Master's Thesis
석사 학위논문

Achieving Robustness by Anomaly Detection using Multiple Sensors

Chorok Gwak(곽 초 록 郭 俏 攉)

Department of Information and Communication Engineering

정보통신융합전공

DGIST

2016

Master's Thesis
석사 학위논문

Achieving Robustness by Anomaly Detection using Multiple Sensors

Chorok Gwak(곽 초 록 郭 俏 攉)

Department of Information and Communication Engineering

정보통신융합전공

DGIST

2016

Achieving Robustness by Anomaly Detection using Multiple Sensors

Advisor: Professor Sang Hyuk Son

Co-Advisor: Ph.D. Joonwoo Son

by

Chorok Gwak

Department of Information and Communication Engineering

DGIST

A thesis submitted to the faculty of DGIST in partial fulfillment of the requirements for the degree of Master of Science in the Department of Information and Communication Engineering. The study was conducted in accordance with Code of Research Ethics[1]

. . 2016

Approved by

Professor (Advisor)	Sang Hyuk Son	(Signature)
Ph.D. (Co-Advisor)	Joonwoo Son	(Signature)

[1] Declaration of Ethical Conduct in Research**:** I, as a graduate student of DGIST, hereby declare that I have not committed any acts that may damage the credibility of my research. These include, but are not limited to: falsification, thesis written by someone else, distortion of research findings or plagiarism. I affirm that my thesis contains honest conclusions based on my own careful research under the guidance of my thesis advisor.

Achieving Robustness by Anomaly Detection using Multiple Sensors

Chorok Gwak

Accepted in partial fulfillment of the requirements

for the degree of Master of Science.

. . 2016

Head of Committee _____(인)

Prof. Sang Hyuk Son

Committee Member _____(인)

Prof. Haengju Lee

Committee Member _____(인)

Ph.D. Joonwoo Son

MS/IC
201422002
곽 초 록. Chorok Gwak. Achieving Robustness by Anomaly Detection using Multiple Sensors. Department of Information and Communication Engineering. 2016. 48p. Advisor Prof. Sang Hyuk Son, Prof. Haengju Lee, Co-Advisor Ph.D. Joonwoo Son.

ABSTRACT

Modern automotive Cyber-Physical Systems (CPS) are equipped with a variety of vehicular sensors to provide driving convenience (e.g. cruise control systems, navigation systems, and pedestrian detection systems, etc.). However, those systems are vulnerable to the CPS attacks and safety becomes a big recent issue. The malicious sensory data can cause the physical destruction of an actuator, so a robust system against sensor faults is essential for improved safety in Intelligent Transportation Systems (ITS). Therefore, this thesis proposes an anomaly detection mechanism under which performs core functions normally by detecting and filtering out the values from malfunctioning sensors. Herein it is assumed that multiple sensors measure a same physical variable. First, we can detect anomalies among the sensory readings according to the Recursive Least Squares (RLS) algorithm. We show that RLS is more suitable for the real-time operation than Least Mean Square (LMS) algorithm in Adaptive Filter. The RLS algorithm detects the anomalies whose sensor values exceed a threshold. Second, the Iterative Filtering (IF) algorithm determines a reliable average value using the normal incoming sensory readings. The average value is provided to the Proportional-Integral-Derivative (PID) controller, and it (i.e. the current speed) is compared with the reference speed while the vehicle is under the normal cruise control. Without employing the proposed mechanism, according to the experiment, a vehicular model in a simulator had the cruise control system failure and faced a fatal accident. In contrast, the cruise control system under the proposed mechanism operated normally in spite of the injected attack signals. We implemented the robust cruise control system using the combination of RLS and IF algorithms in order to detect anomalies and compute the reliable average value.

Keywords: Robustness, Intelligent Transportation Systems, Safety, Anomaly Detection

Contents

Abstract i

List of Contents ii

List of Figures iii

List of Tables iv

I. Introduction ..... - 1 -

II. System configuration ..... - 4 -

III. Filtering Mechanism ..... - 7 -

3.1. Recursive Least Square (RLS) Filtering Algorithm ..... - 8 -

3.1.1. Comparison between RLS and LMS ..... - 10 -

3.1.2. Anomaly Detection using RLS ..... - 14 -

3.2. Iterative Filtering (IF) Algorithm ..... - 16 -

3.2.1. Appropriateness of IF ..... - 21 -

3.2.2. Reliable Average Decision using IF ..... - 23 -

IV. Experiment and Results ..... - 26 -

4.1. Experimental Environment ..... - 26 -

4.2. Simulation Experiment and Results ..... - 29 -

V. Conclusion and Future Work ..... - 43 -

References ..... - 45 -

List of Figures

Figure 1 Overview of Proposed System ..... - 4 -

Figure 2 System Architecture of Anomaly Detector ..... - 6 -

Figure 3 Configuration of PID Controller ..... - 6 -

Figure 4 RLS Algorithm Flow Chart ..... - 8 -

Figure 5 Convergence Speed of RLS Algorithm ..... - 12 -

Figure 6 Convergence Speed of LMS Algorithm ..... - 12 -

Figure 7 Fidelity of RLS Algorithm ..... - 13 -

Figure 8 Fidelity of LMS Algorithm ..... - 13 -

Figure 9 Anomaly Detection using RLS ..... - 15 -

Figure 10 Concept of IF algorithm ..... - 16 -

Figure 11 IF Algorithm ..... - 18 -

Figure 12 Sensor Readings (Input for IF Algorithm) ..... - 19 -

Figure 13 Average Weights of Sensors ..... - 19 -

Figure 14 Changes of Weights for a Measuring time ..... - 20 -

Figure 15 General Average Computation ..... - 22 -

Figure 16 System Architecture of the Employed IF Algorithm ..... - 23 -

Figure 17 Speed Sensor Value (Input of IF Algorithm) ..... - 24 -

Figure 18 Computed Average (Result of IF Algorithm) ..... - 25 -

Figure 19 Computed Average (Result of General Average Decision) ..... - 25 -

Figure 20 Robotic Simulator, Gazebo ..... - 27 -

Figure 21 Robotic Platforms and Indoor Test-bed ..... - 28 -

Figure 22 Design of the Proposed Mechanism for Cruise Control System ..... - 30 -

Figure 23 Initial Sensory Readings ..... - 31 -

Figure 24 Result of RLS ..... - 31 -

Figure 25 Result of IF algorithm ..... - 32 -
Figure 26 Components and Interfaces in Gazebo ..... - 32 -
Figure 27 Injecting Attack Signals..... - 33 -
Figure 28 Failed Cruise Control System under Attack Scenario ..... - 34 -
Figure 29 Rollover Accidents due to the Attacks ..... - 34 -
Figure 30 Achieving Robust Cruise Control System under Attack Scenario ..... - 35 -
Figure 31 Sensor Readings (Single Anomaly)..... - 37 -
Figure 32 Result of the Proposed System under Single Anomaly ..... - 38 -
Figure 33 Sensor Readings under Transient Multiple Anomalies ..... - 39 -
Figure 34 Result of the Proposed System ..... - 39 -
Figure 35 Result of IF-only System..... - 39 -
Figure 36 Result of the Proposed System ..... - 41 -
Figure 37 Result of IF-only System..... - 41 -
Figure 38 Sensor Readings under Persistent Multiple Anomalies..... - 41 -

List of Tables

Table 1 Notations for Mathematical Procedure of RLS Algorithm..... - 9 -
Table 2 Performance Comparison of the Most Used Adaptive Filters ..... - 10 -
Table 3 Average Readings of Sensors ..... - 19 -
Table 4 Result of the Proposed Average Computation Scheme ..... - 23 -
Table 5 Property of Anomaly Signals..... - 40 -
Table 6 Performance Evaluation on Number of Anomalies ..... - 42 -

I. Introduction

Modern vehicles are equipped with a variety of sensors in an intelligent automotive Cyber-Physical Systems (CPS). The sensors are used for a navigation system, collision avoidance, driver assistance, cruise control, and pedestrian detection, etc. Despite the benefits of the advanced functions of the in-vehicular sensors, the vehicles are exposed to a threat of sensor attacks that result in potential unsafe driving. Koscher et al [1] experimentally demonstrated that it is possible to access car's internal networks via the in-vehicular network and a portable devices such as iPod. Additionally, Rouf et al [2] addressed that a fault sensor and its wrong warning make a driver fall into confusion. They covered an issue of privacy and security implications of Tire Pressure Monitoring Systems (TPMS) and its fake message displayed on a dashboard when an attacker is allowed to spoof sensor messages remotely.

When the core functions depend on the singular sensory data, the system cannot normally operate in danger. The general vehicular systems use a single sensor that measures a variable, however, the sensor will be fairly useless in the attacked or failed situation. Therefore, a mechanism using multiple sensory data becomes essential. We expect that the proposed mechanism will contribute to achieve the robustness of the vehicular systems and to provide the improved safety in ITS.

Many previous works have tried to construct a robust system against the anomalies resulting from attacks and faults. To achieve the robustness for vehicular systems, Ivanov et al [3] proposed a mechanism adapting a sensor fusion algorithm according to the size of the fusion interval. They also formalized attacker's goals and constraints, and implemented their algorithm on an autonomous vehicle case-study. Stavrou et al [4] maintained a normal operation of the system by considering uncertainties of the environments via the fault detection. They applied a

model-based fault detection to mobile robots. When an estimation error is out of a calculated error-bound, a fault is detected.

We aim at achieving robustness in an automotive CPS in spite of anomalies by utilizing multiple sensors that measure a same physical variable. Considering that a system cannot operate normally when one of the sensors is abnormal, a mechanism based on multiple sensors becomes necessary. That is, the approach allows the system to operate normally by running core functions using the sensor values except for the abnormal ones. In this thesis, a method to detect the anomalies and determine an appropriate value for the PID controller to let the system operate normally. When multiple sensor's values are incoming, a fused filtering mechanism which is a combination of Recursive-Least Squares (RLS) algorithm and Iterative Filtering (IF) algorithm is proposed.

This thesis considers two cases: 1) when a majority of the sensors are normal, and 2) when the majority of them are abnormal. The former case can be solved by using only IF algorithm, however, the latter requires the RLS algorithm because normal values may be ignored according to the IF algorithm. Additionally, the RLS algorithm cannot determine a value from values of the multiple sensors. It can determine a value from values of homogeneous sensors. Thus, a scheme that determines a value that is transmitted to a controller is needed. The problem resulting from heterogeneous sensors can be solved by IF algorithm.

According to a paper of Cho et al [5], RLS enables real-time anomaly detection and achieves the minimization of the sum of the squares in the modeling errors. Besides, there is a lot of advantages of using RLS such as redundant and successful identification of the anomaly. In contrast, IF algorithm has used for a data aggregation and data trustworthiness assessment for Wireless Sensor Networks (WSN) in a paper of Rezvani et al [6]. The algorithm is used for

computing a reliable average among multiple sensory values in this thesis, which is an essential procedure to transmit the average value to a controller. In order to evaluate the proposed system experimentally, a scenario was considered, and a simulation test was conducted. Most of the used sensory inputs are synthesized to examine the performance of the proposed mechanism.

Note that there is a delicate difference between ‘Robustness’ and ‘Resiliency’. According to the definition [7], the resiliency applies for the changeable system against faults and attacks. The robustness, on the other hand, is defined as the ability to keep typical operations, and it makes the system function despite abnormal inputs [8]. Therefore, the approaches in this thesis are developed to achieve robustness.

The rest of the thesis is organized as follows. Section II describes a proposed system configuration and its principle in detail. Section III presents RLS algorithm and IF algorithm. In Section IV, a scenario for an experiment and simulation tests are stated. Section V concludes the thesis.

II. System Configuration

An overall structure of the proposed mechanism is illustrated in Figure 1. Herein it is assumed that three sensory readings are received by the automotive CPS and one of them is abnormal. In order to keep core functions of the systems and improve safety, it is important to detect the anomaly. An Anomaly Detector model, which is for identifying the anomalies using previously profiled data sets, has been considered. It also detects the abnormal sensory value, and compromises the sensor readings in order to control the system.

Details of the detection model are shown in Figure 2. There is a precondition for the proposed system that there is at least one normal sensor that did not get attacked. Vehicular sensors transmit theirs values that are the inputs for RLS filtering algorithm, and an error is computed by RLS. The sensory values are likely same each other if the sensors are homogeneous and measure an identical variable. However, the measured values thend to be different if the sensors are heterogeneous. There are various reasons for the difference among the normal sensory values such as a capability of the sensor, a noise and a disturbance in the air. The value exceeding a threshold is regarded as the anomaly, and then the value can be adjusted to any number with a purpose of experimenter in Anomaly Handler in RLS. The adjusted value should

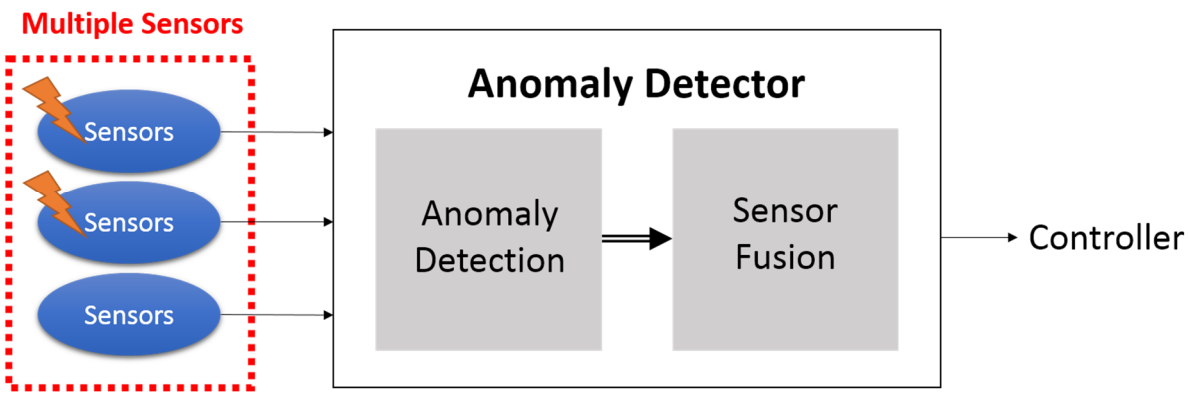


Figure 1 Overview of Proposed System

not affect the compuation of an average in IF algorithm. Anomaly Handler sets the abnormal sensory value around 0 or further down in order to make a classification easier for IF algorithm. The compuation is done while excluding the abnormal sensory readings. Using the rest of the sensors that are ragarded to be normal, a reliable average is computed by the algorithm.

The average value that is computed by IF is transmitted to the controller. It was implemented by using Proportional-Integral-Derivate (PID) model in the controller, which is generally supported by Simulink software. The PID contoller is responsible for deciding whether to increase/decrease the speed of the vehicle according to the acceleration value. In Figure 3, the output means the acceleration value. The cruise control oepartes in a state that the acceleration is close to 0 and a statistic speed is kept during driving. The reference speed is deteremined by a driver. In order to implement the cruise control, the process that finds some parameters (proportion gain, integral gain, and derivation gain) is essential so that this thesis uses PID model that Simulink supports.

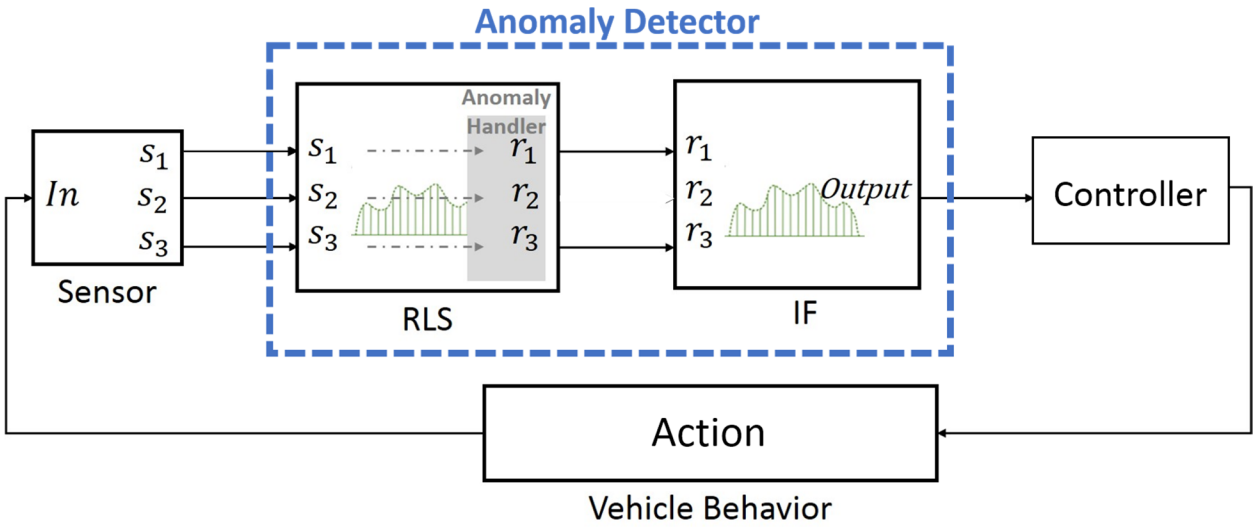


Figure 2 System Architecture of Anomaly Detector

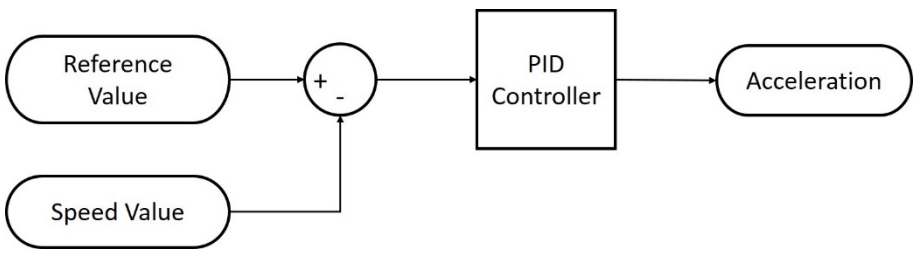


Figure 3 Configuration of PID Controller

III. Filtering Mechanism

This thesis uses RLS algorithm to filter out an anomaly and IF algorithm to compute an appropriate average value from different sensory readings. RLS is known to have the faster convergence speed than Least Mean Square (LMS), which is closely related to the performance of an algorithm. The faster speed herein means the better performance. Furthermore, implementation of the algorithm is easier than Kalman filter algorithm, which can also adapt to a defined system, filter signal noise, and predict signal [9]. The low complexity of the system implementation is related to a computational speed as well as a real-time performance. After an anomaly detection, a scheme to determine an average value that will be transmitted to a controller is needed because the normal values are a little different each other. The general average computation includes normal values as well as abnormal ones, so it is not a reliable scheme. The Median Filtering algorithm computes an average using two values in the middle of them. Therefore, the rest of normal values are excluded. Majority consensus is used to vote a major value, and it can resolve whether the value is true or not, however, it eventually needs another scheme to converge a value. There are no previous works that use both RLS and IF algorithm for anomaly detection in the automotive CPS, so this thesis advances the literature by achieving system robustness by using two aforementioned the filtering algorithms.

3.1. Recursive Least Square (RLS) Filtering Algorithm

This thesis uses RLS in order to identify the abnormal sensory value among the incoming readings. RLS is one of Adaptive Filter family that automatically adjusts a filter parameter and adapts to an unknown signal [10]. It recursively finds filter coefficients that minimize a weighted cost function relating to the input signal. Mateos et al. [11] clarify that RLS algorithm is used for tracking non-stationary processes when data models are not available as well as for reducing complexity and memory requirements. Comparison of the widely used algorithms among Adaptive Filter is done in chapter 3.2. Dhiman [12] analyzed RLS Algorithms in detail, and Patel [13] illustrated a flowchart of RLS algorithm as shown in Figure 4, where $d(n), x(n), y(n),$ and $e(n)$ are the desired, input, output, and estimated error signals, respectively. Notations are summarized in Table 1.

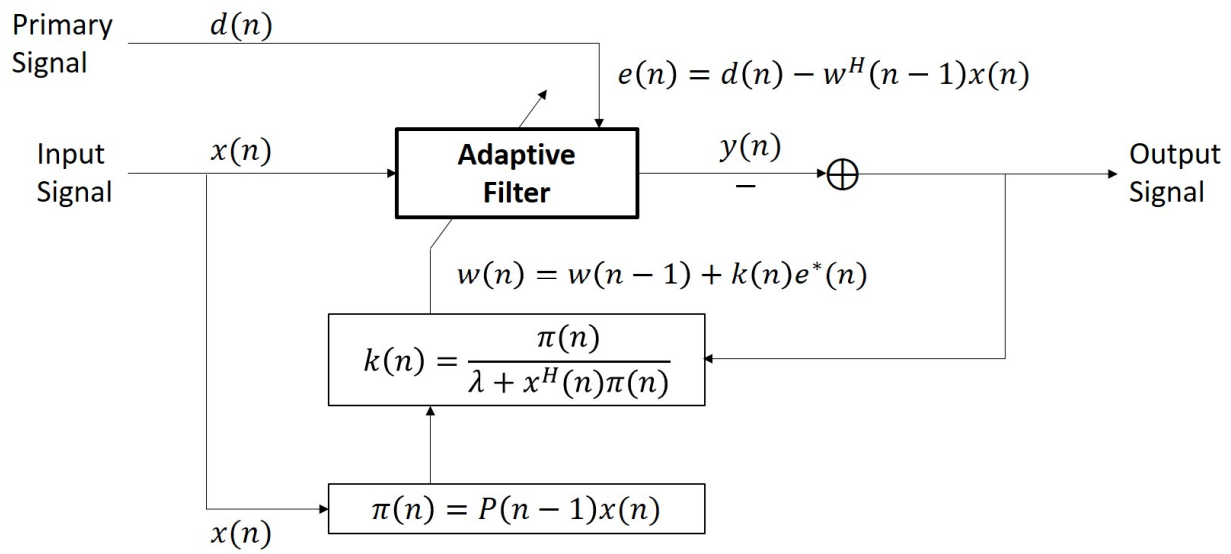


Figure 4 RLS Algorithm Flow Chart

Notation	Meaning
$d(n)$	Desire signal
$x(n)$	Input signal
$y(n)$	Output signal
$e(n)$	Estimated error
$\mathrm{P}(n)$	Inverse correlation matrix
$k(n)$	Gain vector
$\pi(n)$	Intermediary step vector
λ	Forgetting factor ($0 \ll \lambda < 1$)
δ	Regularization parameter
I	Identity matrix of rank $P + 1$
$w(n)$	Weight vector of filter

Table 1 Notations for Mathematical Procedure of RLS Algorithm

RLS algorithm is known as one of least squares methods that recursively compute the filter coefficients that minimize the sum of the squares of the errors [12]. An experimenter can set the constant values: the forgetting factor λ and the regularization parameter δ. The forgetting factor is a small positive constant value between 0 and 1, but it exceedingly closes to 1. It is considered to be more sensitive to recent data samples, and affects the algorithms, convergence and stability. The weight vector and the inverse correlation matrix are initialized as follows.

$$w^H(0) = 0 \qquad \text{…….. (1)}$$

$$\mathrm{P}(0) = \delta^{-1} I \qquad \text{…….. (2)}$$

The following equations are intermediate gain vectors for computing step weights. The gain vector $k(n)$ is computed by the priori estimated error $e(n)$ and updates the weight vector.

$$\pi(n) = \mathrm{P}(n-1)x(n) \qquad \text{…….. (3)}$$

$$k(n) = \frac{\pi(n)}{\lambda + x^H(n)\pi(n)} \qquad \text{…….. (4)}$$

$$e(n) = d(n) - w^H(n-1)x(n) \quad \ldots\ldots\ldots (5)$$

$$w(n) = w(n-1) + k(n)e^*(n) \quad \ldots\ldots\ldots (6)$$

Therefore, the filter vector and the weights are updated, and the inverse correlation matrix $\mathrm{P}(n)$ is computed as in the following equation.

$$\mathrm{P}(n) = \lambda^{-1}\mathrm{P}(n-1) - \lambda^{-1}k(n)x^H(n)\mathrm{P}(n-1) \quad \ldots\ldots (7)$$

3.1.1. Comparison between RLS and LMS

In order to justify the application of RLS algorithm for anomaly detection in this thesis, it is compared with other similar mechanisms. Several previous works compared two commonly used adaptation filtering algorithms: RLS and LMS. Distinguished differences between them are 1) the computational complexity, 2) the speed of convergence to optimal operating conditions, 3) the minimum error at convergence, 4) the numerical stability, and 5) the robustness of the algorithm to initial parameter states according to a study of Vaseghi [14]. A brief comparison is tabulated as follows.

Algorithm	MSE (Mean Square Error)	Complexity	Stability
LMS	1.5×10^{-2}	2N+1 (Less Complex)	Less Stable
RLS	6.2×10^{-3}	$4\mathrm{N}^2$ (High Complex)	High Stable

Table 2 Performance Comparison of the Most Used Adaptive Filters

Selection of algorithms mainly depends on the signal of interest and the operating environment. Especially, the convergence time required and computation power available are important considerations. Table 2 shows that the performance of RLS algorithm is better than that of LMS because of its less MSE value even though the computational complexity of RLS is

higher. In real-time operation, lower time complexity and lower MSE are needed. The reason is that MSE is related to an accuracy of the computations. The bigger MSE implies longer training sequences resulting in lower spectral efficiency. The inaccuracy leads to a poorer steady-state performance. Convergence speed is a significant factor to evaluate the performance of Adaptive Filters. Figure 5 and Figure 6 show the remarkable difference of the convergence speed of RLS and that of LMS, respectively. The ability to estimate the actual filter weights is evaluated for each generated data set. We generated five data sets and examined how quickly each algorithm can estimate the weights. LMS took longer time to converge into the actual weight than RLS, and failed to estimate some weights within the same number of iterations. It took relatively long time for LMS to estimate the right weights. Therefore, in spite of the higher computational order, RLS has faster convergence speed (i.e., the computation would stop at an earlier point). The weight implies gains of each element. Older data has lower weights than newer ones. The order is the number of a regression for each data series. It decides how many most recent data are used for computing the predicted value. Taking large orders can improve the tracking ability but it increases the model complexity. In contrast, taking small orders is computationally simple but it will decrease the tracking ability.

Additionally, there is a different system identification performance between the RLS algorithm and the LMS algorithm as shown in Figure 7 and Figure 8. The simulation was performed under the same coefficient values and the same iteration number. RLS performed higher fidelity than LMS, which means that the estimated value by RLS more accurately matches with the true value than LMS does. LMS algorithm takes longer time to identify the unknown system than RLS does.

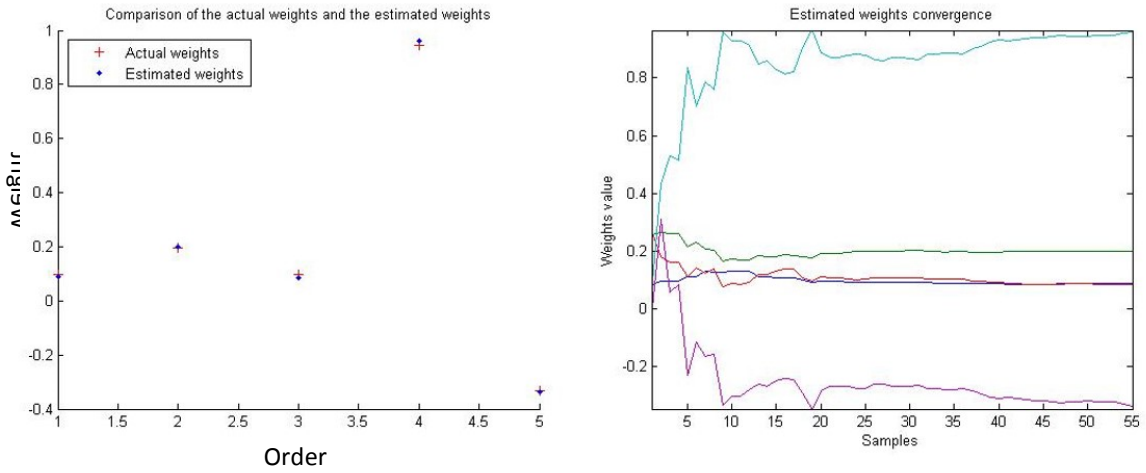


Figure 5 Convergence Speed of RLS Algorithm

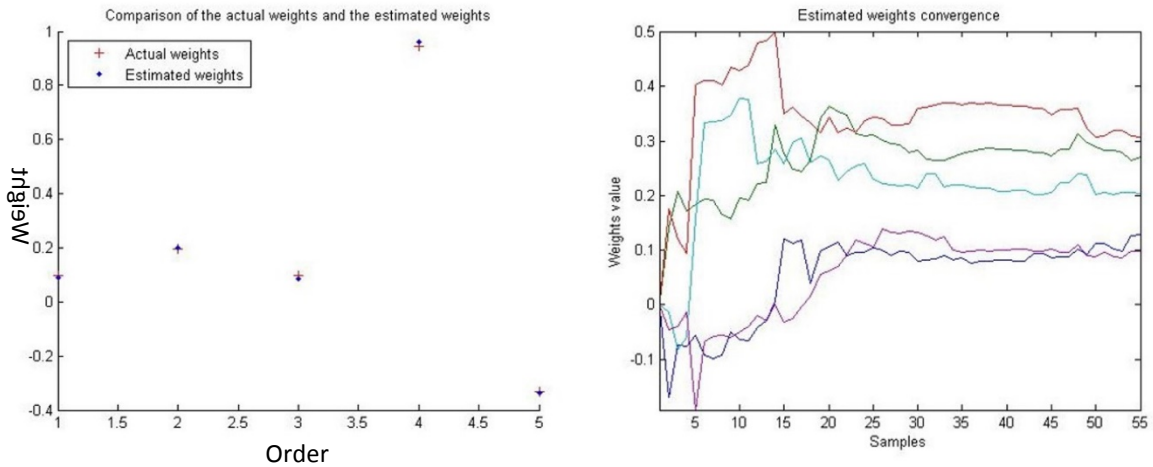


Figure 6 Convergence Speed of LMS Algorithm

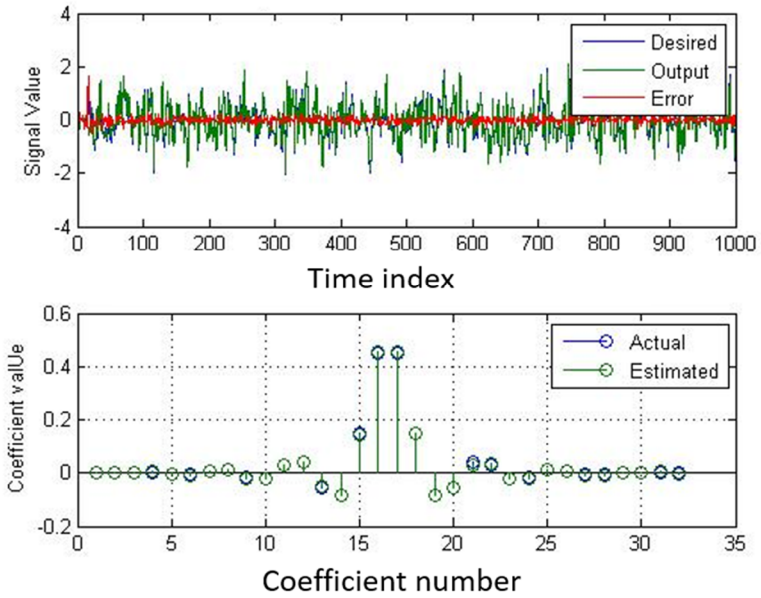


Figure 7 Fidelity of RLS Algorithm

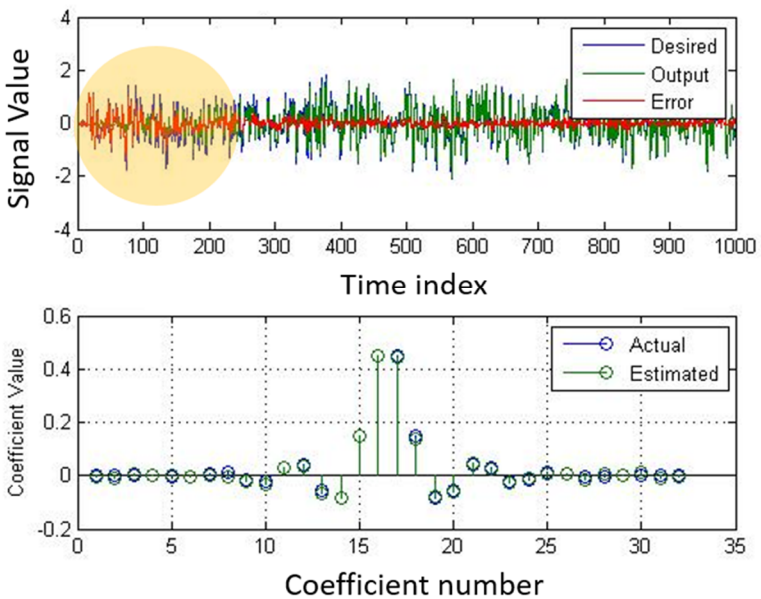


Figure 8 Fidelity of LMS Algorithm

3.1.2. Anomaly Detection using RLS

RLS Algorithm makes profiles using previous data set and predicts an incoming data. A system with n sensors measuring the same physical variable is considered, which is also studied in [15]. There is a previous work [9] that uses RLS to detect abnormality among sensor nodes, however, this thesis focuses on employing the algorithm to the automotive CPS. Figure 9 describes a method of detecting an abnormal sensory value among incoming readings. Compared with the previously profiled values, RLS algorithm determines whether the input value is normal or not, and then the anomaly can be detected. Ω in the following equation includes the sensor values.

$$\Omega = \{s_1, s_2, s_3, \dots, s_n\} \ \textit{s.t.}\ \text{when}\ n\ \text{sensors are used}$$

Normal values are profiled while Ω receives the sensor readings. When the error rate of sensory data is greater than a RLS threshold in a specific iteration, the relevant sensor is regarded to be abnormal. The threshold is determined by a RLS threshold formula using an average, a deviation, and several parameters. Simulation test for examining anomaly detection using RLS algorithm was done by using real ultrasonic sensory data from the sensors built in the robotic platform. A frequency of the ultrasonic sensor is 40 kHz and the estimation is done for about 20 samples each second (required maximum $50m\,sec$). The measuring range is from $1cm$ to $6m$. Total number of samples of the sensory data is 58772, meanwhile, the anomaly is injected by generating the synthesized anomalies. The platform was stopped-state, measuring a distance between a wall and the platform. The sensor readings have intrinsic small errors caused by airflows or noises even under a normal condition. RLS regards those errors to be normal, but prints out the synthesized anomalies as shown in Figure 9. Therefore, the anomaly detection based on RLS is effective.

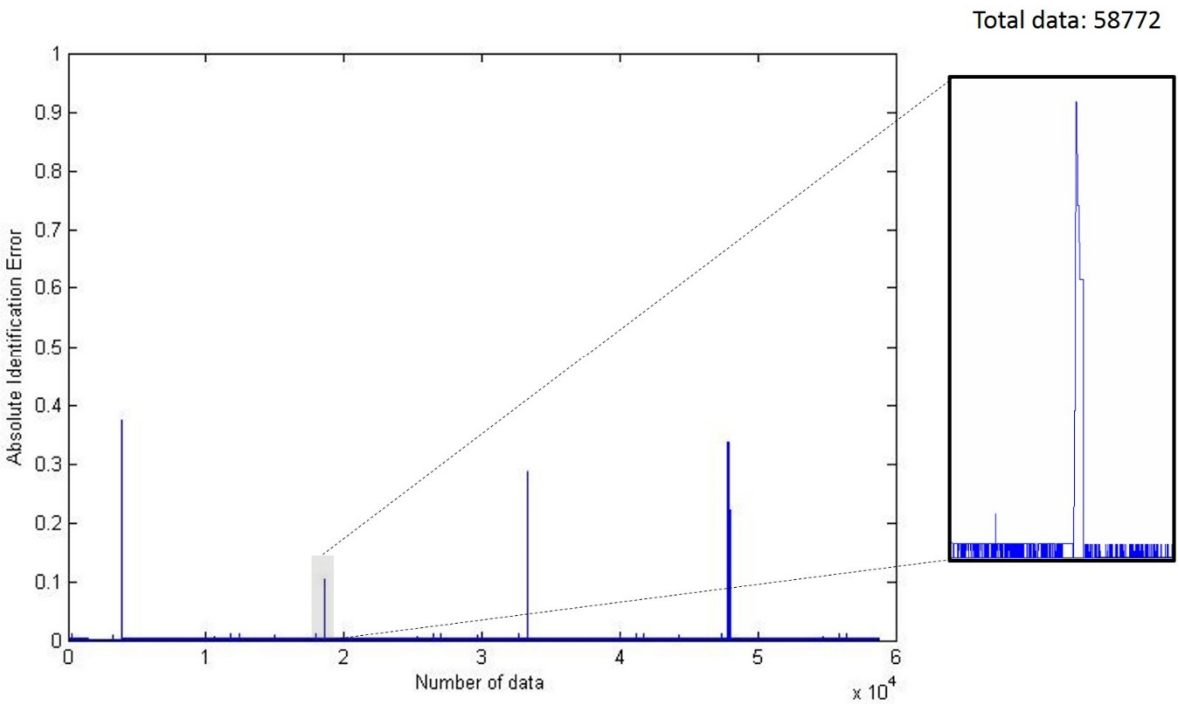


Figure 9 Anomaly Detection using RLS

3.2. Iterative Filtering (IF) Algorithm

IF algorithm is a method to compute reputation of objects and raters in trust management systems for Wireless Sensor Networks (WSN) and detects abnormal nodes according to a study of Roman [16]. Generally, it has been used to compute an average for a sensor's coordinates (x, y, z) in the multi-dimensional environment as shown in Figure 10. The *m* raters evaluate the *m*+*n* items, and updates weights of trust for these votes using *n* objects and *n*×*m* rating matrix [17]. The weights are related to distances between the votes, and the reputation of the objects are evaluated. In a paper of Rezvani [6], the IF algorithm that provides an approximation of the truthfulness of sensor nodes is described. Figure 11 briefly illustrates the computation of reputation based on the updated weights. In this thesis, the IF algorithm is used to determine an average value among the normal sensory values that are filtered out by RLS algorithm. The controller of the proposed system receives the average value, and operates an actuator based on the value. In this thesis, one block of readings at a time is collected, *m* is the number of instances of each block. In case of *m*=1, a block of readings matrix $X = \{x_1, x_2, x_3, \dots, x_n\}$ is defined where *n* represent the number of sensors. The reputation vector $r = [r_1, r_2, \dots, r_m]^T$ that represents

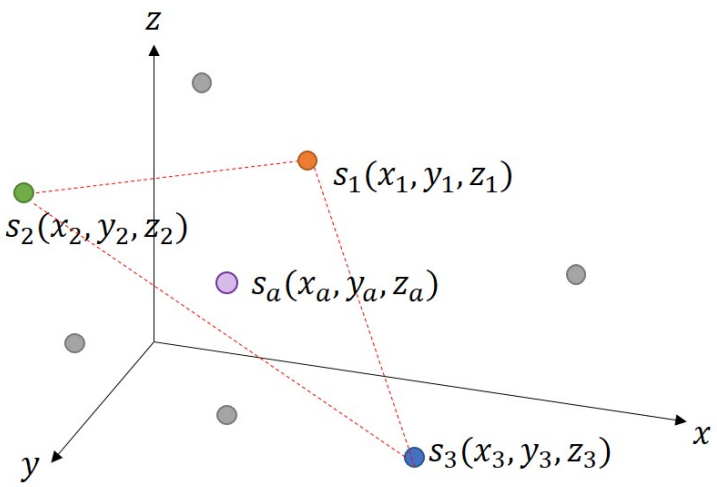


Figure 10 Concept of IF algorithm

reliability, and trustfulness of the sensor is computed iteratively with the weights $w = [w_1, w_2, \dots, w_n]^T$. The weight and reputation vector are initialized in the first round of iteration where $r^{(l)}$ and $w^{(l)}$ are obtained at the lth round of iteration ($l \geq 0$). The weight in each iteration is computed by Equation (8). It repeats until the reputation is converged. The distance between the reputation vector and the sensory readings is represented by Equation (9), and the updated weight is in Equation (10) where $1 \leq i \leq n$. In the scenario of this thesis, the reputation vector is scalar because the physical variable measured is the speed of the vehicle.

$$r^{(l+1)} = \frac{X \cdot w^{(l)}}{\sum_{i=1}^{n} w_i^{(l)}} \qquad \dots\dots\dots (8)$$

$$d_i = \frac{1}{m} \left\| x_i - r^{(l+1)} \right\| \qquad \dots\dots\dots (9)$$

$$w_i^{(l+1)} = e^{-d} \qquad \dots\dots\dots (10)$$

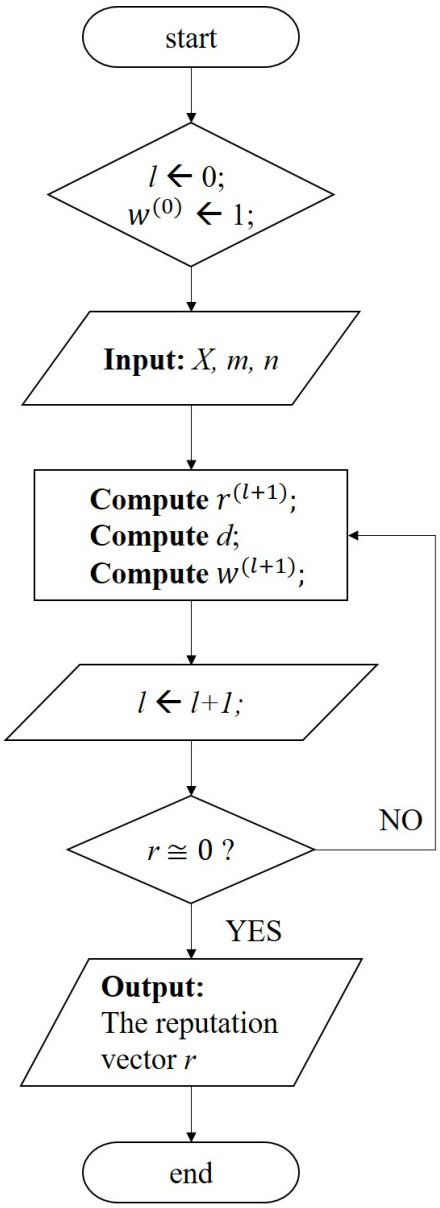


Figure 11 IF Algorithm

The simulation test was conducted using the randomly generated sensory data, and the average weights of each sensor are evaluated as shown in Figure 12 and Figure 13. Assume that the length of measuring time sequence is 50. The average for s_n $(n = 1, 2, 3, 4, 5)$ is tabulated in Table 3. Finally, the value -0.0174 was computed as the reliable average value using IF algorithm.

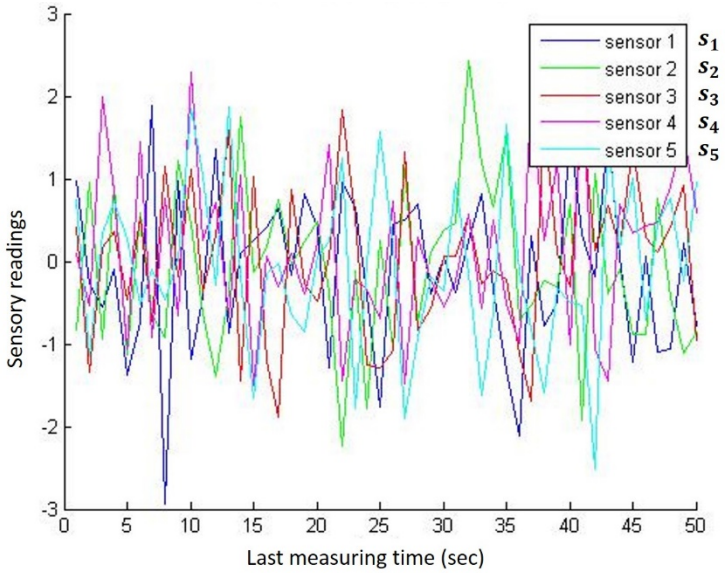


Figure 12 Sensor Readings (Input for IF Algorithm)

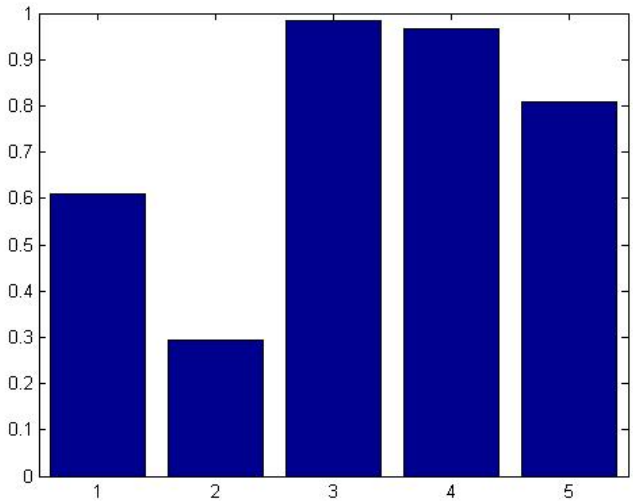


Figure 13 Average Weights of Sensors

s_1	s_2	s_3	s_4	s_5
-0.1206	-0.0713	0.0307	0.1421	-0.0681

Table 3 Average Readings of Sensors

Furthermore, the changes of the weights for the measuring time could be examined in Figure 14. According to the result that is addressed above, the highest weight of s_4 means that its value becomes the most trustworthy.

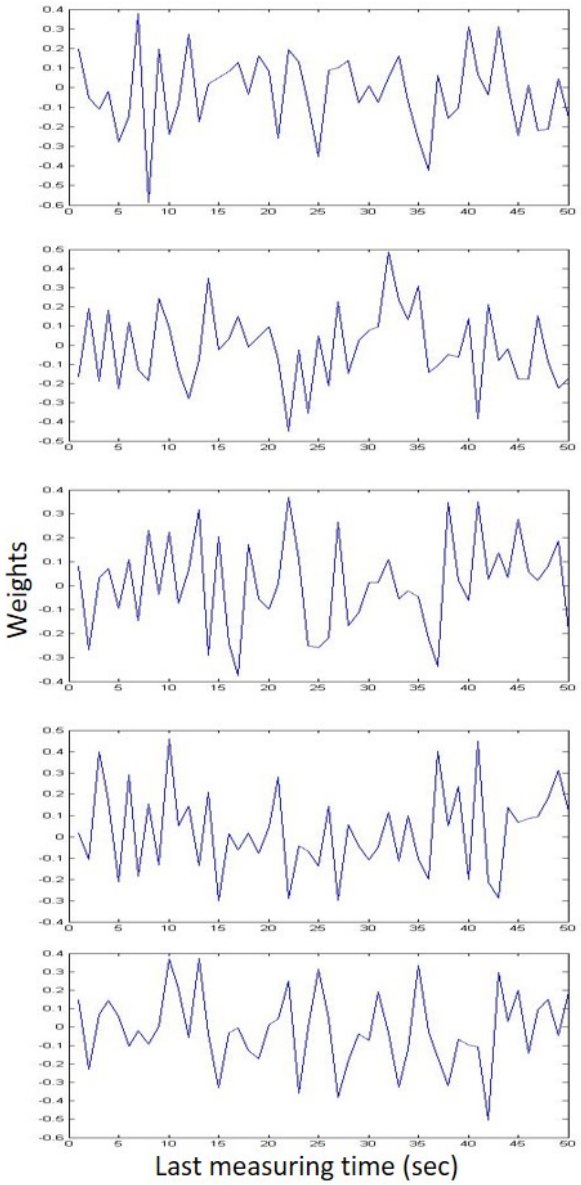


Figure 14 Changes of Weights for a Measuring time

3.2.1. Appropriateness of IF

There are many studies regarding how to decide the average among the collected data such as Majority Consensus, Median Filtering algorithm, and a general average. First, Majority Consensus is one of decision-making methods that make items converged. It aims at making many agreements as possible [18]. Equation 11 is a function from n inputs to one output [19]. However, it is not suitable for the system with multiple sensors. The sensors may generate a little different sensory values even though they measure a same variable. Additionally, when the multiple sensors are abnormal, it is not reasonable. Therefore, the method that aggregates them effectively and determines an average is needed while it decides whether the sensor is normal or not.

$$Majority(p_1, \ldots, p_n) = \left\lfloor \frac{1}{2} + \frac{(\sum_{i=1}^{n} p_i) - \frac{1}{2}}{n} \right\rfloor \quad \ldots\ldots\ldots (11)$$

Second, Median Filtering algorithm is a decision rule that computes the average based on Maximum Likelihood (ML) estimation in the presence of the noise [20], [21]. The algorithm finds the average as in Equation 12. It characterizes the robustness on the polar opposites. Note that it does not use the whole collected data, so the representative value of the population is crucial. That is, its computation includes two middle values so that the rest of the readings are excluded. Moreover, a main weakness of the method is that a large filter size is required especially when there is corruption in aggregated data. But it is simple and commonly used.

$$Me = \begin{cases} X_{(\frac{n+1}{2})} & : n \text{ is even} \\ \frac{1}{2} X_{(\frac{n}{2})} + X_{(\frac{n}{2})} & : n \text{ is odd} \end{cases} \quad \ldots\ldots\ldots (12)$$

The third candidate is the general average, however, there is a big difference between the general average value and the reliable average computed by IF algorithm. Figure 15 visualizes

the result based on the general average computation method in Equation 13. The averages of all cases are same even though the input data set is different. Therefore, the general average is not reliable when the data is distributed, especially for the polar opposites.

$$\overline{X_k} = \frac{1}{n}\sum_{i=1}^{n} X_i \qquad \text{..... (13)}$$

k means kth case (k=1, 2, 3)

Table 4 is the result by the proposed algorithm. The simple experiment using MATLAB

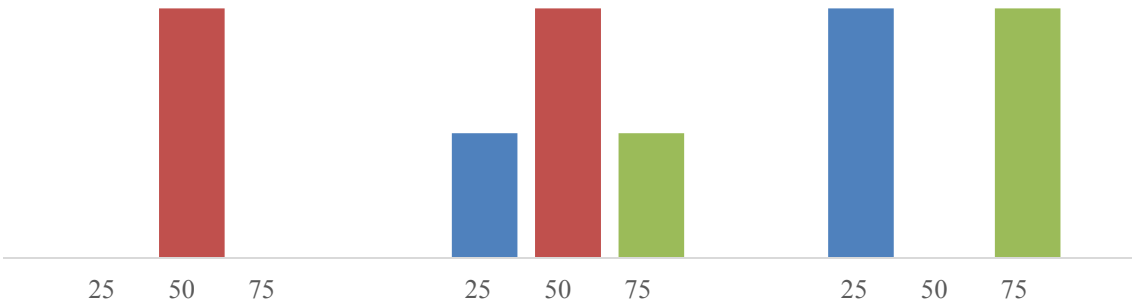


Figure 15 General Average Computation

software was conducted to examine which method is reasonable for the average sensory value. The underlined measurement in Table 4 represents the anomaly, assuming that an experimenter attacks the sensor by injecting the abnormal sensory values on purpose. Anomaly Handler in RLS converts the abnormal value to any number (e.g., 0). Then, IF algorithm computes the average while excluding the value of 0. The replaced number can be any number that has enough gaps from the normal values. Both the majority consensus and the Median Filtering algorithm fail to find a reliable average value when the majority sensors are abnormal.

Case	Input $(s_1,\ s_2,\ s_3,\ s_4, s_5)$	Anomaly Handler + IF algorithm *(an abnormal is replaced to any value for example 0)*	Majority Consensus	Median Filtering algorithm
1	(78, 80, 80, 84, 120)	80.5	80	80
2	(40, 41, 41, 42, 78)	41	41	41
3	(50, 50, 51, 67, 78)	50.3	50	51
4	(30, 30, 87, 86, 91)	30	30	86
5	(55, 54, 78, 100, 20)	54.5	54.5	55
6	(0, 0, 0, 15, 17)	16	0	0

Table 4 Result of the Proposed Average Computation Scheme

3.2.2. Reliable Average Decision using IF

In order to converge sensory values, a system that IF algorithm is employed is implemented as in Figure 16. Vehicular sensory data is inputs for IF algorithm, and the output is transmitted to a PID controller. The inputs have some noise in the real sensory readings, and two anomalies are synthesized sensory values, as shown in Figure 17. IF computes the reliable

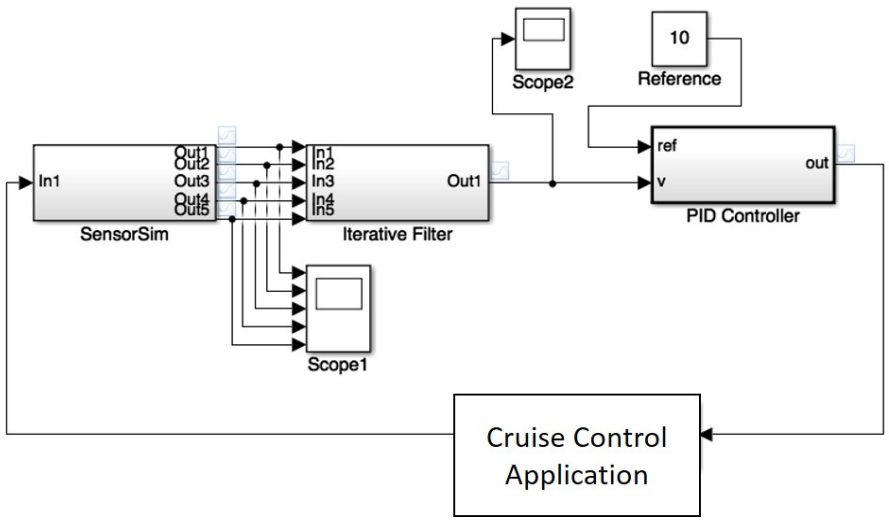


Figure 16 System Architecture of the Employed IF Algorithm

average value when five sensory readings including two abnormal values are incoming. Figure 18 visualizes the determined average, which is delivered to the controller to operate the cruise control system. The increase of speed requires arrival time because the vehicle is under the cruise control. The PID in the controller decides whether the current vehicular speed should be increased or not, according to the difference between the current speed and the reference speed that has been set previously. If the current speed is lower than the reference, the acceleration is a positive number, and then it increases the speed. The result illustrated in this section determines the reliable average value from the incoming readings in order to implement the robust deterministic scheme. In contrast, Figure 19 is a result of the sensor fusion using the general average decision.

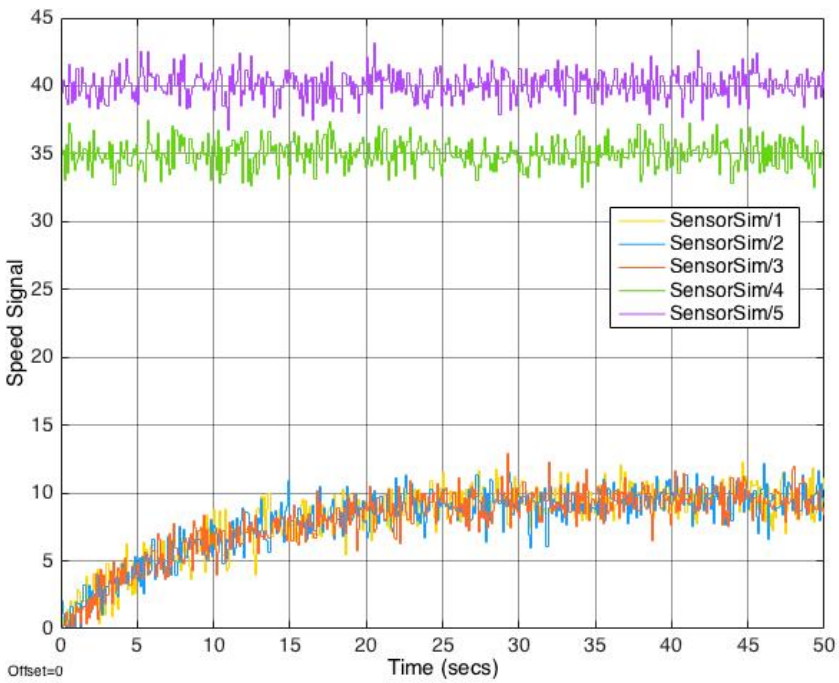


Figure 17 Speed Sensor Value (Input of IF Algorithm)

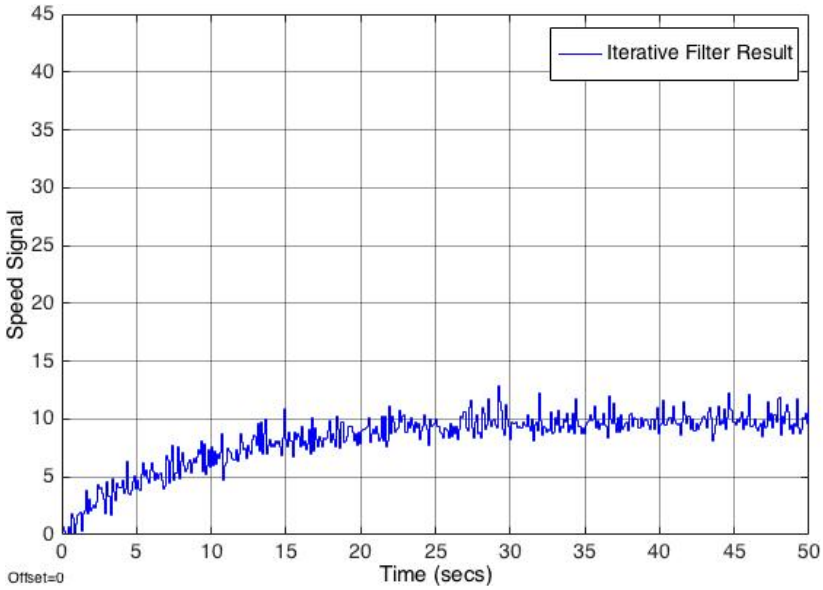


Figure 18 Computed Average (Result of IF Algorithm)

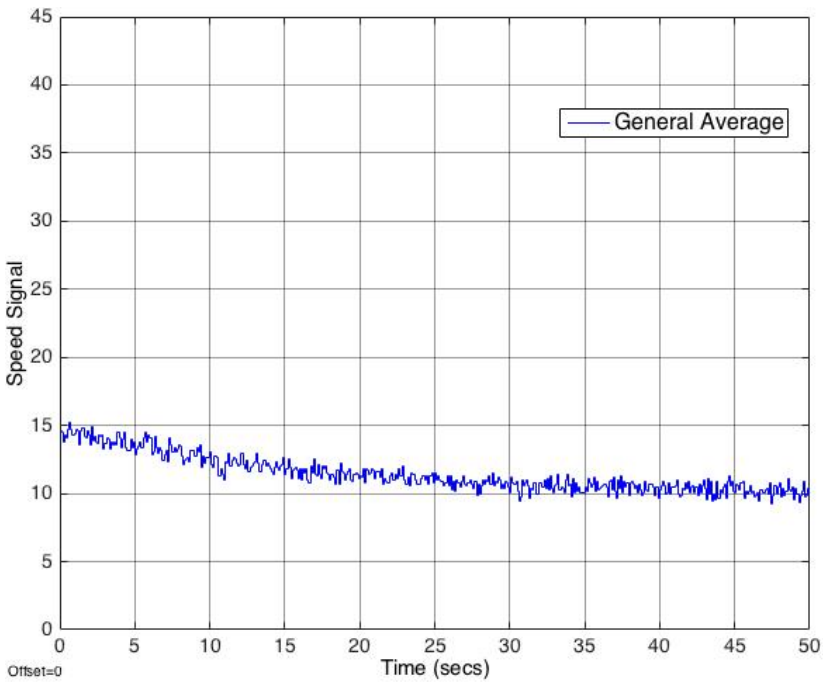


Figure 19 Computed Average (Result of General Average Decision)

IV. Experiment and Results

4.1. Experimental Environment

To test the proposed mechanism, a scenario for the simulation experiment needs to be designed. A robotic platform autonomously runs under the cruise control, and multiple sensors estimate a same physical variable. The experimenter knows what damage the anomaly can inflict on the platform's operation if one of the sensors sends an abnormal value. At this time, the proposed mechanism lets the system capture an accurate sensory value using only normal sensor values. Knowing a reliable value provides the improved safety and the accident prevention such as collision avoidance.

The cruise control system automatically controls the speed of the vehicle, and maintain a steady speed that is set by a driver [22]. It maintains the desired speed and automatically reduce the speed when the distance from a car in front decreases in modern 'adaptive' systems. There are some advantages of using the cruise control systems: 1) it reduces a driver's fatigue during long drives, 2) it improves comfort and vehicle's fuel efficiency on highway, and 3) it keeps speed limits. In the proposed system, the PID controller operates and compares a difference between an acceleration and the reference speed, and determines how much to decrease/ increase the speed of the vehicle. It is under the cruise control when the acceleration is close to 0. The acceleration herein means the rate of speed changes.

In order to evaluate the scenario, simulation-based test was conducted by Gazebo simulator as in Figure 20. It is a 3D multi-robot simulation that generates sensor data, optionally with noise, from laser range finders, camera, etc., and provides realistic rendering of environments [23]. With the simulation, the proposed mechanism can be examined with a safe driving. The simulator is used to emulate motions of a robotic platform without depending physically on the

actual machine so that cost and time can be saved. Real sensory data is collected from a robotic platform named ERP-42 in a realistic indoor test-bed as shown in Figure 21.

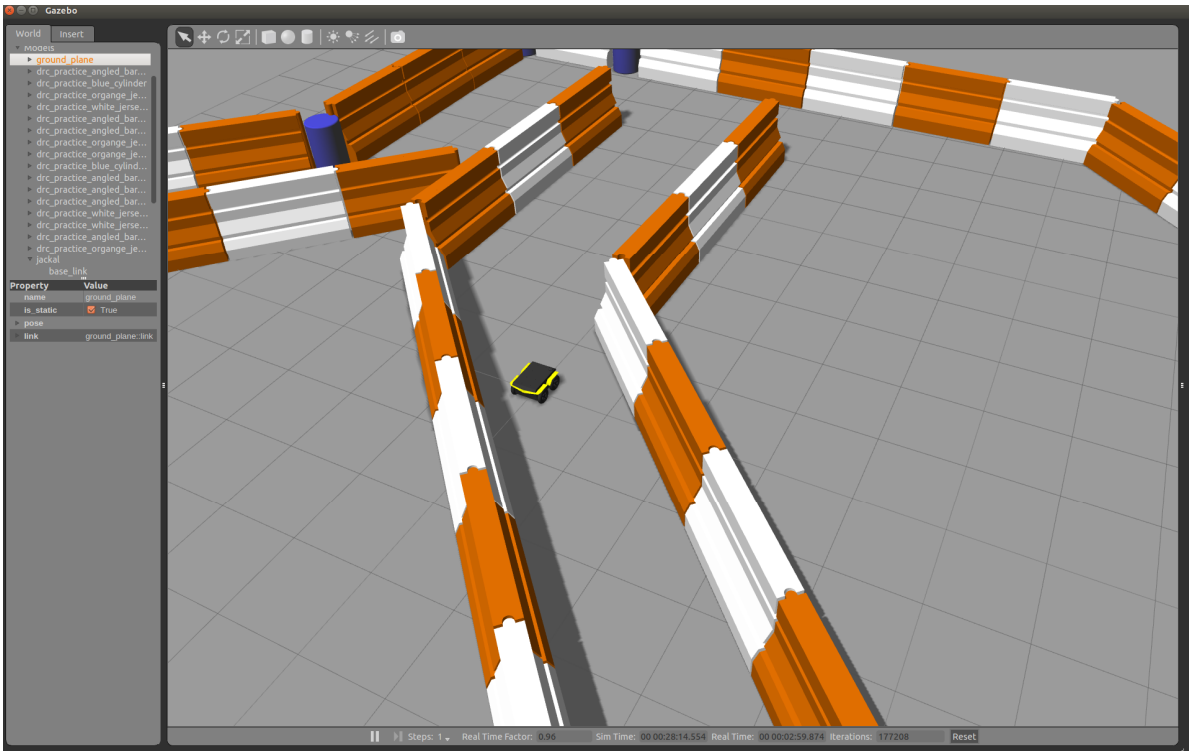


Figure 20 Robotic Simulator, Gazebo

Figure 21 Robotic Platforms and Indoor Test-bed

4.2. Simulation Experiment and Results

Simulation tests were conducted to analyze the robustness of the proposed system on a dangerous ground in spite of in-vehicular sensor's abnormal values. Figure 22 shows the implemented mechanism by using Simulink software. The overall processes of RLS and IF algorithm are shown in Algorithm 1 and Algorithm 2, respectively. Figure 23 illustrates the speed values of the vehicular model, which is delivered to RLS. Assume that the *n*th sensory value is $s_n(n = 1,2,3)$ and s_1 is an anomaly. Note that the value of s_1 is 70 while other normal values are 50. The values measured their errors in RLS are adjusted to the original sensory values and 0, respectively, as shown in Figure 22. The reason why the abnormality should be changed to any digit is that IF algorithm excludes the abnormal sensor. Then, IF computes the average value using the normal sensor readings excluding abnormality. Therefore, the controller uses the average value to operate the cruise control. The bar in the illustrated graphs (from Figure 23 to Figure 24) shows the process in each module. In Figure 23, we assumed that the sensor reading of s_1 is regarded as the anomaly. In our experiment, the precondition is that there is at least one normal sensor reading. Noises are generally coming from rough roads, mechanical defects, etc.

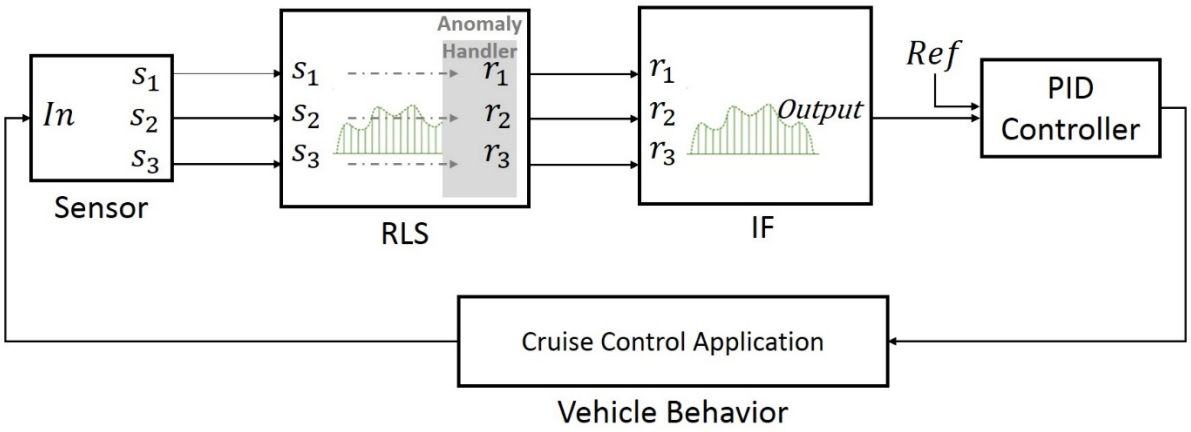


Figure 22 Design of the Proposed Mechanism for Cruise Control System

Procedure RLS

For i := 1 to n

Set ***ths*** as threshold value from formula of RLS ;

If $e_1 > ths$

adjust $s_1 = 0$;

If else $e_2 > ths$

adjust $s_2 = 0$;

Else $e_3 > ths$

adjust $s_3 = 0$;

End procedure

Send the sensor data except $s_i = 0$

Algorithm 1 Pseudocode of RLS

Procedure IF

Input r_i for IF algorithm (i = 1, ..., n)

IF(r_1, ..., r_n);

End procedure

Send the output

Algorithm 2 Pseudocode of IF

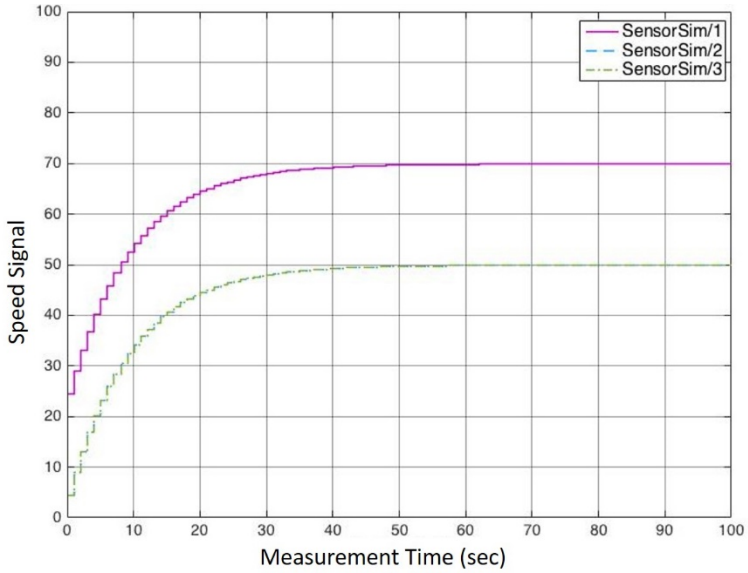


Figure 23 Initial Sensory Readings

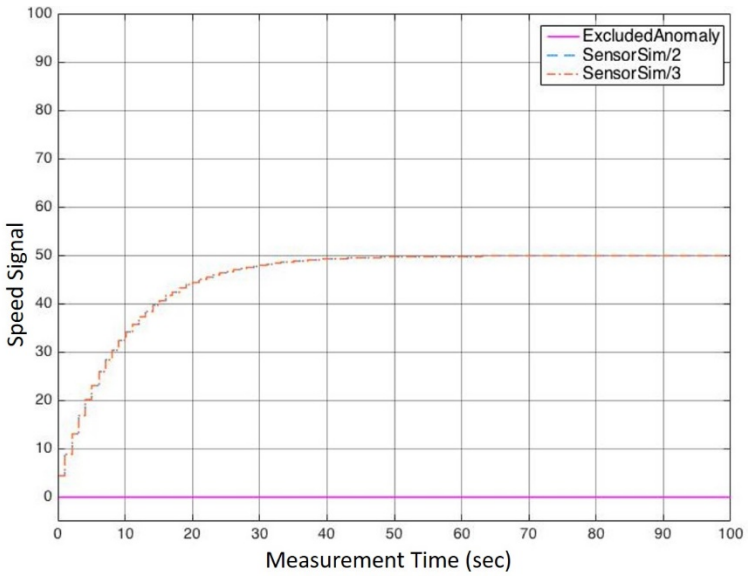


Figure 24 Result of RLS

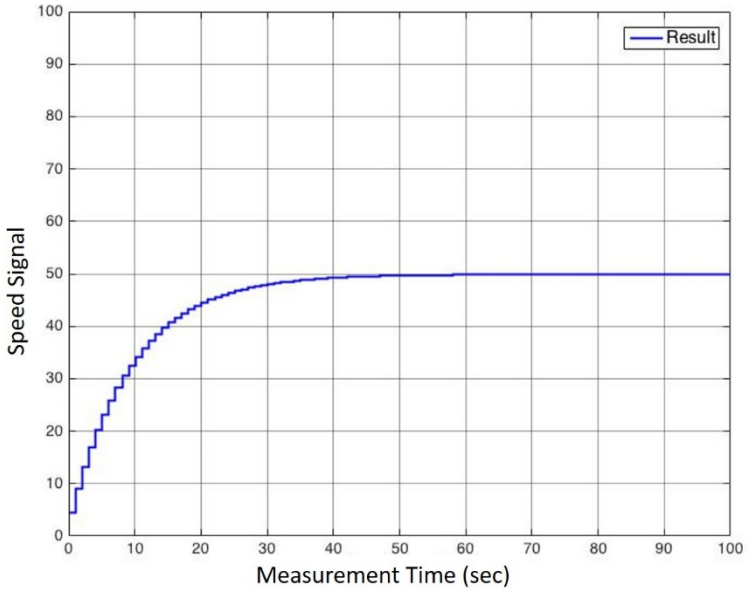


Figure 25 Result of IF algorithm

The proposed mechanism was applied to the Gazebo simulator to examine the performance in the following situations: 1) driving under the attacks without any robust mechanism, and 2) driving with the proposed mechanism in a threatened circumstance with attack signals. Figure 26 describes components in Gazebo Simulator and their interfaces. Nodes for a driver's behavior by a joystick and for an attacker by an anomaly signal were published. The messages are sent to Electronic Control Unit (ECU) in the Gazebo in a simulator.

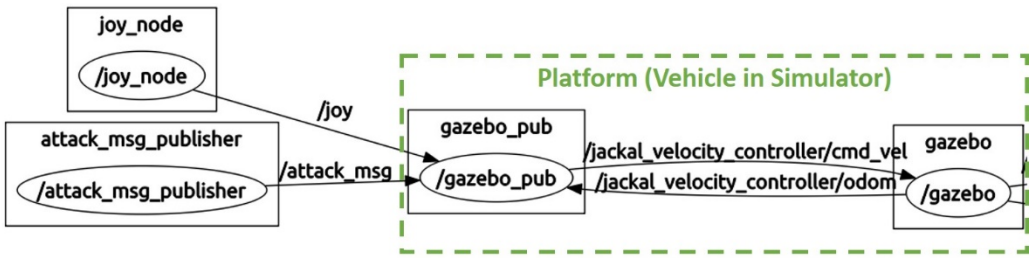


Figure 26 Components and Interfaces in Gazebo

First, we generated a few attack signals purposely as illustrated in Figure 27. The signal affects the system in real-time and repeats both the type of (a) and (b) periodically. Without the

proposed mechanism, the cruise control system became out of order. Here 'Controller_ref', 'Speed_v', and 'Sys_out' denotes the reference speed value, the current speed of the vehicle, and the result value obtained by the proposed mechanism, respectively. A time sequence in the data table implies that the signals input in a real-time. Figure 28 demonstrates the failed cruise control system under the anomaly signals. By comparing the difference between the reference speed and the current platform's speed, the system accelerates. Even though the current vehicular speed of 2.000655 is faster than the reference speed of 1.400000, the failed system required the positive acceleration (i.e., it commands the controller to increase the speed). Eventually, the vehicular platform faced the fatal accident as illustrated in Figure 29.

In contrast, we considered driving with the proposed mechanism under the anomalies. Even though they are the synthesized anomaly signals, the platform normally operated in spite of the attack signals as shown in Figure 30. The same kind of signals injected to the previous practice. The current speed is higher than the reference so that the controller decrease the speed. Therefore, the acceleration is represented by the negative number in order to balance platform's driving speed with the reference speed of the controller. The platform typically runs on the ground under the cruise control.

Time Sequence	Attack Signal
1	Attack = 1
2	Attack = 1
3	Attack = 1
4	Attack = 1
5	Attack = 1
6	Attack = 1
…	…

(a)

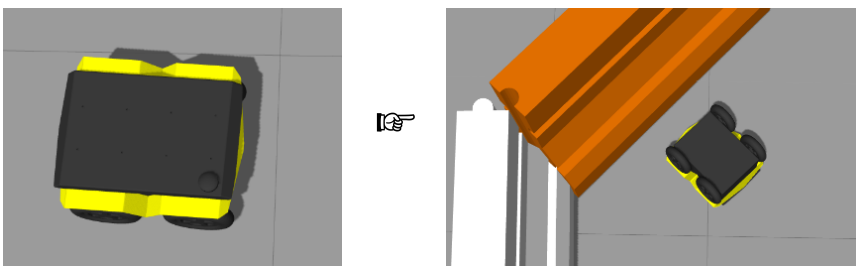
Time Sequence	Attack Signal
1	Attack = 3
2	Attack = 3
3	Attack = 3
4	Attack = 3
5	Attack = 3
6	Attack = 3
…	…

(b)

Figure 27 Injecting Attack Signals

Time Sequence	Index	Value
1	Controller_ref	1.400000
	Speed_v	2.000696
	Sys_out	0.046640
2	Controller_ref	1.400000
	Speed_v	2.000788
	Sys_out	0.046720
3	Controller_ref	1.400000
	Speed_v	2.000788
	Sys_out	0.046800
4	Controller_ref	1.400000
	Speed_v	2.000638
	Sys_out	0.046880
5	Controller_ref	1.400000
	Speed_v	2.000655
	Sys_out	0.046960
…	….	….

Figure 28 Failed Cruise Control System under Attack Scenario



(Usual state) (Accident)

Figure 29 Rollover Accidents due to the Attacks

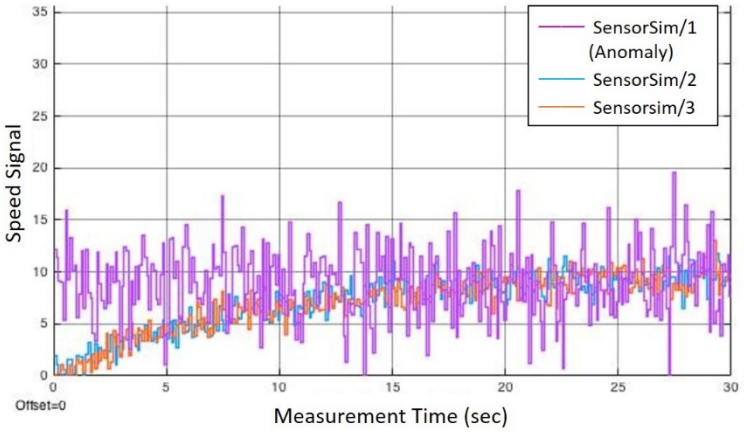
Time Sequence	Index	Value
1	Controller_ref	1.400000
	Speed_v	1.491709
	Sys_out	-0.00025
2	Controller_ref	1.400000
	Speed_v	1.491709
	Sys_out	-0.000044
3	Controller_ref	1.400000
	Speed_v	1.492100
	Sys_out	-0.000101
4	Controller_ref	1.400000
	Speed_v	1.492479
	Sys_out	-0.000157
5	Controller_ref	1.400000
	Speed_v	1.492776
	Sys_out	-0.000205
…	….	….

Figure 30 Achieving Robust Cruise Control System under Attack Scenario

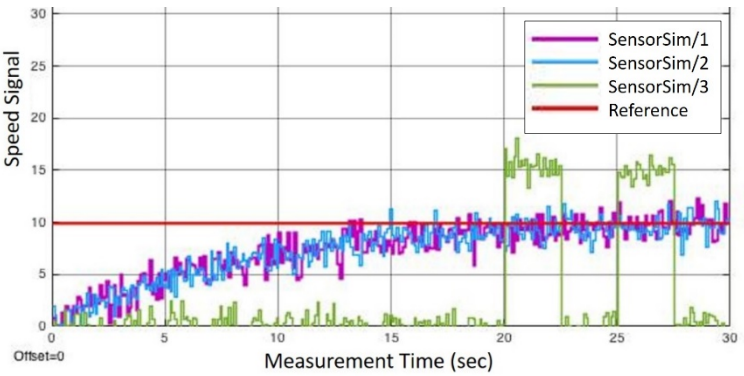
We considered two scenarios: 1) the majority of the sensors are in normal state, and 2) the majority of sensors are abnormal. Common conditions are that there are three sensors that measure a same variable, and the abnormal sensors and the anomaly signal are randomly generated. Also, periods, amplitudes, and delays of the anomaly signals are random.

In the first scenario, there is a single abnormal sensor as shown in Figure 30 (i.e., the majority of sensors are normal). The sensor readings from the abnormal sensor, denoted by s_1, have mean 9 and variance 10. The other normal readings have relatively little noises. The anomaly occurred 100% during measurement time of 30 seconds. Additionally, we injected various types of the anomalies in the single sensor as shown in (b) and (c). The occurrence rates, periods, amplitudes, and delays of the anomaly signals are different each other. However, the proposed mechanism computes the reliable average value to operate the cruise control system normally as shown in Figure 31. Note that the result of the system under the IF-only mechanism showed a same performance under the single anomaly (i.e., the majority of sensors are normal).

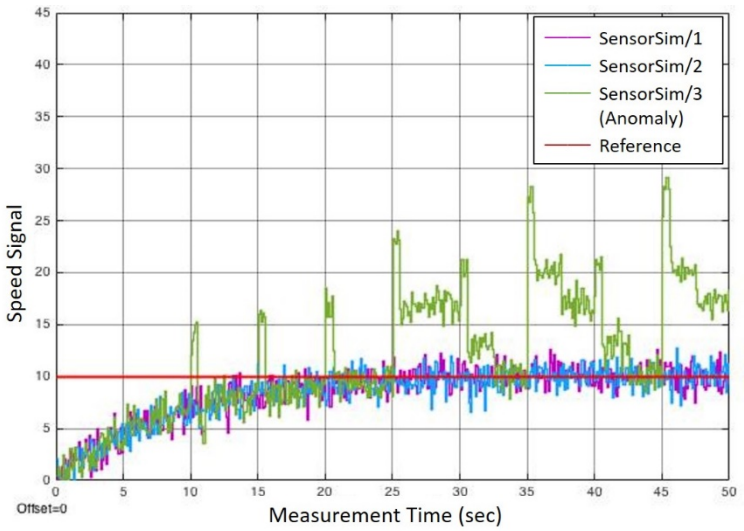
In the second scenario, there are multiple anomalies with lower noises as shown in Figure 34. Likewise, the anomaly signals were generated and injected randomly. During the measurement time, there is an overlapped period of the anomalies for 2 seconds. In Figure 34, there is a little confusion at the point of 20 seconds where the first anomaly affects the system. However, the proposed mechanism finds the reliable average speed signal as shown in Figure 35.



(a) Anomaly Type 1

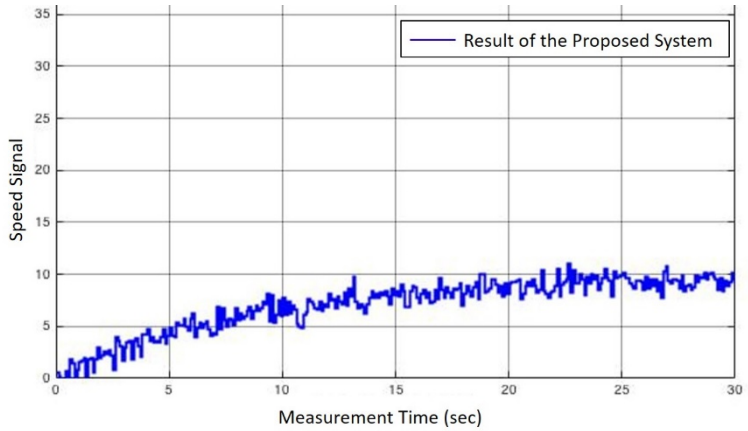


(b) Anomaly Type 2

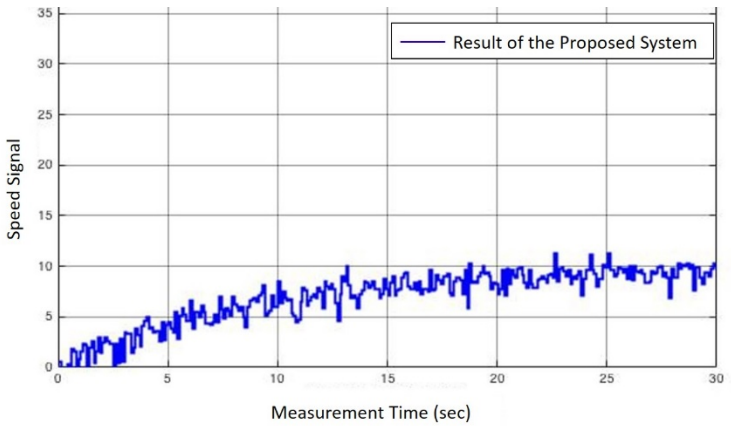


(c) Anomaly Type 3

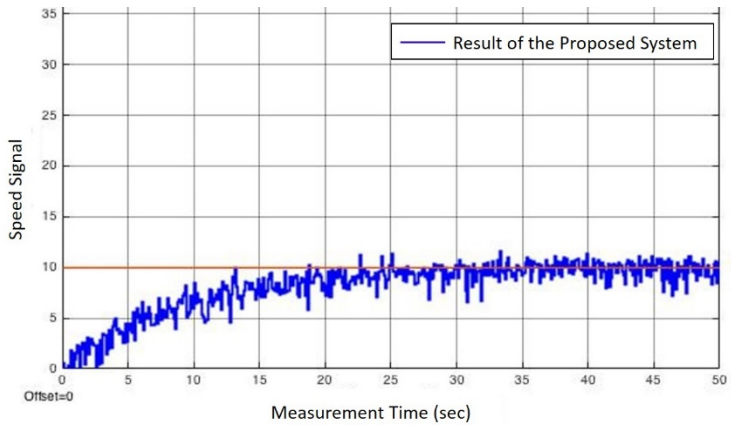
Figure 31 Sensor Readings (Single Anomaly)



(a) Result of Anomaly Type 1



(b) Result of Anomaly Type 2



(c) Result of Anomaly Type 3

Figure 32 Result of the Proposed System under Single Anomaly

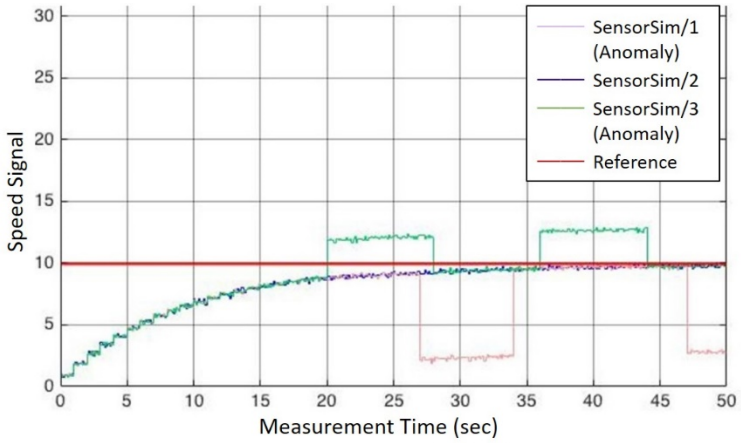


Figure 33 Sensor Readings under Transient Multiple Anomalies

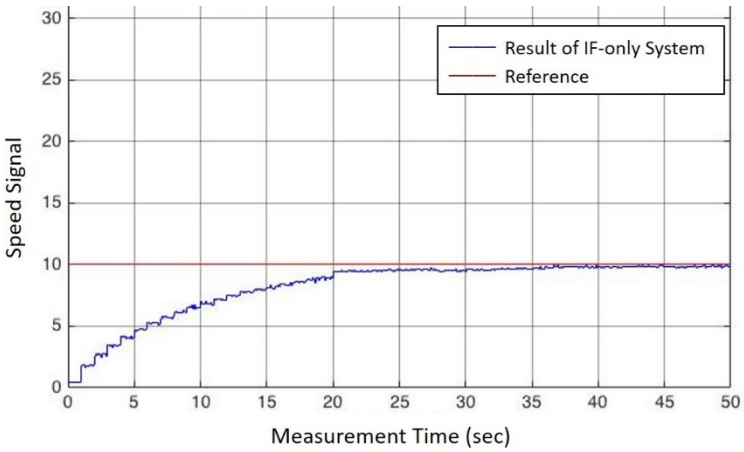


Figure 35 Result of IF-only System

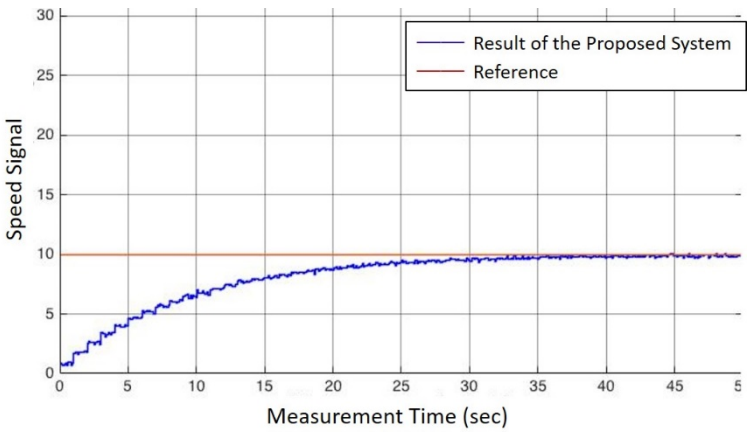


Figure 34 Result of the Proposed System

Additionally, Figure 36 illustrates the input signals under the multiple anomalies that injected during all measurement time. The system employing the IF-only mechanism was operated as shown in Figure 37. At the beginning of the operation, the output speed signal was confused by the anomalies for 12.5 seconds. In a real vehicle driving situation, the time is enough to have a vehicular collision, leading to dangerous situation. During the time, the confusion was caused by the readings of s_1 and s_2 because that of s_3 is not overlapped with others. The properties of the anomalies are tabulated as shown in Table 5. A range of the indices means the difference between the maximum and minimum values. When the reading of sensors has a big gap among them, it is not included in an average computation. However, the system employing the fusion algorithm of RLS and IF computed the reliable output signal as shown in Figure 38. The results of non-anomaly and single anomaly cases can be considered a ground truth of normal cruise driving. The salient result is that the sensor readings of the abnormal sensors were ignored by RLS algorithm and Anomaly Handler in the overall system configuration. The IF-only mechanism can normally operate the system under the single anomaly, though, it computes the average signal by aggregating all sensor readings. According to the simple RLS algorithm, the system can keep a normal operation despite of the multiple anomalies.

Sensor	Standard deviation	Range	Mean
s_1	0.7222	4.118	15.03
s_2	0.3041	2.075	4.99

Table 5 Property of Anomaly Signals

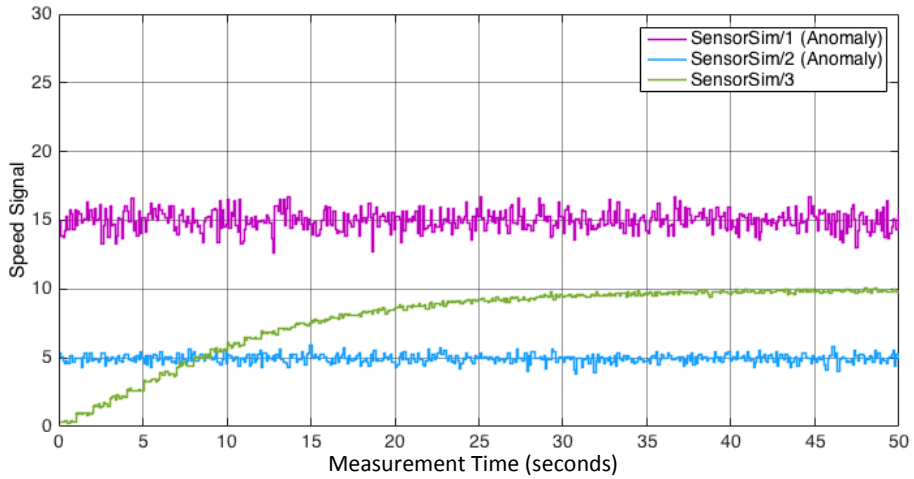


Figure 38 Sensor Readings under Persistent Multiple Anomalies

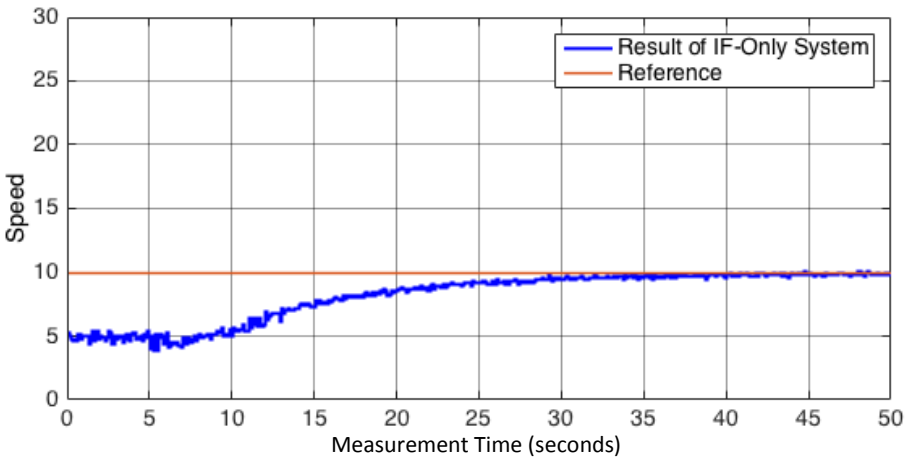


Figure 36 Result of IF-only System

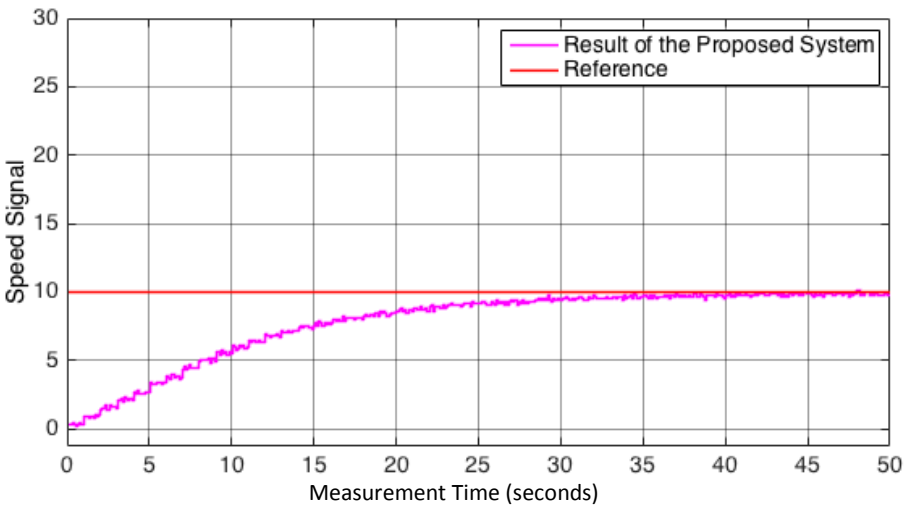


Figure 37 Result of the Proposed System

The evaluation of our proposed mechanism is summarized in Table 6. The evaluation index is the standard deviation of the signal during the confusion time on the basis of the normal signal. We did not evaluate a performance when all sensors are abnormal because our precondition is that at least one normal sensor should exist. However, we examined the case where all sensors are normal. Normal operation means that the cruise control system in the simulator keeps a steady speed of the vehicle in the same measurement time.

The number of anomalies (attacked/fault sensors)	IF-only system	Fusion of RLS and IF system
0	0	0
1	0	0
2	0.1648	0

Table 6 Performance Evaluation on Number of Anomalies

Consequently, we conducted the experiments for the cruise control application to examine how the proposed mechanism operates the system normally against the presence of attacked or failed sensors. The mechanism detected anomalies using RLS, and then the anomalies were classified by Anomaly Handler. The normal values were delivered to IF algorithm module to aggregate and determine the reliable sensor value for the system control. By employing the proposed mechanism (the fusion of RLS and IF), the cruise control system successfully kept a steady state even when the majority of sensors are abnormal.

V. Conclusion and Future Work

Modern vehicles are equipped with diverse vehicular sensors and the smart devices that are connected to the vehicular network. This thesis addressed some issues regarding the attacks on the automotive CPS, and sketched a scheme that achieves the robustness of the vehicular system using the multiple sensors. The methodology proposed in this thesis uses the combination of RLS and IF algorithms in order to identify abnormal sensory values and computes the average by using only the normal sensory values among the readings.

First, we analyzed the algorithms by comparing the similar approaches. Thus, this thesis uses RLS algorithm that has some advantages of a real-time operation, fast convergence speed, and etc. in order to detect and identify the anomalies. The reason why we selected RLS among many kinds of the Adaptive Filtering algorithm is that RLS robustly finds the anomalies even though the attacked sensors are majority. Additionally, IF algorithm determines the reliable average value from the incoming sensory readings by computing the weights and updating the values in each iteration. The PID controller uses the determined average to operate the cruise control system in the vehicle model.

We conclude that proposed mechanism performs safe cruise control under the attacked scenario in the experiment. Without the robust mechanism, the cruise control system broke down so that the vehicular model was led to the fatal accident. The attacks increase the acceleration although the current speed is higher than the reference speed. In contrast, the cruise control system under the proposed mechanism operates safety in the presence of the attack signals.

As a future work, the multiple vehicles under the proposed mechanism will be considered to examine the interface between them. We will examine the performance of the proposed mechanism in Vehicle-to-Anything (V2X) infrastructure because the fully autonomous vehicles

will be widespread soon. The scheme to predict uncertainties on roads under the cruise control will be needed. A server can be considered to save previous data sets in a variety of environments and road conditions. The prediction model computes the expected actions against diverse threats on roads. This will allow safer and more robust driving even with a sudden system failure and obstacles appearing on the roads: This thesis has many possibilities to extend to improve safety in ITS.

References

[1] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, "Experimental Security Analysis of a Modern Automobile," in *IEEE Symposium on Security and Privacy*, 2010.

[2] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe and I. Seskar, "Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study," in *The19th USENIX Security Symposium*, 2010.

[3] R. Ivanov, M. Pajic and I. Lee, "Attack-Resilient Sensor Fusion," in *Design, Automation & Test in Europe (DATE '14)*, 2014.

[4] D. Stavrou, D. G. Eliades, C. G. Panayiotou and M. M. Polycarpou, "Fault detection for service mobile robots using model-based method," *Autonomous Robots,* pp. 1-12, 2015.

[5] K.-T. Cho, K. G. Shin and T. Park, "CPS approach to Checking Norm Operation of a Brake-by-Wire System," in *ACM/IEEE Sixth International Conference of Cyber-Physical Systems (ICCPS '15)*, 2015.

[6] M. Rezvani, A. Ignjatovic, S. Jha and E. Bertino, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks," in *IEEE Transactions on Dependable and Secure Computing*, 2014.

[7] T. resiliNets, "Research Intiative definition of resilience," [Online]. Available: https://wiki.ittc.ku.edu/resilinets_wiki/index.php/Definitions#Resilience.

[8] J. W. Baker, M. Schubert and M. H. Faber, "On the assessment of robustness," *Stuctural Safety,* vol. 30, pp. 253-267, 2008.

[9] R. Yan, Q. Zheng and H. Li, "Combining Adaptive Filtering and IF Flows to Detect DDoS Attacks within a Router," *KSII Transactions on Internet and Information Systems,* vol. 4, no. 3, pp. 428-451, June 2010.

[10] S. Haykin, A. H. Sayed, J. R. Zeidler, P. Yee and P. C. Wei, "Adaptive Tracking of Linear Time-Variant Systems by Extended RLS Algorithms," *IEEE Transactions on Signal Processing,* vol. 45, no. 5, pp. 1118-1128, 1997.

[11] G. Mateos, I. D. Schizas and G. B. Giannakis, "Distributed Recursive LEast-Squares for Consensus-Based In-Network Adaptive Estimation," *IEEE Transaction on Signal Processing,* vol. 57, no. 11, 2009.

[12] J. Dhiman, S. Ahmad and K. Gulia, "Comparison between Adaptive filter Algorithms (LMS, NLMS and RLS)," *International Journal of Science, Engineering and Technology Research (IJSETR),* vol. 2, no. 5, pp. 1100-1103, 2013.

[13] S. R. Patel, S. R. Panchal and H. Mewada, "Comparative Study of LMS & RLS Algorithms for Adaptive Filter Design with FPGA," *Progress In Science in Engineering Research Journal,* vol. 11, no. 2, pp. 185-192, 2014.

[14] V. S. Vaseghi, "Adaptive Filters," in *Advanced Digital Signal Processing and Noise Reduction*, Fourth Edition ed., John Wiley & Sons, Ltd., 2008, pp. 194-225.

[15] J. Park, R. Ivanov, J. Weimer, M. Pajic and I. Lee, "Sensor Attack Detection in the Presence of Transient Faults," in *ACM/IEEE Sixth International Conference on Cyber-Physical Systems (ICCPS)*, 2015.

[16] R. Roman, C. F. Gago and J. Lopez, "Trust and Reputation Systems for Wireless Sensor Networks," in *Security and Privacy in Mobile and Wireless Networking*, Leicester, Troubador Publishing Ltd., 2009, pp. 105-128.

[17] C. D. Kerchove and P. V. Dooren, "Iterative Filtering in Reputation Systems," *SIAM Journal of Matrix Analysis of Applications,* vol. 31, no. 4, pp. 1812-1834, 2010.

[18] "Consensus Decision-Making," 29 8 2011. [Online]. Available: Consensusdeciisonmaking.org.

[19] "Majority function," 27 7 2015. [Online]. Available: https://en.wikipedia.org/wiki/Majority_function.

[20] D. A. F. Florencio and R. W. Schafer, "Decision-based median filter using local signal statistics," *SPIE, Visual Communications and Image Processing '94,* vol. 2308, pp. 268-275, 1994.

[21] I. Djurovic, V. Katkovnik and L. Stankovic, "Median filter based realizations of the robust time-frequency distributions," *Special section on Signal Processing Techniques for Emerging Communications Applications,* vol. 81, no. 8, pp. 1771-1776, 2001.

[22] "Cruise control," Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Cruise_control.

[23] "Gazebo," 2014 Open Source Robotics Foundation, [Online]. Available: gazebosim.org.

[24] K. R. Borisagar and G. R. Kulkarni, "Simulation and Comparative Analysis of LMS and RLS Algorithms Using Real Time Speech Input Signal," *Global Journal of Researches in Engineering,* vol. 10, no. 5, pp. 44-47, 2010.

요 약 문

다중 센서 기반 이상 감지를 통한 강인성 획득

최근 자동차 사이버 물리 시스템이 많은 차량 내 센서를 탑재함에 따라, 이에 대한 공격이슈가 대두되고 있다. 다양한 센서들을 통해 운전자에게 다양한 정보를 전달함으로써 편리성을 도모하는 반면, 이를 악용할 수 있는 여지와 공격 기술들이 보고되고 있다. 이러한 공격은 액추에이터의 물리적 파괴를 야기한다. 따라서, 지능형 교통 시스템에서의 안전성 증진을 위한 강인한 시스템이 요구되었다. 본 논문에서는 이상 탐지 매커니즘을 제안하여, 공격 상황에서 이상 센서를 분별하여 핵심적인 기능을 최대한으로 유지할 수 있도록 한다. 첫 번째로, 재귀 최소 자승법을 통해 이상 상태를 감지한다. 서로 유사한 기능을 하는 적응형 필터링 알고리즘들을 비교하여 재귀 최소 자승법이 리얼타임 운용에 최적임을 밝혀내었다. 또한 이 알고리즘을 통해 다수의 센서가 비정상 상태에 있더라도 그 가운데 문턱값을 초과하는 이상 데이터를 감지할 수 있었다. 두 번째로, 반복 필터링 알고리즘을 통해 정상적인 센서 값들을 이용한 신뢰성 있는 평균 센서 값을 결정하였다. 이 값은 컨트롤러가 크루즈 컨트롤 수행을 위해 참조값과 비교하기 위해 필요한 값이며, 하나의 값으로 제공되어야 한다. 다양한 평균 값 도출 알고리즘 가운데 IF 알고리즘의 신뢰성을 평가하였다. 실험 결과, 공격 신호가 주어질 때, 제안하는 매커니즘이 적용되지 않은 경우에 크루즈 컨트롤 시스템이 실패하여 시뮬레이터 내의 자동차 모델이 사고를 당하는 것을 보았다. 반면, 제안하는 매커니즘이 적용된 크루즈 컨트롤 시스템은 공격 신호가 들어와도 정상적으로 동작함을 확인하였다. 결론적으로, 이상 감지와 신뢰성 있는 평균 센서 값 도출을 위해서 재귀 최소 자승법과 반복 필터링 알고리즘을 함께 사용함으로써 공격에 강인한 크루즈 컨트롤 시스템을 구현할 수 있었다.

핵심어: 강인성, 지능형 교통 시스템, 안전성, 이상 탐지