A Functional Co-Design towards Safe and Secure Vehicle Platooning

Jiafa Liu[1], Di Ma[1]
[1]University of Michigan-Dearborn
{jiafal, dmadma}@umich.edu

Andre Weimerskirch[2]
Lear Corporation
AWeimerskirch@lear.com

Haojin Zhu[3]
Shanghai Jiao Tong University
zhu-hj@cs.sjtu.edu.cn

ABSTRACT

Cooperative adaptive cruise control (CACC) or platooning recently becomes promising as vehicles can learn of nearby vehicles' intentions and dynamics through wireless vehicle to vehicle (V2V) communication and advanced on-board sensing technologies. Violation of cybersecurity often results in serious safety issues as been demonstrated in recent studies. However, safety and security in a vehicle platoon so far have been considered separately by different sets of experts. Consequently no existing solution solves both safety and security in a coherent way. In this paper, we show cyber attacks on an automated platoon system could have the most severe level of safety impact with large scale car crash and argue the importance of safety-security co-design for safety critical cyber physical systems (CPS). We propose a safety-security co-design engineering process to derive functional security requirements for a safe automated vehicle platoon system based on a deep comprehension on the interrelation of safety and security. To our best knowledge, we are the first to apply the safety-security co-design concept to a concrete application. Through this engineering process, we propose a general approach for designing a safe and secure platooning. Following the general approach, we come up with a new platoon control algorithm that takes into account both safety and security. Our defense mechanism implicitly defends against safety-related cyber-attacks and greatly shortens the safe distance required when the platoon is not protected.

CCS Concepts

•**Security and privacy** → **Security requirements; Intrusion/anomaly detection and malware mitigation; Systems security;** *Access control; Security in hardware;*

Keywords

Platoon; Safety-security Co-design; Control Algorithm

CPSS'17, April 02 2017, Abu Dhabi, United Arab Emirates

DOI: http://dx.doi.org/10.1145/3055186.3055193

1. INTRODUCTION

Vehicle platooning has been studied as a method of increasing the capacity of roads since the 1960's. In a vehicle platoon, a group of vehicles, following one another, acts as a single unit through coordinated movements. Because vehicles in a platoon travel together closely yet safely, this leads to a reduction in the amount of space used by the number of vehicles on a highway, thus has the great potential to *maximize highway throughput*. Cooperative adaptive cruise control (CACC) or automated vehicle platooning recently becomes promising as vehicles can learn of nearby vehicles' intentions and dynamics through wireless vehicle to vehicle (V2V) communication and advanced on-board sensing technologies. Automation-capable vehicles in tightly spaced, computer-controlled platoons offer additional benefits such as *improved mileage and energy efficiency* due to reduced aerodynamic forces, as well as *increased passenger comfort* as the ride is much smoother with fewer changes in acceleration.

The complexity of an automated vehicle platoon system – including inter-vehicle communications, vehicle's internal networking and its connection to external networks, as well as complicated and distributed platooning controllers – opens doors to malicious attacks. In-vehicle range sensors that are used to measure the preceding car's speed and location might be altered. For instance, it was recently demonstrated that radar and LIDAR sensors can be spoofed with a modulated laser [1]. The wireless communication channel (DSRC) is vulnerable to manipulation and wireless messages can be spoofed by a motivated attacker [3, 7, 8]. All these attacks could cause a wide array of problems in a deployed platoon, for example, an attacker could cause crashes, reduce fuel economy through inducing oscillations in spacing, prevent the platoon from reaching its (or each individual's) destination(s), or cause the platoon to break up. The full potential of automated vehicle platooning will not be realized until the issues related to communication and application security can be satisfyingly resolved.

The violation of cybersecurity could result in serious safety violations such as car crashes. However, safety and security in a vehicle platoon have so far been considered separately by different sets of experts. On one hand, the safety discipline usually considers system failures (including systematic/random hardware and systematic software failures) or natural disasters as safety hazard resources. Safety solutions developed are usually not evaluated in an adversarial environment. On the other hand, the security discipline considers various attacks that can lead to different consequences

such as loss of life, loss of privacy, financial loss, etc. The variety of security goals to address different types of attacks makes it very unlikely to be aligned with the goal of safety. Consequently security solutions proposed are rarely evaluated in terms of safety. For example, the model-based detection scheme [7], the only scheme proposed so far for platoon security, is designed from the **security point of view** by *monitoring any misbehavior of the preceding car*. Although the scheme is able to detect vehicle misbehavior, whether it can lead to a safe platoon is not answered. To date, no existing platooning solution solves both safety and security in a reconciled and coherent way.

Based on a joint functional safety and security analysis, we are able to reconcile different safety and security risks. For our purpose, we consider the subset of security threats that lead to safety consequences. This allows us to align our security goal with that of the safety. We propose a new platooning control algorithm that is designed from **the safety point of view**. Unlike the model-based detection scheme [7] which is designed from the security point of view where a vehicle treats the one before it as *potentially malicious*, in our scheme, a vehicle concentrates on self-safety, calculates *its own safety status* (instead of predicting other's misbehavior) based on the context information and adjusts its next movement based on one criterion: whether it is safe to do so. If it senses the next step is not safe, the vehicle will switch from the cooperative driving CACC mode to the collision avoidance ACC mode. By centralizing on self-safety, our scheme achieves safety by implicitly defending against cyber attacks that could result in safety consequences.

Contributions: Our contributions are as follows:

- Based on a deep comprehension of the potential security and safety risks, we put emphasis on safety-security co-design and make recommendations related to security and safety in automated vehicle platooning by integrating cybersecurity into safety design strategies. To our best knowledge, we are the first to apply the safety-security co-design concepts to a concrete application (Section 4).
- To fully understand the severity of cybersecurity-induced safety risk, we introduce a leader crash attack to demonstrate the severity of such attack on the safety of vehicle platoon. To ensure the safety of platoons under attacks, We propose the concept of *safe distance* for platoons. A platoon has to travel with at least the safe distance to avoid any collision (Section 4).
- Based on the co-design analysis, we propose a general approach for designing a safe platooning. We inist that platoon should maintain a safe distance and at the same time, detect various potential cyber attacks. When the platoon is under cyber attack, it should switch to fail-safe scheme to avoid collision (Section 5).
- We propose a new platoon control algorithm emphasizing on self-safety. In our scheme, each vehicle cross-checks accelerations predicted by both the CACC and ACC controllers to determine whether the next move is safe. Our defense mechanism greatly shortens the safe distance required when the platoon is not protected (Section 7).

Organization: The organization of the paper is as follows. We overview related work in Section 2. We present system and attack models as well as platooning controllers in Section 3. We perform a joint safety and security risk analysis in Section 4 where we also introduce a leader crash attack to analyze the severity of such attack on safety. Then we propose a general approach for designing a safe platooning in Section 5. We present two safe platooning schemes in Sections 6 and 7. Discussions and future work are presented in Section 8 and Section 9 concludes the paper.

2. RELATED WORK

Vehicle and Vehicle Network Security. Vehicle security is an emerging topic. A number of previous works have demonstrated many insecure designs in modern vehicles [20–23]. Vehicle network security has been extensively studied. Many techniques such as efficient message authentication, anonymous authentication to address various aspects of communication security and privacy have been proposed [24, 25]. Chenxi Zhang [24] presents an efficient batch signature verification scheme for communications between vehicles and roadside units. Xiaodong Lin [25] proposes an efficient social-tier-assisted packet forwarding protocol, for achieving receiver-location privacy preservation in Vehicular Ad hoc Networks.

Platooning Security.

The security of autonomous platooning has been recently studied. Mani Amoozadeh [3] presents a first look at the effects of security attacks on the communication channel as well as sensor tampering of a connected vehicle stream. The work of [7] introduces a set of insider attacks that can cause unexpected behavior in platoons. It suggests switching from CACC to ACC if a crash could happen. Soodeh Dardras [8] presents that a single malicious controlled vehicle can destabilize a vehicular platoon.

Collision Avoidance. For collision avoidance, Gehrig and Stein [9] have proposed the concept of elastic bands and analyzed collision avoidance. Araki [10] presents a system which has automatic braking when the headway distance between the trailing vehicle and the selected vehicle crossed the safety threshold. Ferrara and Vecchio [11] propose a concept of a supervisor for the control system of every vehicle in the platoon to avoid collision.

3. MODELS AND SIMULATION ENVIRONMENT

In this section, we present the system model we use. We also provide information about the simulation platform we will use to carry out the work presented in this paper.

3.1 System Model

We consider a platoon of K cars numbered from 0 to $K-1$ with car 0 being the leader vehicle. We assume the platoon is already formed and do not consider platoon formation and dissolve (we leave platoon dynamics as our future work). All cars drive on a straight line with string stability. The order of cars does not change. We assume homogeneous cars which have the same physics, mechanics, and communication capabilities (this requirement will be relaxed in our future work). They are not immune to hardware/system failures, and cybersecurity attacks, so abnormal behaviors can happen.

3.1.1 Communication and Mobility Models

In order to study the safety and security of a CACC vehicle system, we utilize the PLEXE platform [17] for its built-in communication (IEEE 802.11p) and mobility models. PLEXE is an Open Source extension to the known and widely used Veins simulation framework [18] by adding platooning capabilities and controllers. Veins itself extends the OMNeT++ network simulator and the SUMO road traffic simulator. PLEXE implements a list of classic controllers for Cruise Control (CC), Adaptive Cruise Control (ACC), and Cooperative Adaptive Cruise Control (CACC) to realize platooning capabilities.

3.1.2 Cruise Control

CC is a technology which allows a driver to select a desired speed and the car is driven automatically at the desired speed until CC is switched off by the driver. PLEXE implements the classic Cruise Control algorithm (Equation 1) which is already available on several commercial cars [15].

$$\ddot{x}_{des} = -k_p(\dot{x} - \dot{x}_{des}) - \eta \tag{1}$$

where $\ddot{x}_{des}$ is the acceleration to be applied, $\dot{x}$ is the current speed and $\dot{x}_{des}$ is the desired speed, k_p is the gain of the proportional controller (set to 1 by default), while η is a random disturbance taking into account imprecision of the actuator and of the speed measure (default set to 0).

3.1.3 Adaptive Cruise Control

As CC only takes the desired and actual speed as inputs, the driver needs to manually switch off CC to avoid a collision when approaching a slower vehicle in the front. To avoid collision and also relieve the driver from this duty, high-end cars are now equipped with a radar or laser scanner to estimate distance to the preceding car. If a slower car is detected, the system decelerates and automatically maintains a safe distance. This technology is known as ACC. ACC will automatically slow down the vehicle whenever it finds obstacles in the way.

ACC makes use of radar to detect vehicles in front and calculate the desired acceleration with only preceding car into consideration. ACC will automatically slow down the vehicle whenever it finds obstacles in the way. CACC primarily rely on wireless communication to broadcast driving information to each vehicle. After receiving the message from preceding vehicle and leader vehicle, the controller computes the desired acceleration for the current vehicle. Different from CACC, ACC makes use of radar to detect vehicles in front and calculate the desired acceleration with only preceding car into consideration. ACC will automatically slow down the vehicle whenever it finds obstacles in the way. The control law of ACC [15] used in PLEXE is defined as

$$\ddot{x}_{i\_des} = -\frac{1}{T}(\dot{\varepsilon}_i + \lambda\delta_i) \tag{2}$$

$$\delta_i = x_i - x_{i-1} + l_{i-1} + T\dot{x}_i \tag{3}$$

$$\dot{\varepsilon}_i = \dot{x}_i - \dot{x}_{i-1} \tag{4}$$

where T is the time headway in seconds and $\dot{\varepsilon}_i$ is the relative speed between two consecutive vehicles i and $i+1$. δ_i is the distance error which is the difference between the actual distance $(x_i - x_{i-1} + l_{i-1})$ and the desired distance $T\dot{x}_i$. λ is a design parameter which is strictly greater than 0 and set to 0.1 by default.

The ACC driving functionality in PLEXE is implemented through the use of both ACC and CC controllers. When the ACC driving mode is selected, a car follows the instruction of the one which predicts smaller acceleration rate:

$$\ddot{x}_{des} = min(\ddot{x}_{CC}, \ddot{x}_{ACC}) \tag{5}$$

Basically, if the CC decides to accelerate to reach the desired speed, but the ACC decides to slow down because of a vehicle in front, the car will follow the instructions of the ACC. On contrary, if the ACC decides to accelerate to follow the car in front, but the car has reached its desired speed, the CC will make the car to "detach" from the preceding one. If there is no car in front (assuming that the radar detects no car in front) or the distance is larger than $250m$, the car only considers CC even when it is in the ACC mode. Notice that this might not be the best strategy to implement, but for the sake of simplicity PLEXE [17] chooses to use this straightforward switching mechanism.

3.1.4 Cooperative Adaptive Cruise Control

The CACC controller implemented in PLEXE is a representative CACC controller based on classical control theory [15]. The status of each vehicle depends on the acceleration and speed of the leading and preceding vehicle in order to keep close vehicle following. It is capable of maintaining a fixed distance between cars no matter what the platoon's speed is.

The control law of the i-th vehicle in the platoon is defined as

$$\ddot{x}_{i\_des} = \alpha_1\ddot{x}_{i-1} + \alpha_2\ddot{x}_0 + \alpha_3\dot{\varepsilon}_i + \alpha_4(\dot{x}_i - \dot{x}_0) + \alpha_5\varepsilon_i \tag{6}$$

$$\varepsilon_i = x_i - x_{i-1} + l_{i-1} + gap_{des} \tag{7}$$

$$\dot{\varepsilon}_i = \dot{x}_i - \dot{x}_{i-1} \tag{8}$$

$\ddot{x}_{i\_des}$ is the desired acceleration of i-th vehicle. $\ddot{x}_{i-1}$ and $\ddot{x}_0$ are the acceleration of the preceding vehicle $i-1$ and the leading vehicle. $\dot{x}_i$ and $\dot{x}_0$ are the speed of i-th vehicle and leader vehicle. ε_i is the distance error based on a desired constant distance gap_{des} which is 5 meters by default. l_{i-1} is the length of car and the default value is 4 meters.

The α_i parameters in Equation 6 are defined as:

$$\alpha_1 = 1 - C_1; \qquad \alpha_2 = C_1; \qquad \alpha_5 = -\omega_n^2 \tag{9}$$

$$\alpha_3 = -(2\xi - C_1(\xi + \sqrt{\xi^2 - 1}))\omega_n \tag{10}$$

$$\alpha_4 = -C_1(\xi + \sqrt{\xi^2 - 1})\omega_n \tag{11}$$

C_1 is a weighting factor between the acceleration of the leader and the preceding vehicle, which is set to 0.5 by default. ξ is the damping ratio and set to 1 by default. ω_n is the controller bandwidth and set to 0.2 Hz by default.

In the implementation of the CACC functionality, the interaction between CC and CACC depends on the distance between vehicles. If a vehicle is less than 20 meters from the preceding one, the vehicle follows instructions from CACC: $\ddot{x}_{des} = \ddot{x}_{CACC}$, otherwise, the policy is the same as ACC: $\ddot{x}_{des} = min(\ddot{x}_{CC}, \ddot{x}_{CACC})$.

3.1.5 Controller Comparison

We use Table 1 to summarize distinguished characteristics of each controller strategy. From the table we can see that different controller strategies have diverse design objectives.

Controller Strategy	Characteristic
CC	Maintain desired velocity
ACC	Collision avoidance
CACC	Fixed small gap String stability

Table 1: Comparison between controller strategies

3.2 Simulation Environment

We use PLEXE for all the (attack and defense) simulations carried out in this work. As mentioned earlier, PLEXE extends Veins which further extends the OMNeT++ network simulator and the SUMO mobility simulator. The coupling between the network and the mobility simulation framework is done through the TraCI interface which SUMO exposes. PLEXE extends the interaction through the TraCI interface in order to fetch vehicles' data from SUMO to be sent to other vehicles in the platoon to realize CACC. Platooning protocols and the application logic are realized in the OMNeT++ framework.

To simulate the adversary, we need to provide the functionality that informs the adversary vehicle how to launch the attack. To achieve this, we need to refer to application layer logic. There is a BaseApp in PLEXE which simply extracts data out of packets coming from the protocol layer and updates CACC data via TraCI if such data is coming either from the leading vehicle or from the preceding vehicle. SimplePlatooningApp extends BaseApp and it tells the vehicle to use the controller requested by the user. We modify the SimplePlatooningApp so that to let vehicles follow the instructions of what we want them to do.

4. SAFETY AND SECURITY CO-DESIGN

Safety has a long tradition in many engineering disciplines and has had successful standardization efforts. In automotive systems, the international standard ISO 26262 is the state of the art standard for safety critical system development. J3061 Cybersecurity Guidebook [19] is an overall guidebook on implementing cybersecurity for the entire vehicle. The safety-security co-design is being discussed in the secure software SAE committee at the moment and there is no final product yet. We are able to work with several key members of the SAE cybersecurity committee to understand the concepts and requirements as well as discuss the proposed safety-security engineering process.

4.1 Safety-Security co-Design

We propose a safety-security co-design engineering process which consists of four main steps: (1) Define the safety goal for the system; (2) Define attack model; (3) Derive security goals; (4) Derive functional security requirements.

Safety Goal. Safety is very important in automotive industry and therefore highly regulated. For end users, it means that users do not face any risk or danger coming from the motor vehicle or its spare parts. Unacceptable consequences for safety are loss of human life and injuries. The safety goal of individual vehicle is to protect users from injuries and life threatening risks. In our context, we set up the safety goal of vehicle platoon as avoiding car collisions that can cause human life and injuries.

Attack Model and Security Goal. Unlike safety, cybersecurity has a broader range of unacceptable consequences such as human life and injury (safety), human security, financial loss, loss of privacy [28, 29], etc. Figure 1 shows the interrelation of safety and security. From Figure 1, we can see that safety can be an objective (or impact) of a security attack. It can also be an unintended consequence caused by hardware or software bugs. Meanwhile, cyber attacks can have different impacts. The intersection part concerns both safety and security, or safety-related security risks, which is of interest of this paper.

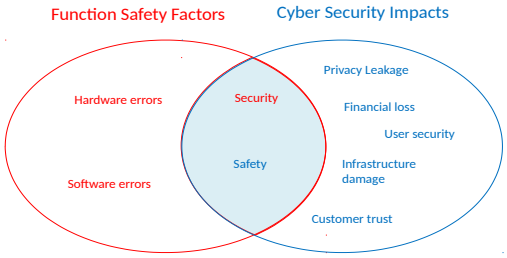

Figure 1: Interrelation of Safety and Security

To derive our attack model that lead to safety, we summarize various of attacks, targeting at automotive platoon systems, extensively studied by researchers in the literature and their corresponding possible consequences in Table 2. From the table, we can see that there are five attacks which can lead to car collisions, result in safety issues, and thus belong to the intersection in Figure 1. Our security goal is to develop a system that is resilient to these attacks.

Adversary Model: We consider insider attacks that can lead to safety issues such as car crashes in this work. Attacks that result in different consequences such as system performance, driver privacy, financial loss, etc. are not considered in this paper as they can be treated in the regular way without considering safety. The adversary or the vehicle controlled by the adversary is part of the platoon system and thus is able to send valid V2V messages. However, there is no guarantee on the correctness of information in the messages it sends. Also the adversary does not need to follow the control law. The adversary is able to control one or more vehicles, including the leader, in the platoon. However, it cannot control all the radars or radar signals of vehicles in the platoon because of the line-of-sight requirement.

Functional Security Requirements. From our analysis above, we can derive functional security requirements as follows:

- It shall not be able for an attacker to spoof a message;
- It shall not be possible to replay an old message;
- It shall not be possible for an attacker to broadcast a message with false information without being detected;
- The system shall be able to take a response action whenever such misbehavior is detected;
- The system shall ensure there is enough time for the system to respond.

Reference	Attack	Impact
[14]	Message falsification attack	Collision
	Message spoofing	Collision
	Message replay	Collision
	DoS (jamming)	Dissolved platoon
	System tampering	Collision
[7]	Collision induction attack	Collision
	Reduced headway attack	Decreased string stability
	Joining without radar	Decreased string stability
	Mis-report attack	Decreased performance
	Non-attack abnormalities	Decreased performance and string stability
[8]	Destabilization attack	Decreased string stability
	Platoon control taken attack	Dissolved platoon

Table 2: Attacks and impacts

4.2 Severity Analysis

The EU project EVITA provides a risk model to measure the security of in-vehicle systems [16]. In response to various safety risks, ISO 26262 severity classification defines four severity levels (S0, S1, S2 and S3) in terms of the estimated personal injury that could result from the risk. S0 refers to no injuries. S1 refers to light or moderate injuries. S2 means severe to life-threatening injuries (survival probable). S3 means life threatening (survival uncertain) or fatal injuries. The EVITA model extends the ISO 26262 safety classification by including a fifth level S4 which means fatal injuries of **multiple vehicles** as cyber security attacks may have more widespread implication than unintended hardware or software bugs can cause.

Previous work [7] has shown that message falsification and collision induction attacks can result in serious safety issue. However, it is not clear the severity level of such attacks. To understand the severity level of a collision that is resulted from a cyber attack, we introduce a new attack called leader crash attack by extending the collision induction attack proposed in [7]. In the leader crash attack, the leading car stops suddenly (intentionally due to being remotely controlled by an attacker or not) and causes the following cars to crash over each other. This crash attack can be mounted by any insider, not just the leader, in the platoon. However it is very likely a crash attack induced by the leader can have the most severe consequence.

We use the PLEXE simulator to demonstrate the consequence of this attack (**severity**). In this simulation, initially a platoon of four vehicles is driving at the speed of 100 km/h with a gap of 5 meters (we will use the same platoon as a concrete example throughout the rest of the paper). At the time of 50s, we instruct the leader vehicle to stop. We set the deceleration of the leader car extremely large so that the speed can decelerate to zero in a very short time interval. In this way, the leader vehicle acts just like it suddenly hits the brake or crashes into something like a wall so that it stops immediately. We see how the following vehicles will respond under the CACC controller strategy. To obtain an insight of speed changing of the platoon in the crash, we utilize the statistics collected from PLEXE which are shown in Figure 2. In Figure 2, Vehicle 0 with the red line is the leader vehicle. Vehicle 0 decelerates from 100 km/h (27.77 m/s) to 0 km/h in a very short time interval. The following vehicles are trying to prevent crash by decelerating, but the 5-meter gap is not long enough for them to fully stop before they crash into the car before it. The above three lines terminating at different time spot shows that each of them has crashed into the leader vehicle.

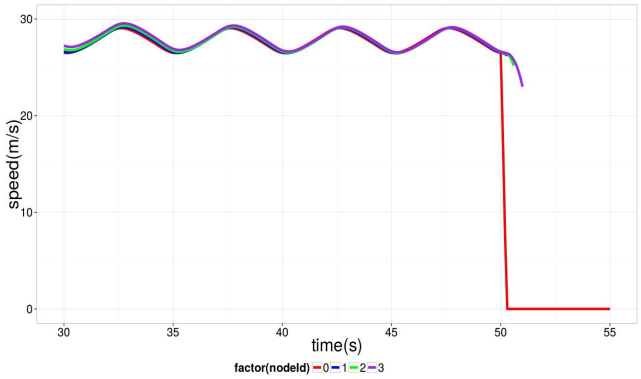

Figure 2: Speed Changes of Platoon during the Crash

More on severity. The above simulation clearly demonstrates that the leader car crash attack can potentially result in multiple car damage and life injuries and has the highest level of safety severity. However, the maximum safety impact of security attack demonstrated is only a **local** event to several vehicles. We believe the worst security impact can potentially be *nation-wide* impacting thousands or millions of cars and suggest a new severity level of **S5: nation-wide wide spread and harmful impact**. For example, in the platoon context, suppose there is a security weakness that has an impact due to forged DSRC messages, also suppose future smart-phones are DSRC enabled and malware spread on smartphones, we can easily see a nation-wide attack platform to attack the platoon mechanism. Due to the severity of security attacks on platoon systems, we strongly argue the importance of designing safe and secure platoon systems.

5. SAFE PLATOONING:GENERAL APPROACH

Based on the safety-security co-design analysis, we propose a general approach to design a safe platooning. There are three steps to take in order to maintain safety and security. First, vehicles in the platoon need to keep a safe distance from preceding vehicle, so that when abnormal driving happens, they have enough distance to brake. Second, ve-

hicles are supposed to detect security attacks while driving. These attacks include message falsification attack, collision induction attack, abnormal driving and so on. There are also many countermeasures to detect these attacks which will be discussed in the following part. Third, when abnormalities are detected, vehicles should switch to fail-safe scheme such as Adaptive Cruise Control (ACC) or Emergency Brake Assist (EBA) to avoid collision.

5.1 Safe Distance

Platoon is designed to keep a small distance between each vehicle so that it can increase the highway capacity. The platoon in SARTRE Project is driving at 90 km/h with a 4-meter gap between vehicles. Meanwhile, Energy ITS maintains a 80 km/h platoon with 4-meter gap. However, when accident happens, there is no enough distance for these vehicles to decelerate. As shown above, leader crash attack can cause multiple vehicle damage and life injuries.

For a safe platooning design, we need to maintain the safe distance to defend against extreme incidents. [26] presents a unique optimal control method of velocity and distance for platooning using model predictive control. Estimation of safe distance is also dependent on the fail-safe scheme adopted. This paper aims to develop an optimal control system for safe distance of platooning. In out paper, we also want to identify the exact safe distance for platooning with the corresponding fail-safe scheme. We will use a concrete example to present the method of obtaining safe distance.

5.2 Attack Detection

To ensure safety, platoon has to detect various cyber attacks. In Bruce DeBruhl's paper [7], he proposes a set of insider attacks that can cause unexpected behaviors in platoons. Mis-report attack is the attack that sends false message to the following vehicle to increase the following distance of the preceding car. Collision induction attack can cause dangerous accidents by broadcasting an acceleration message indicating that they are speeding up, while the attacker starts to aggressively brake. The work of [7] suggests switching from CACC to ACC if a crash could happen. It focuses on the detection of false message attack from the preceding car. In the false message attack, a malicious preceding car driving at a low speed mis-reports it is driving at a high speed. The false message may mis-lead the following car to collide with the malicious preceding car. From the security angle, the proposed solution is to let each vehicle monitor the behavior of the preceding car. If the received status info from the preceding car is different from the one the following car calculates, the following car will think the preceding car may behave abnormally and switch to ACC. However it is not clear whether the switch from CACC to ACC can lead to a safe platoon.

In our paper, we will show that platoon with a safe distance is able to avoid collision in worst cases by switching to ACC. In our scheme, a vehicle concentrates on self-safety, calculates *its own safety status* (instead of predicting others' misbehavior) based on the context information and adjusts its next movement based on one criterion: whether it is safe to do so. If it senses the next step is not safe, the vehicle will switch from the cooperative driving CACC mode to the collision avoidance ACC mode. By centralizing on self-safety, our scheme achieves safety by implicitly defending against cyber attacks that could result in safety consequences.

5.3 Switch to Fail-safe Scheme

Fail-safe is a mechanism which is automatically triggered by failure that reduces or eliminates harm [27]. A fail-safe is not supposed to prevent failure but mitigates failure when it happens. For example, railway trains commonly have air brakes that get applied automatically when the main brake system fails to work. Flight control computers are typically designed with redundancy so that when one goes down another will continue to function. Similarly, platoon's safety is threatened by different kinds of cyber attacks and in some worst cases, such as leader crash attack, vehicles need to switch to fail-safe scheme to eliminate harm. Under this circumstance, vehicles are suggested to switch to ACC or EBA to avoid collision. Moreover, this defense mechanism can only succeed on one condition: there is a safe distance between vehicles. In the following section, we will use an example to show how safe distance can guarantee the safety of platoon and how to shorten the safe distance with attack detection.

6. SAFE PLATOONING: FIRST ATTEMPT

In this section, we propose a naive solution to deal with the worst case in platoon, such as leader crash attack. In the naive solution, we do not detect cyber attacks and we only rely on safe distance to ensure safety. Results show that relying on safe distance alone is not feasible for a safe platooning. We have to follow the three steps in general approach to design a safe platooning.

The platoon in this paper is traveling at 100km/h with a 5-meter gap. From the previous simulation on leader crash attack, we can see that when the leader vehicle in the platoon crashes suddenly, such a short distance between cars is not enough for the following vehicles to decelerate. To avoid collision, without changing the underlying CACC controller, the straightforward idea is to simply increase the distance between cars so that a car can stop before it crashes over the preceding car.

We use PLEXE to test this naive idea to find the required safe distance. In the SimplePlatooningApp, we set the constant space to a specific value at first by using the TraCI interface to update the CACC data. We increase the constant gap between vehicles step by step until we find that when the car-to-car distance is increased to 47 meters, the following vehicles will not crash into preceding vehicles. 47 meters equal to a headway of $T = 1.7s$ when the vehicle is traveling at 100km/h. Figure 3 shows speed changing of vehicles when the gap is increased to 47 meters.

6.1 Theoretical Analysis of CACC Safe Distance

In order to prove that we find the correct safe distance for a platoon under the leader crash attack, we calculate the theoretical safe distance value by using MATLAB and do a cross check with our simulation result. In the CACC controller, the acceleration of each vehicle is calculated based on on the leader vehicle and preceding vehicle. Vehicle 0 is leader vehicle and we study the performance of vehicle 1. If vehicle 1 does not crash into vehicle 0, the following two vehicles will not crash either as there is longer distance for them to decelerate.

In Equation (6), we set $\ddot{x}_0$ and $\dot{x}_0$ to 0 and other variables to their default values. x refers to location of the vehicle. $\dot{x}$ and $\ddot{x}$ refers to the speed and acceleration of the vehicle. In

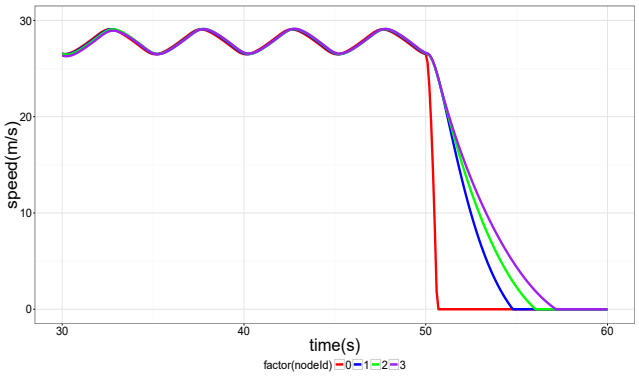

Figure 3: Naive Solution: Speed Changing

this way, we transfer Equation (6) to Equation (12).

$$\ddot{x}_1 = -0.4\dot{x}_1 - 0.04(x_1 - x_0 + l_0 + gap_{des}) \quad (12)$$

Obviously, Equation (12) is a second order differential equation and x_0, l_0, gap_{des} are constant values. x_0 is the location where the leader vehicle crashes. l_0 is the length of vehicle 0 and gap_{des} is the distance between two vehicles. By solving this equation, we acquire the relation between vehicle location x and time t. By differentiating the equation between vehicle location x and time t, we can obtain the relation of a vehicle speed $\dot{x}$ and the time t. With the time t when the vehicle speed decreases to 0, we are able to obtain the location x where the vehicle stops. If location x is smaller than the location of the leader vehicle x_0, we say there is enough safe distance for the platoon.

Algorithm 1 Safe Distance Calculation

1: **Input:** Vehicle Location location, Vehicle Speed speed
2: **Output:** Final Position of the Vehicle
3:
4: Use *dsolve* method to find the relation between location x and time t. Original state is x(0) = location, Dx(0) = speed
5: $x = dsolve(D2x + 0.4Dx + 0.04x - 0.04(x_0 - l_0 - gap), t)$
6:
7: Use $diff$ method to find the relation between speed and time
8: $speed = diff(x)$
9:
10: Find the time when Vehicle 1 decelerates to 0
11: $speedChar = char(speed)$
12: $time = solve(speedChar, 't')$
13:
14: Find the position where Vehicle 1 finally stops
15: $f = inline(x)$
16: $answer = f(time)$

Algorithm 1 is the MATLAB program which is used to estimate the theoretical safe distance a platoon needs to maintain to defend against a leader crash attack. From the statistics collected by OMNeT++, we can get the final position of leader vehicle x_0 which is 1432 meters. The speed of Vehicle 1 $Dx(0)$ in initial state is 27.77 m/s (100 km/h). The default length of vehicle l_0 is 4 meters. Taking the vehicle length into consideration, we hope that the final position of Vehicle 1 which is the output of the algorithm should be 1428 meters. By adjusting the input gap_{des} and the original location of Vehicle 1 $x(0)$, we need to achieve $gap_{des} + x(0) = x_0 - l_0$. Therefore, the gap_{des} is the exact safe distance for the platoon to decelerate during a leader crash attack. After executing the algorithm, we find out that when the gap_{des} equals 51 meters and the position of Vehicle 1 $x(0)$ equals 1377 meters where it starts to decelerate, then it will stop at the distance of 1428 meters. In this way, the safe distance is the difference between two positions which is 51 meters.

From the discussion above, we can see that CACC does not help in achieving better safety under urgent situations. Although increasing vehicle distance can help to achieve safety, this naive solution kills the space efficiency a platoon brings as a headway of $T = 1.7s$ is enough for a human driver to stop safely from a speed of 100km/h.

7. PROACTIVE SAFE PLATOONING

As shown in previous section, the naive approach to safe platooning does not work as it totally removes the space efficiency which is the major reason why vehicle platoon is designed for. This motivates us to design a secure and safe CACC algorithm which achieves safety and security without losing space efficiency. Therefore, in this section, we follow the three steps in general approach to design a safe and feasible platooning.

7.1 Attack Detection

[7] focuses on the safe status of preceding vehicle. It compares the expected behavior and measured behavior of front car, if the error is larger than a specific threshold, current car switches to ACC controller strategy. The parameters of preceding car they choose are acceleration and velocity. Different from previous work, we concentrate on current vehicle's safety status. The parameters we choose are acceleration and distance. The reason why we don't consider velocity is that for ego vehicle, its speed is able to vary all the time and change abruptly in accidents. So we cannot use velocity to determine whether current vehicle's status is safe or not. In the following, we will show how to use acceleration and distance to ensure both safety and security.

7.1.1 Acceleration & Distance

For acceleration, to detect cyber attacks and avoid collision in CACC function, our idea is to include ACC in the design of the CACC function as ACC is designed for collision avoidance. It relies on range sensors like radar or laser scanner to estimate the distance to the preceding car. Real time distance information can be further used to estimate the preceding car's velocity and acceleration. We utilize ACC acceleration as the baseline for safe situation determination. In normal situations, the acceleration rate calculated by CACC is less than the acceleration rate calculated by ACC (i.e., speed change in CACC is usually more smoothly than that in ACC for improved user comfort). Let Δ denote the fluctuation range of ACC acceleration. When the acceleration rate of a vehicle falls into this range $[ACC - \Delta, ACC + \Delta]$ (here, ACC refers to acceleration in ACC controller strategy), it indicates there is no immediate crash threat. On the contrary, if the acceleration of a vehicle is out of the range, it indicates abnormal situation and we need to switch to fail-safe scheme to avoid collision.

Here are some details on how range is defined. From Equation (6) and Equation (2), the accelerations of CACC and ACC in normal state can be calculated. By setting parameters to their default values, we are able to get Equation (13) and Equation (14).

$$\ddot{x}_{i\_cacc} = 0.5\ddot{x}_{i-1} + 0.5\ddot{x}_0 - 0.4\dot{x}_i + 0.3\dot{x}_{i-1} + 0.1\dot{x}_0 - 0.04x_i + 0.04x_{i-1} - 0.04l_{i-1} - 0.04gap_{des} \quad (13)$$

$$\ddot{x}_{i\_acc} = -\frac{1}{T}(\dot{x}_i - \dot{x}_{i-1} + 0.1x_i - 0.1x_{i-1} + 0.1l_{i-1} + 0.1T\dot{x}_i) \quad (14)$$

Let us define

$$\Delta = max(|\ddot{x}_{i\_cacc} - \ddot{x}_{i\_acc}|) \quad (15)$$

In normal situation, the platoon is driving with a fixed speed and constant gap between cars. Therefore, we can assume that $\ddot{x}_{i-1}$ and $\ddot{x}_0$ are 0 with $\dot{x}_i$, $\dot{x}_{i-1}$ and $\dot{x}_0$ are equal. Meanwhile we have $\dot{x}_{i-1} - \dot{x}_i = gap_{des} + l_{i-1}$ so that the acceleration of CACC $\ddot{x}_{i\_cacc}$ is 0. For ACC, T is headway and then we have $\ddot{x}_{i\_acc} = -\frac{1}{T}(0.1T\dot{x}_i - 0.1gap_{des})$. Finally, the guideline for range is achieved with $\Delta = max(|\frac{1}{T}(0.1T\dot{x}_i - 0.1gap_{des})|) = 0.1max(\dot{x}_i) - \frac{0.1gap_{des}}{T}$. $max(\dot{x}_i)$ is the max speed of Vehicle i. This max speed is not the maximum mechanical speed a car can have. Instead, it is the max speed set by automatic driving. Usually the max speed in automatic driving is less than the actual max speed a car can have because passenger comfort is usually an important factor in automatic driving.

For distance, we use a straightforward way to detect cyber attacks. When platooning is driving in normal situation, it maintains a fixed desired gap. The idea is to check whether the gap between vehicles is smaller than desired value, if it is, then we identify a cyber attack.

7.2 Switch to Fail-safe Scheme

Once cyber attacks are mounted on platoon, we need to switch to fail-safe scheme to reduce or eliminate harm. When crash happens, we believe in such urgent situation, autonomous driving responds quicker than human drivers. So we choose to switch cooperative CACC to non-cooperative ACC. There might be other autonomous emergency plans which we will take further investigation in the future. In the following, we will show the fail-safe schemes of different parameters (acceleration,distance) respectively.

7.2.1 Acceleration & Distance

Based on the above analysis, for acceleration parameter, we propose Proactive CACC Algorithm which is shown as Algorithm 2. In our algorithm, a vehicle calculates desired acceleration in both CACC and ACC controller strategy. It switches to ACC if the defense mechanism ($|\ddot{x}_{i\_cacc} - \ddot{x}_{i\_acc}| > \Delta$) is triggered.

In the Proactive CACC Algorithm, *_cc*, *_acc* and *_cacc* are the methods computing the desired acceleration based on CC, ACC and CACC controller strategy respectively. *gap2pred* is the distance to the preceding vehicle. Δ is the threshold that we use to select the proper controller strategy between ACC and CACC.

For distance, the fail-safe scheme is to switch to ACC when the gap between vehicles is smaller than the desired value, otherwise platoon still follows CACC to maintain fixed gap and string stability.

Algorithm 2 Proactive CACC Algorithm

```
1: Input: parameters (vehicle information)
2: Output: desiredAcceleration
3:
4: ccAcceleration = _cc(parameters)
5: accAcceleration = _acc(parameters)
6: caccAcceleration = _cacc(parameters)
7:
8: if |caccAcceleration - accAcceleration| <= Δ then
9:     desiredAcceleration = caccAcceleration
10: else
11:     desiredAcceleration = accAcceleration
12: end if
13: if gap2pred >= 20 then
14:     desiredAcceleration = min(desiredAcceleration,ccAcceleration)
15: end if
```

7.3 Safe Distance

Safe distance is the prerequisite in general approach for designing a safe platooning. Here we present the safe distances under different fail-safe schemes and attack detection mechanisms.

7.3.1 Acceleration

To demonstrate whether the proposed Proactive CACC Algorithm works and to find the safe distance, we conduct a simulation with the example platoon under leader crash attack. When we set the range value to 0.2 m/s^2, the platoon is safe with a safe distance of 9 meters (0.32s).

We modify the PLEXE to make sure that platoon can switch between CACC and ACC whenever it needs. MSCFModel_CC is a vehicle driving model which implements the CACC, ACC and other control strategies, like Cruise Control (CC) and human driving mode. Within the _v() method in MSCFModel_CC, it computes the desired acceleration of each type of controller strategy and then choose the requested one. When it comes to CACC controller strategy, we use CACC proactive algorithm to calculate the desired acceleration. If the difference between CACC and ACC acceleration is within the range Δ, we return CACC acceleration, otherwise we return ACC acceleration. In the experiment, we find out that when we set the range to 0.2 m/s^2, we can achieve string stability and safety both. At the same time, we also achieve a much shorter safe distance which is 9 meters (0.32s).

From Figure 4, we can see that all the vehicles maintain the same velocity. Meanwhile, the acceleration of platoon is a constant value. Therefore, $\ddot{x}_{i\_cacc} = 0$. The highest speed $\dot{x}_i$ is 27.78 m/s and the gap in this experiment is 9 meters (0.32s). Therefore, we obtain $\Delta = 0.22$ m/s^2 which is close to our simulation result. So our algorithm achieves safety and efficiency. In the next section, we prove its security under the two insider attacks.

7.3.2 Distance

For distance, we also conduct an experiment to show how this method defend against leader crash attack. The experiment environment is the same as above setting. We can see from Figure 5 that result is the same too. The safe distance is 9 meters (0.32s).

Attack Defense	Response Time	Leader Crash	Collision Induction	Message Falsification
Acceleration	Fast	Yes	Yes	Yes
Distance	Slow	Yes	Yes	No

Table 3: Comparison between acceleration and distance defense mechanism

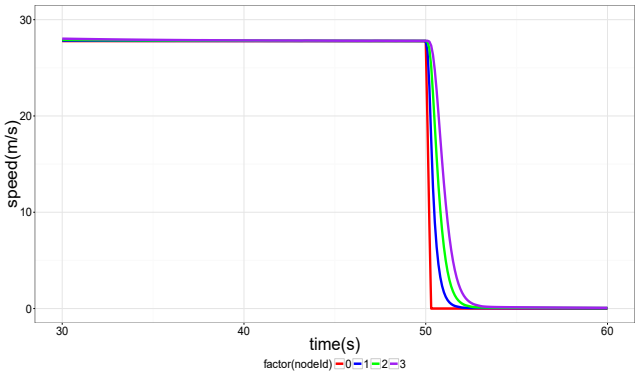

Figure 4: Speed Changes of Platoon : Acceleration

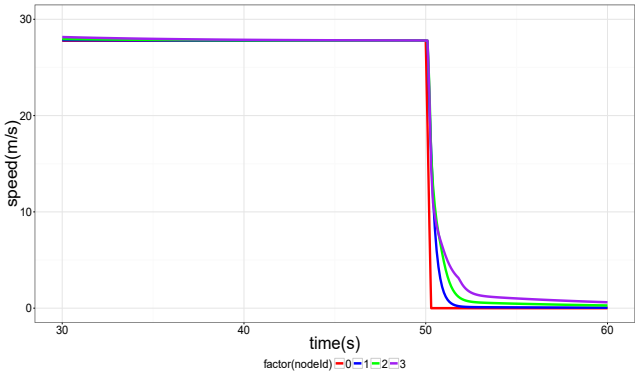

Figure 5: Speed Changes of Platoon : Distance

7.3.3 *Comparison*

In this paper, we recommend using acceleration defense mechanism to defend against attacks rather than distance defense mechanism. As shown in Table 3, when cyber attack happens, acceleration defense mechanism responds immediately, namely, the difference between CACC and ACC acceleration will be larger than the specific range. For distance defense mechanism, it will only be triggered when the vehicle gap is decreased. In the leader crash attack which starts at 50.00s, the ego vehicle switches to ACC at 50.02s by using acceleration defense mechanism and 50.07s by using distance defense mechanism. Furthermore, the kinds of cyber attacks can be defended by distance defense mechanism is limited. For example, in message falsification attack, the malicious vehicle broadcasts false message to tell current car to decelerate. Using distance defense mechanism cannot deal with such situation, but using acceleration defense mechanism can defend against it. Therefore, for the safe platooning design, we recommend using acceleration defense mechanism.

8. LIMITATIONS AND FUTURE WORK

Our analysis, simulation, and evaluation are performed over PLEXE. The controllers (CACC, ACC, and CC) used in PLEXE are classical and representative. Although we believe our approach is general enough to extend to other controllers, still we think it is necessary to evaluate the proposed solution over other realizations of platoon systems using different controllers. We are currently communicating with the Crash Avoidance Metrics Partnership (CAMP) for potential collaboration on its platoon implementation.

In our study, we assume a homogeneous platoon system. In reality, apparently, a platoon consists of heterogeneous vehicle systems. Experiences, lessons and recommendations gained from this study may not apply to a heterogeneous platoon system. Heterogeneous platooning has been studied by the transportation research community. We are going to extend our work by considering heterogeneous vehicle platoon systems.

Our study is based on theoretical analysis and simulation. In reality, the situation can be more complicated. We believe our work provides some insights on the safety and security of platooning and hope it can open a new area of research towards safer and more secure platoon mechanisms.

9. CONCLUSIONS

In this paper, we present our work towards a safe and secure platoon co-design. We have shown that cyber attack on a platoon system can have the most severe and widespread safety impact as defined by the EVITA vehicle security risk model. We argue the importance of safety-security co-design for safety critical cyber physical systems and make the first effort toward a safety-security co-design engineering process which allows functional security requirements to be derived for a safe automated vehicle platoon system. Based on the co-design analysis, we present a general approach for designing a safe and secure platooning. Following the general approach, we propose a new platoon control algorithm that takes into account both safety and security.

10. REFERENCES

[1] Researcher Hacks Self-driving Car Sensors, http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors

[2] Kavathekar, Pooja. Cognitive Vehicle Platooning in the Era of Automated Electric Transportation. Diss. UTAH STATE UNIVERSITY, 2012.

[3] Hamida, Elyes Ben, Hassan Noura, and Wassim Znaidi. "Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures." Electronics 4.3 (2015): 380-423.

[4] Avizienis, Algirdas, et al. "Basic concepts and taxonomy of dependable and secure computing." IEEE transactions on dependable and secure computing 1.1 (2004): 11-33.

[5] Czerny, Barbara J. "System Security and System Safety Engineering: Differences and Similarities and a System Security Engineering Process Based on the ISO 26262 Process Framework." SAE International Journal of Passenger Cars-Electronic and Electrical Systems 6.2013-01-1419 (2013): 349-359.

[6] Burton, Simon, et al. "Automotive functional safety= safety+ security." Proceedings of the First International Conference on Security of Internet of Things. ACM, 2012.

[7] 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.

[8] 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.

[9] Gehrig, Stefan K., and Fridtjof J. Stein. "Collision avoidance for vehicle-following systems." IEEE transactions on intelligent transportation systems 8.2 (2007): 233-244.

[10] Araki, Hideo, et al. "Development of rear-end collision avoidance system." JSAE review 18.3 (1997): 314-316.

[11] Ferrara, Antonella, and Claudio Vecchio. "Second order sliding mode control of vehicles with distributed collision avoidance capabilities." Mechatronics 19.4 (2009): 471-477.

[12] Glas, Benjamin, Jens Gramm, and Priyamvadha Vembar. "Towards an Information Security Framework for the Automotive Domain." AutomotiveâĂŞSafety & Security 2014 (2015) (2014).

[13] Eckhoff, David, and Christoph Sommer. "Driving for big data? Privacy concerns in vehicular networking." IEEE Security & Privacy 12.1 (2014): 77-79.

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

[15] Rajamani, Rajesh. Vehicle dynamics and control. Springer Science & Business Media, 2011.

[16] EVITA: E-safety vehicle intrusion protected applications, http://www.evita-project.org/

[17] Segata, Michele, et al. "Plexe: A platooning extension for Veins." Vehicular Networking Conference (VNC), 2014 IEEE. IEEE, 2014.

[18] Segata, Michele, et al. "A simulation tool for automated platooning in mixed highway scenarios." Proceedings of the 18th annual international conference on Mobile computing and networking. ACM, 2012.

[19] Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, http://standards.sae.org/wip/j3061/

[20] Koscher, Karl, et al. "Experimental security analysis of a modern automobile." Security and Privacy (SP), 2010 IEEE Symposium on. IEEE, 2010.

[21] Checkoway, Stephen, et al. "Comprehensive Experimental Analyses of Automotive Attack Surfaces." USENIX Security Symposium. 2011.

[22] Ishtiaq Roufa, Rob Millerb, et al. "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study." 19th USENIX Security Symposium, Washington DC. 2010.

[23] Miller, Charlie, and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle." Black Hat USA 2015 (2015).

[24] Zhang, Chenxi, et al. "An efficient identity-based batch verification scheme for vehicular sensor networks." INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. IEEE, 2008.

[25] Lin, Xiaodong, et al. "STAP: A social-tier-assisted packet forwarding protocol for achieving receiver-location privacy preservation in VANETs." INFOCOM, 2011 Proceedings IEEE. IEEE, 2011.

[26] Zhao, Xin, et al. "Development of optimal control system for safe distance of platooning using model predictive control." Asia-Pacific Conference on Simulated Evolution and Learning. Springer Berlin Heidelberg, 2010.

[27] 10 Fail-safe Examples, http://simplicable.com/new/fail-safe

[28] Li, Huaxin, et al. "Privacy leakage of location sharing in mobile social networks: Attacks and defense." IEEE Transactions on Dependable and Secure Computing (2016).

[29] Li, Huaxin, et al. "Demographics inference through Wi-Fi network traffic analysis." Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on. IEEE, 2016.