Anomaly Detection based on Recursive Least-Square Filter for Robust Intelligent Transportation Systems

Chorok Gwak, Minsu Jo, Seongkyung Kwon, Homin Park, Sang H. Son
DGIST

{chloe.gwak, Minsu-Jo, sk_kwon, andrewpark, son}@dgist.ac.kr

Abstract

For unmanned autonomous vehicles, obstacle detection is one of the most important aspects to support robust collision avoidance systems. In order to prevent collision, autonomous vehicles are equipped with heterogeneous sensors to monitor surrounding environments. While these sensors assist such needs, recent studies have demonstrated that malicious attackers can manipulate them to yield false values and trigger harms. In addition, unintended sensor failures can also cause critical situations where vehicles cannot reliably avoid the collisions. In this paper, we propose a robust collision avoidance system using an Anomaly detection mechanism. Our approach is based on Recursive Least Squares (RLS) filter, which determines a fault sensor value based on Anomaly detection. We deploy our system in an indoor test-bed and demonstrate improved safety in an intelligent transportation environment.

Ⅰ. Introduction

With increasing demands on unmanned autonomous vehicles for intelligent transportations, robust collision avoidance system has become one of the most essential technologies for public safety. In fact, recent studies [8, 9] have proposed the use of heterogeneous in-vehicular sensors to robustly detect obstacles on the road even when a subset of sensors is malfunctioning. Reports indicate that malicious attacks and unintended failures can cause critical incidents that may bring severe fatalities [1, 2, 3].

In this paper, we propose a method that detects malfunctioning sensors based on an Anomaly detection mechanism. Salient aspect of our method is that we employ the Recursive Least-Square (RLS) filter [7] to build a profile for the normal behaviors to quantify the Anomaly of incoming sensor readings. A subset of sensors is determined to be faulty if the Anomaly exceeds a threshold. How to determine the appropriate threshold is a critical issue and we plan to design it based on theoretical models and experiments in the near future.

The rest of this paper is organized as follows. Section II elaborates on the threat models being considered in our study. In Section III, we illustrate the proposed Anomaly detection mechanism. Section IV addresses the evaluation plans. Finally, conclusions are made in Section V.

Ⅱ. Threat Model

Predicting incoming readings and detecting Anomaly can be possible if threat models are profiled using previous data set. Therefore, an analysis of related malicious attack scenarios on in-vehicular sensors and several threat models is needed at first. We look at two specific types the threat models of several previous experiments: 1) malfunctioning sensor attacks, and 2) unintended system failures. In the former, there are several studies that consider attacks on in-vehicular sensors through an empirical lens as observed in [2, 3]. In the latter, Gordeon-Ross [11] and Karimi [10] addressed a fault-tolerant sensor node model in order to detect unintended system failures which can lead to catastrophes. The related studies above conclude that detection of attacked sensors and system failures is needed for robust performance and keeping core functions of each system running. Compared with the related works regarding attack detection mechanisms have been represented in [4, 5], our approach is essential to improve reliability against unforeseen failures and external malicious attacks. Therefore, we consider Anomaly detection over the threat models that have been discussed previously. The classification of Anomaly is needed herein, which is achieved by RLS filter that will be dealt with in Section Ⅲ.

Ⅲ. Anomaly Detection Mechanism

In order to classify an abnormal value among the input sensory data, the RLS filter is applied to Anomaly detection. The RLS filter is a mechanism that makes profiles with previous data set and predict an incoming data. When the real data is read, the difference between the profiled data and the predicted data is quantified. Mateos et al. [6] has addressed that the mechanism is used not only for reducing

complexity and memory requirements but also for tracking non-stationary processes when data models are not available.

We are primarily focusing on what an attack can be injected to the sensory data through a vehicular network. Similarly to our approaches, a system with n sensors measuring the same physical variable is considered, which has been studied previously in [9]. Figure 1 illustrates a way of detection of abnormal value. Compared with the previously profiled values, faulty can be detected as an aspect of algorithm that decides whether the input value is normal or not. When the sensor values are represented by $\Omega = \{s_1, s_2, s_3, \cdots, s_n\}$, normal values have been profiled while the set of Ω receives the sensor values. If a rate of change of error is greater than a threshold in a specific iteration, the value is eliminated with it regarded as faulty. Assuming an average of value of sensors as a normal state, herein, an excursion over a threshold is decided to an Anomaly. After the lapse of seconds, s_1 is regarded as a normal state's sensor when the value is recovered under the threshold.

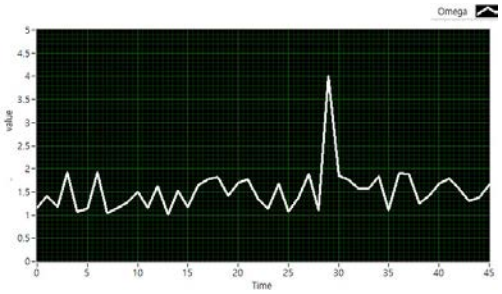

Figure 1 Anomaly Detection

Ⅳ. Evaluation Plan

We implemented an indoor test-bed to examine our collision avoidance system with several robotic platforms. During platooning driving, following platforms depend on ultrasonic sensors to measure a distance between platforms. Even though a malicious input that is injected in the sensory data causes a fault, our collision avoidance system detects faulty depending on RLS filter and uses compromised sensors excluding the attacked sensor to keep core functions running normally.

Ⅴ. Conclusion and Future Work

In this paper, we addressed the concern over collision avoidance. To work on the issue, we first considered a variety of threat models and proposed a method that detects faulty according to Anomaly detection based on RLS filter. An approach to classify faulty was presented based on Anomaly Detection model. The mechanism will be applied to the platforms with compromised heterogeneous sensors. We plan to quantify each fault values, determine an appropriate threshold, and take proper response when the system faces a fatal problem.

ACKNOWLEDGMENT

This research was supported in part by Global Research Laboratory Program (2013K1A1A2A020783 26) through NRF and Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (No. B0101-15-0557, Resilient Cyber-Physical Systems Research).

References

[1] Checkoway, Stephen, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces" Proceeding of USENIX Security Symposium, p. 1-16, 2011.

[2] Karl Koscher, Alexei Czeskis, Franziska Roesner, "Experimental Security Analysis of a Modern Automobile," IEEE Symposium on Security and Privacy, p. 447-462, 2010.

[3] Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study", Proceeding of USENIX Security Symposium, p. 1-16, 2010.

[4] Fabio Pasqualetti, Florian Dorfler, and Francesco Bullo, "Attack Detection and Identification in Cyber-Physical Systems", IEEE Transactions on Automatic Control, Vol. 48, Issue. 11, p. 2715 - 2729, 2013.

[5] Levente Buttyan, Peter Schaffer, and Istvain Vajda, "Resilient aggregation with attack detection in sensor networks", Fourth Annual IEEE International Conference on Pervasive Computing and Communications (PerCom) Workshops, p. 332-336, 2006.

[6] Gonzalo Mateos, Ioannis D. Schizas, and Georgios B. Giannakis, "Distributed Recursive Least-Squares for Consensus-Based In-Network Adaptive Estimation", Proceeding of IEEE Transaction on Signal Processing, Vol. 57, Issue 11, 2009.

[7] Cheng Wang, and Tao Tang, "Recursive least squares estimation algorithm applied to a class of linear-in-parameters output error moving average systems", Applied Mathematics Letters, Elsevier, Vol. 29, p. 36-41, 2014.

[8] Radoslav Ivanov, Miroslav Pajic, and Insup Lee, "Attack-Resilient Sensor Fusion", Proceeding of the conference on Design, Automation & Test in Europe (DATE), No. 54, 2014.

[9] Junkil Park, Radoslav Ivanov, James Weimer, Miroslav Pajic, and Insup Lee, "Sensor Attack Detection in the Presence of Transient Faults", Proceeding of the ACM/IEEE Sixth International Conference on Cyber-Physical Systems (ICCPS), p. 1-10, 2015.

[10] Shahram Karimi, Philippe Poure, Shahrokh Saadate, and Eskandar Gholipour, "Current sensors and power swithes fault detection and compensation for shunt active power filters", IEEE International Symposium on Industrial Electronics (ISIE), p. 3157-3161, 2007.

[11] Arslan Munir, and Ann Gordeon-Ross, "Markov Modeling of Fault-Tolerant Wireless Sensor Networks", Proceeding of 20th International Conference on Computer Communication and Networks (ICCCN), p. 1-6, 2011.