Accident Analysis and Prevention 121 (2018) 148–156

Contents lists available at ScienceDirect

Accident Analysis and Prevention

journal homepage: www.elsevier.com/locate/aap

Influence of cyber-attacks on longitudinal safety of connected and automated vehicles

Ye Li*, Yu Tu, Qi Fan, Changyin Dong, Wei Wang

School of Transportation, Southeast University, 2 Si pai lou, Nanjing, 210096, PR China

ARTICLE INFO

Keywords:
Cyber-attack
Transportation
Safety
Security
Simulation
Trajectory

ABSTRACT

Connected and automated vehicle (CAV) has been a remarkable focal point in recent years, since it is recognized as a potential method to reduce traffic congestion, emission and accident. However, the connectivity function makes CAVs vulnerable to cyber-attacks. An intuitive method to defend cyber-attacks on CAVs is that if the error between expected and measured behaviors exceeds a predetermined threshold, a security scheme should be activated. This study investigates another type of cyber-attack, denoted as slight attacks, in which the communicated data of CAVs are randomly deviated from the actual ones and deviations do not exceed the threshold. The primary objective is to evaluate the influence of slight cyber-attacks on longitudinal safety of CAVs. An empirical CAV model is first utilized to describe vehicle dynamics and generate trajectory data. A rear-end collision risk index (RCRI) derived from safe stopping distance is used to establish relation between longitudinal safety and trajectory data. Two attacked factors, communicated positions and speeds from preceding vehicles are tested. Extensive simulations are conducted and parameters are also tested via sensitivity analysis. Results indicate that (1) when one CAV is under slight cyber-attacks, it is more dangerous if communicated positions are attacked than speeds; (2) when multi CAVs are under attacked, it is possible that a situation with more vehicles under attack at a low severity may be more dangerous than that with fewer vehicles but under attack at a high severity; (3) the impact of slight cyber-attacks on deceleration period is more serious compared to acceleration period. The findings of this study provide useful suggestion for defending cyber-attacks on CAVs and improving longitudinal safety in the future.

1. Introduction

Connected and automated vehicle (CAV) has been a remarkable focal point in recent years, since it is recognized as a potential method to reduce traffic congestion, emission and accident. The CAVs integrate two distinct technologies, the connected vehicle (CV) (Li et al., 2017a, b; Wu et al., 2018a; Yue et al., 2018) and automated vehicle (AV) systems (Li et al., 2016, 2017c; Dong et al., 2018). The former one has been developed in recent fifteen years, which utilizes wireless communication to improve traffic operation. The latter has a longer history, which focuses on vehicle automation. More details about CAVs' development history can be referred in Shladover (2018).

Although CAVs bring enormous benefits to transportation system, there exists many latent problems. For example, the connectivity function makes CAVs vulnerable to cyber-attacks. The CAV utilizes vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication to enhance its performance. With lots of CAVs on roads, a huge and intensive communication network will occur. The high complexity and interdependency of the communication will provide more chances for malicious activities. The attacker can directly alter messages from infrastructures or indirectly spoof sensors on data reading (Canepa and Claudel, 2013). Any type of cyber-attacks may cause severe security issues.

Researchers have been focusing on cyber-attacks problems of CAVs in recent five years. Some studies propose various schemes to detect different attacks. For instance, Baiad et al. (2016) proposed cross-layer cooperative schemes to detect blackhole attack in vehicular ad-hoc networks (VANETs). Biron et al. (2018) proposed a real-time scheme to detect the occurrence of a particular cyber attack and estimate the effect of that on the connected vehicle system. Some researches estimate potential influence of cyber-attacks based on simulations. Reilly et al. (2016) presented a controllability analysis of freeway with coordinated metering to evaluate the influence of cyber-physical attacks based on simulation. Dadras et al. (2015) modified a vehicle control system

* Corresponding author.
E-mail addresses: yeli@seu.edu.cn (Y. Li), yutu@seu.edu.cn (Y. Tu), fanqi0617@163.com (Q. Fan), dongcy@seu.edu.cn (C. Dong), wangwei@seu.edu.cn (W. Wang).

https://doi.org/10.1016/j.aap.2018.09.016
Received 16 July 2018; Received in revised form 25 August 2018; Accepted 14 September 2018

operated by a maliciously actor and demonstrated that one attacked vehicle could destabilize a vehicle platoon. Amoozadeh et al. (2015) presented that cyber-attacks could cause significant instability of cooperative adaptive cruise control (CACC) vehicle stream based on simulation and proposed several countermeasures. The CACC is one type of CAV with only longitudinally automation control system. Feng et al. (2018) investigated cyber-attacks on actuated and adaptive signal control systems by sending falsified data. There are also some paper proposing security schemes to address the potential attacks. Yan et al. (2013) investigated the potential security challenges in vehicular clouds and proposed a security scheme to address these challenges. Liu et al. (2017) proposed a method to detect cyber-attacks based on parameter threshold and designed a safe-secure vehicle platoon. More details about cyber-attacks can be referred in AlDairi (2017) and Parkinson et al. (2017).

Generally, an intuitive method to defend cyber-attacks on CAVs is that if the error between expected and measured behaviors exceeds a predetermined threshold, a security scheme should be activated. We denote this type of cyber-attack as *serious cyber-attacks* in this paper. Most of aforementioned studies utilize this approach to defend serious attacks. However, there may exist another type of cyber-attack, in which the communicated data of CAVs are randomly deviated from the actual ones and deviations do not exceed the threshold. We denote this type as *slight cyber-attacks*. In this case, the preset security scheme may be useless. Furthermore, consider a CAV fleet with multi vehicles under attacked. Even a slight attack may cause hazardous conditions for all vehicles and result in serious safety problems.

Thus, this study focuses on the influence of slight cyber-attacks on longitudinal safety of CAVs. More specifically, we consider the communicated position and speed data from preceding CAVs under attacks. An empirical model is first utilized to describe dynamics of CAVs. Then, a rear-end collision risk index (RCRI) is introduced to establish relation between longitudinal safety and vehicles' dynamic data. Extensive simulation experiments are conducted to test impacts of slight cyber-attacks on CAVs. Parameters are also investigated via sensitivity analysis. The major objective of this study is to answer the following questions:

(1) Whether is it risky when one CAV in a vehicle fleet is under slight cyber-attacks?
(2) Whether is it risky when multi CAVs in a vehicle fleet are under slight cyber-attacks?
(3) Which operation period is more dangerous when under slight cyber-attacks?

For the remainder, Section 2 proposes the methodologies, including an empirical CAV model and rear-end collision risk index, as well as simulation experiment designs. Simulation results are presented in Section 3, and concluding remarks and discussions are provided in Section 4.

2. Methodology

2.1. The research framework

An overview of the research framework is expressed in Fig. 1. An empirical CAV model, proposed by the California Partners for Advanced Transit and Highways (PATH) (Milanés et al., 2014; Milanés and Shladover, 2014) and denoted as PATH CAV model in this study, is utilized to describe vehicle dynamics and generate trajectory data. A rear-end collision risk index (RCRI) based on safe stopping distance is used to establish the relation between longitudinal safety and CAVs' trajectory data. This study focuses on cyber-attacks on communicated data (see Fig. 2). In the PATH CAV model, preceding vehicles' position and speed data are sent via wireless communication. Thus, we investigate the impact of these two factors under slight cyber-attacks. The slight cyber-attacks will randomly fluctuate communicated position/speed within a certain magnitude, denoted as severity. For example, if the speed sent by preceding vehicle is attacked under a 1% severity, it refers to the following vehicle will receive the speed data plus 1% random errors (imprecise data). We want to see whether a slight cyber-attack, such as only a 1% fluctuation of communicated data, will result in serious longitudinal safety problems. All above model and index are integrated into a simulation platform, which is coded in MATLAB 2015b software. A variety of simulation experiments are designed for answering aforementioned three questions, including cyber-attacks on one vehicle, multi vehicles as well as different periods.

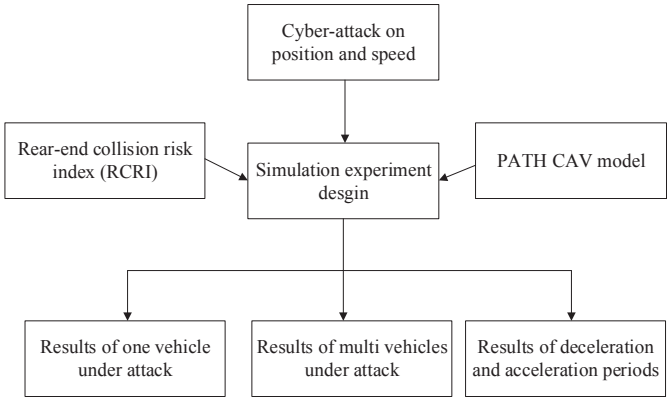

Fig. 1. Illustration of research framework.

2.2. PATH CAV models

The PATH CAV model is proposed by Milanés and Shladover (2014), which is derived from empirical data. The empirical data is from field test of PATH (Milanés et al., 2014). Four Nissan vehicles equipped with CACC controllers are investigated in the vehicle experiments. The PATH CAV model is similar to traditional car-following model (Wang et al., 2017, 2018), which focuses on errors between actual and designed net gap of two successive vehicles. The PATH CAV model can be expressed as follows:

$$e_k = x_{k-1} - x_k - L_{k-1} - t_{hw} v_k \tag{1}$$

$$v_k = v_{k_{prev}} + k_p e_k + k_d \dot{e_k} \tag{2}$$

where e_k represents the gap error of the subject vehicle k, which is the difference between actual net gap and designed net gap; x_{k-1} and x_k represent the position of the preceding vehicle k-1 and the subject vehicle, respectively; L_{k-1} represents the length of the preceding vehicle; v_k represents the speed of the subject vehicle; t_{hw} denotes the current time-gap setting; v_{kprev} denotes the speed of the subject vehicle in the previous iteration; k_p and k_d are the model coefficients; and $\dot{e_k}$ denotes the derivative of gap error.

Note that, the following CAV only receives position and speed of preceding vehicles in the PATH CAV model. Thus, we consider these two factors under cyber-attacks in the research. When the speed of a CAV is determined, the position of it x_k can be calculated by:

$$x_k = x_{k_{prev}} + v_k \Delta t \tag{3}$$

where $x_{k_{prev}}$ is the position of the subject vehicle in the previous iteration, and Δt is the time step.

As shown in Eq. (1)–(3), four parameters, i.e. t_{hw}, k_p, k_d and Δt, are included in the PATH CAV model. In this study, the time gap t_{hw}, k_p and k_d are set to be 0.6 s, 0.45 and 0.25 respectively, based on the experimental tests (Milanés et al., 2014). The simulation time step Δt is set to be 0.1 s and vehicle length L_{k-1} is set as 5 m. Note that, we consider the attacks on communication data (connected side), which is the input for automated side. Thus, the CAV is our concern instead of only CV or AV. For the CAV, the perception-reaction time refers to the total time delay