This article has been accepted for publication in IEEE Transactions on Consumer Electronics. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TCE.2023.3297965

Cyber Attacks via Consumer Electronics: Studying the Threat of Covert Malware in Smart and Autonomous Vehicles

Mohammad Sayad Haghighi, *Senior Member, IEEE*, Faezeh Farivar, *Senior Member, IEEE*,
Alireza Jolfaei, *Senior Member, IEEE*, Azin Bayrami Asl, *Member, IEEE*, Wei Zhou, *Member, IEEE*

***Abstract*—In Industry 5.0, man and machine work alongside each other in production, but smart and autonomous vehicles are examples that show this notion is now being extended to the end consumers. In 2015, a Jeep was remotely hacked through its head unit. This incident drew the public attention to vehicles security and showed how entertainment/infotainment consumer electronics can be used to intrude vehicles. In this paper, we study a novel covert attack that can be launched by malwares spreading through Intelligent Transportation Systems, e.g. via consumer electronics. This malware infects a vehicle module, like the Adaptive Cruise Controller (ACC), and manipulates its setting in a way that is not noticeable to human observers, but gives rise to accidents statistics. We show how this is done and analyze the effect mathematically. We also propose a new Intrusion Detection System (IDS) whose architecture is non-disruptive and can be readily adopted by car manufacturers. We evaluate our proposal with real-world datasets. We demonstrate how a malware/attacker can engineer the crash statistics by manipulating the safe distance value in cruise control scenarios. Then, we put an anomaly-based IDS for ACC modules into test and show how it can effectively detect such covert attacks.**

***Index Terms*—Consumer Electronics, Industry 5.0, Intelligent Transportation Systems, Adaptive Cruise Control, Security, Worm, Intrusion Detection System**

I. Introduction

INDUSTRY 5.0 is a new paradigm in which man and machine find ways to work alongside each other to enhance the efficiency of production [1]. It is interesting that the same concept is being practiced at the end user side, i.e. the consumers. When interconnected machines are employed, humans delegate some of their own tasks to them. Intelligent transportation systems (ITS) are an instance. They provide a range of transportation and traffic management models to help users in being informed, safe, coordinated, and smart to use transportation networks. In the ITS world, sensors are widely employed to measure and collect data from real world conditions [2]. These data are sent either to other vehicle units via intra-vehicle communication channels or to the outside through a ubiquitous dynamic ad-hoc medium called the vehicular ad-hoc network (VANET) [3].

Infrastructure components such as road side units (RSU) installed along roads help smart and autonomous vehicles transfer information to a broader area in VANETs and even exchange data with the Internet. Each vehicle controls its dynamics by employing a control system that uses both the data coming from the VANET and the local sensors. This network communication opens a window to adversaries and exposes vehicles vulnerabilities. Smart vehicles can connect to consumer electronics, and some even embed such units for information delivery or entertainment purposes. A malicious code/worm can propagate via the network or consumer electronics and infect smart or autonomous vehicle modules [4]. The worse scenario is that it is embedded in a module or gadget as a trojan, either through firmware upgrades or by design during the production [5]. Hackers have already shown that targeting smart vehicles is possible. In 2010, Koscher et al. [6], over a set of experiments, demonstrated how an adversary can control many of automotive functions and ignore driver inputs. This included disabling the brakes, selectively braking individual wheels, stopping the engine, etc. In 2015, after two security experts demonstrated how almost every single module of a Jeep Cherokee can be hacked and controlled remotely, Fiat Chrysler recalled 1.4 million vehicles [7]. The hack was initiated by gaining access to the multimedia system (UConnect) of the vehicle's head unit, and then followed by rewriting the firmware of V850 controller to access the vehicle's Controller Area Network (CAN) bus.

Modern vehicles use some sort of local network or bus to interconnect their components. CAN bus is widely employed in these vehicles to allow devices to transmit messages to each other. In this standard, vehicle modules connect to a single bus in order to exchange messages with other modules. Regardless of the vehicle network type, the fact that in smart and autonomous vehicles a route exists from the outside world to the vehicle controlling units should be considered alarming per se. This is apart from the channels like Over The Air (OTA) software updates that can also be exploited by cyber

M. Sayad Haghighi is with the School of Electrical and Computer Engineering, University of Tehran, Iran, and also, the School of Computer Science, Institute for Research in Fundamental Sciences (IPM), P.o.Box 19395-5746, Tehran, Iran, e-mail: sayad@ieee.org, sayad@ut.ac.ir.

F. Farivar is with the Department of Mechatronics and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran, Email: f.farivar@srbiau.ac.ir, farivar@ieee.org (corresponding author).

A. Jolfaei is with the College of Science and Engineering, Flinders University, SA 5042, Australia, Email: alireza.jolfaei@flinders.edu.au.

A. Bayrami is with the Department of Mechatronics and Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran, Email: azin.bayrami@srbiau.ac.ir.

W. Zhou is with the School of Computer Science and Information Security, Guilin University of Electronic Technology, Guangxi, China. Email: weizhou09@gmail.com.

attackers upon detection of a vulnerability in a device [8].

Many of current worms spread by scanning reachable targets via the victims' communication interfaces and using appropriate exploits upon detection of vulnerabilities. Due to the high number of future smart and autonomous vehicles and their inter-connectivity, it is quite predictable that similar malwares are developed for ITS, and more specifically, for vehicles software-dependent modules.

In this paper, we present a new covert cyber attack that can be launched by spreading worms or malwares throughout the transportation system, either through vehicular network or via infecting consumer electronics which are connected or have access to the vehicle internals. This attack is meant to covertly manipulate the Adaptive Cruise Control (ACC) module by changing its settings or rewriting its firmware so that the accident rate is statistically increased in cruise control scenarios in a large infected population. We stochastically model the attack effect and show how the probability of car crashes increase with the change of safe distance. We use real-world datasets to evaluate the outcome of such a mass scale attack. To thwart cyber attacks, we propose a novel Intrusion Detection System (IDS) architecture for smart and autonomous vehicles. We develop a sample IDS for ACC modules based on this architecture and put it to test in a simulated scenario. The contributions of this paper are as follows:

- Proposing a new covert attack for the ACC module in ITS which is launched by worms and malwares that are spread via vehicular networks or consumer devices.
- Stochastic analysis of the covert attack effect on accident rates based on real-world data in Australia.
- Development of an IDS based on a novel non-disruptive architecture to thwart vehicular cyber attacks.

The rest of this paper is organized as follows: In Section II, related studies are reviewed. Preliminaries, including the ACC model and the concept of stopping distance are given in Section III. In Section IV, a new covert attack on the ACC system is designed based on the vehicle brake information and mathematically analyzed. Moreover, an IDS architecture is proposed in this section to counter such attacks. Section V evaluates the proposed attack effect and instantiates the ACC IDS in a simulation setup. Section VI will wrap up the paper.

II. Related Work

Connected smart vehicles are prone to cyber attacks. Regarding this issue, a brief review of related work is presented in this section. Cyber attacks in connected vehicles can be categorized into three groups [9]. (1) DoS: The adversary applies fake requests to keep the network or system busy. Thus, the legitimate requests cannot be accepted because the network/system is unavailable [10]. (2) False Data Injection: The adversary injects false data and disturbs the integrity of transmitted packets [11]. Equivalently, it can compromise system integrity and issue false commands. (3) Replay Attack: The adversary intercepts and retransmits data to disturb the system operation [12].

References [13, 14] introduced several other types of attacks which may maliciously affect the VANET operation. According to this study, attacks may be launched by internal malicious vehicles or external entities. The attacks are said to be message spoofing, message replay, integrity/impersonation, Denial of Service (DoS), and de-anonymization [15].

There exist several studies which address the threats and security issues in smart vehicles. For example, reference [16] presented four types of attacks which affect vehicle operations, namely, the warning light, airbag control system, the window lift, and the central gateway of the Controller Area Network. The authors of [17] introduced another set of attacks that endanger vehicles and their drivers. In reference [18], a survey on remote automotive attack surfaces is presented. A remote attack surface can help one estimate how difficult the remote compromise might be. The architecture of the internal network of each vehicle has been evaluated in this study. Moreover, the features each vehicle possesses that may help in taking the physical control of it were identified. In reference [19], an attacker model and evaluation framework were proposed to evaluate the attack effect on the control system and to investigate the controller robustness against DoS and message injection attacks. In reference [20], spoofing attacks on anti-lock braking systems (ABS) were studied. Electromagnetic actuators are used in anti-lock braking systems. In this study, measured signals were compromised by magnetic fields and malicious signals were injected. Reference [21] proposed a robust monitoring algorithm based on a waveform relaxation method for attack detection and identification.

In reference [22], it was demonstrated how attackers intruded vehicles and took control of the system in the platoon. Reference [23] studied the effects of DoS attack on connected vehicles. A resilient control scheme was then proposed for a platoon of connected vehicles equipped with Cooperative-ACC in order to mitigate the DoS attack effect. In references [24, 25], stability of connected vehicles was studied when the network experiences normal delays. Reference [26] designed two types of covert attacks on ACC modules by manipulating the ego car acceleration and the reference signal. The covert attacks presented were claimed to increase in the risk of accident. In [27], a covert adversarial learning attack was designed to disturb the operation of smart/autonomous vehicles in lane keeping scenarios. In this attack, an adversary manipulates sensory data such that high lateral deviations are experienced with low yet non-zero probabilities. The attacker tunes its power by gradually learning the vehicle response based on the actor-critic learning method. In addition, in this research, detection and compensation algorithms were developed in order to mitigate the attack effect on connected vehicles.

Quick detection of intrusions is a vital requirement to maintain the safety and performance in real-time systems. In this regard, many detection mechanisms have been proposed for connected vehicles. For example, reference [28] proposed a quick way of verifying received VANET messages without relying on pre-trusted agents. The researchers also presented a central algorithm for detection of intruders in the network. Reference [29] proposed an algorithm to detect replay attacks based on the noisy control signal strategy. References [30] and [31] used the kinematic model and data fusion methods to develop an anomaly detection algorithm. Reference [32] designed an sliding mode observer for attack estimation. In [26], the intrusion detection algorithm was designed using neural networks. The algorithm resembles what was proposed for a DC motor as a linear Cyber Physical System (CPS) in [33]. Reference [27] proposed an IDS which uses the GPS data and offline maps for path reconstruction in lane keeping scenarios. As said before, this work proposed a covert attack to disturb safe lateral deviations in smart/autonomous vehicles.

Moreover, many defense and compensation algorithms have been proposed to reduce the effect of cyber attacks in CPS and ITS [26, 34, 35]. For example, reference [36] designed a robust control system to increase the system resiliency to attacks. Reference [37] proposed a compensation strategy to reduce the effects of packet loss in connected vehicles. The algorithm was designed based on observation methods. References [34, 35, 38] proposed compensation mechanisms using intelligent classic control methods in order to create more robustness against faults and even possible attacks in the forward link. The proposed compensation method was specifically applied in a car cruise system which was prone to attack.

III. Preliminaries

A. Adaptive Cruise Control

In this part, we explain the operation of ACC system and its control objectives. A simple ACC model is shown in Fig. 1a and Fig. 1b. We assume the vehicle that is behind (or the so called ego) is equipped with an ACC module. The ego vehicle measures its distance to the front vehicle by using a radar/sensor. The front vehicle is normally referred to as the lead. We may assume that the lead is moving in the same lane as the ego. The goal of the ACC module is to make the ego vehicle go at a speed set by the driver as long as a safe distance is maintained with the lead. This target speed is denoted by v_{cruise} (or in short, v_c) hereafter.

According to situation, the ACC module controls the ego vehicle in two different modes. First, once v_c is set by the driver (or the computer in charge of driving in an autonomous vehicle), the control objective is to make the vehicle go at that speed as long as a safe distance is maintained with the front/lead vehicle. In the second mode, which is activated when the two vehicles get close, the distance to the lead vehicle is controlled (through acceleration or deceleration of the ego vehicle) so as to the ego vehicle remains at a safe distance from the lead. Based on real time distance measurements, either of these two modes can be activated. The following rules simplify the ACC module decisions:

1) $D_{rel} \geqslant D_{safe} \rightarrow$ Speed control mode (Track v_c)
2) $D_{rel} < D_{safe} \rightarrow$ Space control mode (Maintain D_{Safe})

In the above, D_{rel} stands for the relative distance of the ego and the lead and D_{safe} is the safe distance. The safe distance (between the lead and the ego) is composed of a fixed part and a speed-dependent part [27, 39]:

$$D_{safe} = D_{default} + T_{gap} v_e \tag{1}$$

Here, $D_{default}$ is the standstill spacing and T_{gap} is a constant representing the required time gap between the two vehicles.

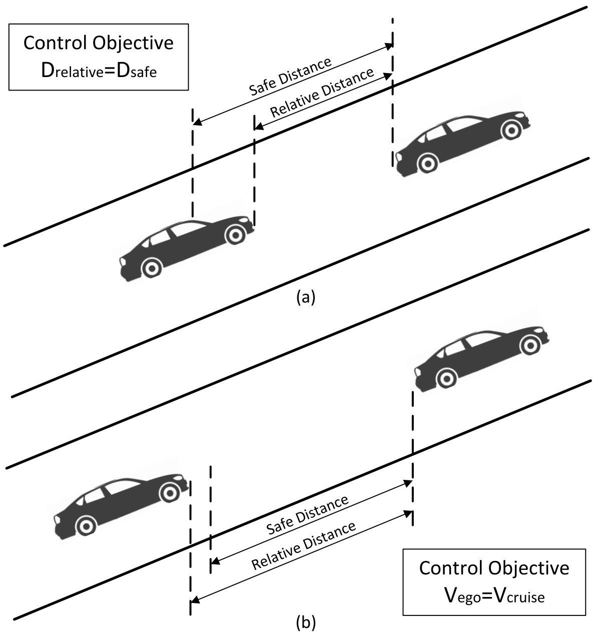


Fig. 1. Adaptive cruise control scenarios: (a) when the relative distance is larger than the safe distance, and (b) when the relative distance is less than the safe distance. In the former case, the ego vehicle uses its cruise speed as the control reference, and in the latter, it uses the safe distance as the reference.

B. Stopping Distance Breakdown

The distance a vehicle travels before it comes to a stop is determined by two major factors; the reaction time of the driver and the deceleration force. Fig. 2 shows the phases the vehicle goes through before coming to an stop. It is obvious that the maximum deceleration value that can be applied depends on the road surface condition, the tires and more importantly, the vehicle brake power and its mechanism.
In a cruise control scenario, due to constant measurement of the relative distance, the reaction time is almost zero, unless hard braking is disabled by a malware in the ACC module. In that case, the (potential) driver may take the control back after the reaction time and brake.

IV. Covert Intrusion Scenario

In this section, we mathematically model the stopping distances upon a sudden brake in a cruise control scenario. We follow the attacker's thinking in designing a possible covert attack which disrupts the control operation and statistically increases the rate of accidents. The intelligent attack manipulates the ego car cruise control module so that when the lead vehicle brakes, the chance of collision is increased.

A. Stopping Distance Analysis

We align the x axis of the coordinates system with the road direction, and assume the position of the lead vehicle back and the ego vehicle front at the time of sudden brake are $x_l(0)$ and $x_e(0)$ along this axis, respectively. Apparently, we consider the time origin/reference to be the braking time.

We further assume both vehicles are cruising at a speed of v_c and they are away from each other by a distance of $D_r(t) =$

$D_s(v_e(t))$, where $D_r(.)$ stands for the relative distance of the two vehicles and $D_s(.)$ represents the safe distance that is obtained from Eq. (1). At the time of brake, $v_l(t=0) = v_e(t=0) = v_c$ and $D_r(t=0) = D_s(v_c)$. The formulas for the position and velocity of the ego vehicle are as below:

$$v_e(t) = \begin{cases} v_c, & t \leq T_r \\ v_c + a_e t & t > T_r \end{cases} \tag{2}$$

$$x_e(t) = \begin{cases} x_e(0) + v_c t, & t \leq T_r \\ x_e(0) + v_c T_r + \frac{1}{2} a_e t^2 + v_c t & t > T_r \end{cases} \tag{3}$$

where T_r is the reaction time. Assuming that the origin is set to be the front of the ego vehicle at the braking time of the lead vehicle, $x_e(0) = 0$. The mathematical model defining the position and velocity of the lead car is as follows.

$$x_l(t) = x_l(0) + \frac{1}{2} a_l t^2 + v_c t \tag{4}$$

$$v_l(t) = v_c + a_l t \tag{5}$$

where a_l and a_e are the deceleration values which are negative and presumably vehicle-dependent. Here, $x_l(0) = D_s(v_c)$. It is worth mentioning that the air resistance impact on a_e and a_l have been ignored by approximation. It is also assumed that the (hard) braking decelerations remain constant till the vehicles stop. The position at which the lead vehicle comes to a complete stop can be calculated by the following equations.

$$t_{stop}^{(l)} = -\frac{v_c}{a_l} \tag{6}$$

$$x_l(t_{stop}^{(l)}) = -\frac{v_c^2}{2a_l} + D_s(v_c) \tag{7}$$

The ego vehicle has different dynamics and travels at a constant speed before braking. Therefore, the position at which it stops (regardless of any potential crashes with the lead vehicle) is calculated as follows.

$$t_{stop}^{(e)} = T_r - \frac{v_c}{a_e} \tag{8}$$

$$x_e(t_{stop}^{(e)}) = v_c T_r - \frac{v_c^2}{2a_e} \tag{9}$$

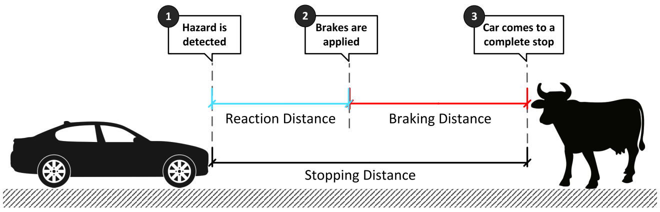


Fig. 2. Vehicle stopping process is composed of two phases; a perception plus reaction phase, and a braking phase. The durations of these two along with the vehicle speed, weight, braking force, and the road condition determine the braking distance.

B. The Covert Attack Scenario

In this section, we present a stealth attack and analyze its effect on the road safety in ITS. As mentioned in the initial sections, smart and autonomous vehicles use itra-vehicle communications, usually via CAN bus, to do their jobs. Some of the units sitting on the bus/local network are connected to the outside world, via e.g. vehicular networks or cellular ones.

A worm or virus can infect a vehicle unit (in this case the ACC unit) by propagating through network link, both from one vehicle to another and from the internet to cellular-connected vehicles. The designer of the covert worm does not make any substantial changes to the ACC unit functions and merely rewrites the formula by which it calculates the safe distance, i.e. Eq. (1). If the attacker manages to reduce this value trivially, it remains covert but certainly increases the statistics of the accidents in cruise control scenarios when many vehicles are infected. Theoretically speaking, in a sudden brake scenario (apparently initiated by the lead car upon detection of hazard), we can argue that a crash happens if the stopping position of the ego vehicle is greater than that of the lead one. This argument, however, might not always be accurate. In very rare scenarios, this simplified model might not hold. But with the real-world deceleration values of the 600-vehicle dataset, assuming that reaction delays are under $2.9s$, we did not come across such cases. This implies that the above collision model is accurate enough in practice. A detailed study on this is done by [40]. To summarize, the collision model translates into the following:

$$\begin{gathered} x_e(t_{stop}^{(e)}) > x_l(t_{stop}^{(l)}) \\ v_c T_r - \frac{v_c^2}{2a_e} > D_s(v_c) - \frac{v_c^2}{2a_l} \end{gathered} \tag{10}$$

which after some simplification becomes,

$$-\frac{1}{a_e} > -\frac{1}{a_l} + \frac{2(D_s(v_c) - v_c T_r)}{v_c^2} \tag{11}$$

a_l and a_e are vehicle-dependent. From a top view, the types of lead and ego vehicles are not known beforehand, thus both of these can be considered i.i.d random variables. This implies that their inverses are also random variables. If we define $X \triangleq -1/a_e$, $Y \triangleq -1/a_l$, and $C \triangleq 2(D_s(v_c) - v_c T_r)/v_c^2$, the above inequality is simplified as,

$$X > Y + C \tag{12}$$

Visually speaking, this is a region in a 2D space constructed by these two new random variables. Figure 3 demonstrates the region on which the above inequality holds.

The covert attacker/worm is interested in increasing the rate of accidents in cruise control scenarios. When infected ego vehicle is following the lead vehicle stably at the cruise speed and at a distance of $D_{rel} \simeq D_{safe}$, the chance of having a crash if the lead suddenly brakes (e.g. as a result of seeing a hazard) can be calculated as follows.

$$\begin{aligned} P_c &= P\{X > Y + C\} \\ &= \int_{Y=0}^{\infty} \int_{X=Y+C}^{\infty} f_{XY}(X,Y) dX dY \end{aligned} \tag{13}$$

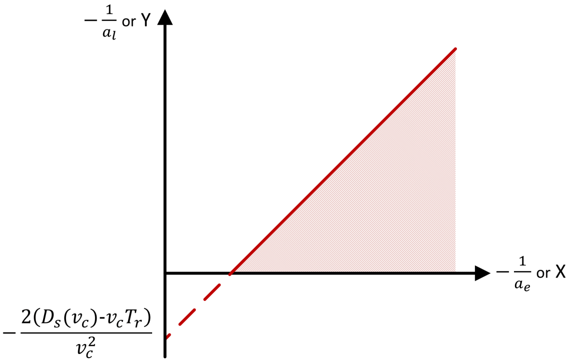


Fig. 3. Visual presentation of the 2D area in which the two vehicles in the cruise scenario will crash.

and since X and Y are independent, $f_{XY}(X,Y) = F_X(X)F_Y(Y)$. Equation (13) can now be easily calculated. We will do numerical experiments in Section V to show how a worm can manipulate the safe distance to statistically increase the rate of accidents among the infected vehicles.

C. Intrusion Detection

Reaction time is critical in real-time systems such as vehicles. Early detection increases the chances of compensation or driver reaction. In this section, we propose an intrusion detection architecture for vehicular Cyber Physical Systems (CPS). The Intrusion Detection Systems (IDS) developed on the basis of this architecture have the ability to capture both cover and non-covert attacks.

Figure 4 shows the proposed IDS architecture for smart and autonomous vehicles. The demonstration is based on CAN bus, however, any similar communication protocol can accommodate this architecture. The design is non-intrusive, meaning that car manufacturers do not need to change their electronic designs for car modules such as ACC, ABS, or Electronic Control Unit (ECU). Each sensitive device sitting on the communication medium/bus can have a dedicated IDS which is put between the module and the bus. It monitors both the incoming and outgoing messages. Since each IDS has access to the bus, it can collect other necessary information for its operation (e.g. the data sent by sensors over the bus).

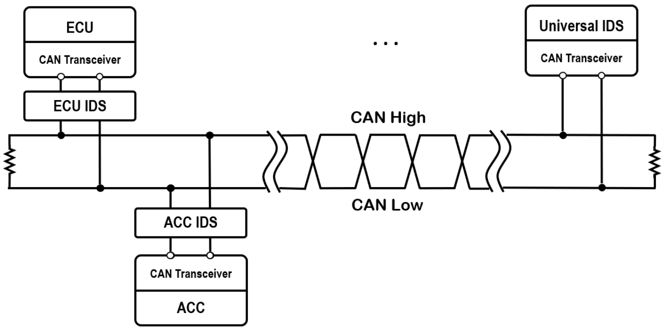


Fig. 4. The proposed IDS architecture for smart and autonomous vehicles. Each device sitting on the CAN bus can have a dedicated IDS with a potential ability of intervention. A universal IDS can also be used with a tap on the bus to monitor the exchanged messages for possible anomalies.

In the proposed architecture, a dedicated IDS acts as a ”Man in the Middle”, thus can optionally intervene upon detection of an intrusion, virtually detach the infected module and take over to compensate for the attack too. Some compensation strategies have already been developed for smart/autonomous vehicle modules [26]. An instance for ACC dedicated IDS module is provided in the evaluations section.

A universal IDS also exists in this architecture. This component can make higher-level observations (e.g. to detect if certain chain of commands issued by different modules are normal or not) and also cross-correlate the reports sent by dedicated IDS modules. This module actually works as a miniature Security Operation Center (SOC) and makes federated intrusion detection possible.

V. Experiments & Discussions

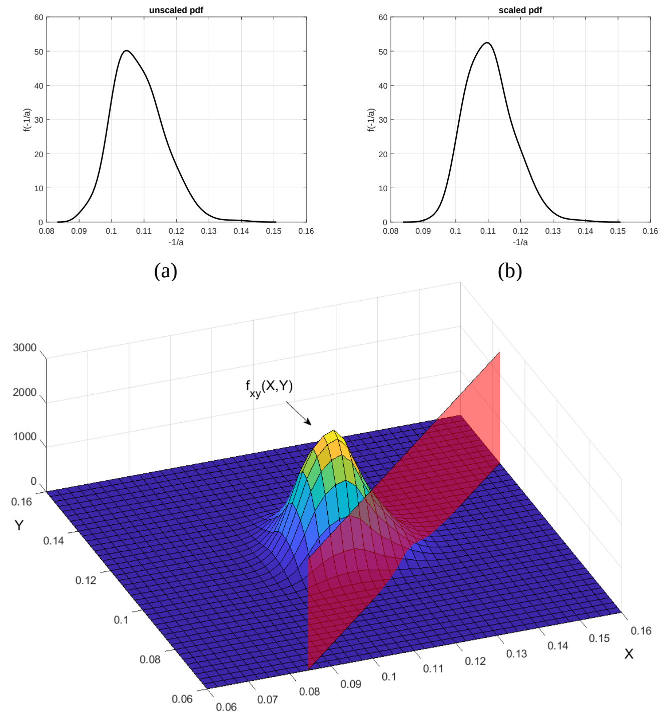
In this section, we conduct a set of experiments and discuss the consequences of launching the introduced covert attack on ACC. We additionally design a dedicated IDS for this module to show how car manufacturers can deal with such threats.

A. Performance Evaluation of the ACC Covert Attack

We use the dataset provided by performancedrive.com.au in our experiments [41]. This Australian source reviews vehicles and measures a few performance indicators like the stopping distance (at 100km/h and on a dry flat road) from which the maximum deceleration can be estimated. The dataset includes around 600 vehicles which are driven in Australia. We refer to this dataset as PD henceforth.

We additionally use the information provided by the Australian Bureau of Statistics on the makes of vehicles registered in Australia in 2021 [42]. Australian vehicle owners must register their vehicles to be allowed to drive them on roads. Registration is usually done on a yearly basis. This bureau’s dataset details the top 29 makes (brands) with the highest number of vehicles on roads. It collects all the others under the 30th group. According to this dataset, there was a total of 14,850,675 vehicles registered in Australia in 2021.

In the previous section, we explained that X and Y (or $-1/a_e$ and $-1/a_l$) are independent but identically distributed. We derived the inverses of the maximum deceleration values from the PD dataset. Figure 5a shows the corresponding pdf. However, to calculate the probability of having a crash in the ACC hard brake scenarios, we need to calculate Eq. (13) the 2D integration must be done over $F_X(X)F_Y(Y)$, however, $F_X(X)$ or $F_Y(Y)$ are not represented by Fig. 5a. The pdf in Fig. 5a is unscaled. It shows the pdf of the inverses of maximum decelerations, but in its calculation, each vehicle has been counted once. However, in reality, the probability of experiencing a certain $-1/a$ upon picking a vehicle randomly depends on the population of each make and model. We created a scaled pdf based on the data provided by the Australian Bureau of Statistics. We populated the vehicles based on their makes. For each make, we made an approximation and randomly picked one model that has been reviewed in PD. Figure 5b shows the scaled pdf of X and Y. Figure 5c shows the joint pdf (i.e. $f_{XY}(X,Y)$) along with the area in



(a) (b)

(c)

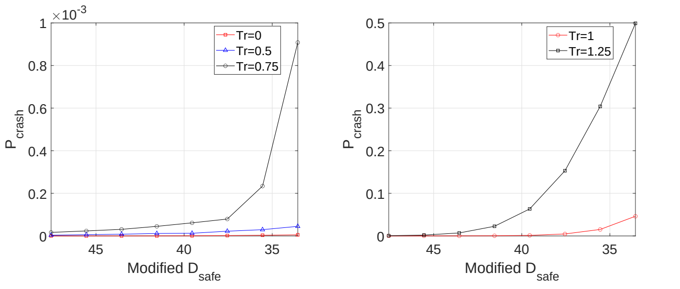
Fig. 5. (a) Presentation of the probability density function of $-1/a$ for an arbitrary car (derived based on PerformanceDrive dataset [41]. Each car (make and model) is counted once in this pdf calculation). (b) The probability density function of $-1/a$ for an arbitrary car (derived based on performancedrive.com.au dataset. The cars makes and models are populated/scaled according to the statistics provided by the Australian Bureau of Statistics in 2021 [42]. (c) A 3D presentation of the joint pdf of X and Y along with the area in which the two vehicles crash (at the right side of the red intersecting plane). The two axes are random variables whose pdfs are found through scaling and based on the inverses of vehicles braking decelerations.

which the two vehicles crash (at the right hand side of the red intersecting plane which is for a sample modified D_{safe}). Now, calculating Eq. (13) should be straight forward.

Figure 6 shows the probability of having a car crash or collision versus D_{safe}, which is modified by the covert worm/attacker. The cruise speed is assumed to be $96.6km/h$. A zero T_r (in Fig. 6a) means that the worm/attacker has not disabled the automatic hard braking of ACC. But all other curves have non-zero T_r values which imply that the hard braking has been disabled and the driver has responded after a delay. The $T_r = 0$ curve shows that if the worm or attacker does not disable the hard braking of ACC, the effect of attack will not be significant. However, if it does so, the crash probability will heavily depend on the reaction time of the driver (if it is not a completely autonomous and driverless vehicle). In all other curves of Fig. 6, we have assumed that the driver reacts after some time (i.e. $T_r > 0$), meaning that he/she takes the control back from the ACC module upon seeing the front vehicle's sudden brake. The curves are divided across two plots to better show the wide scale of crash probabilities. In this part, we design an evaluate a dedicated ACC IDS based on the framework proposed in Section IV-C. There are two approaches to design such an IDS module. One can make a strict IDS which also monitors the expected behavior of the specific ACC controller installed on the vehicle, or a generic less strict one which checks the high-level behaviors expected from the ACC module under different conditions. In this section, we take the second approach.

Following machine learning principles, we define four features, namely D_{rel}/D_{safe}, v_e/v_c, a (acceleration) and τ, where τ is the duration of stay in undesired/unsafe zones. We will explain this feature later. The ingredients of the first three features have already been introduced. These three construct a 3D space as shown in Fig. 7. Note that the actual decision space is four dimensional. However, since demonstration of a 4D space is not possible on paper, we have left the fourth one out and will explain it later.

Normal operation of an ACC creates some points in the feature space. We argue that these features are discriminant and anomalies can be separated from the normal working points in this space. Figure 7 shows a few symbolic normal working points in the space. It is obvious that if $D_{rel} < D_{safe}$ and $v_e < v_c$, the vehicle should accelerate. However, if $D_{rel} < D_{safe}$ or $v_e > v_c$, the vehicle should decelerate. Any other behavior is considered abnormal. We have drawn two imaginary lines on the figure at $D_{rel} = D_{safe}$ and $v_e = v_c$ which divide the plane into four regions (and the 3D space into eight regions of cubic shape with open ends at the acceleration and deceleration directions). According to our discussion, four of the cubic regions contain normal working points, thus the other four should be deemed abnormal (ignoring the fourth dimension). Now that we have explained the first three features and the space they make, we introduce the fourth one (i.e. τ). τ is the longest time the vehicle spends in the abnormal regions. If the ACC controller is not compromised and is genuine, it tries to bring the vehicle back to a safe working point in a reasonable time. This fourth feature can cause a delay in decision making (as we have to wait for the measurement to finish), but significantly reduces the false positives (and indirectly false negatives). If τ is too small, the IDS might raise false alarms as a result of controller overshoots. If it is too long, the IDS can miss short-duration attacks. With these four features, we have a 4D space in which the normal working area of a vehicle ACC is well defined and separable from potential



(a) (b)

Fig. 6. The probability of having a car crash (collision) for different reaction times versus D_{safe} which is modified by the worm/attacker. Due to the difference in scales, the curves are divided into two groups; (a) $T_r = 0s$, $T_r = 0.5s$, and $T_r = 0.75s$ (b) $T_r = 1s$ and $T_r = 1.25s$. Non-zero T_r values imply that the worm/attacker has disabled hard braking of the ACC module and the driver has reacted after T_r seconds.

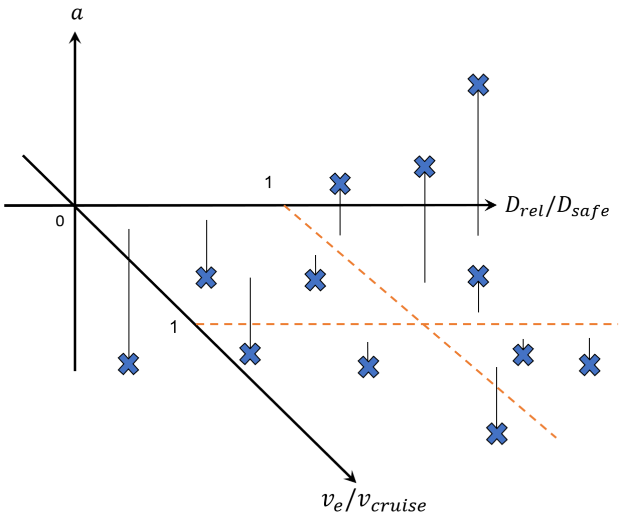


Fig. 7. Three features of the ACC intrusion detection system space along with a few symbolic normal working points. The three features are D_{rel}/D_{safe}, v_e/v_c (or v_e/v_{cruise}) and a. The fourth one is τ which could not be demonstrated.

abnormal ones. We design a decision-tree binary classifier based on the features introduced. We set $\tau = 0.3s$ which along with the 3D regions introduced, defines the normal operation boundaries. Any working point outside these boundaries in the 4D space is considered anomaly and triggers the IDS flag.

To test this ACC IDS, we conduct a simulation. In a specific scenario, we pick a 2019 BMW Z4 sDrive30i to be the lead and a 2019 Suzuki Jimny to be the ego, thus the maximum decelerations will be $a_l \simeq -10.6m/s^2$, and $a_e \simeq -7.2m/s^2$ (based on approximations on the PD data). The other parameter values used in the experiment are as follows. The initial position of the lead vehicle and that of the ego vehicle are $x_l(0) = 80m$ and $x_e(0) = 0m$. The initial velocity of the lead vehicle and that of the ego vehicle are $v_l(0) = 27.78m/s$ and $v_e(0) = 25m/s$. We also assume that $T_r = 1s$, $Tgap = 1.4s$, $D_{default} = 10m$, and $v_c = 32m/s$. We assume the worm/attacker has changed $D_{default}$ to 0 and disabled automatic hard braking in ACC when it infected the module and that this experiment happens after the infection.

B. Intelligent Intrusion Detection System

Figure 8 shows the simulation result. As it can be seen, the lead car hard brakes at $t = 40s$ and the ego car's driver reacts after T_r (since as we mentioned, the worm/attacker has disabled automatic hard braking in the infected ACC module). The crash happens at $t = 43.5s$. To show what would happen if there was only one car in the scenario, we have continued the simulation afterwards, as if the cars were in parallel lanes. The red lines show the cars dynamics after the collision time. Note that in reality when the ego is behind the lead, these red curves change. For example, D_{rel} flattens at 0 and both accelerations are zeroed after the crash.

Nevertheless, way before all these happen, the IDS that works based on the original values of $D_{default}$ and T_{gap}, has raised a flag (at $t = 10.3s$). In this simulation scenario, we have not included any compensators in the IDS module. Without compensation or driver intervention, this scenario leads to an accident. However, if the early warning of IDS was brought to the driver's attention (in order to take the control back from the ACC) or a compensator was embedded in the dedicated IDS module, the accident would be avoided.

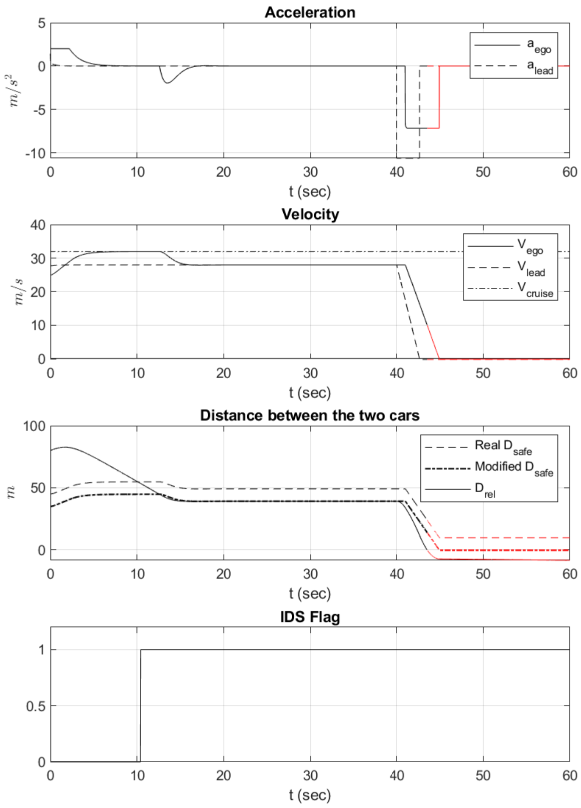


Fig. 8. The cover attack scenario that is launched by changing D_{safe} (from $49.2m$ to $39.2m$). At $t = 40$ the lead vehicle hard brakes and the crash happens at $t = 43.5$. The red lines are imaginary and show independent behaviors of the cars after the crash time (as if they were in parallel lanes).

VI. Conclusion

In this paper, we devised a novel covert attack that can be launched by malwares or worms spreading in intelligent transportation systems via either vehicular networks or consumer devices. The idea is to infect vehicle electronic modules and covertly manipulate the module operation or settings so that human observers are not alarmed but a rise in accident statistics is experienced. As a case study, we analytically studied the effect of such an attack on the Adaptive Cruise Controller (ACC) module. We additionally proposed a new add-on-like Intrusion Detection System (IDS) to defend against these attacks. The architecture of our IDS is non-disruptive and does not require any redesign of vehicle modules, thus can be easily adopted by car manufacturers. By conducting simulations, we tested both the proposed attack and an instance of ACC IDS with real-world datasets acquired from the Australian sources. The results confirm our expectations about the power of the attack as well as the effectiveness of the designed IDS. As a future work, we will study other critical vehicular modules and extract their behavioral features to build dedicated IDSs.

REFERENCES

[1] D. P. F. Mller, H. Vakilzadian, and R. E. Haas, "From industry 4.0 towards industry 5.0," in *IEEE International Conference on Electro Information Technology*, 2022, pp. 61–68.

[2] M. S. Haghighi and K. Mohamedpour, "Neighbor discovery: Security challenges in wireless ad hoc and sensor networks," in *Trends in Telecommunications Technologies*. Intech, 2010.

[3] N. Toorchi, M. A. Attari, M. S. Haghighi, and Y. Xiang, "A markov model of safety message broadcasting for vehicular networks," in *IEEE Wireless Communications and Networking Conference*, 2013.

[4] M. S. Haghighi, S. Wen, Y. Xiang, B. Quinn, and W. Zhou, "On the race of worms and patches: Modeling the spread of information in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 12, pp. 2854–2865, 2016.

[5] J. Y. V. M. Kumar, A. K. Swain, K. Mahapatra, and S. P. M. verify, "Fortified-noc: A robust approach for trojan-resilient network-on-chips to fortify multicore-based consumer electronics," *IEEE Transactions on Consumer Electronics*, vol. 68, no. 1, pp. 57–68, 2022.

[6] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno *et al.*, "Experimental security analysis of a modern automobile," in *IEEE Symposium on Security and Privacy*, 2010, pp. 447–462.

[7] BBC News. (2015, accessed on 01.011.2019) Fiat chrysler recalls 1.4 million cars after jeep hack. [Online]. Available: https://www.bbc.com/news/technology-33650491

[8] B.-C. Choi, S.-H. Lee, J.-C. Na, and J.-H. Lee, "Secure firmware validation and update for consumer devices in home networking," *IEEE Transactions on Consumer Electronics*, vol. 62, no. 1, pp. 39–44, 2016.

[9] Z. A. Biron, S. Dey, and P. Pisu, "Real-time detection and estimation of denial of service attack in connected vehicle systems," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 12, pp. 3893–3902, 2018.

[10] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Int. Workshop on Hybrid Systems: Computation and Control*, 2009, pp. 31–45.

[11] L. Xie, Y. Mo, and B. Sinopoli, "False data injection attacks in electricity markets," in *IEEE International Conference on Smart Grid Communications*. IEEE, 2010, pp. 226–231.

[12] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Annual Allerton conference on communication, control, and computing (Allerton)*. IEEE, 2009, pp. 911–918.

[13] B. Mokhtar and M. Azab, "Survey on security issues in vehicular ad hoc networks," *Alexandria engineering journal*, vol. 54, no. 4, pp. 1115–1126, 2015.

[14] D. Djenouri, L. Khelladi, and N. Badache, "Security issues of mobile ad hoc and sensor networks," in *IEEE Communications Surveys Tutorials*, vol. 7, no. 4. IEEE Communications Society, 2005, pp. 2–28.

[15] M. Sayad Haghighi and Z. Aziminejad, "Highly anonymous mobility-tolerant location-based onion routing for vanets," *IEEE Internet of Things Journal, in press*, 2019.

[16] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive can networks–practical examples and selected short-term countermeasures," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2008, pp. 235–248.

[17] C. Miller and C. Valasek, "Adventures in automotive networks and control units," *Def Con*, vol. 21, no. 260-264, pp. 15–31, 2013.

[18] C. Miller and C.Valasek, "A survey of remote automotive attack surfaces," *black hat USA*, vol. 2014, p. 94, 2014.

[19] R. Van der Heijden, T. Lukaseder, and F. Kargl, "Analyzing attacks on cooperative adaptive cruise control (cacc)," in *IEEE Vehicular Networking Conference (VNC)*. IEEE, 2017, pp. 45–52.

[20] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava, "Non-invasive spoofing attacks for anti-lock braking systems," in *Int. Conference on Cryptographic Hardware and Embedded Systems*, 2013, pp. 55–72.

[21] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE transactions on automatic control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[22] S. Dadras, R. M. Gerdes, and R. Sharma, "Vehicular platooning in an adversarial environment," in *ACM Symposium on Information, Computer and Communications Security*, 2015, pp. 167–178.

[23] Z. A. Biron, S. Dey, and P. Pisu, "Resilient control strategy under denial of service in connected vehicles," in *American Control Conference (ACC)*. IEEE, 2017, pp. 4971–4976.

[24] S. Öncü, J. Ploeg, N. Van de Wouw, and H. Nijmeijer, "Cooperative adaptive cruise control: Network-aware analysis of string stability," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 4, pp. 1527–1537, 2014.

[25] W. B. Qin, M. M. Gomez, and G. Orosz, "Stability analysis of connected cruise control with stochastic delays," in *American Control Conference*. IEEE, 2014, pp. 4624–4629.

[26] F. Farivar, M. S. Haghighi, A. Jolfaei, and S. Wen, "On the security of networked control systems in smart vehicle and its adaptive cruise control," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3824–3831, 2021.

[27] F. Farivar, M. Sayad Haghighi, A. Jolfaei, and S. Wen, "Covert attacks through adversarial learning: Study of lane keeping attacks on the safety of autonomous vehicles," *IEEE/ASME Transactions on Mechatronics*, vol. 26, no. 3, pp. 1350–1357, 2021.

[28] I. Mirzadeh, M. S. Haghighi, and A. Jolfaei, "Filtering malicious messages by trust-aware cognitive routing in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

[29] R. Merco, Z. A. Biron, and P. Pisu, "Replay attack detection in a platoon of connected vehicles with cooperative adaptive cruise control," in *Annual American Control Conference*, 2018, pp. 5582–5587.

[30] F. Alotibi and M. Abdelhakim, "Anomaly detection in cooperative adaptive cruise control using physics laws and data fusion," in *IEEE Vehicular Technology Conference*, 2019, pp. 1–7.

[31] F. Alotibi and M.Abdelhakim, "Anomaly detection for cooperative adaptive cruise control in autonomous vehicles using statistical learning and kinematic model," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3468–3478, 2020.

[32] T. Keijzer and R. M. Ferrari, "A sliding mode observer approach for attack detection and estimation in autonomous vehicle platoons using event triggered communication," in *IEEE Conference on Decision and Control (CDC)*. IEEE, 2019, pp. 5742–5747.

[33] F. Farivar, S. Barchinezhad, M. Sayad Haghighi, and A. Jolfaei, "Detection and compensation of covert service-degrading intrusions in cyber physical systems through intelligent adaptive control," in *IEEE International Conference on Industrial Technology*, 2019.

[34] M. S. Haghighi, F. Farivar, A. Jolfaei, and M. H. Tadayon, "Intelligent robust control for cyber-physical systems of rotary gantry type under denial of service attack," *Journal of Supercomputing*, 2019.

[35] F. Farivar, M. S. Haghighi, A. Jolfaei, and M. Alazab, "Artificial intelligence for detection, estimation, and compensation of malicious attacks in nonlinear cyber-physical systems and industrial iot," *IEEE transactions on industrial informatics*, vol. 16, no. 4, pp. 2716–2725, 2019.

[36] R. Merco, F. Ferrante, and P. Pisu, "A hybrid controller for dos-resilient string-stable vehicle platoons," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1697–1707, 2020.

[37] Z. Abdollahi Biron, S. Dey, and P. Pisu, "Sensor fault diagnosis of connected vehicles under imperfect communication network," in *Dynamic Systems and Control Conference*, 2016.

[38] F. Farivar and M. N. Ahmadabadi, "Continuous reinforcement learning to robust fault tolerant control for a class of unknown nonlinear systems," *Applied Soft Computing*, vol. 37, pp. 702–714, 2015.

[39] S. C. Dekkata and S. Yi, "Improved steering and adaptive cruise control for autonomous vehicles using model predictive control," *Journal of Mechatronics and Robotics*, vol. 3, pp. 378–388, 2019.

[40] M. Sayad Haghighi, "A Note on the Security of ITS: Car Crash Analysis in Cruise Control Scenarios," Tech. Rep. arXiv:2307.08899, ANS1104, 2023.

[41] Performance Drive, "Acceleration and braking performance dataset." [Online]. Available: https://performancedrive.com.au/performance-data/

[42] "Motor vehicle census systems," Australian Bureau of Statistics, Tech. Rep. 93090DO001_2021, June 2021.