Poster Abstract: Performance Analysis of Sensor Fusion Models using Unmanned Ground Vehicle

Minsu Jo[1], Youngmi Baek[2], Jin-hee Lee[2], Sang Hyuk Son[1]
[1]Department of Information & Communication Engineering, DGIST, Daegu, Korea
[2]CPS Global Center, DGIST, Daegu, Korea
{Minsu-Jo, ymbaek, jhlee07, son}@dgist.ac.kr

***Abstract*—In this paper, we analyze the performance of various sensor fusion models using an unmanned ground vehicle. In a given attack scenario, we examine how attacks influence on each fusion model by comparing the results of different models. We conduct the experiments with real measurement data obtained from an unmanned ground vehicle.**

Keywords— Sensor Fusion Model; Attack; Resiliency

I. INTRODUCTION

As the cyber security has been an important issue in Cyber Physical Systems (CPS), recent systems exploit many sensors measuring the same physical variable (e.g., Encoder, IMU and GPS) in order to provide more reliable value for a controller, and ensure the resilient operation against abnormal conditions. Many researchers have developed various fusion models [1], [2]. Therefore, we evaluate the performance of each fusion model based on the real measurement data obtained from an unmanned ground vehicle in several attack scenarios.

II. EXPERIMNET ENVIRONMENT AND EVALUATION

Jackal has many sensors, such as Encoder, IMU and GPS for measuring a velocity (maximum speed of 2m/s) as shown in Fig. 1. To gather the data for our evaluation, we measured the velocity of Jackal by driving it on straight lines with a constant speed.

Fig. 1. Unmanned Ground Vehicle Called Jackal.

A. Evalution Using Simulink

For analyzing the performance of each model with MATLAB, we consider biased attack scenario in GPS data.

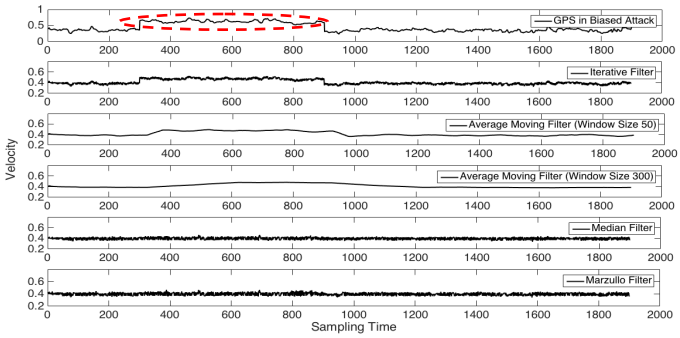

Fig. 2. Result in Simulink.

The biased attack is inserted only in GPS as shown in the first one of Fig. 2 (red circle). It shows that the fused result is not smooth as much as the result of median and Marzullo filter although both the iterative and the moving average filter tend to reduce the effect of the attack. However, note that the performance of the average moving filter is getting better as the window size of it increases. Therefore, moving average filter can be more successful than iterative filter at enduring the given attack.

B. Evalution Using an Unmanned Ground Vehicle

For more practical evaluations, we have already implemented several algorithms on Jackal in the cruise control scenario (reference speed of 0.4m/s). Among the algorithms, we compared the median filter with the average method under the biased attack (red circle). From the experiment results of Fig. 3, the average method is significantly influenced by the attack compared to the median filter.

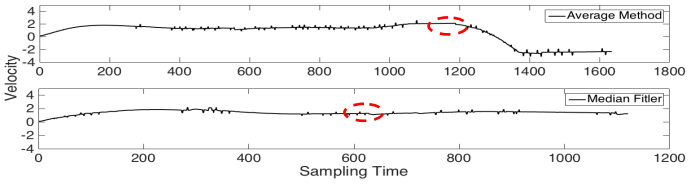

Fig. 3. Results obtained from Jackal.

III. CONCLUSIONS AND FUTURE WORK

The performance of sensor fusion models is analyzed using an unmanned ground vehicle called Jackal. We consider biased attack scenarios. As a result, each model has the difference performance. Using these results, we plan to implement our resilient algorithm into Jackal, analyze its performance using simulation, and then will verify it in a real environment.

ACKNOWLEDGMENT

This research was supported in part by Global Research Laboratory Program (2013K1A1A2A02078326) through NRF, and the DGIST Research and Development Program (CPS Global Center) funded by the Ministry of Science, ICT & Future Planning (MSIP).

REFERENCES

[1] AS. Willsky. "A survey of design methods for failure detection in dynamic systems." *Automatica* 12.6 (1976): 601-611

[2] Ao, Buke, et al. "On Precision Bound of Distributed Fault-Tolerant Sensor Fusion Algorithms." *ACM Computing Surveys (CSUR)* 49.1 (2016): 5.