ISSN : 1226-7244 (Print)
ISSN : 2288-243X (Online)
논문번호 21-02-03
j.inst.Korean.electr.electron.eng.Vol.25,No.2,252~260,June 2021
https://doi.org/10.7471/ikeee.2021.25.2.252
19

Identification of Wi-Fi and Bluetooth Signals at the Same Frequency using Software Defined Radio

Van An Do*, Biswarup Rana**, Ic-Pyo Hong*★

Abstract

In this paper, a method of using Software Defined Radio (SDR) is proposed for improving the accuracy of identifying two kinds of signals as Wireless Fidelity (Wi-Fi) signal and Bluetooth signal at the same frequency band of 2.4 GHz based on the time-domain signal characteristic. An SDR device was set up for collecting transmitting signals from Wi-Fi access points (Wi-Fi) and mobile phones (Bluetooth). Different characteristics between Wi-Fi and Bluetooth signals were extracted from the measured result. The SDR device is programmed with a Wi-Fi and Bluetooth detection algorithm and a collision detection algorithm to detect and verify the Wi-Fi and Bluetooth signals based on collected IQ data. These methods are necessary for some applications like wireless communication optimization, Wi-Fi fingerprint localization, which helps to avoid interference and collision between two kinds of signals.

Key words : Wi-Fi, Bluetooth, Signal Identification, Software Defined Radio, Time Domain

Ⅰ. Introduction

The frequency band of 2.4 GHz so-called industrial, scientific and medical (ISM) band [1] is a free band unlike many other kinds of the frequency band. The devices operating at the ISM band are permitted without any licenses. Wi-Fi and Bluetooth technology are the two types of technology that are the most popular technology working at ISM band. As their wide application in human life, like as wireless LAN, internet access, file transferring, CCTV video streaming or some other kinds of IoT applications, there is a bulk quantity of device transmitting/receiving these kinds of signals, along with high power density of Wi-Fi and Bluetooth signals in a wireless communication environment. It is necessary to optimize the quality of service, signal power strength, enhance the error tolerance or the ability to identify noise from other sources in a complex communication environment with multiple types of signal or noise at the same frequency band [2].

Different types of methods were proposed to resolve these kinds of issues like Wi-Fi signal beamforming direction optimization using intelligent reflecting surface [3], Wi-Fi signal direction optimization by Wi-Fi fingerprinting indoor localization

* Dept. of Information & Communication Eng., Kongju National University
** Smart Natural Space Research Centre, Kongju National University
★ Corresponding author
E-mail : iphong@kongju.ac.kr, Tel : +84-41-521-9199
※ Acknowledgment
Manuscript received Apr. 23, 2021; revised May. 31, 2021; accepted Jun. 1, 2021.
This work was supported in part by the Basic Science Research Program under Grant 2020R1I1A3057142, and in part by the Priority Research Centers Program through the National Research Foundation of Korea under Grant 2019R1A6A1A03032988.

[4], FHSS(frequency hopping spread spectrum), DSSS(direct sequence spread spectrum), optimizing fault-tolerance topology in wireless mesh network [5]. The primary requirement of any wireless signal optimization method is to recognize and identify the noise source first. Both Wi-Fi and Bluetooth signals are transmitted at the same 2.4 GHz frequency and interference happened. A detection algorithm based on a signal characteristic would help to identify Wi-Fi and Bluetooth signals in this experiment. There are various techniques available in the literature for the identification of wireless signal interference. Some commercial system uses their customize hardware and software to detect signal interference like Spectrum XT, CleanAir, AirMaestro. Different researchers use different modulation types like QPSK, BPSK, GMSK in their study.

The most common method of modulation detection and classification is spectrum cyclostationary [6], [7]. Nowadays, some researchers use the neural network or some statistical classification method to detect signals which are based on data science and machine learning. Along with multiple methods of signal classification, there are many kinds of parameter or feature may be extracted, such as bandwidth, spectral signature, pulse signature [8], inter-pulses signature, pulse spread, FHSS mechanism, DSSS mechanism.

In this paper, a new method of analyzing and identifying signals based on time-domain using a Software Defined Radio (SDR) device is proposed combined with an integrated database for smart computing. This method is easy to implement, cost-efficiently, and highly accurate for real-time enforcement.

HackRF One device is leveraged for SDR devices. Because of its cost-effectivity, portability, and programmability, this kind of device is very popular with researchers who are involved in the digital signal processing study[9]. The scientist could use the SDR device as an alternative Spectrum Analyzer, and the developer can use the HackRF device for mobile communication, GPS locating device, Hacking tool for jamming frequency band, replay attack for unlocking a car door, magnetic rolling door [10], etc. In military or civil applications, HackRF can be used to track Aircraft by ADS-B signal [11], track marine ship by AIS signal [12], or even track a satellite and receive photoshoot from satellite [13]. In military wireless communications, the information should be secure. It requires complex, flexible and strong algorithms to encode the data before transmitting it over the air. Developers or engineers can use the HackRF device to program and implement any kind of encoding or decoding algorithms without fabricating the RF hardware. The user, researcher, or developer just needs a HackRF device connected to a computer via a USB cable. The user could adjust the frequency band to measure and collect RF data in the range of 1 MHz to 6 GHz, and the bandwidth of 20MHz. There are many kinds of dedicated software for signal observation, measurement, or programming which are compatible with SDR devices.

In this study, GNU Radio Companion and Universal Hacking Radio for signal measurement and collection, programming for processing baseband IQ data were used. About the algorithm for Wi-Fi and Bluetooth Identification, based on signal pulse characteristic and inter-pulse duration, we developed an algorithm to compute these kinds of features then classified them based on measurement results and the theory of Wi-Fi and Bluetooth signal features. While other studies of Wi-Fi and Bluetooth identification using the method of identifying Wi-Fi and Bluetooth based on frequency domain features, it is hard to identify Wi-Fi signal from Bluetooth signal in case of interleaving. We utilize the extracted features of signal pulse in the time domain and this kind of method helps us identify exactly the kind of signal pulse or the inter-pulse interval following their location on the time domain. Based on the output database of a signal pulse position, the signal pulse and inter-pulse interval can be identified. We could calculate the proportion of interleaving and collision between two kinds of mixing transmitted signals.

Ⅱ. Signal Characteristics

In this study, the RF signal is measured at 2.4 GHz center frequency with 20MHz bandwidth, received by HackRF One device, and stored under baseband IQ data type samples. The sampling rate was set up to 100,000 samples per second. The central processing unit of HackRF processes every vector 2047 to 4096 samples rotationally. The IQ sample data is shown visually by Universal Radio Hacker software on the time domain or frequency domain.

1. Wi-Fi Signal

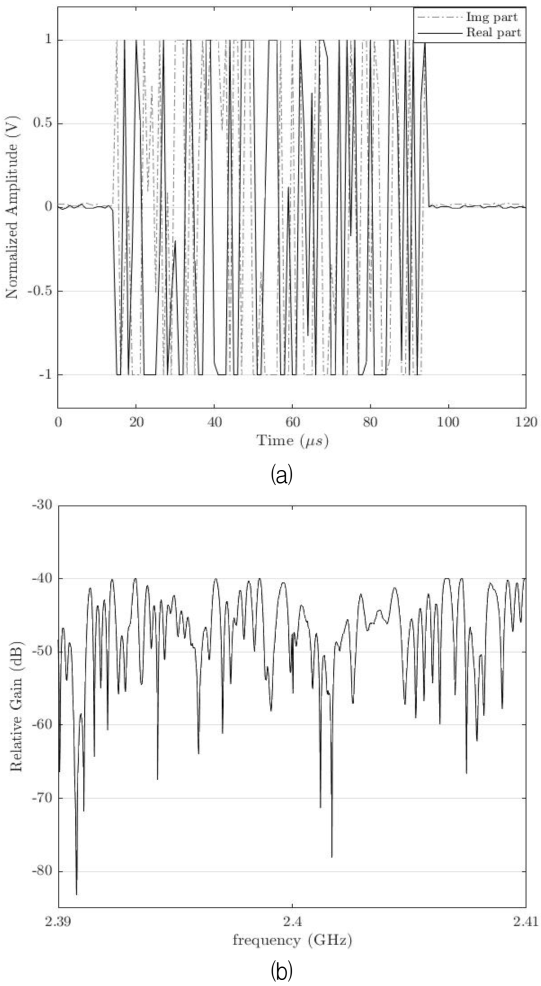


Fig. 1. (a) Wi-Fi signal pulse;
(b) Wi-Fi Signal in frequency domain.

Figure 1(a) depicts the Wi-Fi signal pulse shape in the time domain. As an OFDM symbol in 802.11x standard [14], a Wi-Fi signal pulse range up to 80 samples, including 64 samples point for FFT/IFFT in OFDM modulation/demodulation, and 16 samples for cyclic prefixes. The Wi-Fi signal pulse's length in Figure 1(a) is 80 samples. In some cases, the Wi-Fi pulse's length may be unstable due to noise or interference from another signal source. Figure 1(b) depicts the Wi-Fi signal pulse transformed into the frequency domain. As the frequency band in the experiment is 2.4 GHz and the range of measured bandwidth is 20 MHz, Figure 1(b) depicts a Wi-Fi signal pulse occupied full band of 20 MHz for Wi-Fi signal transmission.

2. Bluetooth signal

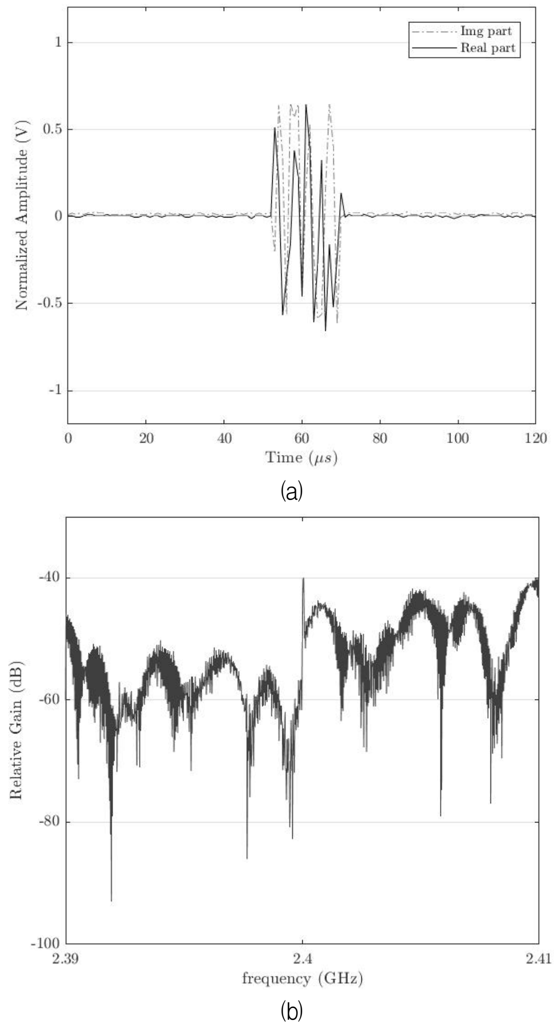


Fig. 2. (a) Bluetooth signal pulse;
(b) Bluetooth signal in frequency domain.

Figure 2(a) illustrated our measurement result of Bluetooth signal pulse. This result pointed out the length of the Bluetooth signal pulse is shorter than Wi-Fi. The length of the Bluetooth signal pulse is calculated to occupy in range 14-17 μs, the most common value is 16 μs per signal pulse.

Another clear difference between Wi-Fi and Bluetooth signal pulses is the dispersal level of signal peak magnitude. While the peak magnitude of Wi-Fi is high proportion stable, the magnitude of Bluetooth signal got higher dispersal level. Figure 2(b) illustrates Bluetooth signal spectrum spread in the range of 1 MHz to 2 MHz as regulation in IEEE 802.15.1 WPAN standard. As the measurement result, the Bluetooth signal band occupied in range of 1 MHz to 2 MHz and implement FHSS mechanism, while the signal band of Wi-Fi occupied full measurement band 20 MHz. An identification system may use a correlation method for detecting Bluetooth spectrum signals, but this method is so sensitive to noise and interference, especially in the case of Wi-Fi and Bluetooth interference.

3. Wi-Fi and Bluetooth signal coexistence

Every device of RF technology should improve its ability to reduce interleaving, collision, or enhance fault tolerance. In case Wi-Fi and Bluetooth coexist in the same band, to reduce the ability of interleaving, they use different inter-pulse duration.

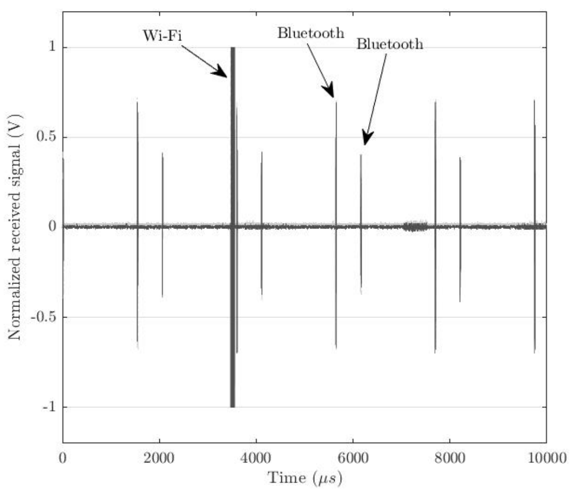


Fig. 3. Wi-Fi and Bluetooth coexistence in time domain.

In the measurement figure below, we capture a wide range of signals in the case of Wi-Fi and Bluetooth signal coexistence on the time domain.

20 MHz is the standard of 802.11a and 802.11g by IEEE and the usual option for Wi-Fi channel bandwidth. In our study, we also scanned signal waves at the maximum bandwidth of 20 MHz of HackRF, with 8-bit ADC converter resolution [15]. As the spectrogram result illustrated the range of bandwidth in Figure 3, Wi-Fi signal occupies a full measurement channel.

Wi-Fi signal of Figure 3 uses a longer range of time interval between Wi-Fi signal pulse, while Bluetooth signal uses much shorter inter-pulse time interval, and the interval value may be changed following time flow based on the design of each manufacturer. As in this study experiment, the inter-pulse arrival time between Wi-Fi pulse is approximately 20000 μs and 500 μs for Bluetooth signal.

III. Measurement Scenario and Setup

The experiment set up in an indoor building environment, where Wi-Fi signal source is available from multiple sources like Access Points. Bluetooth signals may also be received from many kinds of devices like wireless mouses, wireless speakers, or cell phones in active mode. As mentioned in Section I, Wi-Fi and Bluetooth are two typical types of wireless technology affected and widely used in human life which operate on ISM band, therefore it's easy to get the signal source of Wi-Fi and Bluetooth from civil, home appliance equipment. Implicitly, building indoors is quite ideal for implementing this experiment. Our measurement setup for an experiment is configured as shown in Figure 4 below.

To configure and program for collecting and computing, processing data, HackRF One device connected to Laptop PC via a USB 2.0 cable. A proper driver necessary for PC recognizes peripheral devices like HackRF needs to be installed and dedicated software for configuring HackRF and collecting data. In this study, we use the GNU Radio Companion (GRC).

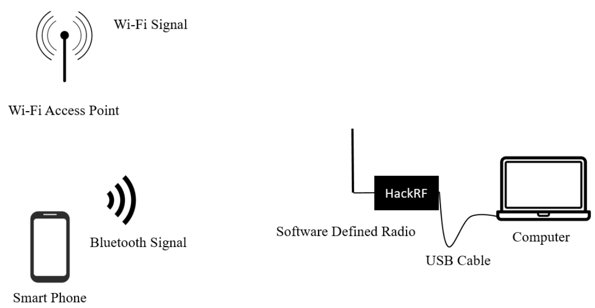


Fig. 4. Measurement Setup.

IV. Identification Algorithm

1. Wi-Fi and Bluetooth Signal Identification

Wi-Fi and Bluetooth signals appeared under pulse form. Therefore to discriminate signal pulse from background noise in the time domain, we should choose a proper energy threshold parameter. The baseband IQ data samples in the time domain contain the sample point's amplitude stays in range -1 to 1 due to normalization. As OFDM and 801.11a standard, every Wi-Fi pulse occupies 80 samples, therefore the signal pulse length threshold was set with that standard. Also, applying this method for Bluetooth pulse, pulse length threshold for determining Bluetooth signal is in range 13 to 17 samples.

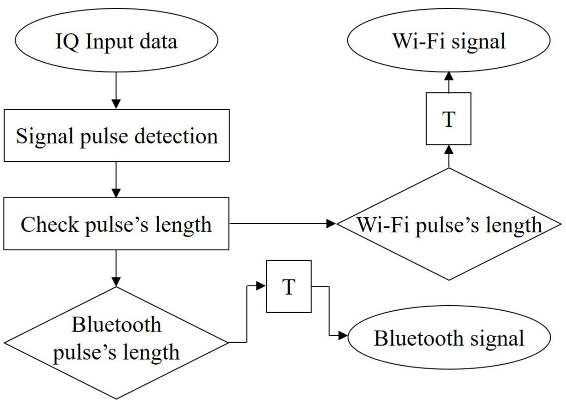


Fig. 5. Algorithm of Wi-Fi and Bluetooth identification.

The threshold for the distance between signal pulse also has to be set, to determine every location of a signal pulse including starting point, endpoint, length of the signal pulse, derived from those parameters, the distance between signal pulse could be computed. An algorithm presents in Figure 5 to detect Wi-Fi and Bluetooth signals will process and compute every 2047 to 4096 IQ samples per input vector.

2. Inter-pulse time interval computing

In this Section, the algorithms for computing the inter-pulse time interval between adjacent signal pulse and the time interval between the same type of signal-pulse (Wi-Fi to Wi-Fi, Bluetooth to Bluetooth) is proposed.

Table 1. Database structure for storing data and computing collision detection.

Field	Description
Signal ID	Auto-assigned increasing ID for every array of IQ data samples following sliding window size to process sequentially
Signal length	Storing data of array length each time processing
Pulse ID	Auto-assigned increasing ID for each pulse detected in each IQ signal sliding window
Pulse type	Storing data of pulse type included: Wi-Fi, Bluetooth, or Others
Pulse length	Length of signal pulse, help determine the type of signal pulse
Start point	Start point of signal pulse in array following the sequence of sample points in array
End point	End point of signal pulse in array following the sequence of sample points in array
Distance to last pulse	Number of IQ sample points between adjacent pulses
Distance to last same type of pulse	Number of IQ sample points between adjacent same type of pulses, like Wi-Fi to Wi-Fi, Bluetooth to Bluetooth
Distance to end of Array	Number of sample points from End point of signal pulse to end point of Array

To support computing, a structured database is developed for storing, querying the signal feature data. The system process bulk of input IQ data following the size of the sliding window on the time domain, therefore all of the signal features like signal pulse, position, signal pulse length, sliding window size, etc, need to be calculated and stored in the database. The algorithm may calculate inter-pulse time intervals based on stored data in the database.

The structure of the database includes fields is shown in Table 1. The database structure proposed in Table 1 helps the detection system not only working in the offline phase but also helps the detection system working in the online phase for real-time processing. Besides that, this database structure help decreasing RF received data size by extracting some important parameter like as: pulse position, pulse type, pulse distance will be computed in Algorithm B presented in Figure 6.

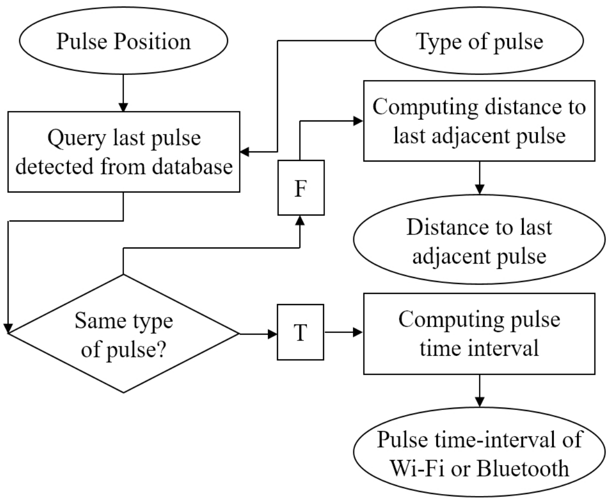


Fig. 6. Algorithm for Wi-Fi and Bluetooth distance computing.

3. Collision Detection

The collision case happens when a Wi-Fi pulse and a Bluetooth pulse overlapping. To the case of overlapping, we took the computed distance between the last Bluetooth pulses saved in the database. Because the distance value between Bluetooth pulses repeated with a rule, we could develop an algorithm for predicting the next position of Bluetooth pulse based on position and distance between the last detected Bluetooth pulses.

Figure 7 shows the distance between Bluetooth or Wi-Fi pulses repeated with a rule. The case of Wi-Fi and Bluetooth collision happens when Wi-Fi and Bluetooth signal pulses overlapped. This algorithm would detect based on prediction the next position of Bluetooth pulse, and check with the real signal received Wi-Fi or Bluetooth. If the received signal is Wi-Fi at the predicted position, we detected the collision case.

To apply the prediction method for detect collision case, the detection system was designed by algorithm which is presented in Figure 8.

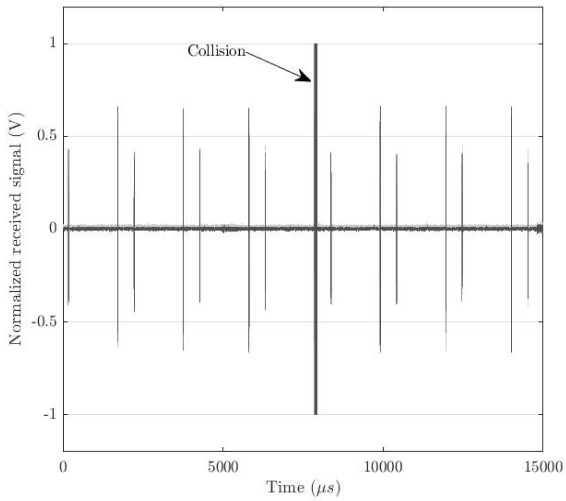


Fig. 7. Wi-Fi and Bluetooth collision.

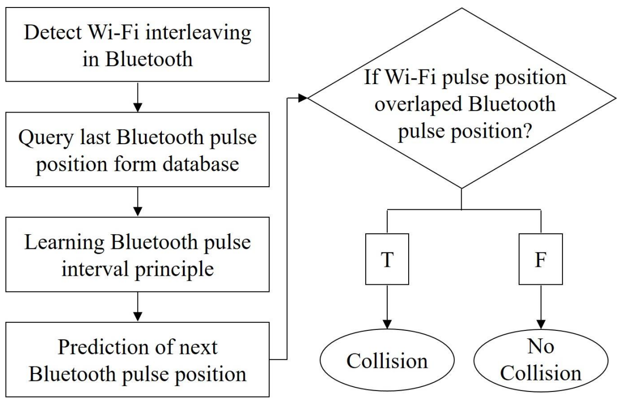


Fig. 8. Algorithm for Wi-Fi and Bluetooth collision detection.

4. Result

After implementing the experiment of Wi-Fi and Bluetooth identification for approximately 44 seconds in an indoor building environment by our method, the system detected a total of 12,932 signal pulses from raw IQ data.

Figure 9 shows the quantity of Wi-Fi, Bluetooth pulses detected, and the quantity of interleaving and collision cases between detected Wi-Fi and Bluetooth pulse.

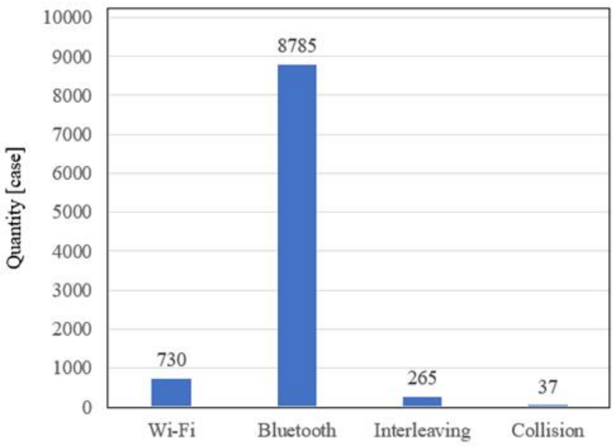


Fig. 9. Quantity of Wi-Fi and Bluetooth pulses detected.

As shown in Figure 9, 730 pulses of Wi-Fi, 8785 pulses of Bluetooth, 265 cases of Interleaving, and 37 cases of Collision between Wi-Fi and Bluetooth are detected. Utilizing the HackRF device, the system also located the position of every pulse in each IQ data sample array collected. Each sample point is equivalent to 1 µs in the time domain. From the first point and last

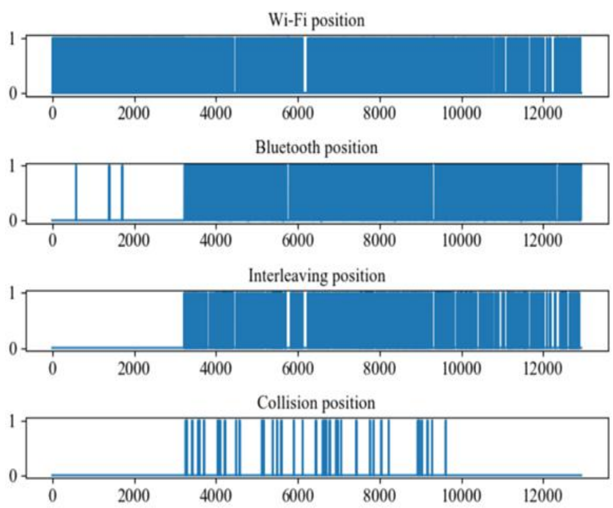


Fig. 10. Wi-Fi and Bluetooth pulses sequential location.

point position, the system could calculate the length of the signal pulse. Following the sequence of 12932 pulses detected, all signal pulses are classified by their sequential location and each case of interleaving and collision in Figure 10 below.

In another study in [16], the method approached to analyze signal on the time-frequency domain, applying Hidden Markov Model and Expectation-Maximization algorithm for Wi-Fi and Bluetooth signal detection and classification based on detected signal bandwidth. With the algorithm and system setup using the SDR device from our algorithm, not only Wi-Fi and Bluetooth signals are detected, but the system also located the position of every kind of signal in the following time domain, then computed and point out the position in which interleaving and collision cases happened.

V. Conclusion

This study focused on analyzing signal characteristics on the time domain for identifying Wi-Fi and Bluetooth signals. We mainly focused on the length feature of the pulse between many features of the pulse signature for determining the type of signal. This method is especially useful in case identifying Wi-Fi and Bluetooth interleaving. By locating exactly every signal pulse, the length of the signal pulse could be calculated. Moreover, the distance between two pulses adjacent and distance between two Wi-Fi pulses or two Bluetooth pulses are also computed, even in the case of interleaving thanks to the structured database. This result is very important for implement the next step is computing the collision rate. By our self-developed prediction algorithm, based on input data is the distance between Bluetooth pulses, the algorithm help predicted the location of Bluetooth pulse which is at risk of collision with Wi-Fi. The method and result of collision detection experiment may helpful for another study about wireless communication optimization or telecom devices maker to choose the appropriate time interval between each time of signal pulse transmitted, or designing an algorithm for time interval hoping to avoid collisions, similar to FHSS method in the frequency domain.

For further study, from our method of locating signal pulse, other researchers may analyze and extract other features of pulse signature like variance or distribution of amplitude or analyzing parameters on frequency transformed data, etc for classifying multi-type of the signal pulse. Moreover, the algorithm and database of inter-pulse distance computing are also helpful in addition to enrich the dataset in signal identification, especially applying in the machine learning algorithm.

References

[1] D. Denkovski, M. Pavloski, V. Atanasovski and L. Gavrilovska, "Parameter settings for 2.4GHz ISM spectrum measurements," *2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)*, pp.1-5, 2010. DOI: 10.1109/ISABEL.2010.5702772

[2] T. Kikuzuki, A. Wada, M. Hamaminato and T. Ninomiya, "Automatic Standard Classification Method for the 2.4 GHz ISM Band," *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, Sydney, NSW, pp.1-5, 2017. DOI: 10.1109/VTCSpring.2017.8108218

[3] B. Ning, Z. Chen, W. Chen and J. Fang, "Beamforming Optimization for Intelligent Reflecting Surface Assisted MIMO: A Sum-Path-Gain Maximization Approach," *IEEE Wireless Communications Letters*, vol.9, no.7, pp.1105-1109, 2020. DOI: 10.1109/lwc.2020.2982140

[4] Tan, J., Fan, X., Wang, S., & Ren, Y. "Optimization-Based Wi-Fi Radio Map Construction for Indoor Positioning Using Only Smart Phones," *Sensors (Basel, Switzerland),* Vol.18, No.9, pp.3095. 2018. DOI: 10.3390/s18093095

[5] Q. Xin and Y. Zhang, "Optimal fault-tolerant broadcasting in Wireless Mesh Networks," *2008 International Conference on High Performance Switching and Routing*, Shanghai, pp.151-157, 2008. DOI: 10.1109/HSPR.2008.4734436

[6] K. Kim, I. A. Akbar, K. K. Bae, J. Um, C. M. Spooner and J. H. Reed, "Cyclostationary Approaches to Signal Detection and Classification in Cognitive Radio," *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*, Dublin, pp.212-215, 2007. DOI: 10.1109/DYSPAN.2007.35

[7] E. Jones, "Software Defined Radios, Cognitive Radio and the Software Communications Architecture (SCA) in relation to COMMS, radar and ESM," *2008 IET Seminar on Cognitive Radio and Software Defined Radios: Technologies and Techniques*, pp.1-7, 2008. DOI: 10.1049/ic:20080393

[8] S. Nadaud and J. F. Trouilhet, "Modelling and classification of acoustic pulse signals by wavelet networks," *1997 IEEE International Conference on Acoustics, Speech, and Signal Processing, Munich*, vol.4, pp.3337-3340, 1997. DOI: 10.1109/ICASSP.1997.595508

[9] Z. Shaik, A. Puschmann and A. Mitschele-Thiel, "Self-Optimization of Software Defined Radios through Evolutionary Algorithms," *2016 28th International Teletraffic Congress (ITC 28)*, Würzburg, pp.53-59, 2016. DOI: 10.1109/ITC-28.2016.116

[10] Y. Takefuji, "Connected Vehicle Security Vulnerabilities [Commentary]," *IEEE Technology and Society Magazine*, vol.37, no.1, pp.15-18, 2018. DOI: 10.1109/MTS.2018.2795093

[11] H. Zha, Q. Tian and Y. Lin, "Real-World ADS-B signal recognition based on Radio Frequency Fingerprinting," *2020 IEEE 28th International Conference on Network Protocols (ICNP)*, pp.1-6, 2020. DOI: 10.1109/ICNP49622.2020.9259404

[12] G. Sahay, P. Meghana, V. V. Sravani, T. P. Venkatesh and V. Karna, "SDR based single channel S-AIS receiver for satellites using system generator," *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Bangalore, pp.1-6, 2016.

DOI: 10.1109/ANTS.2016.7947788

[13] S. Mahmood, M. T. Mushtaq and G. Jaffer, "Cost efficient design approach for receiving the NOAA weather satellites data," *2016 IEEE Aerospace Conference*, Big Sky, pp.1-6, 2016.
DOI: 10.1109/AERO.2016.7500854

[14] P. T. K. Dinh, L. Lanante, M. D. Nguyen, M. Kurosaki and H. Ochi, "An area-efficient multimode FFT circuit for IEEE 802.11 ax WLAN devices," *2017 19th International Conference on Advanced Communication Technology (ICACT)*, Bongpyeong, pp.735-739, 2017.
DOI: 10.23919/ICACT.2017.7890190

[15] A. C. Bechet, R. Helbet, I. Bouleanu, A. Sarbu, S. Miclaus and P. Bechet, "Low Cost Solution Based on Software Defined Radio for the RF Exposure Assessment: A Performance Analysis," *2019 11th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, Bucharest, Romania, pp.1-4, 2019.
DOI: 10.1109/ATEE.2019.8724739

[16] Z. Weng, P. Orlik and K. J. Kim, "Classification of wireless interference on 2.4GHz spectrum," *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pp.786-791, 2014.
DOI: 10.1109/WCNC.2014.6952168

BIOGRAPHY

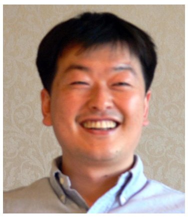
Van An Do (Member)

2012 : BE degree in Vietnam Maritime University, Vietnam.
2020~current : M.S. degree in Information and Communication Engineering, Kongju National University, South Korea.

Biswarup Rana (Member)

2007 : BS degree in Physics, Vidyasagar University, India
2009 : MS degree in Electronics, Vidyasagar University, India
2012 : MTech Degree in Electronics and Communication Engineering, West Bengal University of Technology, India
2017 : PhD Degree in Engineering(Electronics and Telecommunication Engineering), Indian Institute of Engineering Science and Technology, Shibpur, India
2017 : Post. Doc. Researcher, Seoul National University of Science and Technology, Republic of Korea
2020~current : Post. Doc. Researcher, Kongju National University, Republic of Korea

Ic-Pyo Hong (Member)



1994 : BS degree in Electronics Engineering, Yonsei University.
1996 : MS degree in Electronics Engineering, Yonsei University.
2000 : PhD degree in Electronics Engineering, Yonsei University.
2000~2003 : Senior Engineer in CDMA Mobile Research, Samsung Electronics.
2006 : Visiting Scholar with Texas A&M University.
2012 : Visiting Scholar with Syracuse University.
2003~current : Professor, Department of Information and Communication Engineering, Kongju National University.