Robust Estimation of Connected Automated Vehicles While Performing Cooperative Tasks in Presence of Malicious Agents

Roberto Merco
Clemson University International Center for Automotive Research, Greenville, SC, 29607, USA
rmerco@clemson.edu

ABSTRACT

This research focuses on the identification and mitigation of malicious vehicles in cooperative tasks between automated connected vehicles. The approach aims to design estimators which employ the number and diversity of sensors that autonomous vehicles are equipped with in order to enrich the knowledge of the surrounding environment of each vehicle in the wireless communication network range. Since an event-triggered communication network is considered to increase the overall performance of the communication channels, the estimators have to be designed to take into account aperiodic and asynchronous measurements.

1. PROBLEM STATEMENT

Autonomous vehicles are equipped by a full set of sensors as GPS, Inertia Measurement Unit (IMU), lidars, radars, depth sensors, cameras and ultrasonic sensors (Figure 1). Those devices are integrated inside the vehicles in such a way to obtain the real-time knowledge of vehicle's location and vehicle's surrounding environment by a suitable sensor fusion. The awareness of location and environment obtained by the onboard sensors is limited and varies with respect to environment conditions as weather and obstacles like other vehicles or road and land topologies.

To enhance their awareness range, the autonomous vehicles will employ vehicle to vehicle (V2V) communication technology [2], which enables a multitude of new cooperative applications by helping vehicles to broadcast data, such as location, direction and speed to nearby vehicles. Among these cooperative applications are worth mentioning convoy driving, such as Cooperative Adaptive Cruise Control (CACC), cooperative lane change/merge and cooperative intersection management. In each of these applications, the knowledge of other vehicles position, velocity and heading is fundamental to achieve high level of cooperation and to improve performances of the overall task. Each vehicle runs its own control law designed to control the vehicle dynamics by using its awareness of the surrounding environment and vehicles, which is obtained through on-board sensors and the data broadcast by the neighbor cars.

Exchanging data among vehicles exposes vehicles to network vulnerabilities such as unreliable network, as packet dropping and communication delays, as well as malicious entities (or agents) whose goal is to interact with other vehicles to interfere with the task of the cooperation by achieving malicious targets as collisions or degradation of performances. For example, by referring to the case of lane merge, a malicious agent driving in the highway can share its fake data regarding its position, velocity and heading with the purpose of making the merging vehicle believe that the approaching malicious car is either farther or slower than it is. In such a scenario an uncomfortable situation for the passengers of the vehicles, or a collision where the passengers are involved can be generated. This kind of malicious behavior could be exploited by hackers or manufacturers of autonomous fleets to illicitly decrease the market of the competitors.

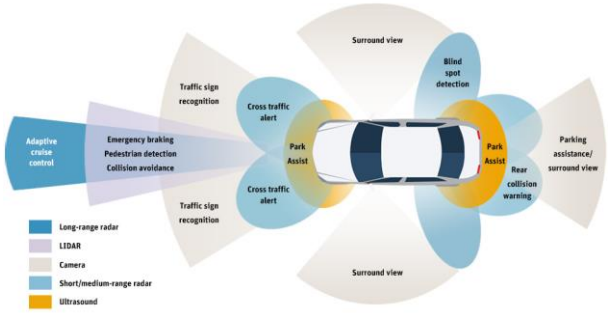

Figure 1 Automotive sensors and representation of their range and applications [1].

Even though the autonomous vehicles would be equipped by several sensors, it is still possible to face some circumstances where the topology of the road or other obstacles could limit the visibility range of the sensors. In such a situation, the information coming from the V2V network would be important for the autonomous vehicle control algorithm to complete its task.

Furthermore, the wireless communication network is affected by imperfections induced by the digital nature of the communication network: the communication is based on packets sent through a channel which has a limited bandwidth and it is subject to communication delays and packets dropping. As shown in [3], in case of

cooperative tasks as the CACC communication imperfections as delays can influence the performance of the CACC system. Thus, the best way to employ the communication network without degrading the performance of the cooperative task would be employing the highest as possible transmission rate and the lowest delays. These properties can't be achieved at the same time since the high communication rate degrades the reliability of the wireless channel and decreases the transmission delays as reported in [4]. This can be considered as a further network restriction whenever the vehicles involved in the V2V network start broadcasting a large amount of information which leads to a decreasing quality of the network itself. The network limitations mentioned above have been addressed in networked control systems by using event-triggered communications; this framework has been used in multi-agents control system and one application on connected vehicles can be found at [5]. In such a framework, each vehicle broadcast information whenever conditions related on its dynamics is triggered. Since the communication triggers are related to the vehicles dynamics of each car, it is expected that the information is sent at different time instants, which leads to consider controllers and estimators algorithms to run by relying on asynchronous time of arrival of each packet.

2. EXPECTED CONTRIBUTIONS

The significance of the topic pertains to maintain the health of connected vehicles in case a malicious car is broadcasting fake information through a V2V imperfect network characterized by aperiodic and asynchronous data. The identification and mitigation of malicious behavior is based on estimator design that employs each connected vehicle as a node in a dynamic wireless sensor network. The number of sensors that are installed on autonomous vehicles leads to a richness of information about the surrounding environment that can be shared by each car in the V2V network. By receiving this information, each vehicle must be able to elaborate the V2V information and derive its own enlarged environment awareness while being robust to network imperfection and while being robust to the a-synchronicity of the received data.
In the following the vehicle where the estimation is running is named as ego-vehicle.

2.1 Modeling

Each vehicle can be represented by a kinematic car-like model (Figure 2), with a nonholonomic constraint that restricts the wheels to roll with no slip.
The vector $p_c = (x_c, y_c, \theta_c)$ denotes the configuration of the vehicle, where (x_c, y_c) is the location of the midpoint of the rear axle, θ_c is the angle between the x-axis and a reference line on the vehicle frame that identify the heading direction of the vehicle. Let the control $u = (a_c, \omega_c)$ where a_c is the longitudinal acceleration and ω_c the angular velocity of the rigid body around the center O. The vehicle's motion state is then

$$\dot{\psi}(t) = \begin{bmatrix} \dot{x}_c(t) \\ \dot{y}_c(t) \\ \dot{\theta}_c(t) \\ \dot{v}_c(t) \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & \cos\theta_c(t) \\ 0 & 0 & 0 & \sin\theta_c(t) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_c(t) \\ y_c(t) \\ \theta_c(t) \\ v_c(t) \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_c(t) \\ \omega_c(t) \end{bmatrix}$$

which can be rewritten as $\dot{\psi}(t) = f(t, \psi(t), a_c(t), \omega_c(t))$.

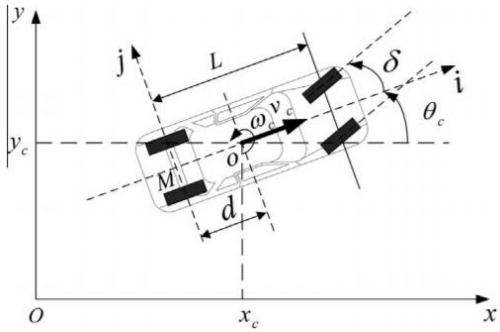

Figure 2 Kinematic Vehicle Model [6]

Each vehicle is assumed to be able to measure its own position, velocity and heading and to estimate the same dynamics variables of the surrounding vehicles, whenever they are within the sensors range.

2.2 Information shared between vehicles

Vehicles information is broadcast through the wireless communication network. Furthermore, each vehicle is assumed to be equipped by sensors like lidar, radar, cameras, ultrasonic sensors and depth cameras which allow the car to identify and to reconstruct the surrounding environment in order to have an estimation of the vehicles around itself.
As discussed in the previous session, in order to increase the performance of the V2V communication network, each vehicle is broadcasting information accordingly to an event-triggered mechanism, where the transmission instants are determined online by a "smart" triggering conditions which depend on, for example, output measurements of the system. In such a way, transmissions are scheduled when needed to guarantee safety and performance properties. See [7] for recent overview on event-triggered control systems.

2.3 Resilient estimation of malicious agents

The ego-vehicle receives all the information regarding other vehicles in the V2V network and their surrounding cars. By employing the knowledge of the topology of the road and its position and velocity, the estimation algorithm of the ego-vehicle can ignore the information that is not related to cars that are not interacting with for the cooperation purpose. The remaining data, along with

the information coming from the cooperative vehicles (which might be malicious), can be used to improve the estimation of the vehicles needed for the cooperative task.
Each surrounding vehicle to be estimated can be modeled by

$$\dot{\psi}_j(t) = f(\psi_j(t), a_{c_j}(t), \omega_{c_j}(t))$$
$$\phi_{onB}(t) = g_{onB}(\psi_j(t), a_{c_j}(t), \omega_{c_j}(t))$$
$$\phi_{i_{V2V}}(t) = g_{i_{V2V}}(\psi_j(t), a_{c_j}(t), \omega_{c_j}(t))$$

Where ϕ_{onB} and $\phi_{i_{V2V}}$ are the set of measurements available for the estimation. ϕ_{onB} are the measurements coming from the on-board sensors of the ego-vehicle and $\phi_{i_{V2V}}$ are the measurements of the same surrounding vehicle coming from the other cars involved in the same V2V network; i represents the index of the sending vehicle.
Due to the dynamicity of the vehicular formation, the on-board sensors of the vehicles might not be able to detect the vehicle needed for the cooperation. Thus, the measurement sets ϕ_{onB} and $\phi_{i_{V2V}}$ might not be always all available. Furthermore, unlike the onboard measurements of the ego-vehicle which are available at periodic high rate, the information coming from the other vehicles has different time of arrival due to the even-triggered communication. Hence, the ego-vehicle estimator needs to be designed to handle properly these aperiodic and asynchronous measurements.
Comparing the estimation of the cooperative vehicles by using data of the vehicle sensors network and the information sent by the actual cooperative vehicles, it is possible to evaluate the trustworthiness of the received data and then identify the malicious car. The malicious vehicle is identified by comparing the information it sent with its estimation elaborated by the ego-vehicle using data sent by other cars in the V2V network. In such a way the detection algorithm is applying a consensus strategy to verify the data sent by each cooperative vehicle.

2.4 Broader impact

Goal of the research is to achieve results which are not specific to the selected application but can be easily applied and extended to many other multi-agent applications where a reliable estimation of the agents is sensitive.

3. RESEARCH PLAN

The research problem stated in this paper incorporates two main researches topic: event-triggered estimation and asynchronous estimation. Even-triggered based estimation defines its own triggers without relying on the triggering conditions already employed by the event-triggered controller, while the asynchronous estimation algorithms are based on timestamps knowledge (which is another source of potential cyber-attack) and put limitation in observability of the system which has never been studied within the even-triggered framework. The research will enrich the performance of the existing algorithms to achieve a robust estimation.

3.1 Work Performed

This PhD project started with modeling each vehicle as a double integrator in a static formation in a plan and by considering no network imperfections and periodic but asynchronous measurements.

3.2 Remaining Work

Future work will enlarge the connected vehicle case study by: adding aperiodic measurements, network imperfection in a static formation. A dynamic formation will follow where nonlinear dynamics will be also included in the model.

4. CONCLUSION

In this research the identification and the mitigation of a malicious vehicles in cooperative tasks which involve connected automated vehicles is proposed.
The architecture of a robust estimator to aperiodic and asynchronous measurements as well as to network imperfection is introduces.

REFERENCES

[1] https://www.ansys.com/ko-kr/about-ansys/advantage-magazine/volume-xii-issue-1-2018/autonomous-vehicle-radar

[2] NHTSA, "U.S. DOT advances deployment of Connected Vehicle Technology to prevent hundreds of thousands of crashes," 13 December 2016. [Online]. Available: https://www.nhtsa.gov/press-releases/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands.

[3] M. di Bernardo, A. Salvi, and S. Santini, “Distributed consensus strategy for platooning of vehicles in the presence of time-varying heterogeneous communication delays,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 1, pp. 102–112, Feb. 2015.

[4] T. Batsuuri, R. J. Bril, and J. J. Lukkien, Model, Analysis, and Improvements for Inter-Vehicle Communication Using One-Hop Periodic Broadcasting Based on the 802.11p Protocol. New York, NY, USA: Springer, 2015.

[5] Dolk, Victor S., Jeroen Ploeg, and WP Maurice H. Heemels. "Event-triggered control for string-stable vehicle platooning." IEEE Transactions on Intelligent Transportation Systems 18.12 (2017): 3486-3500.

[6] You, Feng, et al. "Trajectory planning and tracking control for autonomous lane change maneuver based on the cooperative vehicle infrastructure system." Expert Systems with Applications 42.14 (2015): 5932-5946.

[7] W. P. M. H. Heemels, K. H. Johansson, and P. Tabuada, Event-Triggered and Self-Triggered Control. London, U.K.: Springer, 2013.