Vehicle Trust Management for Connected Vehicles

FINAL RESEARCH REPORT

Insup Lee (PI), Nicola Bezzo, Jian Chang

Contract No. DTRT12GUTG11

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the U.S. Department of Transportation's University Transportation Centers Program, in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof.

Problem:
The goal of this project is to research a wide range of transportation-related issues including: improving health and safety for all users of the transportation system, including bicycles, pedestrians and transit modes; reducing carbon emissions and other environmental impacts of transportation through a transition to zero-emission vehicles and fuels; and evaluating how increasingly autonomous vehicles affect driver behavior, safety and performance.

Consider a scenario where a vehicle on a highway broadcasts a message with an incident report (e.g., accident, traffic congestion, broken bridge) to the vehicles immediately behind it using the underlying V2V network. Each receiving vehicle forwards the message further downstream. Additionally, if a forwarding vehicle (that is, the user driving it) believes the message itself, it will endorse the message by signing it. A vehicle originating an incident report will always endorse it. Consequently, a vehicle receiving a V2V incident report will have at least one endorsement associated with it. Upon receiving an incident report, a vehicle needs to make a decision on whether it trusts the report based on all the vehicles that have endorsed the report. This decision is taken based on: (1) a trust triple computed for each of the endorsers, and (2) combining the individual endorser trust triples to produce an aggregate trust score for the message.

Approach:
To solve the problem above, we build an adaptive recursive estimator (RAE), which uses a filter approach to estimate the state while reducing the malicious effects introduced by an attacker.

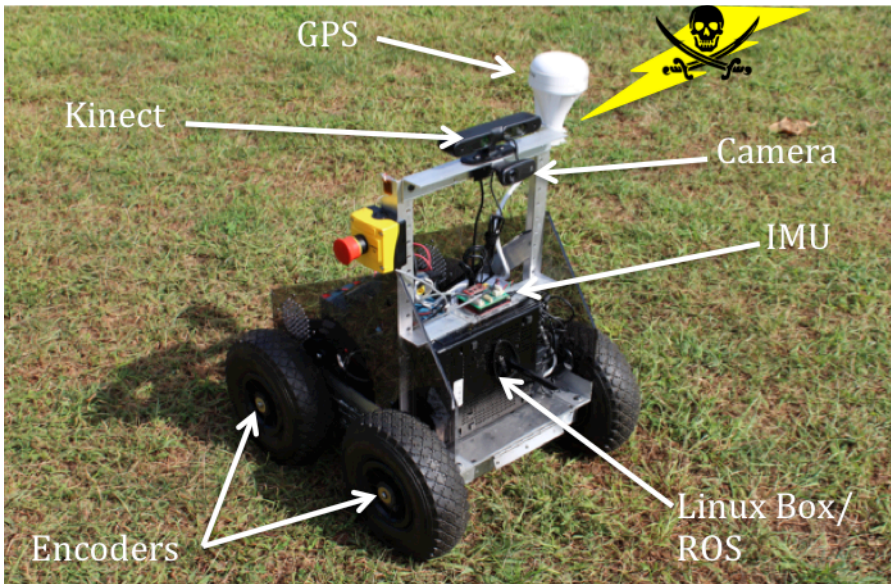


Figure 2: Experimental vehicle platform used to test the attack detection/mitigation scheme developed for this project.

Methodology:

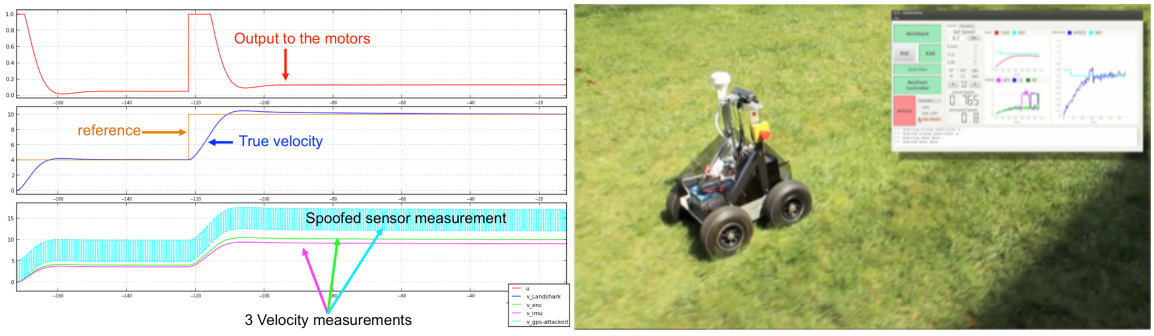
Our recursive algorithm is motivated by the results found in the Kalman Filter implementation with some modifications to accommodate the possible presence of an attack in one of the sensors. Together with the *prediction* and *update* phases found in the Kalman implementation we include a *shield* procedure. If an attack is present and such that one of the measurements is corrupted, the goal is to remove it or mitigate its effect. Since the attack vector is generally unknown, the strategy we implement changes the covariance matrix associated with the measurement error in order to increase the uncertainty where the measurement is different from the predicted state estimate.

Our formulation is hierarchical and use feedback to control the motion of the vehicle and achieve the desired state. Specifically the application focus of this work is cruise-control for ground vehicles. Each sensor measures a specific environmental variable correlated with speed. The sensor measurements are passed to a security module, which is in charge of attack detection and state estimation and outputs an estimate of the velocity of the vehicle. The estimate is sent to a controller (in our application a P.I.D. loop) that returns the control inputs to drive the actuators to the desired state.

Findings:

Several data were collected to extract the dynamical model of the vehicle. These tests were conducted on different type of surfaces both indoor and outdoor and, as a result, a seventh order model was extracted that capture both the electromechanical and kinematical constraints of the vehicle.

Extensive simulations run in Matlab/Simulink (Fig. 2(a)) has shown that the vehicle can reach and maintain the desired state even when one of the sensors is compromised by a malicious attack. Specifically we showed that if less than N/2 sensors are under attack, we can estimate the correct state of the system and maintain the desired cruise speed.



(a) (b)

Figure 2: Results from when GPS signals are spoofed and the performance of the autonomous vehicle.

The trust on an endorser is computed as a triple (t, c, f). Here, t is the measured reputation value computed based on the endorser's history of providing a correct and incorrect endorsement. It could be measured as simply as (# of endorsements of factual reports/total # of endorsements) assuming independence of individual endorsements. The value c is the

level of confidence on the measured reputation t, computed based on the goodness of fit of the distribution of the endorser's behavior to a specific user behavior. Finally, f is the default reputation value that is essential to reason about reports received from a vehicle that does not have any historical information available for it. The value of f is computed using static information about the endorser such as (1) vehicle make (e.g., Ford, BMW, etc.), (2) vehicle model (e.g., Corolla, Focus, etc.), (3) vehicle history (e.g., Carfax report), (4) vehicle type (e.g., ambulance, police car, etc.), (5) context information (e.g., current location: North Philly; current time: 2:00am). The vehicle uses the V2I network to obtain the static information about the endorsers, usually from the registration authority that assigns vehicle ids. Additionally, the user specifies policies to determine f, by explicitly stating its value for various combinations of static and contextual information.

Conclusions:

Thanks to the large availability and quality of modern sensors and the high CPU computation power, modern vehicles are becoming more and more autonomous increasing the overall driving comfort. However these vehicles are not built with security in mind. In fact hackers could compromise vehicle safety by spoofing sensors or by injecting malicious/malformed data through their network system.

In our work we investigate techniques to detect and defend against malicious cyber attacks on modern vehicles. Our first target has been to develop techniques for one vehicle. Now that we have developed reliable attack resilient techniques for one system, we are expanding the current research to incorporate multi-vehicle networks interacting with each other using V2V and V2I technologies.

Recommendations:

Future work will focus on extending the proposed technique on multi-vehicle systems incorporating V2V (vehicle-to-vehicle) and V2I (vehicle-to-infrastructure) protocols. We are also targeting more complex hardware implementation such as adaptive cruise control, waypoint navigation, and complex attack vectors on both sensors and actuators as well as experimenting with passenger automobiles.