Impacts of Security Attacks on The Effectiveness of Collaborative Adaptive Cruise Control Mechanism

Shantanu Sardesai*, Denis Ulybyshev†, Lotfi ben Othmane‡, Bharat Bhargava†
*Continental Teves AG & Co.oHG, Germany
shantanu.sardesai@continental-corporation.com
‡Electrical and Computer Engineering Department; Iowa State University; Ames, USA
othmanel@iastate.edu
†Computer Science Department, CERIAS; Purdue University; West Lafayette, USA
{dulybysh, bbshail}@purdue.edu

***Abstract*—Connected vehicles are equipped with devices that enable them to communicate with external entities, such as other vehicles. This capability is currently used to implement Cooperative Adaptive Cruise Control (CACC). This paper discusses the impact of security attacks on safety of using CACC. It reports about simulating the impact of four security attacks on the effectiveness of CACC in the context of a merging scenario of an abstract system. The simulation showed that attacks on the communication between the vehicles cause collisions with non-negligible proportion. The results suggest the need for strong security assurance for CACC applications.**

Keywords: vehicle security, intelligent transportation, Cooperative Adaptive Cruise Control

I. Introduction

Road traffic accidents have a major impact on public health and the economy. The Automobile Association of America (AAA) studied the crashes in 99 urbanized areas and estimated the cost to be 164.2 B$ in 2005 and 299.5 B$ in 2009 [1]. Traffic accidents can be partly mitigated through programs that promote safe road behavior, such as reducing speed and usage of seat belts.

Connected vehicles are equipped with On-Board Units (OBUs) that enable them to communicate with external entities, such as other vehicles. This capability is currently used to implement intelligent transportation systems applications, including CACC [2]. However, this capability has been used to attack vehicles. For instance, Checkoway et al. [3] demonstrated a set of attacks on a connected vehicle that has e-call application. Woo et al. [4] demonstrated remote injection of CAN command messages to the CAN network of a connected vehicle that shutdown the engine. The likelihood of the risk of these attacks has been shown to be worrying [5], [6], especially when the threats are: manipulating speed limit, Denial of Service (DoS) attacks on the engine, unauthorized brake, and attacks on active brake function.

There is a widespread availability of attack tools and techniques [7] and the availability of demonstrations that security attacks could cause harm, e.g. [8].

978-1-5386-5959-5/18/$31.00

To the best knowledge of the authors, the only research project that investigates in-depth modelling of both the security and safety aspects and implicitly performance for critical system is SESAMO [9]. However, the main focus of the SESAMO project is safety assurance. We proposed in [8] to extend safety assurance cases to consider harm caused by unintended and intended system failure through the use of extended safety assurance cases, which consider safety and security aspects related to assuring that the system does not potentially cause harm.

Experimental system for merging of two vehicles is tested against external attacks and vulnerabilities are studied. Experimental results show that such safety systems are also not safe if they are not secured against external threats. Any external security attack or threat impacts the passenger safety, even with collaborative ITS safety application CACC available and running. This paper evaluates this hypothesis and investigates the relationship between security and safety.

Using MATLAB packages, we simulated the impact of 4 security attacks on the CACC effectiveness in the context of a merging scenario of an abstract system. We found that 5% of attacks on the communication between the vehicles cause collisions [10]. Attacks could be classified as targeted attacks and random attacks. In the context of connected vehicles, the first class concerns attacks that aim to take control of targeted vehicles by sending them targeted messages and cause damage. The second class concerns sending specific messages to reachable vehicles randomly, with the aim to e.g., foul safety systems such as cooperative adaptive cruise control. The work of this papers applies to the second class. The work is an initiation to quantifying the relation between security and safety in the context of connected vehicles. The measurements were done from the perspective of one vehicle and did not consider communication between the two vehicles-this should include aspects, such as message delivery delays and message processing rate. They are also done based on an abstract scenario, not a concrete one.

The rest of the paper is organized as follows. Section II gives an overview of the related work. Adaptive cruise control system for merging scenario is discussed in Section III.

Section IV presents the simulation results. Section V concludes the paper.

II. Related work

Several studies showed that connected vehicles are insecure. For instance, Hoppe et al. [11] demonstrated 4 attacks; they were able to "maliciously" operate the window lift, warning light, airbag control system, and even the central gateway of the Controller Area Network (CAN) bus. Also, Miller and Valasek demonstrated a set of attacks [12], [13], that can impose danger to driver and vehicle, and provided an analysis of the attack surfaces for a set of vehicles [14]. There are several high-level research projects that contributed to addressing security threats in connected vehicles [15]. These include the OVERSEE [16], EVITA [17], and SEVECOM [18].

Checkoway et al. [3] analyzed remote exploits on modern automobiles and concluded that exploitation is feasible via a broad range of attack vectors, including mechanics tools, CD players, Bluetooth and cellular radio. "Wireless communication channels allow long distance vehicle control, location tracking, in-cabin audio exfiltration and theft" [3].

Van der Haijden et al. [19] proposed attacker model and evaluation framework to quantify the impact of attacks on controllers. Resilience of several types of controllers against jamming (DoS) attacks and message injections is evaluated. The results show that most CACC controllers are vulnerable against DoS and message injection attacks, providing broad window of opportunity for the attacker.

Fawzi et al. [20] addressed the problem of state-estimation of a linear dynamic system when integrity of sensor data is not provided since sensor measurements might be corrupted by an attacker. Error correction algorithm is proposed.

Shoukry et al. [21] evaluated spoofing attacks on anti-lock braking systems that can be performed by electromagnetic actuator installed underneath the body of a vehicle. Magnetic fields can distort true signal measured by sensors and can inject malicious measurements.

In [22] robust centralized and distributed monitors for attack detection and identification are proposed based on optimal distributed attack detection filter using a waveform relaxation method.

In [23] a general technique for safety vs. security analysis is proposed. The technique relies on combination of component fault trees and attack trees, which model attacks. The approach demonstrates the ability to adapt qualitative and quantitative analysis to combination of trees.

III. Adaptive Cruise Control system for merging scenario

Prestl et al. developed a scenario to evaluate Adaptive Cruise Control (ACC) for BMW [24]. The scenario has been used to evaluate CACC, for example, by Xu and Sengupta [25]. In CACC system, instead of traditional RADAR and LIDAR, V2V messages are used. V2V messages make the system more efficient and reduce sudden braking situations. These messages are general heart beat messages notifying about its presence and movement towards the merging point. This message contains three fields: time stamp, current position, and current speed.

We use the scenario in this paper, which we describe in the following.

Speed of the preceding vehicle is constant throughout the scenario at 12.5 meters/sec. Cut-in vehicle also has the same velocity for the complete scenario. Host vehicle has initial velocity of 25 meters/sec, it drops till 10 meters/sec to accommodate the cut-in vehicle in front. Then because of the control loop it increases again till 12.5 meters/sec. Hence, desired speed of host vehicle is also 12.5 meters/sec, which remains constant after the merging scenario ends after 20 seconds. Vehicles are assumed to merge at the crossing and hence the angle of merging is 90 degrees. This assumption makes inter-vehicle distance calculation easier.

The scenario is divided in 4 parts. In the first part of the scenario (see Figure 1) both vehicles are traveling on their separate roads. Cut-in vehicle is traveling on merge-in lane approaching the merging point at a constant speed. Host vehicle is traveling on the main lane and it maintains the safe distance with its original predecessor. In the second part (see Figure 2), merging occurs and CACC system ensures that there is no possibility of collision between the two vehicles. After merging in front, cut-in vehicle is the new predecessor of the host vehicle. In the third part (see Figure 3), both vehicles are on the main lane. CACC system continuously checks for safe distance between two vehicles. In the fourth part the cut-in vehicle drifts away. Then the previous predecessor vehicle is again in front of our host vehicle and the merge-in scenario ends.

Part 1: Time period from sec 1 to sec 6. The cut-in vehicle is traveling at a constant speed of 12.5 meters/sec on merge-in lane, towards the merging point. This vehicle is sending V2V Co-operative Awareness Messages (CAMs) to the vehicles on the main lane. The position is with respect to the merging point and it is gradually decreasing every second. Speed is constant throughout the journey at 12.5 meters/sec. Host vehicle also has its distance calculated till the merging point on the main lane in order to estimate the remaining distance to merging point. CACC system keeps the distance safe from the vehicle in front. Vehicles traveling on the main lane receive messages sent from cut-in vehicle with frequency of 3-4 messages per seconds. After receiving these CAMs, each vehicle decides whether the cut-in vehicle is going to affect its own movement. If the message is not relevant, then the main lane vehicles ignore it. In our case host vehicle adjusts its own speed in response to these messages. CACC system shows warning at the start to notify driver about the cut-in vehicle. CACC system is decelerating the speed of the host vehicle to accommodate a cut-in vehicle. At the end of the first part, cut-in vehicle has almost reached the merging point at a uniform speed of 12.5 meters/sec and a host vehicle is also nearby the merging point with its speed reduced accordingly.

Part 2: Time period from sec 7 to sec 10. This is the critical time period for CACC system. In this time interval,

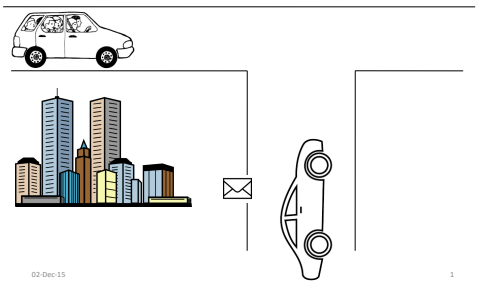

Fig. 1. Merging scenario part 1.

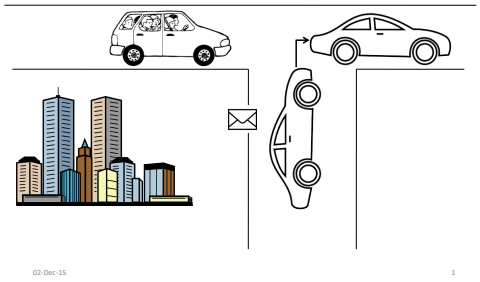

Fig. 2. Merging scenario part 2.

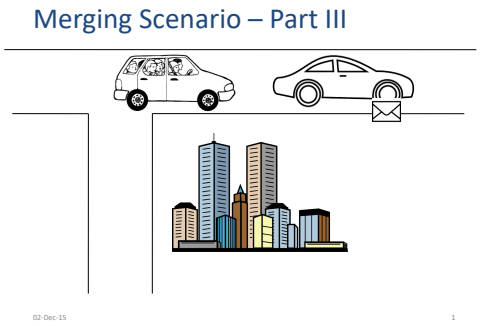

Fig. 3. Merging scenario part 3.[a]

[a]Cliparts are from: http://zlwis.me and https://www.kisspng.com

cut-in vehicle merges on the main lane. The system calculates the diagonal distance between two vehicles to check for the possibility of a collision. The other two distances are the distances remaining to the merging point for both vehicles. Each vehicle keeps track of its remaining distance to the merging point. A threshold of eight meters is considered to indicate a collision between vehicles. This threshold is taken with consideration that the average length of a car is five meters and hence the safe diagonal distance between cars is eight meters. If the inter-vehicle distance is less than the threshold, there is a chance of collision. CACC system then raises a danger signal and advises driver to take manual control. When manual control is taken over, CACC or ACC system disables itself. Now it is driver's responsibility to avoid collision by taking the appropriate preventive action, in this case braking the vehicle or even stopping it. If there is no chance of collision, still the system shows a warning saying that the cut-in vehicle is merging in. Host vehicle's driver is also notified about the distance between the two vehicles as an alert.

Part 3: Time period from sec 11 to sec 16. By this time, the cut-in vehicle is on the main lane and has become the new predecessor of the host vehicle. For this period of 6 seconds, they both travel on the same lane. CACC system keeps inter-vehicle distance within the safe limit. From this point onward, 'position' field in V2V message is the distance to the merging point which gradually increases every second. Host vehicle is also keeping track of its distance to the merging point. The set speed for the host vehicle is 12.5 meters/sec. Hence, the speed of the host car increases till 12.5 and then it remains constant. Cut-in vehicle also has its distance to the merging point as a 'position' field in the messages. Host vehicle calculates its own distance traveled to the merging point. The inter-vehicle distance threshold is checked for the collision possibility. Threshold distance in this case is five meters, which is approximate length of a vehicle. If a calculated inter-vehicle distance is less than five meters, alarm message is displayed and the driver is asked to take manual control in order to avoid possibility of collision. If not, the driver is still notified about the distance to the front vehicle as a warning.

Part 4: Time Period from sec 17 to sec 20. This is the last part of the scenario. During this time period, the cut-in vehicle is drifting away from the main lane. After this, the original predecessor vehicle will again be in front of the host vehicle and the initial state will be achieved. The inter-vehicle distance threshold of five meters is checked for the collision possibility. If there is a possibility, the same alarm message is flashed to alert the driver about the potential dangerous condition. Driver is also notified with a warning message that the cut-in vehicle is drifting away now. When the cut-in vehicle successfully drifts away, the scenario ends and we are back to the initial starting state.

IV. Experimental Evaluation

The CACC abstract system is implemented using MATLAB. Table I provides the simulation parameters. The host vehicle uses its own position and speed and receives periodically the speed and position of the cut-in vehicle. The function of computing the speed of Cut-in vehicle is $rand * 25$ ($rand$ is a uniform random number generator function) and the function of computing the speed of the host vehicle is $currentspeed - rand * 2$. The functions are arbitrary but include randomness. The positions of both cut-in and host vehicles are computed based on the speed values.

Both host and cut-in vehicle distances to the merging point are used to calculate the inter-vehicle distance to check the collision possibility. Distance remaining to the merging point for a cut-in vehicle can be obtained from the latest 'position' field value of V2V message. The inter-vehicle distance is

compared against the decided threshold to check the collision possibility. The driver is warned about collision possibility when potential collision is detected. CACC system disengages the system and the driver takes the manual control of the vehicle.

TABLE I
SIMULATION PARAMETERS.

Fixed Parameters	Value
Number of Runs	40
Number of Vehicles involved 2 Simulation Time(seconds)	20
Frequency of messages per second	2
Speed of the Cut-in Vehicle(meters/sec)	12.5
Distance traveled by cut-in vehicle before merging(meters)	125
Distance traveled by cut-in vehicle after merging(meters)	125
Distance of Merging Point on Main Lane(meters)	175
Distance of Merging Point on Cut-in Lane(meters)	125

Host vehicle can be attacked by V2V message injection and in-vehicle message injection. We focus on the first type of attack only. V2V passive attacks such as message injection, DoS, Replay and others, target the messages sent by cut-in vehicle to the host vehicle. This is done by spoofing the 'speed' field of V2V messages. For each V2V message some random value is generated as cut-in vehicles speed. This value affects the value of remaining distance in calculation of Position. Hence, it also affects the inter-vehicle distances for checking collisions.

There are two error conditions: false positive and false negative. False positive means that the driver is warned by CACC system about the possibility of collision, but in reality there is no chance of collision. This situations may lead to e.g., abrupt braking, constant change from CACC mode to manual driven mode. We do not consider collision possibilities that may be caused by this distraction.

The other possibility is false negative error, which is worse. The false negative condition occurs when CACC system is unaware of real possibility of collision. This may lead to a collision unless quickly intervened by the driver. Using the normal behavior deductions, we are predicting the realistic possibilities of a collision. By checking the inter-vehicle distance values, host vehicle's speed and the notification messages sent to the driver, collision probabilities are calculated.

The goal of the work is to demonstrate the impact of the security attacks on the safety application and not to quantify this impact. Therefore, we do not vary the simulation parameters to show e.g., margins or sensitivity threshold.

Figure IV shows the statistics for the above cases of simulation scenarios. The possibilities of false positive and false negative are higher than the possibility of actual collision. The last portion ("Undecided" on Figure 4) relates to the case when system behaves close to normal and hence conclusions can not be drawn for the first three cases.

V. CONCLUSION

Cooperative Adaptive Cruise Control (CACC) relies on the use of V2V communication. There has been extensive research

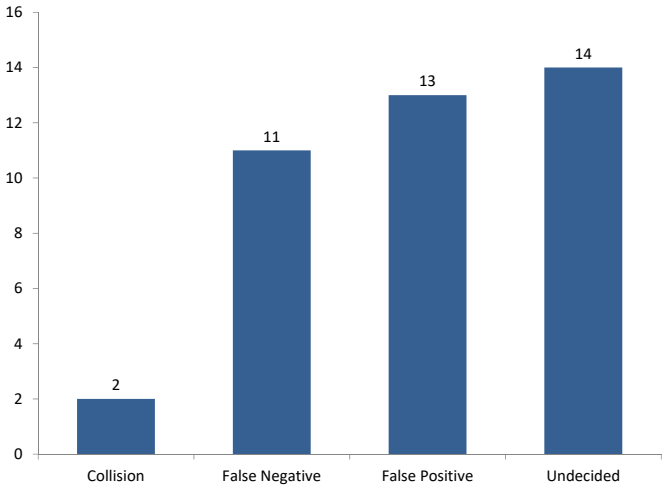

Fig. 4. Passive V2V attacks. Results: 2 out of the 40 simulation runs created collisions; that is, 5% collision possibility.

on addressing the security challenges of this networking and application domains. The projects OVERSEE, CANAuth, EVITA, IntelliDrive, and SEVECOM are some of the examples. However, the applications, communication stack, and security mechanisms must be implemented in software. Given that vulnerabilities are frequently found in software, we argue that the risks of potential attacks should still be considered.

This paper simulates the impact of security attacks on the safety of using CACC in the context of vehicles merging scenario. The simulation showed that V2V injection attacks on the communication between the vehicles cause collision with non-negligible proportion. The results emphasize the need for strong security assurance for CACC applications.

VI. ACKNOWLEDGMENT

This publication was made possible by NPRP grant # [7-1113-1-199] from the Qatar National Research Fund (a member of Qatar Foundation). The statements made herein are solely the responsibility of the authors. This work was also partially supported by the Northrop Grumman Cybersecurity Research Consortium.

REFERENCES

[1] Automobile Association of America: Crashes vs. congestion whats the cost to society? (2011)
[2] Ioannou, P., Xu, Z., Eckert, S., Clemons, D., Sieja, T.: Intelligent cruise control: theory and experiment. In: Proceedings of 32nd IEEE Conference on Decision and Control. (Dec 1993) 1885–1890 vol.2
[3] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T.: Comprehensive experimental analyses of automotive attack surfaces. In: Proc. of the 20th USENIX conference on Security, Berkeley, CA (2011) 6–6
[4] Woo, S., Jo, H., Lee, D.: A practical wireless attack on the connected car and security protocol for in-vehicle can. IEEE Transactions on Intelligent Transportation Systems **PP**(99) (2014) 1–14 To appear.

[5] Ruddle, A.: Security risk analysis approach for on-board vehicle networks. In: The Fully Networked Car Workshop at the Geneva International Moto Show, Geneva, Switzerland (Mar. 2010) http://evita-project.org/Publications/Rud10.pdf.

[6] ben Othmane, L., Fernando, R., Ranchal, R., Bhargava, B., Bodden, E.: Likelihood of threats to connected vehicles. International Journal of Next-generation Computing (IJNGC) **5**(3) (Nov. 2014) 290–303

[7] Bloomfield, R., Netkachova, K., Stroud, R.: Security-informed safety: If it's not secure, it's not safe. In: 5th International Workshop on Software Engineering for Resilient Systems (SERENE 2013), Kiev, Ukraine (2013)

[8] ben Othmane, L., Al-Fuqaha, A., ben Hamida, E., van den Brand, M.: Towards extended safety in connected vehicles. In: The 16th International IEEE Conference on Intelligent Transportation Systems. IEEE-ITSC 2013, The Hague, The Netherlands (Oct. 2013)

[9] SESAMO: Security and safety modelling (sesamo). http://www.sesamo-project.eu

[10] Sardesai, S.: Impacts of security attacks on the effectiveness of collaborative adaptive cruise control system (2015) Advisor: Lotfi ben othmane.

[11] Hoppe, T., Kiltz, S., Dittmann, J.: Security threats to automotive CAN networks–practical examples and selected short-term countermeasures. Reliability Engineering & System Safety **96**(1) (2011) 11 – 25 Special Issue on Safecomp 2008.

[12] Miller, C., Valasek, C.: Adventures in automotive networks and control units. http://www.youtube.com/watch?v=n70hIu9lcYo (Aug. 2013) Presented at DEF CON 21 Hacking Conference. Accessed on Mar. 2014.

[13] Miller, C., Valasek, C.: Adventures in automotive networks and control units. http://blog.ioactive.com/2013/08/car-hacking-content.html (2014) Accessed on March 2014.

[14] Miller, C., Valasek, C.: A survey of remote automotive attack surfaces. http://illmatics.com/remote attack surfaces.pdf (Aug. 2014) Presented at DEF CON 22 Hacking Conference. Accessed on Sep. 2014.

[15] ben Othmane, L., Weffers, H., Mohamad, M.M., Wolf, M. In: A Survey of Security and Privacy in Connected Vehicles. Springer, New York, NY (2015) 217–247

[16] OVERSEE project: Open vehicular secure platform (oversee). https://www.oversee-project.com/ (2014) accessed on Jan. 2014.

[17] EVITA project: E-safety vehicle intrusion protected applications (evita). http://www.evita-project.org/ (2014) accessed on Jan. 2014.

[18] SeVeCom project: Secure vehicular communication eu funded project. http://www.sevecom.org (2014) accessed on Jan. 2014.

[19] van der Heijden, R.W., Lukaseder, T., Kargl, F.: Analyzing attacks on cooperative adaptive cruise control (cacc). arXiv preprint arXiv:1710.05789 (2017)

[20] Fawzi, H., Tabuada, P., Diggavi, S.: Secure state-estimation for dynamical systems under active adversaries. In: 2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton). (Sept 2011) 337–344

[21] Shoukry, Y., Martin, P., Tabuada, P., Srivastava, M. In: Non-invasive Spoofing Attacks for Anti-lock Braking Systems. Springer Berlin Heidelberg, Berlin, Heidelberg (2013) 55–72

[22] Pasqualetti, F., Drfler, F., Bullo, F.: Attack detection and identification in cyber-physical systems. IEEE Transactions on Automatic Control **58**(11) (Nov 2013) 2715–2729

[23] Steiner, M., Liggesmeyer, P.: Combination of safety and security analysis - finding security problems that threaten the safety of a system. In: 32nd International Conference on Computer Safety, Reliability and Security, France (Sep 2013)

[24] Prestl, W., Sauerand, T., Steinle, J., Tschernoster, O.: The BMW active cruise control (ACC). https://doi.org/10.4271/2000-01-0344 (2000)

[25] Xu, Q., Sengupta, R.: Simulation, analysis, and comparison of ACC and CACC in highway merging control. In: Proc. of IEEE Intelligent Vehicles Symposium, Columbus, OH, USA (2003) 237 242