REAL-TIME SENSOR ANOMALY DETECTION AND RECOVERY IN CONNECTED AUTOMATED VEHICLE SENSORS

Yiyang Wang
yiyangw@umich.edu

Neda Masoud
nmasoud@umich.edu

Anahita Khojandi
khojandi@utk.edu

Word Count: 1108 words + 3 table(s)

Submission Date: January 7, 2020

Keywords: Cyber-physical systems, Fault diagnosis, Intelligent vehicles, Car-following model, Vehicle safety, Anomaly detection, Signal filtering

INTRODUCTION

In this paper we propose a novel observer-based method to improve the safety and security of connected and automated vehicle (CAV) transportation. Toward this end, we develop a anomaly detection method that seeks to minimize both false negatives and false positives by utilizing the trajectory of the leading vehicle of a CAV, thereby capturing the reaction of the CAV to changes in the traffic stream. The proposed method combines model-based signal filtering and anomaly detection methods. Specifically, we use an adaptive extended Kalman filter (AEKF) to smooth sensor readings of a CAV based on a nonlinear car-following model. Using the car-following model the subject vehicle utilizes the leading vehicle's information to detect sensor anomalies by employing a set of previously-trained One Class Support Vector Machine (OCSVM) models. This approach allows the AEKF to estimate the state of a vehicle not only based on the vehicle's location and speed, but also by taking into account the state of the surrounding traffic. A communication time delay factor is considered in the car-following model to make it more suitable for real-world applications. Five types of sensor anomalies according to (*1, 2*) are considered. Our experiments show that compared with the AEKF with a traditional χ^2-detector, our proposed method achieves a better anomaly detection performance. We also demonstrate that a larger time delay factor has a negative impact on the overall detection performance.

METHODOLOGY

In this work, we apply an adaptive extended Kalman filter (AEKF) to estimate the state of a vehicle, and use the resulting innovation for anomaly detection. To develop a motion model for AEKF, we recast a car-following model with time delay to describe the motion (also known as state-transition) model. A time delay is applied to the input vector of the car-following model, which represents the communication, sensing, and/or reaction delay. Based on this motion model, we formulate a state-space model with a continuous state-transition model and discrete measurements. The continuous state-transition model represents the intrinsic nature of a vehicle's response to the actions of its immediate downstream traffic, and the discrete measurement model represents the mechanics of sensor sampling, as is the case in practice.

One of the traditional fault detectors used in conjunction with Kalman filter is the χ^2-detector (*3–5*). Since AEKF is a special type of Kalman filter, the χ^2-detector can be seamlessly applied to AEKF as well, as long as the innovation sequence follows a zero-mean Gaussian distribution. However, in practice, the innovation can follow a non-zero mean Gaussian distribution if there is bias in the background (e.g., due to non-zero mean process noise or imperfect model). In the context of our problem, the time delay introduced in the formulation of state-space model can generate such a bias, and the resulting bias would degrade the performance of the χ^2-detector. In such a scenario, the χ^2-detector would not be a good detector since it will generate higher rates of false positives and false negatives. Consequently, we use one-class support vector machines (OCSVMs) (*6*) to adaptively learn the normal boundary of the innovation sequence, which has no requirement for the innovation distribution. Specifically, we train several OCSVM models using normal (i.e., non-anomalous) sensor data with different parameter values (i.e., anomaly percentages). Then we use the pre-trained OCSVM models for detecting anomalies in real-time.

RESULTS

In this section, we use a well-known car-following model, namely the Intelligent Driver Model (IDM), proposed by Treiber et al. (*7*) as the motion model of AEKF. Additionally, we compare the anomaly detection performance of the traditional χ^2-detector and the OCSVM models. The experiments are separately implemented into three scenarios, where scenario 1 contains a χ^2-detector without the IDM motion model, scenario 2 contains the χ^2-detector with the IDM model, and scenario 3 contains OCSVM with the IDM model. Each scenario is implemented under three experimental settings generated by varying the value of the anomaly parameter c_i, where the anomalous readings become more subtle, and generally more difficult to detect, from setting 1 to setting 3. All five anomaly types are randomly injected into the vehicle trajectory.

Tables 1-3 present the AUC values of the three scenarios in our three experiment settings, with time delays of $\tau = 0$, 0.5, and 1.5 seconds, respectively. The experiments indicate that the IDM observer-based fault detection method provides significant improvement (up to 23%) compared with the performance of AEKF without the IDM model, regardless of the value of time delay. Additionally, we can see that OCSVM consistently achieves a better fault detection performance than the χ^2 detector. Results also indicate that there is a degeneracy of performance for each method as the parameter c_i becomes smaller. This observation is in line with intuition, since smaller c_i makes the anomaly more subtle and therefore harder to detect. Additionally, the trends of AUC values indicate that as we increase the time delay, the overall detection performance systemically deteriorates. This suggests that the time delay of the car-following model may have a negative impact on the detection performance.

TABLE 1 AUC OF THREE SCENARIOS WITH $\tau = 0$ SECOND.

	χ^2 without IDM	χ^2 with IDM	OCSVM with IDM
$c_i = 1$	0.9059	0.9723	0.9806
$c_i = 0.1$	0.7764	0.9453	0.9470
$c_i = 0.05$	0.7294	0.9228	0.9357

TABLE 2 AUC OF THREE SCENARIOS WITH $\tau = 0.5$ SECOND.

	χ^2 without IDM	χ^2 with IDM	OCSVM with IDM
$c_i = 1$	0.9024	0.9703	0.9793
$c_i = 0.1$	0.7637	0.9402	0.9452
$c_i = 0.05$	0.7258	0.9118	0.9260

TABLE 3 AUC OF THREE SCENARIOS WITH $\tau = 1.5$ SECOND.

	χ^2 without IDM	χ^2 with IDM	OCSVM with IDM
$c_i = 1$	0.8939	0.9701	0.9782
$c_i = 0.1$	0.7681	0.9201	0.9294
$c_i = 0.05$	0.7208	0.8875	0.8940

CONCLUSION

This paper proposes an anomaly detection method to protect CAVs against anomalous sensor readings and/or malicious cyber attacks. We use an adaptive extended Kalman filter, informed by

not only the vehicle's onboard sensors but also the leading vehicle's trajectory, in order to detect anomalous information. The well-known IDM car following model is used to incorporate the leading vehicle's information into AEKF. Lastly, to improve the anomaly detection performance, and given the fact that using AEKF the innovation is not normally-distributed, we replace the traditionally used χ^2-detector with an OCSVM model. We quantify the effect of these contributions by conducting experiments under three scenarios. Results show that the AEKF enhanced with OCSVM and the IDM model outperforms the traditional χ^2-detector-based anomaly detection used in conjunction with AEKF. Furthermore, our results indicate that by utilizing the leading vehicle's information to inform the AEKF and using OCSVM for anomaly detection, the proposed method can not only effectively filter out the sensor noise in CAVs, but also detect the anomalous sensor values in real-time with better performance than that without utilizing leading vehicle's information. This high performance is showcased by high AUC values in our experiments. Moreover, we study the general relationship between the delay in receiving information and the performance of anomaly detection. We show that as the time delay of signal transmission becomes larger, the overall detection performance deteriorates.

REFERENCES

1. van Wyk, F., Y. Wang, A. Khojandi, and N. Masoud, Real-Time Sensor Anomaly Detection and Identification in Automated Vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 2019.
2. Sharma, A. B., L. Golubchik, and R. Govindan, Sensor faults: Detection methods and prevalence in real-world datasets. *ACM Transactions on Sensor Networks (TOSN)*, Vol. 6, No. 3, 2010, p. 23.
3. Brumback, B. and M. Srinath, A chi-square test for fault-detection in Kalman filters. *IEEE Transactions on Automatic Control*, Vol. 32, No. 6, 1987, pp. 552–554.
4. Bar-Shalom, Y. and X.-R. Li, *Multitarget-multisensor tracking: principles and techniques*, Vol. 19. YBs Storrs, CT, 1995.
5. Geng, Y. and J. Wang, Adaptive estimation of multiple fading factors in Kalman filter for navigation applications. *Gps Solutions*, Vol. 12, No. 4, 2008, pp. 273–279.
6. Schölkopf, B., J. C. Platt, J. Shawe-Taylor, A. J. Smola, and R. C. Williamson, Estimating the support of a high-dimensional distribution. *Neural computation*, Vol. 13, No. 7, 2001, pp. 1443–1471.
7. Treiber, M., A. Hennecke, and D. Helbing, Congested traffic states in empirical observations and microscopic simulations. *Physical review E*, Vol. 62, No. 2, 2000, p. 1805.