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & -\eta_0^{-1} & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \quad (15)$$

Attack Strategies

- Reduced Headway Attack

To implement this attack we change the attacker's headway parameter to $h_{d,a} < h_{d,min}$ where $h_{d,min}$ is the recommended minimum headway speed.

- Joining Without Radar

This attack is implemented by changing the attacker's control law to $u_a = u_{ff,a}$ and ignoring the feedback portion of the control law.

- Mis-report Attack

The attacker defines a mis-report percentage $\beta \in [0, 1]$ and then implements the attack by reporting $\hat{u}_a = (1 - \beta)u_a$ if $u_a > 0$ and $\hat{u}_a = (1 + \beta)u_a$ if $u_a < 0$.

- Collision Induction Attack

Assuming that cars have a range on their inputs defined as $u_i \in [u_{min}, u_{max}]$ we can implement this attack by setting the attackers control parameters to $u_a = u_{min}$ and $\hat{u}_a = u_{max}$.

- Non-attack abnormalities

To model abnormal driving in our system we vary the value of η_a for a vehicle that we call the attacker even though their intent may not be malicious.

Model Based Attack Detection

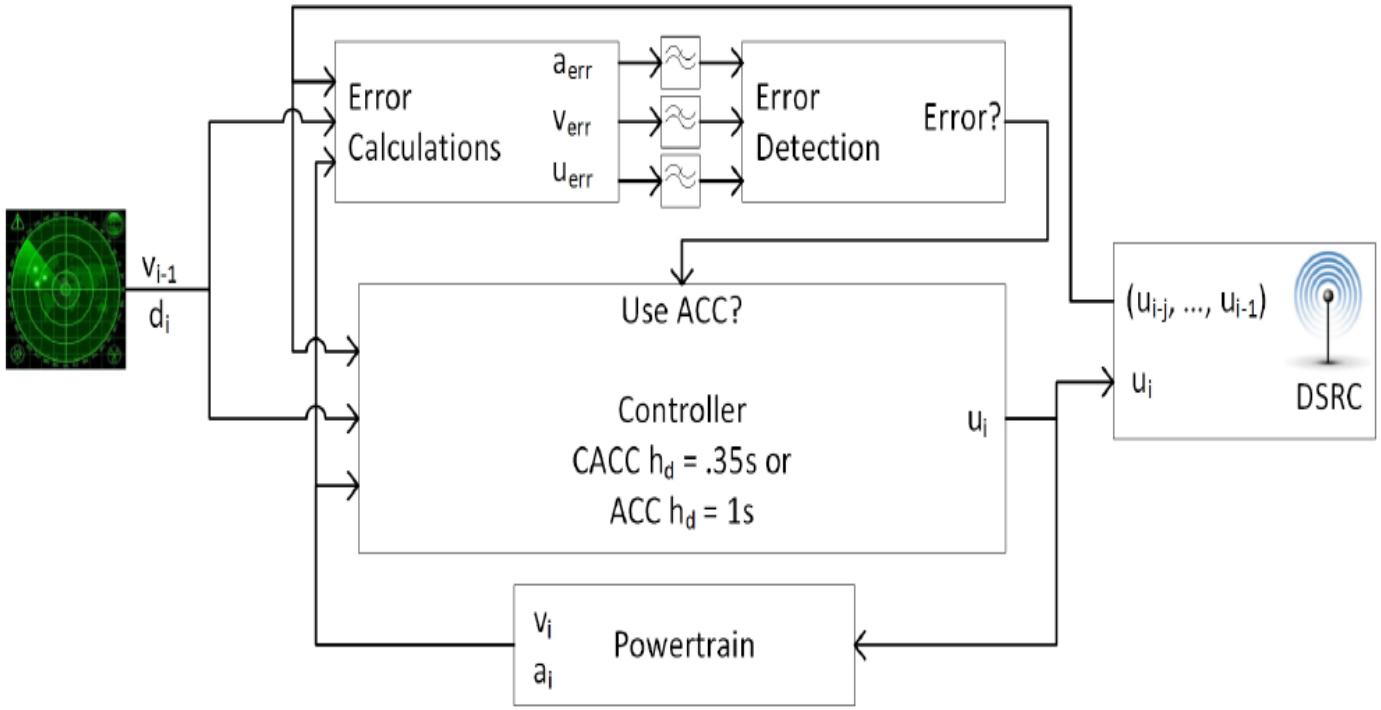


Figure 5: In this figure, we show a detailed diagram of our proposed detection scheme. A model of the expected behavior of the car in front of the monitoring car is made from the broadcasted upstream control information. This is compared to the measured behavior of the car in front of the monitoring car. If the error is larger than expected, the monitoring car switches to a non-cooperative ACC algorithm.

Attack Results

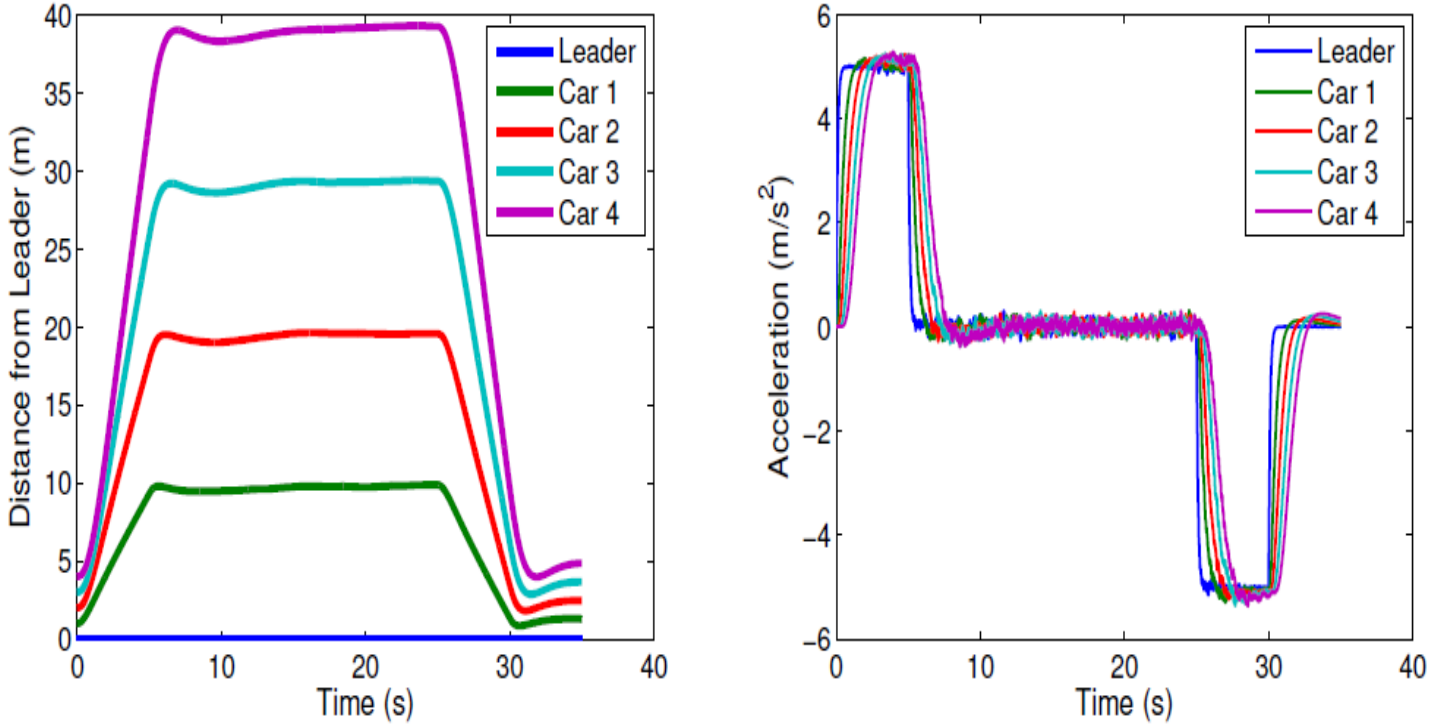


Figure 6: In this figure, we show the system operating under noisy conditions with the variance in noise set to .001 of the vehicles velocity. On the left we show the distance from the leader and on the right we show the acceleration for each of the vehicles.

Attack Detection Results

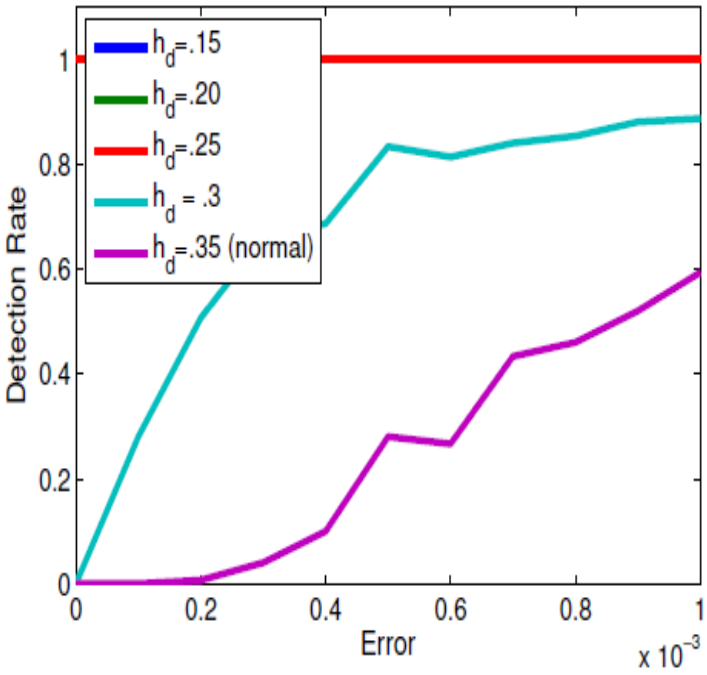


Figure 8: In this figure, we show the headway attack detection results, we calculate the false positive rate across 75 trials with an acceleration rate of $2\frac{m}{s^2}$ and 75 trials with an acceleration rate of $5\frac{m}{s^2}$.

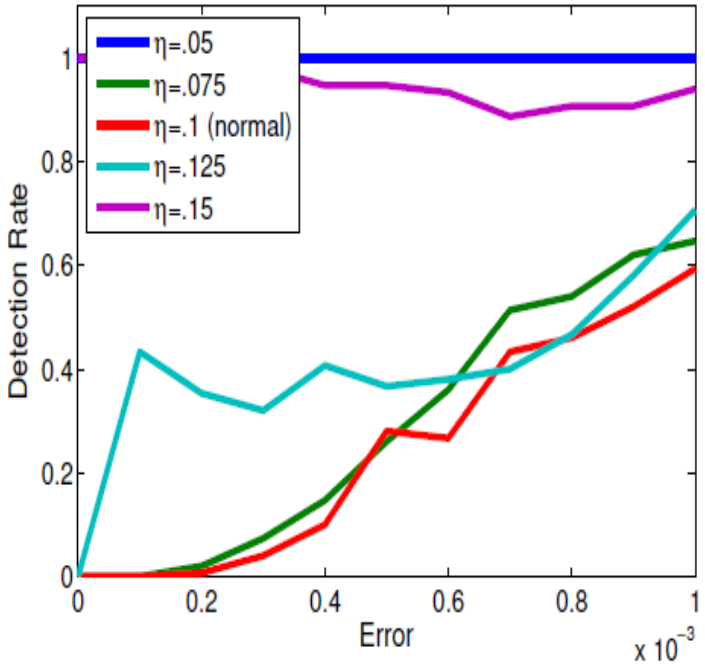


Figure 9: In this figure, we show the abnormal behavior detection results, we calculate the detection rate across 75 trials with an acceleration rate of $2\frac{m}{s^2}$ and 75 trials with an acceleration rate of $5\frac{m}{s^2}$.

Lecture outline

1. Fundamental Concepts of Platooning
2. Current Platooning Projects
3. Vehicle Communication Attack
4. Vehicle Collision Attack
5. String Stability Attack

Abstract

- This paper[3] shows that a single malicious controlled vehicle can destabilize a vehicular platoon

- They prove that the attack can be successful at any position in the platoon and at frequencies that can be realized by the other vehicles in the platoon

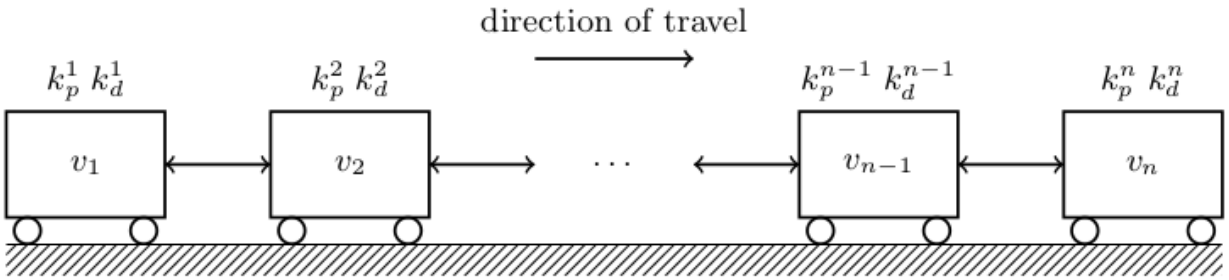
- They show that an attacker is theoretically capable of gaining control over the individual position and velocity of other vehicles in the platoon

[3] Dadras, Soodeh, Ryan M. Gerdes, and Rajnikant Sharma. "Vehicular platooning in an adversarial environment." *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ACM, 2015.

Platoon Model

- We use bi-directional proportional-derivative(PD) controller of to demonstrate the catastrophic effect

- It allows us to show that an attacker can affect the platoon solely through malicious movement and needn't rely on interfering with communication between vehicles



(a)

platoon size	3	4	5	6
$k_d \geq$	2.1	2.7	3.3	4.2
platoon size	7	8	9	10
$k_d \geq$	5.1	6	7	7.7

(b)

Figure 2: (a) An n-vehicle platoon employing a bi-directional control law. Arrows represent the flow of information. (b) The minimum derivate gains necessary to guarantee string stability ($k_p = 1$).

String Stability

The stability/string stability condition in the homogeneous case states that spacing errors between vehicles should attenuate as they move upstream. Allowing $z_i = x_i - x_{i+1}$ to represent the spacing error between the i^{th} and $i^{\text{th}}+1$ vehicles, the string stability criterion may be stated as [33]

$$|G_i(s)| = \left| \frac{z_i}{z_{i+1}} \right| < 1 \text{ for } i = 1, \ldots, n-2 \qquad (3)$$

where $s = \jmath\omega$ and ω is the angular frequency. $|G_i(s)|$ represents the magnitude of the (error) transfer function between the i^{th} and $i^{\text{th}}+1$ vehicles. The transfer function varies ac-

String Instability Analysis

To violate the string stability condition an attacker must select a gain, $\tilde{k}_d$, such that the inequality of (3) is reversed. Even though the attacker gain may appear in more than one transfer function, the attacker need only cause a single $|G_i(s)| = \left|\frac{z_i}{z_{i+1}}\right| > 1$ to breach the stability criterion. In

Platoon Controllability

DEFINITION 3 (CONTROLLABILITY). *A system is said to be controllable if and only if it is possible, by means of the input, to transfer the system from one state to another state in finite time.*

A LTI system represented by

$$\dot{x} = Ax + Bu \tag{17}$$

where $x \in \mathbb{R}^n$, $A \in \mathbb{R}^{n \times n}$, $u \in \mathbb{R}^m$, and $B \in \mathbb{R}^{n \times m}$. is controllable if the controllability matrix

$$\mathcal{C} = \begin{bmatrix} B & AB & A^2B & \cdots & A^{n-1}B \end{bmatrix} \tag{18}$$

is full rank (i.e $rank(\mathcal{C}) = n$) [6].

Analysis Result

- Based on their analysis, whether lead vehicle is affected by followers or not, the attacker can control relative position and velocity between all the vehicles