ISSN: 0974-5823 Vol. 6 No. 3 December, 2021

International Journal of Mechanical Engineering

Research and Development of Artificial Intelligence Intrusion Detection System Using Radar Detection Technology

Won-Hyuk Choi
Professor, Department of Marine Sports, Hanseo University, Taean 32158, Korea

Abstract
This paper introduces the development of an external intruder monitoring system that combines big data and machine learning technology based on 24GHz FMCW (frequency modulated continuous wave) RADAR. This project includes development of big data and machine learning-based intrusion detection server, sensor IoT hardware development, 2D spatial information-based monitoring software development, and server interworking communication protocol design. For external intrusion detection, we designed a data collection server to store radar sensor and vibration sensor data in a database and a structure of an intrusion detection server that detects intrusion through machine learning algorithms, and built a platform for big data processing. A function to collect and store radar detection data was developed. Also, the practicality of a machine learning algorithm and signal analysis visualization tool optimized for intrusion detection was demonstrated through analysis of radar signal data measured by different obstacles and noise environment scenarios. In addition, 2D spatial information-based monitoring GUI software for administrators was developed for each mobile operating system such as iOS and Android to facilitate monitoring area mapping, sensor status management, and data analysis.

Keywords: FMCW Radar, 24GHz, Intrusion Detection, Big-data, Machine-learning

I. Introduction

After the terrorist attacks on trade centers in the United States in 2001, the need to strengthen surveillance of public safety around the world was highlighted, and it became an opportunity to increase R&D requirements for security technologies [1][2]. Since then, various types of intrusion detection systems, including video surveillance systems, have been developed, but many problems and limitations have been found due to external environmental factors or the performance of the sensor itself. This is because the existing intrusion detection system simply uses the data acquired from the sensor one-dimensionally to determine whether there is an intrusion, so the disadvantages due to the limitations of the sensor are exposed. Recently, as an effort to compensate for this, a 'convergence system' that applies two or more sensors is being developed, but these also do not overcome the limitations of the sensor. Therefore, our research team uses a 24GHz FMCW RADAR sensor with high resolution and excellent detection performance for moving objects, and by processing the detected data by fusion of big data and machine learning technology. It removes unnecessary clusters and intelligently detects whether there is an intrusion. The limitations of the sensor were overcome by configuring the system to make judgment possible. In addition, for efficient management, the 'manager monitoring system' provides a 2D spatial information-based GUI that can be ported to mobile devices, increasing scalability, immediacy, and intuition for the future.

In Chapter 2 of this paper, an overview of the FMCW RADAR system is introduced, and in Chapter 3, research cases and algorithms for intrusion detection system implementation, and the design of sensor application hardware and software are introduced. And finally, in Chapter 4, conclusions and future research directions are presented and the thesis is concluded.

II. FMCW Radar Overview

Radar was put into practical use in Germany and England in the early 1930s, and was mainly used for military purposes during wartime. However, as components become smaller and cheaper today, radar sensors are being used in various fields such as aviation, shipping, road traffic, and security in the civil sector as well as in the defense sector [3]. As a moving object detection sensor used for commercial purposes, a frequency modulated continuous wave (FMCW) radar is widely used.

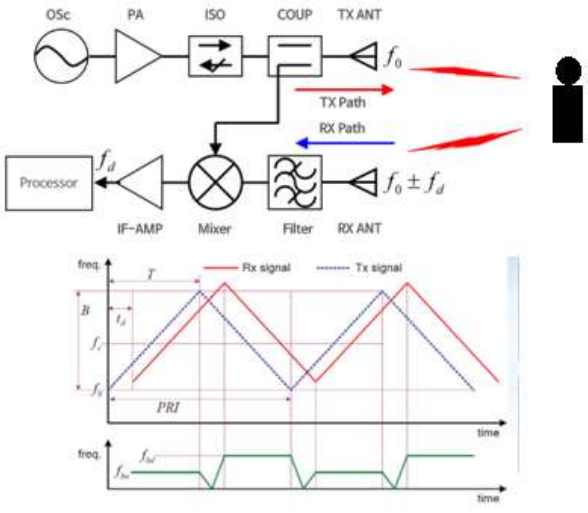

Figure 1. FMCW Radar (Ref. : @craeca.com)

This is because it has a simple structure compared to the conventional pulse radar in system implementation [4][5][6][7]. The FMCW radar converts a triangular or sawtooth wave signal having a linear change with time into FM and emits it, and compares the incoming signal reflected from the target with the transmitted signal. The upper part of Figure 1 describes the

radar's transmission/reception signal processing procedure, and the graph on the bottom shows the frequency of the transmitted signal and the signal reflected from the target. The fast-chirp train modulation method of FMCW RADAR uses 2D FFT (Fast Fourier Transform) to perform distance-velocity mapping, so it is effective because it can easily distinguish a moving target from surrounding noise (clutter). The transmitted signal and the received signal mixed from the radar sensor pass through the LPF, leaving a bit frequency, which is a difference frequency component.

$$F_r = \frac{t_d B}{T}, R = \frac{cTF_r}{2B}$$

When the relative speed of the target with respect to the radar sensor is 0, the time delay td with the target occurs, so the frequency Fr due to the distance difference, and the distance R can be obtained from this. where c is the speed of light, T is the sweep time, and B is the frequency modulation bandwidth. A moving target (when the relative velocity is not 0) has a frequency shift Fd due to the Doppler effect [8][9][10][11].

$$F_r = \frac{B_{btm} + B_{up}}{2}, F_d = \frac{B_{btm} - B_{up}}{2}$$

The resolution (distance resolution ΔR, velocity resolution ΔV_r) of a radar sensor is determined by the sensor-related center frequency (F_c), B, T, sampling frequency (F_s), and the number of FFT points (N).

$$\Delta R = \frac{cT\Delta F}{2B}, \Delta V_r = \frac{c\Delta F}{2F_c}$$

III. Intrusion detection system design and development

1. Big data and machine learning-based intrusion detection server development

1) Intrusion detection system structural design

The data collection server receives the radar signal and vibration sensor data from the sensor IoT board, stores it in the database, and delivers it to the intrusion detection server. Data such as intrusion alarm events, sensor management information, and system information are stored in the database.

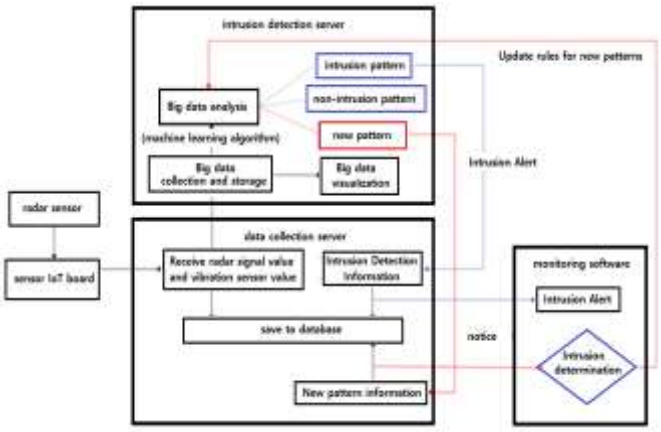

Figure 2. Intrusion detection server structure

The intrusion detection server stores radar signal data and vibration sensor data in Hadoop's HDFS, determines intrusion detection through a machine learning algorithm, and notifies the data collection server when an intrusion is detected. When a radar signal of a new pattern is detected, the rule for intrusion detection is updated by requesting the administrator to determine whether it is an intrusion.

2) Building a big data platform

The existing RDBMS was mainly used for processing structured data, but it is somewhat inappropriate for processing large amounts of data and unstructured data. Big data is used not only to quickly and efficiently process unstructured data and large amounts of data, but also to generate meaningful and precise data by combining it with machine learning [12]. In this regard, the types of big data platforms currently mainly used include Hadoop, Spark, Hive, Sqoop, Pig, ZooKeeper, and the like. In this study, big data and machine learning were used to collect a large amount of data and to obtain accurate intrusion detection results. All programs related to big data were installed and run on Ubuntu 18.04 LTS. In this study, a combination of Hadoop + Spark was used to use big data [13]. Hadoop itself can store and process data, but due to the difference in data processing method between Spark and Hadoop, Spark's processing efficiency is about 10 to 100 times faster than Hadoop, so Hadoop is used for data storage, Data processing was performed using Spark. Finally, a database was built for real-time data inquiry and management of past records in the control PC.

3) Radar detection data collection and big data storage function development

The radar detection data consists of radar signal data and vibration sensor data. The sensor IoT board collects 'radar signal data' and 'vibration sensor data' and sends it to the intrusion detection server. The intrusion detection server collects radar and vibration sensor data from the IoT sensor board and transmits it to the big data server. The socket communication method between the sensor IoT board and the intrusion detection server uses TCP/IP protocol, and the sensor IoT board asynchronously transmits data collected from radar and vibration sensors to the intrusion detection server.

4) Development of sensor data collection and analysis procedures

Radar detectors and cameras were installed at four specific test sites, and the signal values of the radar sensors and the vibration sensor data were collected over a total of six times (five times during the day and once at night). The difference in reflected signal values between the case where the human body was detected and the case where it was not detected within the sensing area was compared, and distance data for each case was extracted and classified.

Figure 3. Equipment for Data Acquisition

Using the data collected in this way, the radar reflection signal value and distance data distribution were analyzed, and data thresholds were defined in the case of detecting the human body and the case of not detecting the human body. In addition, data were collected in various scenarios as follows to confirm the ability to identify intruders. Scenarios were composed in various ways, such as wall transmittance test, error possibility test due to internal shaking, fixed obstacle test, and facility proximity test, so that intrusive objects could be identified from vibrations that could cause a detection error or noise in the initial surroundings.

A procedure was developed to analyze the actual radar signal data collected through this procedure by item according to each scenario.

5) RADAR Sensor IoT hardware and software implementation

The IoT hardware to which the intrusion detection sensor is applied uses a low-power processor so that it can operate for a long time in places and environments where power supply is difficult. The IoT board analyzes the data collected from the 9-axis sensor, measures the vibration intensity, and transmits the radar sensor data to the server PC in real time. When intrusion detection and abnormality are detected, the buzzer attached to the sensor IoT device sounds an alarm to warn a dangerous situation. The sensor IoT hardware was designed to minimize power consumption by using a low-power processor of the STM32F4 series, and the radar sensor was designed to be controlled through the STM32F4 serial interface. In addition, an Ethernet chip for socket communication with the server and an LED and buzzer circuit diagram for expressing abnormal status were included in the design. The board is implemented in the form of an Arduino expansion interface circuit that can add various sensors such as temperature/humidity and barometric pressure sensors in the form of a module.

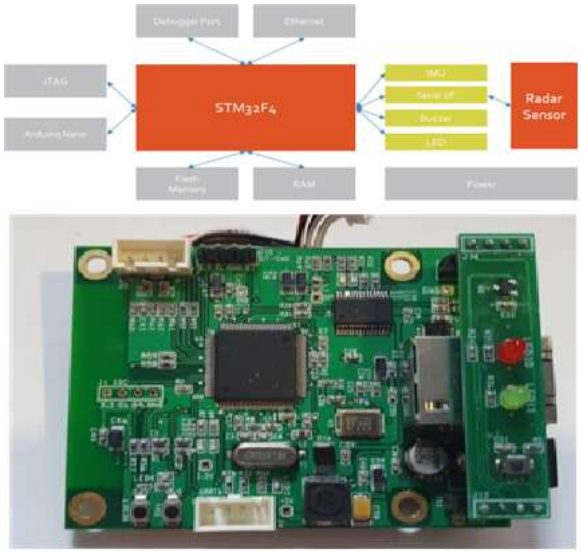

Figure 4. IoT H/W block diagram and Board configuration

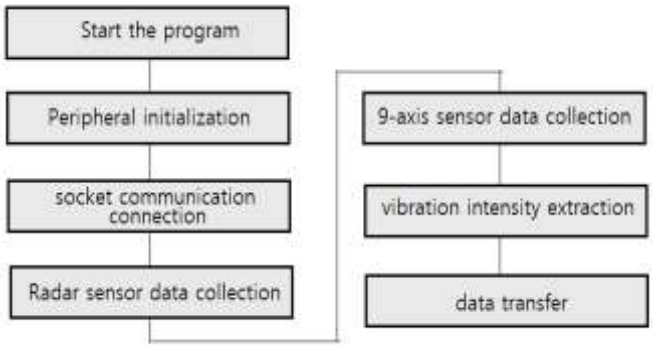

Figure 5. Sensor IoT module S/W configuration

Since the Radar sensor module uses a serial interface, the serial device of the sensor IoT board is initialized to receive data. The operation mode was set to operate in the interrupt mode to accurately check the data reception time. It checks whether the received data is the beginning of the Radar sensor module data, and if a header message is received, receives the Radar data and transmits the received data to the server using T_{cp} socket communication. To measure vibration, initialize the 9-axis sensor and receive Roll/Pitch/Yaw data values. The vibration intensity is calculated using the received Roll/Pitch values, and then the Roll/Pitch/Yaw and vibration intensity values are transmitted to the intrusion detection server. The vibration intensity measurement calculation formula is as follows. You can adjust the sensitivity of the vibration intensity by setting the scale value, and the default setting value is 100. Here, V_s is the intensity of vibration, and S_v is the scale value.

$$V_s = \sqrt{\left((Roll \times Roll) + (Pitch \times Pitch)\right)} \times * S_v$$

2.Signal analysis by sensor data collection scenario

Scenarios consisted of a wall transmittance test, an obstruction test by an obstacle, an interference test by a nearby facility, and a moving target detection error test by a moving object in the vicinity.

The wall transmittance test was conducted using a table tennis table, white board, glass window, etc. As shown in the figure 6, when there is a wall, the signal level did not exceed 900, but it was confirmed that the signal level exceeded 2000 when recognized by a person.

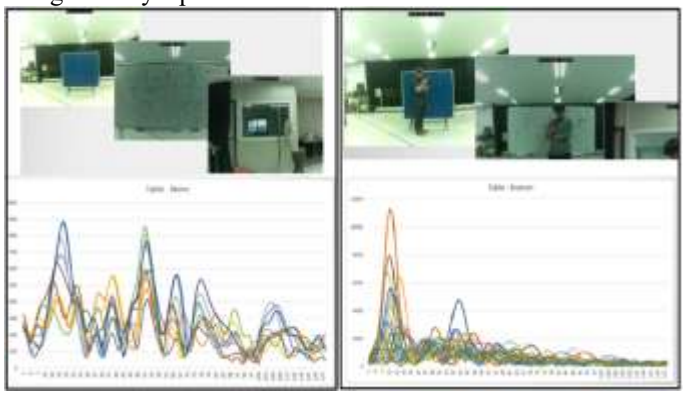

Figure 6. Wall transmittance test (L: without person)

In the test for the possibility of interference by an obstacle, a potted plant was used. As shown in the figure 7, when there is an obstacle, the signal level does not exceed 800, but when a person is recognized, it can be confirmed that the signal level exceeds 2000 or more.

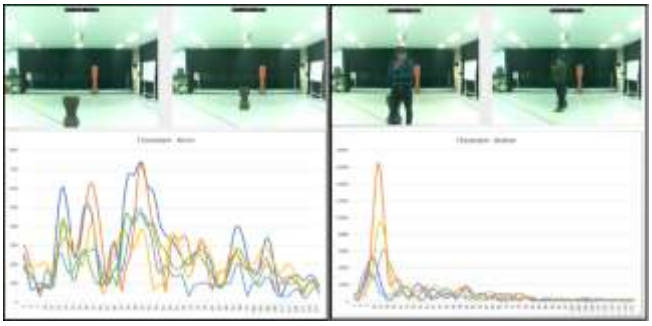

Figure 7. Target non-detection possibility test by obstacles (L: without person)

The interference test of adjacent facilities was tested using a fan, air conditioner, etc. As shown in the figure 8, when there is an obstacle, the signal level did not exceed 600, but it was confirmed that the signal level exceeded 2000 when a person was recognized.

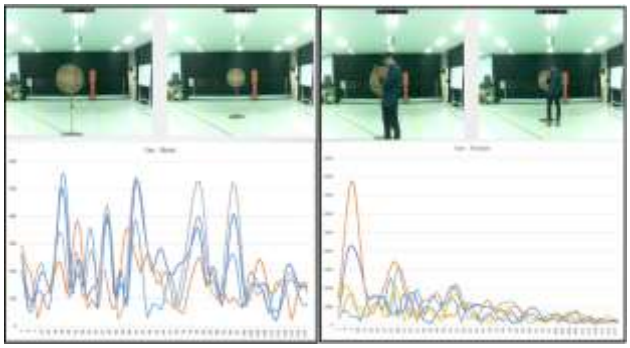

Figure 8. Detection test near ancillary facilities

The detection error test by a moving object was tested using a curtain, etc. As shown in the figure 9, when there is a curtain, the signal level does not exceed 1200, but when a person is recognized, it can be confirmed that the signal level exceeds 2000.

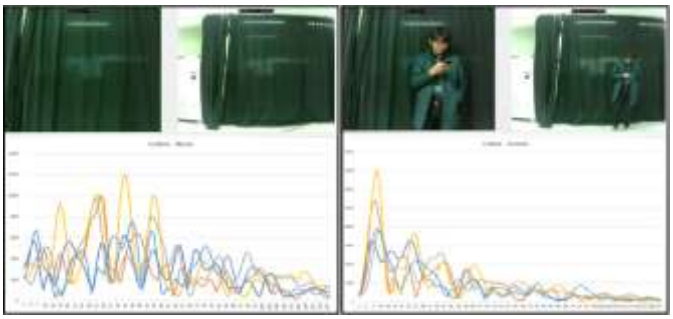

Figure 9. Possibility test of detection error due to shaking of surrounding objects

As shown in Table 1, through tests conducted in various environments, it was confirmed that there was no problem in recognizing the radar signal level because there was a large difference in the presence or absence of a person. Therefore, even if there are obstacles or facilities in the vicinity, it was judged that it is possible to apply an algorithm that detects the peak value by extracting the average value or the signal band for the signal level at which these signals are formed.

Table 1. Signal analysis results for each scenario

Test Scenarios	Without Man	With Man
Wall transmittance	~900	2000~
Obstruction by obstacles	~800	2000~
Interference nearby facilities	~600	2000~
Moving target detection error by surrounding moving objects	~1200	2000~

3. Designing Machine Learning Algorithms for Intrusion Detection

1) Moving Average Algorithm

The Moving Average method recognizes an intrusion detection when a person's motion is detected and the signal value suddenly soars. Moving Average is often used to see the stock price trend, and it is a technique used to see the stock price trend by figuring out the phenomenon from the average value of the past.

When a sudden change in value occurs, moving average is used to identify it. Intrusion is detected using the same method.

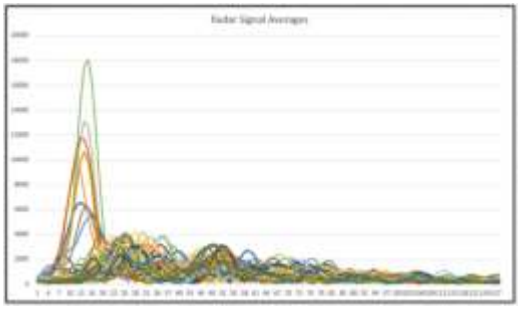

Figure 10. Moving Average Method

Obtain the moving average of 5 minutes for the radar signal and the moving average for the standard deviation for the period of 15 minutes. And when a specific signal value exceeds 3 sigma of the standard deviation from the moving average line, it is judged as abnormal and determined to be intrusion detection. The window size for the mean was set to 5 minutes, the window size for the standard deviation to 15 minutes, and the confidence interval standard was set to 3 sigma.

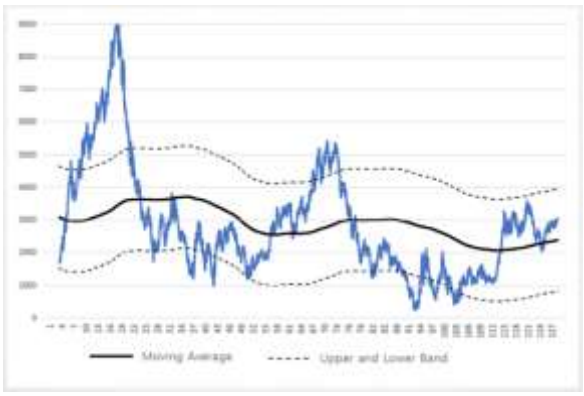

Figure 11. Moving Average

2) GAN(Generative Adversarial Network) Algorithm

Using GAN algorithm of machine learning, a signal band corresponding to the normal range is formed, and when it is out of this range, it is recognized as intrusion detection. The GAN algorithm is one of the generative models that generate results, and is a method of learning how to generate results by competing two opposing neural networks.

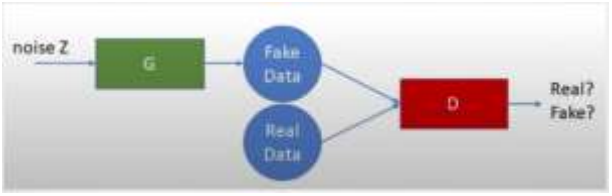

Figure 12. GAN Algorithm

The GAN algorithm consists of two neural networks. One neural network called 'Generator' generates new data, and the other 'Discriminator' evaluates the authenticity of the data. In other words, the discriminator determines whether each data instance reviewed is an actual training data set or not. When generating data using a generator, it is possible to create data that does not actually exist, but imitates it, and it enables the creation of numerous fake data similar to real data. In this case, a random noise z is given as an initial input value.

3) Implementation of intrusion detection algorithm applying GAN

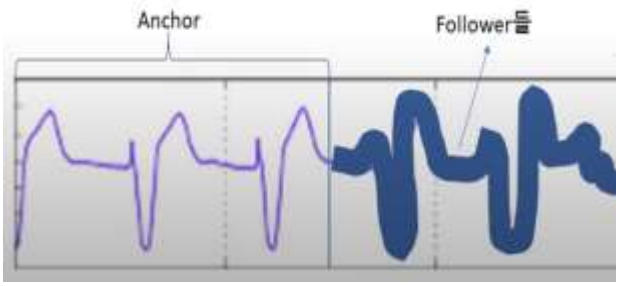

Figure 13. Anchor and Follower

A normal radar signal obtained from the database is defined as the actual data (Anchor), and these signals also show a slight difference when the input (Follower) is continuously accumulated. By continuously overlapping using these data, a range of data belonging to the normal can be created. This normal range is generated using the GAN model. Afterwards, the learned generator can generate signal data similar to real data.

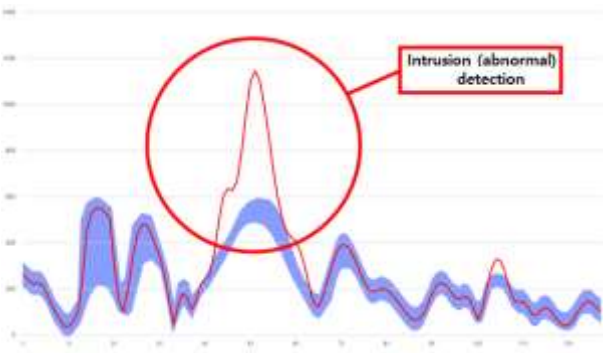

Figure 14. Intrusion (anomaly) detection

The intrusion detection algorithm puts normal data as an anchor and receives an input signal along with noise and determines that the data is out of the normal range as abnormal. The intrusion detection algorithm implemented with GAN can immediately determine whether real-time data is out of range, so real-time intrusion (abnormality) detection and prediction is possible. Algorithm implementation using the GAN model consists of the following 6 steps.

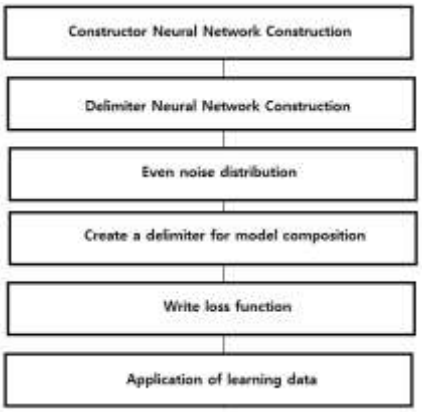

Figure 15. GAN Model Algorithm

The first stage is the construction of the generator neural network, and the generator and the delimiter are simultaneously learned using the GAN model. The second step is the configuration of the discriminator neural network, and the discriminator uses the same variables when discriminating real radar sensor data and fake radar data. Step 3 is a noise uniform distribution step, and the noise generation utility function is written to generate noise with an even distribution. Step 4 is the delimiter creation step for model configuration, and the generator is configured and delimiters are created one by one using the real radar sensor data and the radar sensor data created by the generator. And, by adding label information to the generator, it was induced to generate radar sensor data corresponding to the label information later. Step 5 is the loss function creation step. The code was written so that the value of the variable that determines the real radar sensor data is close to 1 and the value of the variable that determines the fake radar sensor data is close to 0. The last 6 step is the application of the learning data, and the actual data is inputted using only the generator by the written algorithm to obtain the tolerance band, and then, the real-time data and the tolerance band value are compared to detect abnormalities.

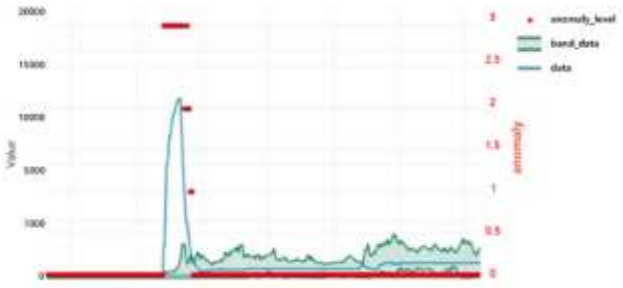

Figure 16. Anomaly detection using normal band

As a result of running in the test environment, as shown in Fig. 16, it had a value of 0.5 or less under normal conditions, but when an intrusion was detected, an anomaly value close to 3 could be obtained.

4.Implementation of 2D spatial information-based monitoring software

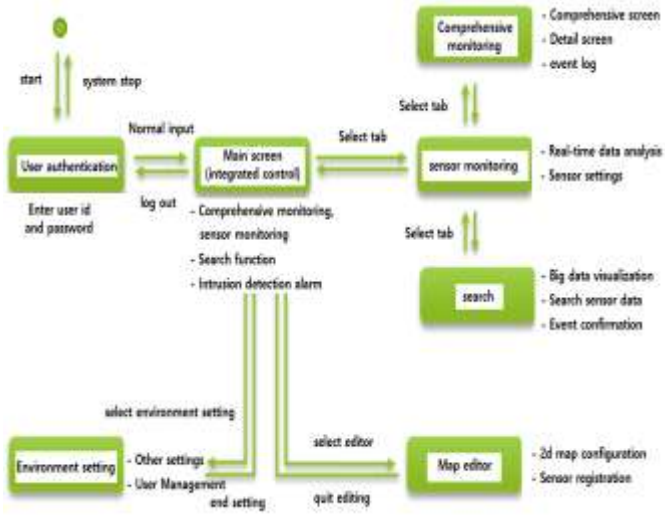

Figure 17. S/W function block diagram

The monitoring software was written for the purpose of effective facility management by providing the operator with real-time information on whether or not intrusion into the facility has occurred. In order to provide this monitoring function more intuitively and efficiently, it is composed of a 2D map-based display and includes individual sensor data analysis and search functions. The 2D map, which is a basic configuration, was applied to the software through image work for the building where the intrusion detection system will be installed. The monitoring software intuitively displays the status of the radar intrusion detector, and is designed to display intrusion information events in real time to enable immediate alert recognition and response.

Figure 18. GUI Screen configuration

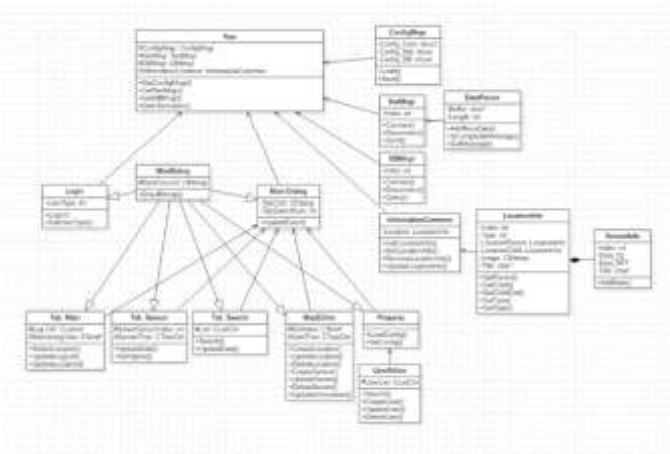

Figure 19. IOS App development class diagram

The GUI configuration of the monitoring software consists of login, main screen for integrated control, system comprehensive monitoring page, monitoring page for each registered sensor, search page including big data visualization and log analysis function, map editing page for 2D map environment management, program Configuration pages for managing configuration parameters required for execution are included.

Mobile apps for administrators were written separately for Android and iOS, and classes were added according to the method of operation on each screen by dividing them into classes that compose the screen of the app for each function. Figure 19 is an example of an iOS app development class.

IV. Conclusion

Globally, the importance of social safety is being highlighted, and as a result, R&D investment in the field of security technology is increasing. Various types of intrusion detection systems, including video surveillance systems, are continuously being developed, but the monitoring performance is limited due to various reasons such as the surrounding environment and sensor functions. To solve these problems, we developed an intrusion detection system hardware using a 24GHz FMCW RADAR sensor with high resolution and high detection performance, and realized an algorithm capable of intelligently processing the detected data in real time by fusion of big data and machine learning technology. In addition, through repeated tests for each different condition scenario in the field, the performance of the system capable of separating the intrusion signal from the surrounding cluster into a signal size of three times or more was verified and the practicality of the intrusion detection system was confirmed. In addition, for efficient monitoring, a 2D spatial information-based GUI app that can be ported to Android and iOS operating system mobile devices is provided to increase scalability, immediacy, and intuitiveness for the future.

In the future, the radar sensor-based intrusion detection system will be mounted on a search/reconnaissance robot or vehicle to conduct real-time area mapping, intruder (target) detection, and identification under continuously changing environmental conditions.

This paper was researched with the research funding of Hanseo University Industry-University Cooperation Foundation.

References

[1] Kang, Wonho, Choi, Gyunghyun, “R&D Opportunity Technology Selection in Intelligent Video Surveillance Industry”, Journal of Korea Technology Innovation Society, Volume 20 Issue 3, pp.781-804 , 2017.

[2] Jeong yongtaek, “Security Sensor Status and Prospect”, The Magazine of the IEIE, Volume 36 Issue 10, pp.49-59, 2009.

[3] G. Reina, D. Johnson and J. Underwood, “Radar Sensing for Intelligent Vehicles in Urban Environments,” MDPI Sensors, Vol.15, pp.14661-14678, 2015.

[4] M. A. Richards, Fundamentals of Radar Signal Processing, McGraw-Hill, New York, pp.198-201, 2005.

[5] M. S. Lee and Y. H. Kim, “Design and Performance of a 24-GHz Switch-antenna Array FMCW Radar System for Automotive Applications”, IEEE Trans. on Vehicular

Technology, Vol.59, pp.2290-2297, 2010.
[6] E. Hyun, Y. S. Jin and J. H. Lee, “A Pedestrian Detection Scheme Using a Coherent Phase Difference Method Based on 2D Range-Doppler FMCW Radar,” MDPI Sensors, Vol.124, No.16, 2016.
[7] J. Park, D. Jung, K. Bae and S. Park, "Range-Doppler Map Improvement in FMCW Radar for Small Moving Drone Detection Using the Stationary Point Concentration Technique," in IEEE Transactions on Microwave Theory and Techniques, vol. 68, no.5, pp. 1858-1871, May 2020.
[8] M. Kronauge, C. Schroeder and H. Rohling, “Radar Target Detection and Doppler Ambi guity Resolution,” In Proceedings of the 11th International Radar Symposium, pp.1-4, 2010.
[9] M. Andres, W. Menzel, H. L. Bloecher and J.Dickmann, “Detection of Slow Moving Targets using Automotive Radar Sensors,” In Proceedings of the 7th German Microwave Conference, pp.1-4, 2012.
[10] C. Schroeder and H. Rohling, “X-Band FMCW Radar System with Variable Chirp Duration,” IEEE Radar Conference, pp.1255-1259, 2010.
[11] V. Winkler, “Range Doppler Detection for Automotive FMCW Radar,” In Proceedings of European Microwave Conference, pp.166-169, 2007.
[12] Chen, M., Mao, S. & Liu, Y. Big Data: A Survey. Mobile Netw Appl 19, pp.171–209, 2014.
[13] Ilias Mavridis, Helen Karatza, "Performance evaluation of cloud-based log file analysis with Apache Hadoop and Apache Spark", Journal of Systems and Software, Volume 125, Pages 133-151, 2017.