1. Title: Hazard Identification and Mitigation Strategies for Overtaking Maneuvers on Two-lane Rural Roads

Authors: Linda Capito and Keith Redmill
Affiliation: The Ohio State University

Extended Abstract:

Vehicle automation and Advanced Driver-Assistance Systems (ADAS) have evolved from being relatively simple, self-contained systems such as Autonomous Emergency Braking, which will apply brakes if an imminent collision is sensed, and Lane Keeping Assistance, which can keep the vehicle between the lane boundaries in some situations, to increasingly unified systems that handle a significant number of driving functions and involve a number of disparate sensors, estimation, control, and behavior generation algorithms, and coordination and cooperation both on-board the vehicle and with other vehicles, road users, and infrastructure components. As these systems become more complex, it has become more challenging for control and systems engineers to identify and quantify potential failure and attack modes and provide mitigations to ensure safety in the face of hardware or software failures, especially when meeting failures of the intended function of the assistance system.

A particularly challenging ADAS is the overtaking assistant. Risks during an overtaking maneuver include detecting oncoming traffic too late or incorrectly estimating the relative speeds and distances of the vehicle being overtaken and of oncoming traffic. This can lead to particularly dangerous scenarios on two-lane rural roads, where an overtaking assistant system has to execute lane-change maneuvers and acceleration and braking actions on a potentially narrow road with potentially limited line-of-sight visibility. The complexity of such a system comes from the particular combination of sensor information that has to be processed and from the complex decision making algorithm that the vehicle needs to execute to successfully complete the maneuver. Sensors available on the ego-vehicle may include GNSS and other position sensors, mapping data, short and long range radars, cameras, and LiDARs, and the decision making and control algorithms may be either entirely internal to the vehicle or may have access to additional information by communication with other vehicles (V2V) or to the infrastructure (V2I). Furthermore, depending on the configuration of the road (multi-lane highway vs two-lane rural road) and the external actors (lead vehicle, lead trailer, oncoming vehicle in the other lane), the number and type of hazards become more difficult to define and analyze. In general, types of hazards that may appear in complex systems are addressed by two standards. Functional Safety Standard (ISO 26262) is about hazards that are induced by software or hardware failures. Safety of the Intended Functionality Standard (SOTIF ISO/PAS 21448) intends to identify performance shortcomings in ADAS systems that may happen when there is no system failure, but rather limitations in the nominal performance.

There are several hazard analysis techniques that are applied to the aforementioned standards. Failure Modes and Effects Analysis (FMEA) is a traditional method that considers that hazards are the result of a sequence of chain events caused by individual components' failures that propagate throughout the system. Hazard and Operability Study (HAZOP) is a top down hazard analysis method for complex systems that consists of evaluating each component in a chain process and find potential situations that would provoke hazards. Finally, STPA is a hazard analysis method that provides a systematic process to evaluate interfaces between systems components, controllers and people, using process feedback loops, functional control diagram, system requirements, hazard scenarios, safety constraints and safety requirements.

In this study, we focus on analyzing the complexity of an overtaking assistant on a two-lane rural road utilizing HAZOP and STPA (step 1) for the vehicle level hazard analysis and FMEA and STPA (step 2) for the overall safety analysis. Previous studies have shown that the combination of two or more hazard analysis methods have lead to better identifying potential hazards and mitigation strategies.

Furthermore, we implement a simulation of the proposed scenario on a two lane rural highway, where the ego-vehicle possesses an overtaking assistant based on Vehicular Ad hoc NETworks (VANETs) that relies on the exchange of status messages (beacons). Among the Operational Domain Design (ODD) specification, we vary the continuous variables for the ego-vehicle, the lead vehicle and the oncoming vehicle to create

Proposal 24 submitted to 2021 IEEE International Intelligent Transportation Systems Conference (ITSC). Received February 16, 2021.

potentially unsafe situations. Four types of failure modes are implemented to correspond to the previous hazard analysis: scenario level (e.g. occlusions), vehicle communication level (e.g. communication range, packet error rate, sensor and estimation inaccuracies), position and timing sensor level (e.g. GNSS dropout during various periods of time, noise level, position jumps), and potentially other sensing systems.

The scenario configuration allows us to study multiple attack modes and obtain simulated runs of the scenario that can be quantitatively analyzed to find the variable/ODD configurations that lead to hazard situations involving collisions or near collisions. We compare this against the results from the theoretical analysis. We finally select a subset of hazard situations and implement the mitigation strategies obtained by the theoretical analysis and evaluate its impact in the overall system.

The contribution of this work is twofold: (1) We provide a detailed hazard analysis with mitigation strategies for the proposed system. (2) We validate our analysis through a detailed simulation specification, for both hazards discovery and mitigation strategies evaluation.

2. Title: Effects of Autonomous Technology on Vehicle Miles of Travel (VMT)
Authors: Katherine Asmussen, Aupal Mondal, and Chandra Bhat
Affiliation: University of Texas at Austin

Extended Abstract:
Autonomous vehicles (AVs) are likely to alter individual activity-travel behavior and mobility patterns, thanks to technologies that, in some future, will not even require the human to pay attention to the road. However, while fully autonomous vehicles were hailed as the wave of the very immediate future even five years back, such aggressive predictions of the availability and use of fully autonomous vehicles have simply not materialized. Thus, investigating the potential activity-travel behavior impacts of fully autonomous vehicles (designated as Level 5 automation on the Society of Automotive Engineers or SAE scale) can only be undertaken through stated preference or SP surveys (that is, asking individuals how they may change their mobility patterns in a hypothetical environment with a Level 5 vehicle). Unfortunately, according to the information sciences literature, the validity of such responses is highly questionable, because individuals may not be in a position to provide appropriate responses when thrust into a hypothetical environment that is difficult to conjure up.

While the stated timeline for the introduction of full automation in vehicles has now been pushed back, there has been substantial progress in testing, refining, standardizing, and implementing lower levels of autonomous technology in vehicles. In this context, SAE Level 1 features (such as adaptive cruise control or parking assist features) are in most new vehicles today, while many higher-end vehicles today also achieve Level 2 automation (such as vehicles with an Autopilot feature that includes not only adaptive cruise control, but also hands-free lane changing and self- parking). The availability and use of these vehicles today, albeit with lower levels of automation, can provide important and reliable insights on how travel patterns may change with advancing technology.

In this paper, we propose to examine potential mobility changes due to technology features that exist today in vehicles. Importantly, while some earlier studies have examined consumer acceptance of existing vehicle technology, we go beyond consumer acceptance to also examine how individuals with and without automation features in their vehicles differ in their annual vehicle miles of travel (VMT). In doing so, we develop a multivariate model that captures self- selection effects. That is, we accommodate for the effect of observed individual demographic characteristics (such as age and gender) that may make a person more likely to embrace specific technology features as well as drive more. At the same time, we also control for unobserved latent individual characteristics (such as tech-savviness and eagerness to explore) that positively affect both technology acceptance and VMT. By jointly modeling vehicle technology features (VTFs) in the vehicles of individuals, along with the corresponding annual VMT of the vehicles, we are able to accommodate the aforementioned self-selection effects, thus enabling the estimation of the “true causal” impact of VTFs on VMT. Such an analysis not only provides insights regarding the effects of

automation technology on VMT, but also can offer an assessment of safety impacts through the potentially increased exposure effect due to increased VMT.

The foundational basis for our joint model is the use of stochastic latent attitudes/lifestyle constructs (also referred to as psycho-social latent constructs), along with observed individual and built environment (BE) variables, as the drivers of VTF adoption and VMT. Four such latent constructs are used: (need for) driving control, (need for) mobility control, concerns with safety (safety concern), and an individual's interest in productive travel time. The VTFs considered are the following: lane keeping system, backup camera, adaptive cruise control, automated braking system, and blind spot monitoring. Each of these VTF dependent variables takes the form of a binary variable. The VMT dimension takes the form of a grouped dependent variable, because annual mileage information is typically elicited from respondents in bracketed categories. Thus, our joint model system constitutes a limited-dependent equation system that captures self-selection effects. After accommodating these self-selection effects, any remnant "true causal" effect of each VTF on VMT is estimated by including the binary indicators of each VTF on the right side of the VMT equation.

The data used for the analysis is drawn from a 2019 "emerging mobility" survey conducted in the Austin metropolitan area in Texas, which resulted in a sample of 978 respondents. To investigate policy implications, we translate the estimated results to (a) treatment effects of each VTF on VMT, as well as the treatment effects of each demographic and BE attribute on VMT, (b) VMT changes in response to different scenarios for the temporal evolution trajectories of demographics and VTFs, (c) safety impacts due to technology adoption-caused VMT increase, supported by external predictions of potential safety benefits of the VTFs themselves, and (d) equity considerations by examining the disparate adoption rates of VTFs across demographic and ethno- racial segments, as well as consequent VMT impacts. Our results underscore the important potential impacts of VTFs on VMT patterns, and provide insights for policy/regulation in the coming era of fully automated vehicles. In addition, our results highlight the value of using psycho- social latent constructs in studies related to investigating the activity-travel behavior effects of advancing mobility options, both in terms of improved prediction fit as well as proactive strategies to design equitable, risk-adverse, and community-driven transportation systems.

3. Title: Impact Evaluation of GNSS Signal Attacks on Cooperative Perception
Authors: Yi Guo, Kelly Cohen, and Jiaqi Ma
Affiliation: University of Cincinnati and UCLA

Extended Abstract:
Cooperative perception is an emerging technology to enhance the perception capability of connected and automated vehicles (CAVs) by exchanging their raw or processed sensor data with the surrounding CAVs via vehicle-to-vehicle (V2V) communications. It helps extend the line-of-sight and field-of-view of CAVs and improves the accuracy of detection. For cooperative perception, the localization information of CAVs plays an essential role. However, the localization information provided by commercial GNSS (Global Navigation Satellite System) is not secure enough as expected, and the GNSS receivers may suffer the jamming and spoofing attacks. Those attacks can mislead the GNSS receivers, and therefore may significantly impact the effectiveness of cooperative perception.

In this study, we investigate the impact of GNSS signal attacks on cooperative perception. Under the proposed framework, four steps are implemented to model and simulate GNSS signal attacks. A long short-term memory (LSTM) network is trained with collected data to perform the cooperative perception. Numerical simulations are conducted with different random seeds, and the impacts are evaluated. Preliminary results indicate that GNSS signal attacks can impact the cooperative perception in terms of location estimation. The impact of slight jamming attacks is marginal, and the effective penetration rate (EPR) reduces 3.2% and 1.8% on average with different accuracy ranges. However, even with a short attack window, the spoofing attacks can significantly affect the cooperative perception and reduces the EPR by 7% and 6.2%, correspondingly.

The paper will adopt the following framework, consisting of four steps:
Step 1: Model the traffic flow. Vissim is used to simulate the traffic, and the calibrated car-following models are required for both human-driven vehicles (HDVs) and CAVs. In this study, a calibrated Wiedemann 77 car-following model is used to simulate HDVs' behavior, and a platooning protocol proposed in the previous study is used for CAVs to regulate their behavior. Step 2: Conduct simulations and collect required data. Numerical simulations are conducted with different random seeds. At each simulation time-step, all vehicles' location and speed information will be recorded. For CAVs, their acceleration information will also be recorded to support the cooperative perception. Step 3: Train the cooperative perception model. A data-driven cooperative perception model is used in this study to estimate HDVs' positions. It needs to be trained with collected data before applying. Note that we assume there are no GNSS signal attacks during the training process. More details about the cooperative perception model will be introduced in the next section. Step 4: Simulate different types and levels of GNSS signal attacks. GNSS signal jamming and spoofing are simulated with different levels, including slight, moderate, and severe. CAV cannot receive GNSS signal and loses location information during the jamming attack, and receives forged GNSS signal during the spoofing attack. In the slight scenario, we assume that each CAV is attacked with an attack window of 1 attack input (i.e., 1 second since the location input frequency is 1 Hz) when implementing the cooperative perception. In the moderate and severe scenarios, the attack windows are set to 4 and 8 attack inputs, correspondingly.

4. Title: Autonomous Signal-Situational-Awareness (SSA) in a Terrestrial Radionavigation System
Authors: Ronnie X.T. Kor, Peter A. Iannucci and Todd E. Humphreys
Affiliation: University of Texas at Austin

Extended Abstract:
Global navigation satellite systems (GNSS) struggle to provide coverage in deep-urban and indoor environments. Current and upcoming terrestrial radionavigation systems (TRNS) like Locata and NextNav seek to address these needs by locating powerful ranging beacons throughout the urban environment. Just as GNSS faces fundamental challenges in signal authentication and anti-spoofing, so does TRNS. Many of these vulnerabilities are shared between the two domains because they arise from fundamental properties of radio systems. However, TRNS operates in a quantitatively distinct region of parameter space: security code estimation and replay (SCER) attacks are amplified by attackers' access to high signal-to-noise ratio (SNR) and ultra-low-latency signal replicas; receiver quantization and dynamic range effect limit mitigations based on simultaneous demodulation of spoofed and authentic waveforms; and the potential for poor spatial and angular separation between authentic and spoofed signals renders controlled reception pattern antenna (CRPA)-based solutions far less effective.

Extensive scholarship concerning GNSS vulnerabilities largely carries over to TRNS. In addition, TRNS has its own unique vulnerabilities that have been recently outlined. Nevertheless, novel commercial TRNS' clean-slate design offers an opportunity to exploit unique advantages for enhanced security. These new security measures can leverage the best spoofing defenses produced by two decades of research effort in securing GNSS.

Radionavigation security includes both cryptographic and non-cryptographic techniques. These techniques represent an overlapping and layered defense against spoofing: receivers should like to identify reliable signals both by their content and by their context. In this framework, one may envision two types of receivers with differing needs: mobile users, and infrastructural monitors. Previous work proposed a multi-tiered navigation message encryption (NME) + message authentication code (MAC)-leavened navigation message authentication (NMA) scheme. NME is used for selective availability and enhanced data security. However, the exposed spreading codes of a high-SNR TRNS signal makes it trivial to replicate the embedded spreading codes in a SCER or meaconing attack: that is, NME+NMA cannot fully protect against ultra-low-latency record-and-replay attacks.

To address the gap in the defense against such attacks, this paper proposes an autonomous signal-situational-awareness (SSA) overlay function within the TRNS network. The SSA function augments basic

TRNS operations with cooperative monitoring among adjacent beacons. While not all spoofers can be detected in this way, SSA gives TRNS operators the best possible chance of detecting threats and warning users without resorting to costly full-duplex techniques. This type of autonomous SSA would not be possible for GNSS space vehicles in medium Earth orbit, which can neither hear each others' signals nor detect low-power ground-based spoofers. This work seeks to place SSA on a solid theoretical and practical footing. First, signal authentication techniques for SSA are developed based on the prior works. Second, simulations with theoretical model of multipaths and spoofing signals will quantify the effectiveness of autonomous SSA under some of the myriad operating conditions encountered by a generic TRNS.

With resilient cryptographic scheme and autonomous SSA, TRNS will be able to advance the security of PNT beyond what is achievable with traditional civil GNSS. While perfect defense is not possible in radionavigation, TRNS has the potential for a quantum leap in mitigation of man-in-the-middle (MITM) attacks on PNT.

5. Title: Multi-Constellation GNSS Integrity Monitoring Fused with Terrestrial Signals of Opportunity for Vehicular Navigation in Urban Canyons

Authors: Mu Jia[1], Halim Lee[2], Joe Khalife[1], Jiwon Seo[2], and Zaher (Zak) M. Kassas[1]
Affiliation: University of California, Irvine[1]; and Yonsei University, Korea[2]

Extended Abstract:

In recent years, many applications based on the global navigation satellite systems (GNSS) emerge in the urban environment, including safety-critical ones, such as intelligent transportation systems. The safety of the passengers riding autonomous ground vehicles (AGVs) depends on the accuracy and reliability of the navigation system. With the navigation accuracy keeping improving, the concept of integrity also attracts more and more attention from urban users. This is because positioning using GNSS signals can be unreliable in deep urban canyons, due to the blockage, reflection or diffraction of the GNSS signals by the buildings. Recently, fusing signals of opportunity (SOPs) in GPS navigation systems has been proven to improve the accuracy and integrity of navigation solutions, when GPS signals become unavailable or degraded. To further improve the navigation integrity in the GNSS-challenged urban environments, this paper proposes an integrity monitoring (IM) framework incorporating multi-constellation GNSS and SOP measurements. The performance of this IM framework will also be characterized through numerical simulations and verified by experiments.

For AGVs, knowing the trustworthiness of the navigation solution is of great importance. In order to safely navigate in urban environments, autonomous vehicles needs to tightly bound the navigation errors and ensure that the probability of navigation errors not properly bounded is below a certain limit. However, the urban environment brings great challenges to the current ground vehicles' navigation systems. This is mainly because the GNSS positioning performance can be severely degraded by the limited satellite visibility, multipath effect, and interference. Research has been done to mitigate the multipath effects and non-line-of-sight (NLOS) error at different levels, such as the antenna design techniques, the receiver-based techniques, as well as the post-receiver techniques, Recent work has shown SOPs' capability as a complement or alternative to GNSS signals in GNSS-challenged environments. Different SOPs, e.g. cellular signals, digital television signals, AM/FM radio signals, and low Earth orbit satellite signals are exploited to produce navigation solutions in a standalone fashion or as an aiding source for an INS in the absence of GNSS signals. For vehicular navigation, cellular signals are particularly attractive with their favorable characteristics, such as abundance in urban canyons, geometric and spectral diversity, high received power, and large bandwidth. Cellular signals have been demonstrated to achieve meter-level accuracy for ground vehicles in a standalone fashion and lane-level localization accuracy fused with lidar data.

Aside from improving navigation accuracy, introducing IM to urban GNSS receivers has also been studied intensively. Among the IM frameworks, receiver autonomous integrity monitoring (RAIM) is exceptionally attractive, as it is a cost-effective technique which does not require building additional infrastructure. Multi-constellation measurements (e.g. Galileo, GLONASS, and Beidou) and aiding sensors (e.g., INS-GPS, lidar-GPS and vision-GPS) have been incorporated to improve IM performance. In addition, several SOP-

based IM studies have been conducted recently. Cellular SOPs have been characterized and outlier detection and exclusion methods have been developed to deal with environment-induced faults, such as severe multipath conditions. GPS-SOP RAIM was proposed to support safe autonomous driving. GPS- SOP RAIM was also considered to improve the IM of unmanned aerial vehicles (UAVs). The protection level reduction for ground vehicles was shown to be possible even with highly unreliable SOPs.

While multi-constellation GNSS and cellular SOPs have been exploit to improve navigation integrity, they have not been incorporated together for IM. Since the redundancy of the measurements is essential for the RAIM-based IM framework, incorporating more measurements in a favorable source/user geometry could significantly enhance the performance of the integrity monitoring. Increasing the number of GNSS signals by using GLONASS, Galileo, and Beidou can significantly improve the availability of navigation signals. On the other hand, incorporating SOPs will help compensate the vulnerability of GNSS signals and provide more geometric diversity. This paper makes three contributions. First, a framework based on advanced RAIM (ARAIM) is proposed to incorporate multi-constellation GNSS and cellular SOPs. Second, the integrity performance after fusing different GNSS constellations and SOP pseudorange measurements will be characterized and compared to support future IM algorithm design. Third, field experiments will be conduct to validate the performance evaluation.

6. Title: Collaborative Navigation to Detect PNT System Operational Anomalies

Authors: Charles Toth and Dorota Grejner-Brzezinska
Affiliation: The Ohio State University

Extended Abstract:

Conventional GNSS-based PNT systems are increasingly becoming susceptible to RF interference, which could be both intentional or deliberate, and the threat of jamming and spoofing is not theoretical anymore. As technology keeps advancing and hardware is becoming so inexpensive, it takes a modest effort to disrupt the normal operation of almost any PNT systems, posing hazard to transportation systems, but in particular, this situation presents an extreme threat for autonomous systems. Finding protection against any interference to PNT systems is happening on multiple levels. GPS modernization has introduced new signals, providing significant capabilities to increase protection on both signal and receiver level. In parallel, the proliferation of GNSS systems in the past decade has substantially increased the signal availability, so PNT systems using all the potentially available signals can exploit the benefits of redundancy. Nevertheless, there are limits what can be done against RF interference in PNT systems, and therefore, using totally independent sensor technologies is mandatory to detect malfunctioning and potentially offering mitigation to some extent. Sensor integration is the general approach to increase reliability; in fact, modern PNT systems are typically based on GNSS signal and IMU sensor integration. More recently vision-based systems, including both active and passive imaging sensors have become popular as they can provide very good performance for relative positioning and navigation. As communication capabilities are expanding, a group of vehicles can easily share data when they operate in close vicinity. This gives opportunity to position and navigate the vehicles based on a jointly computed navigation solution, resulting in a potentially more accurate and reliable operation. This method, usually called collaborative navigation is considered here for detecting any malfunctioning of a GNSS-based PNT system due to any reason, such as hardware problem, jamming or spoofing. The model we are investigating assumes the availability of communication and range measurements between the vehicles. The communication method could be V2V, V2I or V2X in general, and no raw data is shared on general navigation parameters. The ranging measurements can come from different sensors, including LiDAR, RADAR, UWB, vision, etc. Note that some RF sensor can do both communication and ranging. In this study, both simulated and real data will be used for assessing the feasibility and performance potential of data sharing in collaborative vehicles scenarios. Obviously, the ranging measurements can be extended to other traffic participants and infrastructure, and thus absolute positioning information can be exploited too.