A CONTROL-ORIENTED PERSPECTIVE FOR SECURITY IN CONNECTED AND AUTOMATED VEHICLES

Advanced connectivity features in today's smart vehicles are giving rise to several promising intelligent transportation technologies. Connected vehicles are one such technology where a set of vehicles can communicate with each other and the infrastructure via dedicated communication networks. Connected vehicles have the potential to improve the traffic throughput, minimize risk of accidents and reduce vehicle energy consumption. However, despite these promising features, vehicular communication networks endure several challenges from reliability and security perspectives. These challenges can occur due to cyberattacks with purposes of disrupting the performance of the connected vehicles system. In order to improve safety and security, advanced vehicular control systems must be designed to be resilient to cyberattacks. This article describes a resilient control architecture that consists of several control strategies for different network attacks, and a decision-making system to select the best countermeasure.

BY PIERLUIGI PISU
ASSOCIATE PROFESSOR
DEPARTMENT OF
AUTOMOTIVE ENGINEERING
CLEMSON UNIVERSITY

JIM MARTIN
ASSOCIATE PROFESSOR
SCHOOL OF COMPUTING
CLEMSON UNIVERSITY

ZOLEIKHA ABDOLLAHI BIRON
POST-DOCTORAL RESEARCHER
DEPARTMENT OF
AUTOMOTIVE ENGINEERING
CLEMSON UNIVERSITY

V2V COMMUNICATION AND VULNERABILITIES IN CONNECTED VEHICLES

Connected vehicles (CV) present a significant advancement in transportation for improvement of safety, mobility, and energy consumption. Connected vehicles are able to communicate with other vehicles or the Department of Transportation (DOT) network resources through vehicular application and network (VANET). A variant of Wi-Fi referred to as Dedicated Short Range Communications (DSRC) is a candidate for use in a VANET that supports both public safety and private communication [1]. The communication environment of DSRC is both vehicle-to-vehicle (V2V) and vehicle-to/from-roadside infrastructure (V2I). DSRC aims to provide a high data rate and at the same time minimize latency within a relatively small communication zone. The broadband access speed can be up to 27 Mbps along with low latency (less than 50ms) over a range of up to 1 km, and uses a 75MHz block of spectrum in the 5.9 GHz band, which has been allocated by the FCC for automotive applications [2]. However, the DSRC communication network has not yet been fully evaluated and analyzed through field experiments in a systematic manner and has some issues regarding packet delivery and reliability of network specifically in real experimental scenarios [3]. The packet delivery ratio is affected by the velocity of mobile nodes. Experimental results show that the ratio of successful packet delivery (DSRC IEEE 802.11p) drops significantly (as large as 10 percent) as the relative velocity between the sender and receiver is about 60 mph, and this rate increases exponentially when the velocity increases further. These losses may be acceptable for cellular and stream applications, but pose a great challenge for networked control and diagnosis, which are typically vulnerable to message losses. Also, the communication delay is affected by the network interaction topology, which can increase exponentially with an increase in the size of the network. CVs have to constantly communicate with the infrastructure to acquire information for their maneuver actions. The accuracy requirement of networked control and diagnosis becomes difficult to maintain as vehicle speed increases [4]-[5]. A typical vehicle application utilizing DSRC communication is Cooperative Adaptive Cruise Control (CACC), where each individual vehicle automatically accelerates and decelerates to keep a desired distance from its preceding vehicle utilizing onboard sensors, such as radar, to measure the inter-vehicle distance and relative velocity while information of the preceding vehicle(s), such as their acceleration, is broadcast through the DSRC network. This enables vehicles to obtain information beyond the line-of-sight of onboard

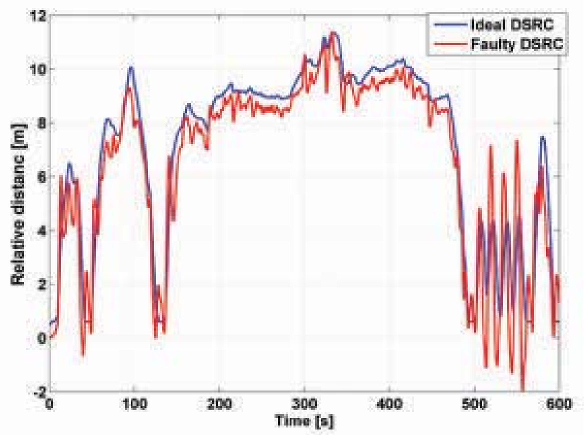


FIGURE 1 Impact of communication delay on relative distance between two connected vehicles.

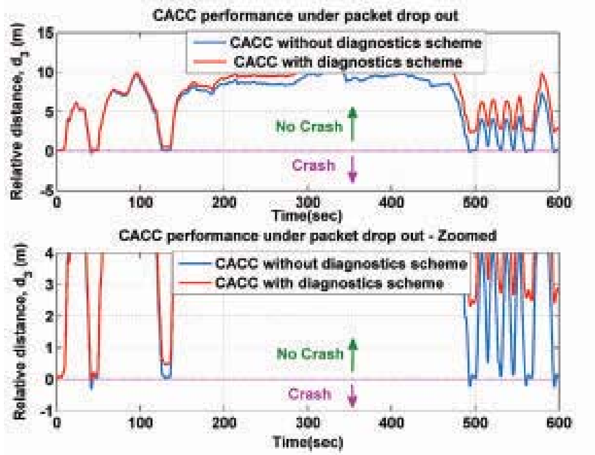


FIGURE 2 Impact of intermittent communication on relative distance between two connected vehicles.

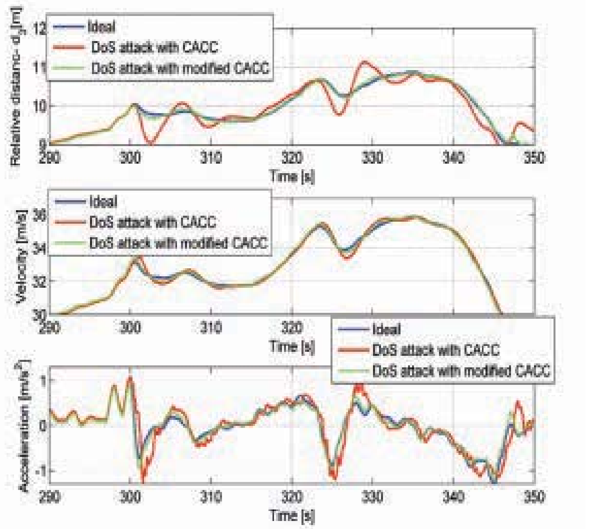


FIGURE 3 Impact of Denial of Service attack on relative distance between two connected vehicles, velocity, and acceleration of vehicles.

sensors and to obtain information of other vehicles that cannot be retrieved otherwise. As a result, short inter-vehicle distances can be realized, thus increasing traffic throughput, without compromising safety. Hence, the performance in terms of minimizing the inter-vehicle gap is enhanced, while guaranteeing string stability and disturbance attenuation in the platoon [6], specifically compared to conventional adaptive cruise control (ACC), which is operated without wireless communication [7]. Sharing information through the wireless communication network makes connected vehicles vulnerable to cyberattacks and network failures as well as physical faults. In [8], the capability of attackers to intrude vehicles is explored. It is shown that the attacker is theoretically able to take control over the individual position and velocity of other vehicles in the platoon.

Figure 1 shows the effect of network failure in cooperative adaptive cruise control (CACC). Here a platoon of connected vehicles is considered while their acceleration information is exchanged through the DSRC network. The leader vehicle follows the US06 driving cycle (a particular velocity profile defined by the Environmental Protection Agency for emissions testing) and the relative distance between two vehicles is considered as a criterion of vehicle performance while the network communication has some imperfection due to random transmission delay. In an ideal DSRC-based system, the relative distance between vehicles could potentially be as small as 0.5 meters. However, in real systems that include network impairment and possibly physical and software failures, the optimal distance between two vehicles would likely vary over time making the vehicles subject to crash. A way to avoid this issue is to improve robustness and capabilities of connected vehicle applications by enhancing safety and vehicular control.

EFFECTS OF ATTACKS ON COOPERATIVE CONTROL

Intermittent communication

Wireless links are known to be prone to errors and failures. Packet dropping is the most common failure in communication networks, causing intermittent communication, and occurs due to a number of factors including occasional hardware failures, degradation in link quality, and channel congestion. Although many network protocols have re-transmission mechanisms embedded, for real-time feedback control data, it may be advantageous to discard the failed packets on their first transmission because re-transmitted packets may have too large latency to be useful [9]. Re-transmission may also delay the transmission of new packets. In connected vehicles, due to limited computing power of the communication modules, error correction techniques are not common on the lower network levels. **Figure 2** shows the effect of packet dropping in the DSRC network in a platoon of vehicles equipped with CACC. To illustrate the effect, we have plotted the relative distance of two vehicles in a platoon. Without modifications, the CACC algorithm with intermittent communication will have degraded performance particularly if it doesn't switch to ACC algorithm. To enhance the performance of the CACC under packet dropping, an observer-based algorithm that estimates the lost information can be utilized [10]. The results are shown in **Figure 2** with the red curves.

DOS Attack

Cyberattacks are different from network failures because they are designed smartly by attackers. Hence, modeling the cyberattacks from a control perspective is more challenging than network failures, and requires detailed analysis over network and attacker capabilities.

Denial of service (DoS) attacks are perhaps the most detrimental attacks that affect the packet delivery because they have been proven capable of shutting off an organization from the Internet or dramatically slowing down network links [11]. The definition of DoS attack may vary in different studies; however, all describe the effect of DoS attack as the same. The violation of availability of sensor and control data is known as denial-of-service. DoS attacks can be classified into several different types, among which the packet flooding attack and data jamming, induced by a malicious adversary, are prevalent [12]-[13]. Attackers may flood a network with a large volume of data to deliberately consume the limited resources, such as CPU cycles, memory, network bandwidth, and packet buffers. Consequently, time delay and packet loss of transmitted information in connected vehicles become worse under such attacks, which in turn may significantly impair the system performance. In the existing literature, there are two main methodologies to model Denial of Service attack from a control perspective: time delays or packet loss [11]-[12]. Indeed, based on the network communication protocol and attacker capabilities, DoS attacker can flood the network with data, creating congestion and consequently packet loss. However, if the attacker does not make the attack too obvious on the network, it may flood the packets randomly on the network and try to increase the service time on the communication network [13]. **Figure 3** shows the effect of DoS attack, which is modeled as a time delay in the DSRC network. By developing a resilient strategy for DoS attack [14], the effect of the attack can be compensated (**Figure 3**, green line).

False data injection

In connected vehicles, false data injection attacks refer to a class of cyberattacks in which the attacker wishes to alter the integrity of a system by compromising either a subset of sensors and sending inaccurate readings to the controller or actuators data from the controller [15]. To carry out the attack, the input to the controller needs to be carefully designed since abnormal sensor measurements will generally trigger an alarm [16]. In the control literature, false data injection attacks are typically modeled as an additive sensor or actuator fault on the original data. Hence, existing fault detection algorithms, including Kalman filter [15], [16] and observer design [17], are capable of detecting the false data injection attack in the system. However, there are cases in which these types of attacks are not diagnosable with standard fault detection methodologies. To illustrate an example of this case, consider a smarter false data injection attack where the attacker uses fake identity to inject fake vehicle data into the DSRC network to disrupt the performance of the whole platooning of vehicles. The attacker provides fake vehicle information to increase or decrease the inter-vehicle distance, which can degrade the platoon performance and disrupt the stability of the string. Indeed, the attacker has the capability to develop a fake identity to insert fake cars into the platoon. Having a fake vehicle in the platoon (see **Figure 4**), makes decisions difficult for the follower car due to the conflict between physical observations and network observations. In this case, it is not clear if the following car should fill the physically open gap or follow the ghost injected vehicle. In [18] a solution is proposed based on a partial differential equation (PDE) model of a platoon of cooperating vehicles using PDE observer design for the identification of the fake data injection attack.

DECISION-MAKING RESILIENT CONTROL

The previous sections have explained how different attacks can affect the cooperative control in connected and automated vehicles and how appropriate resilient control strategies can avoid collision and maintain functionality as long as safety can be guaranteed. Now the question is how to combine the aforementioned strategies in an integrated control scheme capable of selecting the appropriate strategy under unknown attack conditions. A hybrid format controller is required to determine which type of cyberattack is happening in the system and what are the corresponding actions to minimize the effect of that specific attack. In this section, an example of a decision maker using an optimum control algorithm to select the best control signal among

ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation (NSF) under grant No. CNS-1544910. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

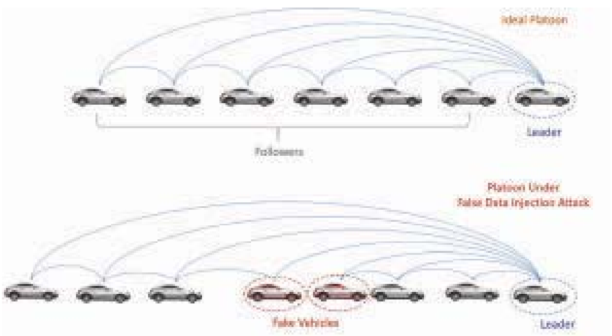


FIGURE 4 False data injection attack in a platoon of connected vehicles as ghost vehicle impacting density of the traffic.

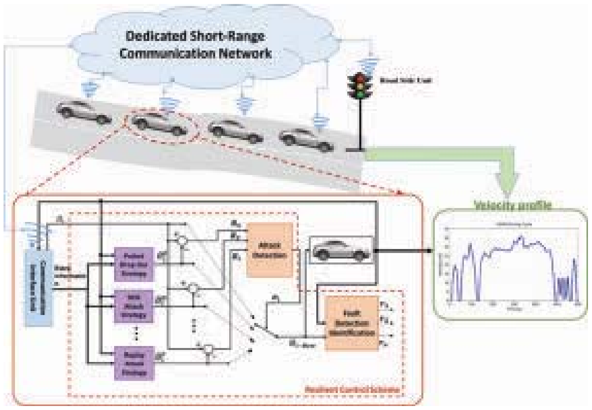


FIGURE 5 Developed CACC attack-resilient control scheme.

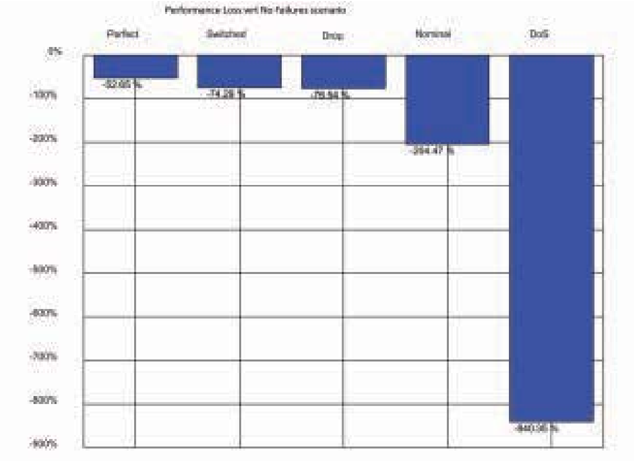


FIGURE 6 Performance loss associated with selection of the wrong strategy.

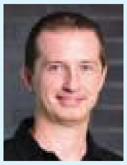
the available choices is shown [18].

The attack detection and switching strategy in **Figure 5** is formulated as an MPC-like optimization problem where the control variable is constrained to one of the three strategies described in the previous section and applied in a receding horizon fashion. The choice of the cost function plays an important role in the performance of the system. In this case, the problem was formulated to penalize aggressive driving while maintaining safe distance from the preceding vehicle. **Figure 6** shows the results of the switching strategy with respect to the case with no networks attacks or failures using the RMS of the jerk as measure of comfort (performance index). By comparison with the perfect case, in which the attacks are perfectly identified and the correct strategy selected immediately, there is approximately a 22 percent strategy improvement that could still be achieved by changing the switching strategy.

CONCLUSIONS

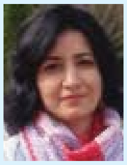
Network attacks are a real potential threat to the deployment of cooperative control functions in CVs. This article provides an overview of potential attacks that can impact CV technologies and highlights how a resilient control scheme can be effective to mitigate the effect of these attacks by allowing the system to safely operate with reduced performance. Further research in this area can offer more mature solutions to implement such strategies in a real production vehicle. ■

ABOUT THE AUTHORS



Pierluigi Pisu is an Associate Professor of Automotive Engineering in the Carroll A. Campbell Jr. Graduate Engineering Center at the Clemson University International Center for Automotive Research, with a joint appointment in the Holcombe Department of Electrical and Computer Engineering at Clemson University. Dr. Pisu is the faculty-elected Leader of the Connected Vehicle Technology Faculty Research Group in the College of Engineering, Communication and Applied Science and the Leader of the Deep Orange 10 Program. He is the Director of the DOE GATE Hybrid Electric Powertrain Laboratory and the Creative Car Laboratory. Dr. Pisu has a Ph.D. in Electrical Engineering from The Ohio State University (2002) and a "Laurea" in Computer Engineering from the University of Genoa, Italy. His research interests lie in the area of functional safety, security, control and optimization of Cyber-Physical Systems for next generation of high performance and resilient connected and automated systems with emphasis in both theoretical formulation and virtual/hardware-in-the-loop validation.

Jim Martin is an Associate Professor in the School of Computing at Clemson University. His research interests include broadband access, wireless networks, Internet protocols, and network performance analysis. Current research projects include heterogeneous wireless systems and DOCSIS 3.x cable access networks. He has received funding from NSF, NASA, the Department of Justice, BMW, CableLabs, Cisco, Comcast, Cox, Huawei, and IBM. Dr. Martin is leading an effort at Clemson University that is deploying advanced network infrastructure to support vehicular wireless communications. Dr. Martin received his Ph.D. from North Carolina State University. Prior to joining Clemson, Dr. Martin was a consultant for Gartner, and prior to that, a software engineer for IBM.



Zoleikha Abdollahi Biron received the Ph.D. in Automotive Engineering at Clemson University, Clemson, SC, USA in 2017, and the MSc. degree in control engineering from K.N. Toosi University of Technology, Tehran, Iran, in 2011. She is currently a Post-Doctoral Fellow in Department of Automotive Engineering at Clemson University. Her current research interests include control, estimation, diagnosis in connected vehicles and cyber-physical systems. She is a member of the American Society of Mechanical Engineers (ASME) and the Institute of Electrical and Electronics Engineers (IEEE).

REFERENCES

1 J. Guo and N. Balon, "Vehicular Ad Hoc Networks and Dedicated Short-Range Communication", University of Michigan, 2006.

2 US Department of Transportation, "Dedicated Short Range Communications" http://www.its.dot.gov/DSRC/ Retrieved Jan 10, 2015.

3 F. Bai and H. Krishnan, "Reliability Analysis of DSRC Wireless Communication for Vehicle Safety Applications", *Proceedings of the IEEE ITSC*, 2006, pp. 355-363.

4 J. P. Singh, N. Bambos, B. Srinivasan and D. Clawin, "Wireless LAN Performance under Varied Stress Conditions in Vehicular Traffic Scenarios", *IEEE Vehicular Conference*, VTC, vol. 2, 2002, pp. 743-737.

5 S. Sivavakeesar and G. Pavlou, "Quality of Service Aware MAC Based on IEEE 802.11 for Multihop ad-hoc Networks", *IEEE Wireless Communications and Networking Conference*, vol.3, 2004, pp. 1482-1487.

6 P. Seiler, A. Pant and K. Hedrick, "Disturbance propagation in vehicle strings," *IEEE Trans. Automotive Control*, vol. 49, no. 10, Oct. 2004, pp. 1835–1842.

7 G. J. L. Naus, R. P. A. Vugts, J. Ploeg, M. J. G. van de Molengraft and M. Steinbuch, "String-stable CACC design and experimental validation: A frequency-domain approach," *IEEE Trans. Vehicle Technology*, vol.59, no.9, Nov. 2010, pp. 4268–4279.

8 S. Dadras, R. M. Gerdes and R. Sharma, "Vehicular platooning in an adversarial environment," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ACM, 2015, pp. 167–178.

9 Z. H. Pang, G. Liu and Z. Dong, "Secure Networked Control Systems under Denial of Service Attacks", *18th IFAC world Congress*, 2011, pp. 8908-8915.

10 Z. A. Biron, S. Dey and P. Pisu, "Fault Diagnosis of Connected Vehicles Under Unreliable Networks," In *Proceedings of the ASME 2016 Dynamic Systems Control Conference*, Oct 12-14, Minneapolis, MN, 2016.

11 A. Housholder, A. Manion, L. Pesante, G. Weaver and R. Thomas, "Managing the Threat of Denial of Service Attack", Carnegie Mellon CERT Coordination Center, Pittsburgh, PA.

12 S. Amin, A. Cardenas and S. Sastry, "Safe and Secure Networked Control Systems under Denial of Service Attacks", HSCC 2009, LNCS 5469, 2009, pp. 31–45.

13 M. Long, C. Wu and J. Hung, "Denial of Service Attacks on Network-Based Control Systems: Impact and Mitigation", *IEEE Transaction on Industrial Information*, vol. 1, no. 2, 2005, pp. 85-96.

14 Z. Biron and P. Pisu, "Resilient Control Strategy Under Denial of Service in Connected Vehicles," *American Control Conference 2017*, Seattle, WA, 2017.

15 L. Xie, Y. Mo and B. Sinopoli, "False data injection attacks in electricity markets," 2010 First IEEE International Conference in Smart Grid Communications (SmartGridComm), pp. 226–231, IEEE, 2010.

16 Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in Preprints of the *1st workshop on Secure Control Systems*, 2010, pp. 1–6.

17 Y. Liu, P. Ning and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, 2011, p. 13.

18 Z.A. Biron, "A Resilient Control Approach to Secure Cyber-Physical Systems (CPS) with an Application on Connected Vehicles" (2017). All Dissertations, 1869.