악의적 사이버 공격을 무력화하기 위한 FIR 필터에 관한 연구

이상수*, 김관수*, 강현호*, 유성현*, 이동훈*, 이동규*, 김영은**, 안춘기*
*고려대학교 전기전자공학과
**고려대학교 메카트로닉스
e-mail : physism@korea.ac.kr

FIR Filter for Defense Mechanism against Malicious Cyber Attacks

Sang-Su Lee*, Kwan-Soo Kim*, Hyun-Ho Kang*, Sung-Hyun You*, Dhong-Hun Lee*, Dong-Kyu Lee*, Young-Eun Kim**, Choon-Ki Ahn*
*Dept. of Electrical Engineering, Korea University
**Dept. of Mechatronics, Korea University

Abstract

In this paper, we propose a finite impulse response (FIR) filter under malicious cyber attacks. The FIR filter shows the robust performance against the malicious cyber attacks. The Kalman filter (KF), one of the widely used filters, is introduced as a comparison of robust performance of the proposed method. The robust performance of the proposed method under malicious cyber attacks is demonstrated through experimental results.

1. Introduction

Until recently, research on Internet of things (IoT) has been continuing and commercialization has been successful. By controlling the temperature of the between house and outside the house, it becomes easy to see the control of the desired product anytime and anywhere through the Internet. In addition, it was not difficult to see the drones communicating with each other, communicating with each other without going through the crowd [1].

As wireless communication becomes widespread, debate about cyber attack issue has been becoming active. Particularly in autonomous vehicle research, the cyber attack could lead to unintentional traffic accidents. This leads directly to human casualties, which raises the question of the stability of autonomous vehicles. In addition to this, IoT technology is expected to be expanded further, so the response to cyber attack is also expected to become a bigger issue [2], [3].

In the wireless environment, this part can be supplemented by an appropriate state estimation algorithm when the input data is damaged due to the cyber attack. In this paper, we design a state estimator for cyber attack and propose a robust algorithm using finite impulse response (FIR) filter. The inertial measurement unit (IMU) is constructed to perform the experiment for demonstrating the performance of the proposed filter.

This paper consists of three sections. In Section 2, the modeling of cyber attacks and design of the FIR filter are presented. In Section 3, the experimental setup, and experimental results with IMU model are demonstrated. Finally, in Section 4, concluding remarks are presented.

2. Design of FIR Filter

A. Cyber Attack modeling

In this paper, the cyber attacks are injected as follows:

$$\bar{y}(t) = y(t) + c_A(t), \tag{1}$$

where $\bar{y}(t), y(t), \text{and } c_A(t)$ represent sensor output which includes malicious cyber attacks, sensor output without cyber attacks, and cyber attacks, respectively. In (1), $c_A(t)$ is defined as 3 models; Impulse cyber attack, and missing cyber attack.

The mathematical model of the cyber attacks can be represented in terms of the moment when the attack comes in where it is defined as t_A. Firstly, (1) can be reformulated by considering the impulse cyber attack as follows:

$$\bar{y}(t) = \begin{cases} K, & t = t_A, \\ y(t), & otherwise. \end{cases} \tag{2}$$

where $R(c_A(t))$ can be obtained through a probability density function (PDF), indicating the probability that the cyber attack, $c_A(t)$, can have a certain value.

At last, (1) can be rewritten in consideration of the missing cyber attack as follows:

$$\bar{y}(t) = \begin{cases} NaN, & t = t_A, \\ y(t), & otherwise. \end{cases} \tag{4}$$

In (4), *NaN* represents an empty value, and the measurements does not return any value when the missing cyber attack injected.

B. FIR Filter

In this section, the system modeling for the FIR filter is

considered. In the linear system, the current state can be represented as a linear combination of the previous states as follows:

$$x_k = Ax_{k-1} + Bu_k + w_k, \tag{5}$$

where *x, k, A, w* denote a state which size is 2 by 1 vector, a discrete time index, system matrix, and system noise, respectively. As shown in (5), the *k*th state is determined by the *(k-1)*th state, the *k*th external input, and the system noise. In this paper, a constant velocity model is used as a model for estimating angular velocity from angles. Therefore, current state and system matrix can be defined as follows:

$$x_k = \begin{bmatrix} \theta_k \\ \dot{\theta}_k \end{bmatrix}, \quad A = \begin{bmatrix} 1 & \Delta t \\ 0 & 1 \end{bmatrix}. \tag{6}$$

In (6), θ, and $\dot{\theta}$ represent the *k*th Euler angle and angular velocity, respectively. Δt denotes a sampling time for receiving the sensor measurements, which means that the kth state is the state at $k\Delta t$ when assuming the time to start the estimation as zero. Those assume that the *k*th angular velocity obtained through the system is equal to the *k*th velocity. However, the actual previous angular velocity and the current angular velocity have different values, and the resulting system error can be expressed as system noise. The system noise shows a large value if the velocity changes abruptly, and a small value if it has a moderate velocity change. The system input is set to zero because there is no external input.

The measured values of the *k*th Euler angles obtained from the IMU can be expressed as follows:

$$y_k = Cx_k + v_k, \tag{7}$$

where

$$C = [1 \quad 0].$$

In (7), v_k represents a measurement noise that is assumed to be mutually uncorrelated with the process noise and zero-mean white Gaussian. The measured value is sum of the current actual Euler angle and the measurement noise.

The FIR filter is a filter with finite impulse response which is considering only finite interval called horizon and defined as *N*. If the impulse response of the filter in the discrete time system with a sample time of Δt lasts to $N\Delta t$, the *k*th output will be determined by the $k-N$ to $k-1$th inputs. The impulse response function and output of the system can be expressed as follows:

$$\begin{aligned} y &= b_0 x[n] + b_1 x[n-1] + \cdots + b_N x[n-N] \\ &= \sum_{i=0}^{N} b_i x[n-i]. \end{aligned} \tag{8}$$

In (19), *n* denotes the *n*th input signal. *n* can be denoted as $n\Delta t$ in consideration of the sampling time.

The FIR filter can be defined as follows [4]:

$$\hat{x}_k = HY_{k-1}, \tag{9}$$

where

$$H = \begin{bmatrix} p_1 & p_2 & \cdots & p_4 \\ q_1 & q_2 & \cdots & q_4 \end{bmatrix},$$

$$Y_{k-1} = [y_{k-N} \quad y_{k-N+1} \quad \cdots \quad y_{k-1}],$$

where H, and Y_{k-1} represent the filter gain and stacked measurements during horizon, respectively. Each component of gain matrix can be obtained through Lagrange function and multiplication, one of the method to solve the equation as follows:

$$H\bar{C}_N = I, \tag{10}$$

where $\bar{C}_N$ represent the observability matrix of the FIR filter and the (10) is derived from the batch from of (5) and (7) under unbiased condition. Because of the horizon, the FIR filter shows robust performance in the presence of cyber attacks.

3. Experiment

Experiments were performed to estimate angular velocity by measuring angle data to show the robust performance of the FIR filter. The hardware for the experiment was constructed base on the Arduino, Servo Motor, and IMU as shown in Fig. 1.

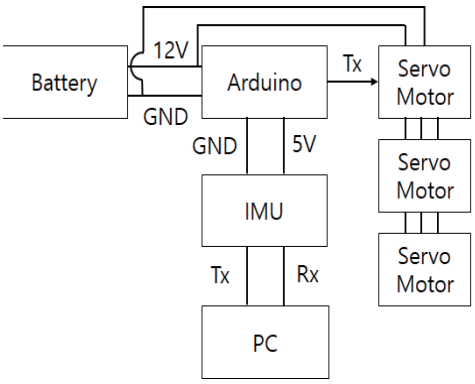

Fig. 1 Hardware block diagram.

A. *Communication*

The communication between the Arduino and Servo Motor is composed of TTL communication, and the communication between IMU and PC is composed of RS232 communication. In the case of Baud Rate, TTL communication was communicated using 100000 bit/s and RS232 communication using 115200bit/s.

B. *Experimental Setup*

The angular data of IMU is received at the same angular velocity and the same angular displacement. After applying each cyber attack model, the angular velocity applied by each filter is compared. The performance of the filter is determined by comparing the mean square error (MSE) with the reference value.

When receiving the angle value, the motor performs a periodic motion. To reduce the error, 2000 values are received. Then, the first 500 and the last 500 number of values are ignored, and the experiments are performed with 1000 number of values.

The angular velocity is estimated using each filter, and qualitative analysis and quantitative analysis are carried out together. Qualitative analysis is performed by observing the graph of angular velocity and recording the characteristic. In the case of quantitative analysis, the time zone in which the angular velocity is being performed is determined, and the angular velocity at that time is extracted, and compared with the reference, the MSE is obtained and compared.

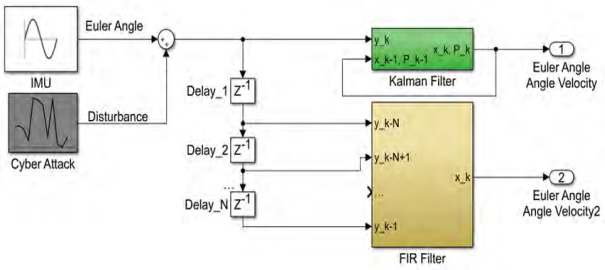

Fig. 2 Experimental system block diagram.

The experiment is performed through the MATLAB Simulink as shown in Fig. 2. The horizon size *N* of the FIR filter is set to 10.

C. Cyber Attack Modeling

In case of impulse cyber attack, impulse is given with a certain probability to disturb the signal. In case of missing cyber attack, the data is deleted with a certain probability to make the data discontinuous and disturb the signal.

D. Experimental Results

The impulse cyber attack is generated with a probability of 5% and an impulse value of 300.

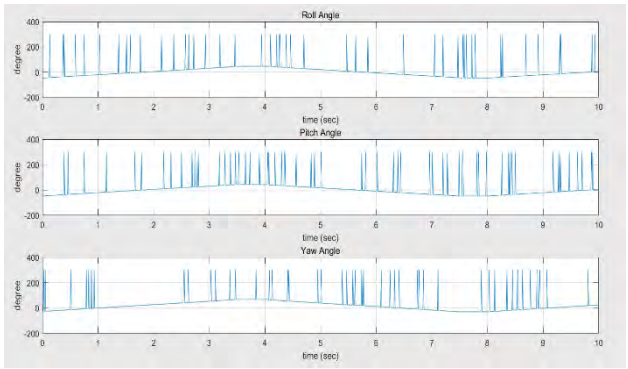

Fig. 3 The measurements under impulse cyber attack.

The experimental results, estimated states from the FIR filter and KF, are shown in Fig. 4, and Fig. 5 under impulse cyber attack.

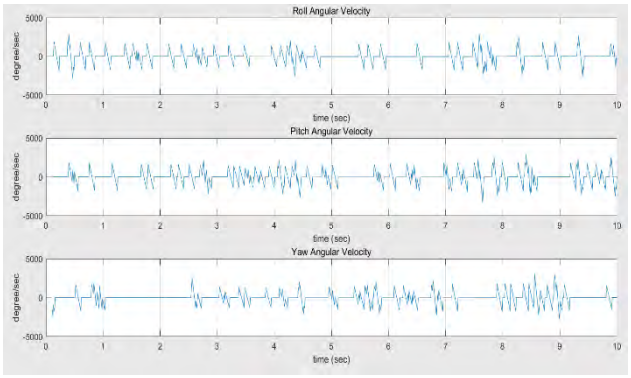

Fig. 4 The estimated angular velocities through FIR filter under impulse cyber attack.

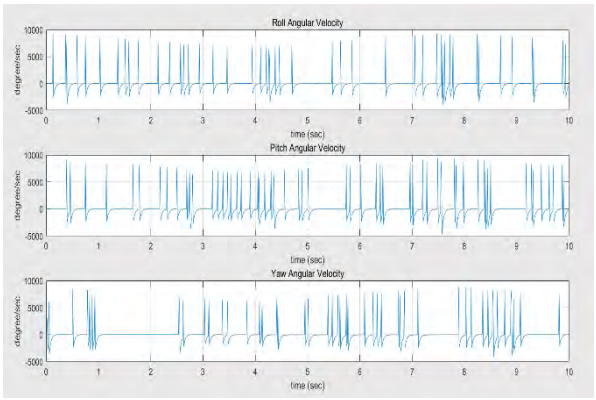

Fig. 5 The estimated angular velocities through KF under impulse cyber attack.

The missing cyber attack is generated with a probability of 50% to eliminate the measurement.

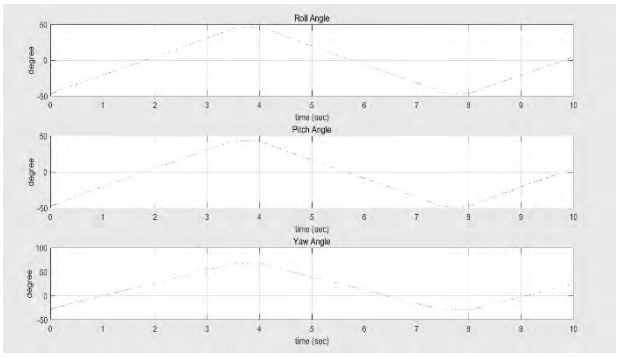

Fig. 6 The measurements under missing cyber attack.

The experimental results, estimated states from the FIR filter and KF, are shown in Fig. 7, and Fig. 8 under missing cyber attack.

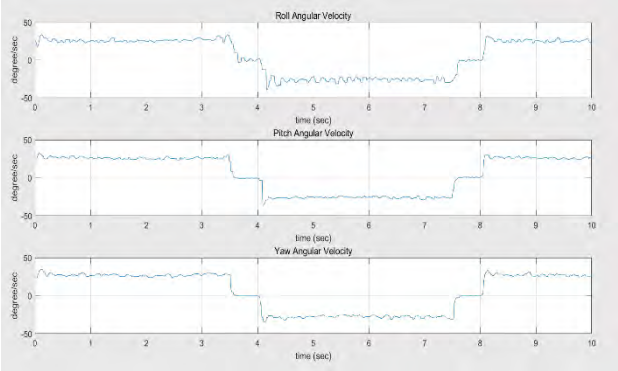

Fig. 7 The estimated angular velocities through FIR filter under missing cyber attack.

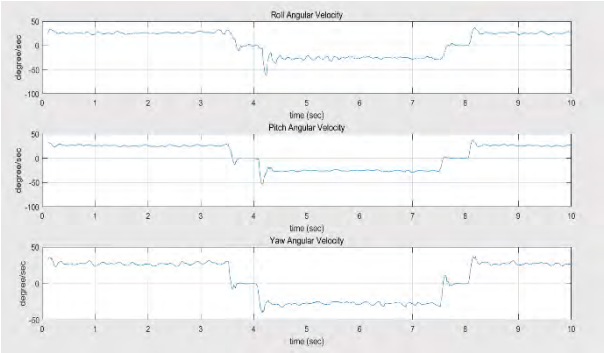

Fig. 8 The estimated angular velocities through KF under missing cyber attack.

In both cases, as shown in Fig. 7 and Fig. 8, the graphs show that the effect of cyber attack is slightly increasing compared to the experimental results without cyber attacks. It was confirmed that the effect is greatly increased every time when the angular velocities are rapidly changed in the KF. In the quantitative analysis, it was confirmed that the error of the KF is slightly larger than the error of the FIR filter.

TABLE I
MSE COMPARISON

MSE	FIR filter (proposed)	KF
Impulse cyber attack	$1.28*10^6$	$1.00*10^7$
Missing cyber attack	32.79	44.12

The MSE comparison of the FIR filter and KF is written in Table I. Overall, the FIR filter shows more robust performance.

4. Conclusion

In this paper, the FIR filter is proposed to estimate the state under malicious cyber attacks. Under all of the predefined cyber attack models (i.e., impulse and missing cyber attacks), the FIR filter shows the robust performance. The robustness of the FIR filter is demonstrated through the experimental using IMU and comparison of MSE. In summary, the performance of the FIR filter seems to be superior to the cyber attacks. Furthermore, through the experimental results of missing cyber attacks, the FIR filter seems to be an appropriate filter for the situation such as disconnection of communication or error occurred in transmission of data.

ACKNOWLEDGMENT

This work was supported partially by the NRF through the Ministry of Science, ICT, and Future Planning under Grant NRF-2017R1A1A1A05001325 and partially by "Human Resources program in Energy Technology" of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) granted financial resource from the Ministry of Trade, Industry & Energy, Republic of Korea (No. 20174030201820)

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*., vol. 29, no. 7, pp. 1645-1660, 2013.

[2] H. Teymourlouei, "Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users," *World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering*., Vol. 9, No. 3, pp. 678-684, 2015.

[3] A. Centinkaya, H. Ishii, and T. Hayakawa, "Networked Control Under Random and Malicious Packet Losses," *IEEE Trans. Automatic Control.*, vol. 62, no. 5, pp. 2434-2449, May. 2017.

[4] You S., Pak J., and Kim J, "Optimal Horizon Size for Unbiased Finite Memory Digital Phase-Locked Loop," *IEICE Electronics Express*., vol. 14, no. 3, pp. 1-9, Jan. 2017.

[5] R. Faragher, "Understanding the Basis of The Kalman Filter Via A Simple and Intuitive Derivation," *IEEE Signal Processing Magazine*., vol. 29, no. 5, pp. 128-132, Sep. 2012.

[6] Kim P., and Huh L., "Kalman Filter for Beginners," *United States CreateSpace*. 2011.