Albahit Journal of Applied Sciences
"open-access, peer-reviewed biannual journal"
eISSN: 2708-8936, pISSN: 2708-244X
Volume 5, Issue 1, 2026
Page No: 98-109
Website: *https://albahitjas.com.ly/index.php/albahit/en/index*

WiFi Transient Signal Detection Based on Akaike Information Criterion

Ismail S. Almarimi [1*], Malak K. ABDULLAH [2], Aya G. OTHMAN [3], Saleh A. AJOUAT [4]
[1,2,3] Department of Communication Engineering, College of Electronic Technology, Bani Walid, Libya
[4] Libyan Center for Engineering Research and Information Technology L.C.E.R.I.T Bani Walid/ Libya
[*]*Corresponding author:* ismail.salem@yahoo.com

Received: 15-12-2025	**Accepted:** 13-02-2026	**Published:** 20-02-2026

Abstract:
Detection of Wi-Fi signals is indispensable in a wide range of applications, such as network security and signal analysis. Wi-Fi transient signals, though brief, carry important information that can significantly enhance the accuracy and reliability of signal detection. This paper introduces a new technique designed to detect Wi-Fi transient signals named the Akaike Information Criterion (AIC). This method captures fleeting signals by discriminating between noise and the start of the transmitting signal with high precision, making it particularly useful in environments where early detection and response are critical, such as in detecting unauthorized devices or monitoring network performance. The comprehensive implementation of the proposed method is presented and the performance evaluations were conducted under varying signal-to-noise ratio (SNR) levels. The applied method offers simplicity, accuracy and performs well even in low SNR conditions.

Keywords: Akaike Information Criterion, Transient Detection, WiFi Signal.

كشف الإشارات الانتقالية لشبكة *WiFi* بالاعتماد على معيار أكايكي للمعلومات

إسماعيل سالم المريمي [1*]، ملاك عبد الله [2] ، أية عثمان [3] ، صالح أبو القاسم خليفة [4]
[1،2،3] قسم هندسة الاتصالات، كلية التقنية الإلكترونية، بني وليد، ليبيا
[4] المركز الليبي للبحوث الهندسية وتقنية المعلومات (*L.C.E.R.I.T*)، بني وليد، ليبيا

الملخص
يُعدّ الكشف عن إشارات Wi-Fi أمرًا ضروريًا في مجموعة واسعة من التطبيقات، مثل أمن الشبكات وتحليل الإشارات. وعلى الرغم من أن الإشارات الانتقالية لشبكات Wi-Fi قصيرة المدة، إلا أنها تحمل معلومات مهمة يمكن أن تعزز بشكل كبير دقة وموثوقية الكشف عن الإشارات. تقدم هذه الورقة تقنية جديدة مخصصة لاكتشاف الإشارات الانتقالية لشبكات Wi-Fi تُعرف باسم معيار أكايكي للمعلومات (Akaike Information Criterion - AIC). تعتمد هذه الطريقة على التقاط الإشارات العابرة من خلال التمييز بدقة عالية بين الضوضاء وبداية إشارة الإرسال، مما يجعلها مفيدة بشكل خاص في البيئات التي تتطلب الكشف المبكر والاستجابة السريعة، مثل اكتشاف الأجهزة غير المصرح بها أو مراقبة أداء الشبكة. تم عرض تنفيذ شامل للطريقة المقترحة، كما أُجريت تقييمات الأداء تحت مستويات مختلفة من نسبة الإشارة إلى الضوضاء (SNR). وتُظهر الطريقة المطبقة بساطةً ودقةً عاليةً، مع أداء جيد حتى في ظروف انخفاض نسبة الإشارة إلى الضوضاء.

الكلمات المفتاحية: معيار أكايكي للمعلومات، كشف الإشارات الانتقالية، إشارات Wi-Fi.

INTRODUCTION

Monitoring and securing wireless networks by identifying and analyzing the presence and behavior of wireless signals can help detect unauthorized devices, monitor network performance [1], and mitigate potential security threats. By capturing and analyzing the unique characteristics of Wi-Fi signals, it becomes possible to distinguish between legitimate and malicious activity on the network. Today, the increasing reliance on modern wireless communication technologies exposes users to a range of external security threats, potentially leading to harmful consequences from malicious attacks. To mitigate such risks, techniques based on the physical layer of wireless communication devices, known as Radio Frequency Fingerprinting (RFF) have been developed [2]. These methods leverage the unique signal characteristics of each device, making it harder for attackers to disguise malicious actions. Combining Wi-Fi signal detection with RFF can significantly enhance network security, providing an additional layer of protection against potential threats [3]. In the Radio Frequency Fingerprinting (RFF) process, unique characteristics of the physical waveforms transmitted by wireless devices, known as RF fingerprints, are used to classify legitimate users on the network and identify potential threats [4]. These characteristics can be extracted from either the transient or steady-state portions of the transmitted signals. However, the transient regions typically provide more reliable features, making them particularly effective for detecting threats and identifying devices [5]. Meanwhile, detecting transient signals is challenging due to their short duration and channel noise. Overcoming these difficulties, particularly in consistently identifying the exact starting point of the transient signal, remains a significant challenge [6].

In the literature, several methods that accurately detect the starting point of the transient signals have been proposed so far. One of them is Variance Fractal Dimension Threshold Detection (VFDTD) which detects transient signal by using the fractal dimension calculated from the variance of signal amplitude [7]. Bayesian Step Change Detection (BSCD) method is another method that detects the transients by means of a posterior probability distribution function [8]. Phase Detection (PD) is the other method that exploits phase characteristics of signals for transient detection [9]. Mean Change Point Detection (MCPD) method is also presented in [10] to detect the Wi-Fi transient starting point by calculating the maximum of the difference of statistic. Furthermore, the study presented in [11] proposed the permutation entropy (PE) and generalized likelihood ratio test (GLRT) detector for detecting the start point of the transient. A method that utilizes the energy criterion (EC) technique was recently proposed for detection Wi-Fi signals in [12]. Recently, the Akaike Information Criterion AIC method appeared high accuracy for detecting the start point of transient portion of Bluetooth signal in [13]. Since it is known that transient behavior depends on the phase of the electronic components of the transmitter, and since it is also known that the transmission system of a Bluetooth device differs significantly from that of a Wi-Fi device, this is clearly evident in mobile devices. This result is a clear difference in the transit signals between them.

The transient signal pattern exhibits significant variation across different wireless device types. Consequently, ensuring robust analysis of transient onset detection accuracy necessitates incorporating substantial device diversity within the dataset. Studies relying on datasets lacking sufficient size and variety are likely to yield unreliable results. This methodological limitation represents a critical concern that warrants careful attention.

Consequently, this research aims to mitigate the identified data diversity concern through a comprehensive evaluation of the Akaike method's robustness for detecting transient onsets within a substantial dataset of Wi-Fi emissions sourced from heterogeneous devices.

In short, the contributions of this article are:

a. The study is the first to assess the effectiveness of the Akaike method to detect the transient start point of WiFi signal.

b. This work has evaluate the proposed algorithm in comparison with well-known algorithms.
c. The experiments are performed with real noise signals which are recorded from High-End receiver and scaleled and added regulary with incoming signals to produce real SNR levels.

Data Capture & Signal Pre-processing

Wi-Fi Signal Collection

The signal collecletion took place in a dedicated lab situated on the second basement level. To minimize potential interference, all nearby electronic devices were powered down before starting the signal capture process.

As illustrated in Fig. 1 the data acquisition setup mainly consists of a high-performance Tektronix TD57404 oscilloscope served as the receiver for capturing the Wi-Fi signals, this device was connected to a standard commercial Wi-Fi antenna, which gathered the signals from the environment. After collection, these signals were moved to a computer for storage and subsequent analysis. The smartphone(s) involved in the test were positioned precisely 30 cm from the antenna. Crucially, each smartphone was set to flight mode throughout the procedure to prevent it from generating any extraneous signals that could affect the results.

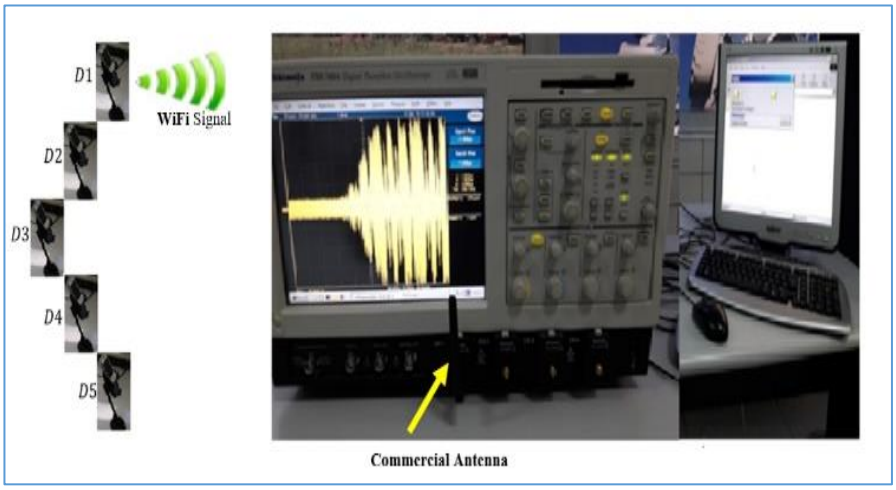


Figure 1. *Wi-Fi Transient Signals Gathering System*

Signals were recorded at a 20 Giga-samples per second (Gsps) sampling rate using five different smartphone models: an Apple iPhone 5, a Samsung Galaxy S8, a Huawei P Smart, a Xiaomi Mi A1, and a LeEco Le Max2. Table 1 illustrates the number of transient signals that collected from every smartphone included in the test, one hundred distinct Wi-Fi signal captures were collected.

Table 1 Used Devices & Brands.

Brand	Ege/year	Signals/device
iPhone 5S	5	100
Samsung S8	2	100
Huawei P smart	1	100
LeEco Max2	2	100
Xiaomi Mi A1	1	100

Signal Pre-processing

Once the Wi-Fi signals were captured and saved, the next step involved adding noise to create the aimed SNR levels wich start from 30 to -3 dB. This way secure the effectivness of the experements for simulation the real environment. Then, for eliminating the unwanted interference (spurs) introduced by the oscilloscope. This was achieved by first converting the recorded signal into its analytical form. The Hilbert transform (HT) was employed for this conversion. The analytical signal underwent down-conversion to baseband. Subsequently, a low-pass filter (LPF), was employed to eliminate unwanted spectral content. Finally, the signal amplitude was standardized through normalization. All these steps are shown in the Fig. 2.

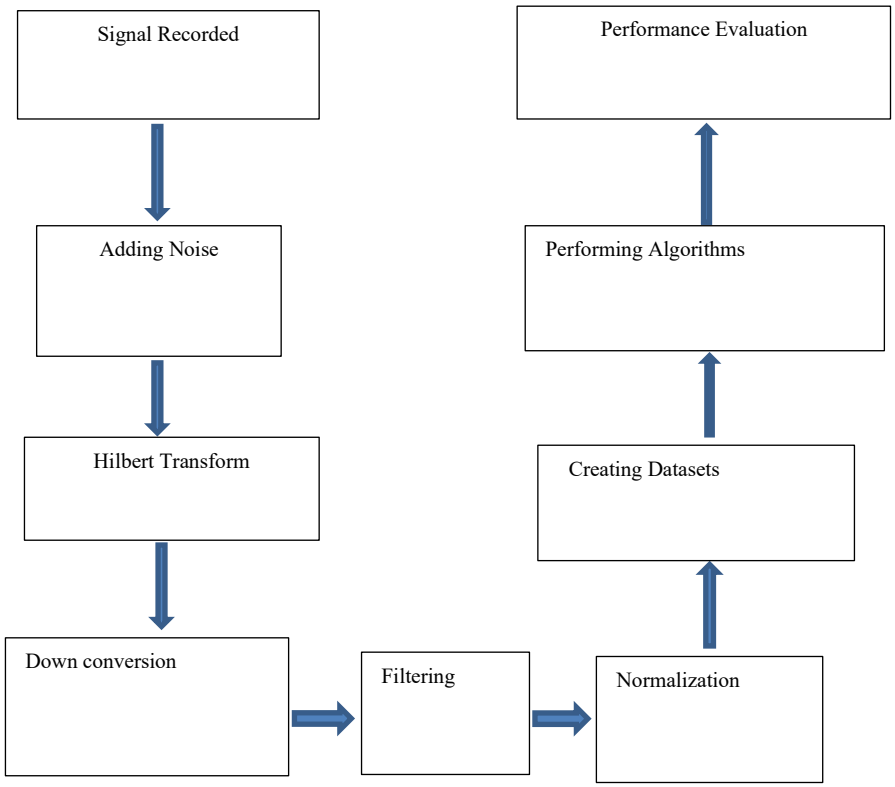


Figure 2. *Experimental Workflow*

Transient Detection Based on AIC

The detection or automatic detection of Wi-Fi transient signals is crucial due to the unique nature of these signals. Transient signals are short, non-repetitive bursts that occur at the beginning of a transmission, containing key information about the device's hardware characteristics [14]. Their brief and nonstationary nature makes manual detection challenging, requiring reliable automatic detection methods. Automated transient detection ensures high accuracy by quickly identifying these signals. This automation is critical in modern Wi-Fi networks, where the volume of transmissions and potential for interference demand fast, and consistent signal analysis without human intervention. Automatic detection enhances security and supports network performance optimization by continuously monitoring signal behavior.
The detection task is initially done by observing the occurence of change point manually which serves as ground truth for validation. In the case of Wi-Fi signal, which is based on high-order modulation, the studied signal contains a ripple known as a leading response [15], as seen in the Fig. 3(a), In addition, there is no regularity or linear trend of the unwrapped phase of the demodulated Wi-Fi signal as depicted in Fig. 3(b).

In this work, we have observed that the leading response is a mixture of noise and very low values of the Wi-Fi signal, which leads to a weakening of the statistical features when we take

it into account [15]. So, the S2 is the actual start point of the transient signal, and will be assigned by visualize the start of the ripple that synchronize with the start of regularity of unwrapped phase signal. Since, the Akaike detection algorithm is based on the modulated captured Wi-Fi signal.

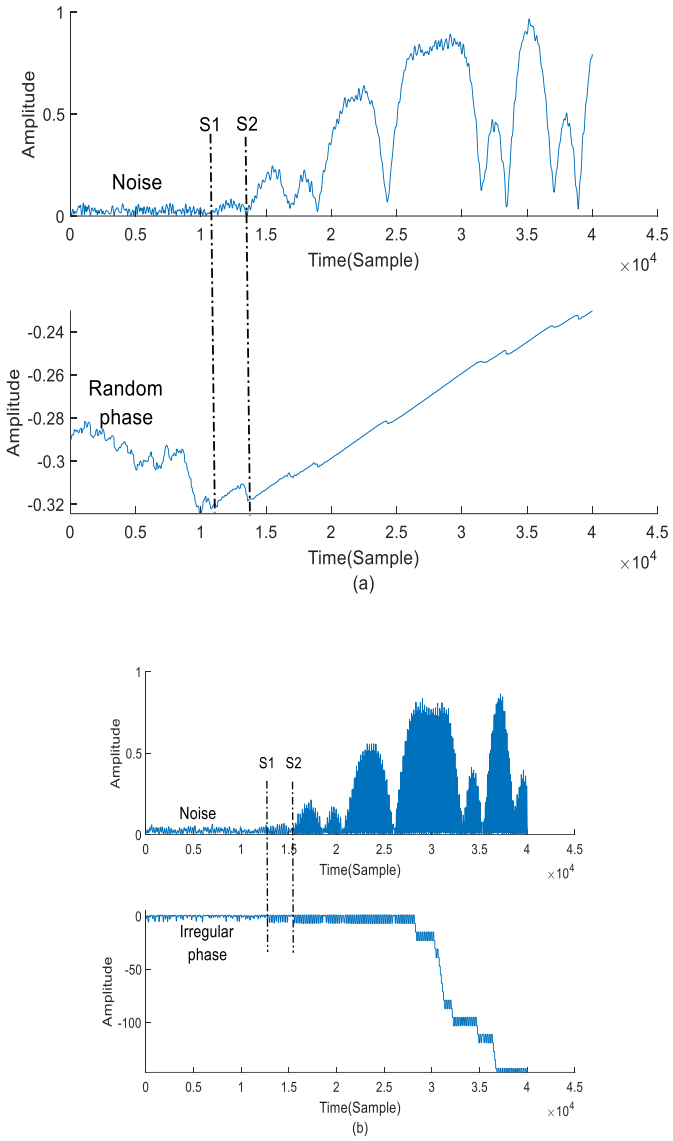


Figure 3. *The detected actual transient starting point on the instantaneous amplitude (a) & unwrapped instantaneous phase (b).*

AIC algorithm

In our implementation, we looked at two different ways to calculate the AIC: one that relies on Auto-Regressive (AR) coefficients and one that skips them entirely. We treated the AIC detector as a logical 'split-point' evaluator, working under the assumption that the signal data changes its fundamental nature before and after the device turns on.

To keep the system as fast as possible, we focused on a version of the AIC detector that bypasses AR coefficients. By pulling the metrics directly from the raw time-series signal, we were able to run the calculations instantly. This shortcut is what allowed us to maintain the high-speed processing we needed for the hundreds of Bluetooth samples in our dataset.

For Wi-Fi record x of total N samples, the AIC_{min} is given by [16]:

$$\boldsymbol{AIC(k)} = k \times \log\left(var\left(x(1,k)\right)\right) + (N-k-1) \times \left(\log\left(var(x(1+k,N))\right)\right) \qquad (\mathbf{1})$$

Where; k is movement step over the samples from 1 to k and samples from k+1 to the end of signal.

Implementation of AIC

The instantaneous amplitude was used to calculate AIC(k) via equation (1). The AIC curve corresponding to the noise part will gradually decrease, since the noise part of the instantaneous amplitude signal has a negative direction. Conversely, the AIC curve satisfying the transient part will gradually increase, because the transient part of the instantaneous amplitude signal has a positive direction. Then, the global minimum point will be located on AIC curve which will be indicated to the transient starting point.

The AIC has implemented her to effectively detected a transient starting of the Wi-Fi signal and its methodology has illustrated by the following steps:

(i) After applying Hilbert transform HT to the captured Wi-Fi; analytical signal will be produced in time domain, which is useful to extract the main features of the received signal. As a result, all negative frequencies will be removed in frequency domain.

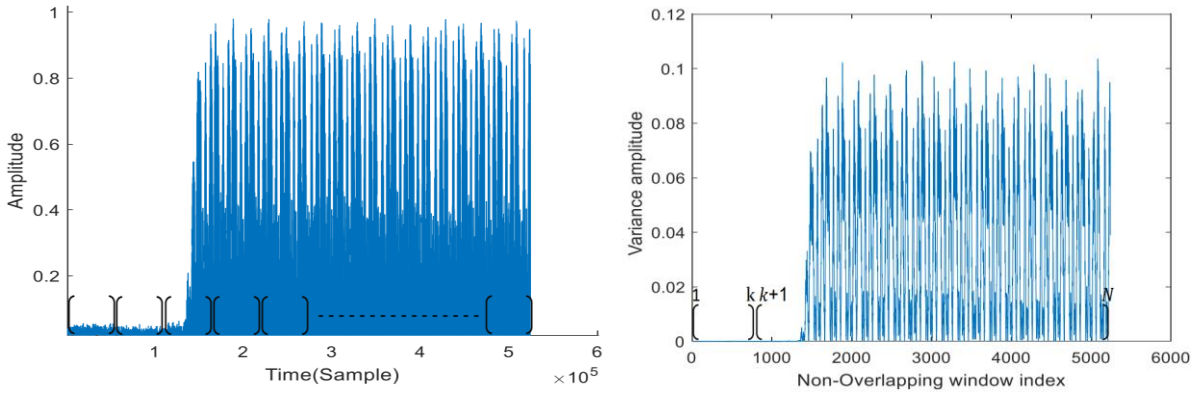
(ii) Down convert the complex spectrum to a baseband spectrum, by multiplying the signal with a complex exponential signal $e^{-iw_o t}$ in time domain. By setting $w_o = 2.5\ GHz$. Then, the baseband signal will be centralized at 0 Hz.

(iii) LPF filter is used to remove unwanted frequencies components, with cutoff frequency $100\ MHz$.

(iv) The in-phase I_n and quadrature component Q_n of a baseband signal are used, to calculate the instantaneous amplitude of the Wi-Fi signal [4], as:

$$a_n = \sqrt{{I_n}^2 + {Q_n}^2} \qquad (\mathbf{2})$$

The instantaneous amplitude vector is divided into windows of equal lengABth that are not overlapping, and the variance is calculated for each window. As shown in the Fig. 4(a).



(a) **(b)**

Figure 4. *The vector of instantaneous values is divided into windows (a)*, and *the variance calculation which is divided into two windows (b).*

(v) A new vector of length N is obtained, which is divided into two windows:

- The first window from 1 to k, where k is an integer from one to N.
- The second window from k+1 to the end of the vector N as shown in the fig 4(b).

(i) AIC(K) is computed at each new value of k to obtain an AIC curve

$$AIC(k) = k.\log\left(sum\left(w(1,k)\right)\right) + (N-k-1).\log\left(sum(w(k+1,N))\right) \quad (3)$$

(ii) The global minimum of the AIC curve indicates to transient starting point as shown in Fig. 5(b)

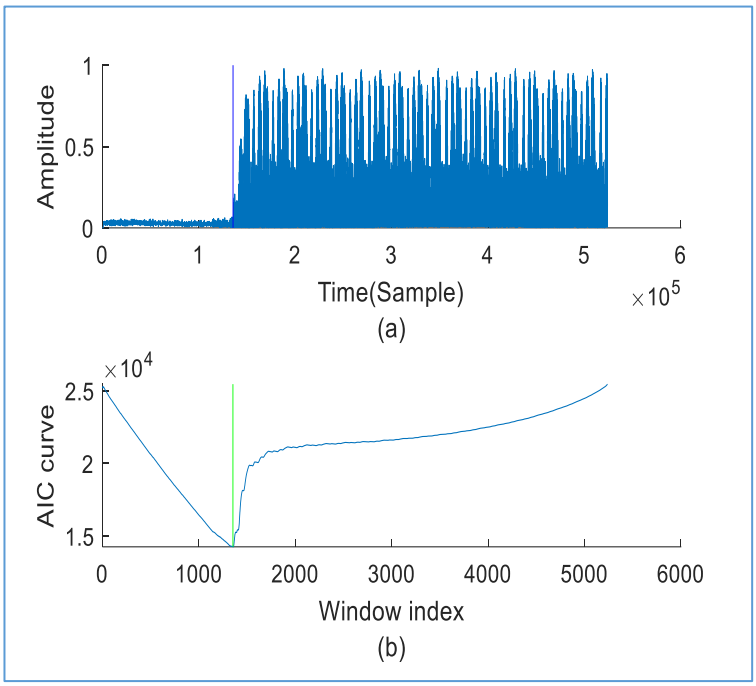


Figure 5. *Instantaneous amplitude signal (a), the AIC curve based on amplitude signal (b)*

Pseudocode of AIC Algorithm

```
%Algorithm: Find signal start using AIC
%Input: signal
%Output: start_point
% 1. Clean signal
clean_signal = filter(signal)
% 2. Extract amplitude envelope
amplitude = envelope(clean_signal)
% 3. Compute AIC for each possible change point
aic_values = []
for k = 1 to N-1:
aic = AIC_criterion(amplitude, k)
aic_values.append(aic)
%4. Find global minimum AIC value
change_point = argmin(aic_values)
%5. Convert to sample index
start_point = change_point * window_size
```

Signal-to-Noise Ratio

Typically, signal to noise ratio SNR is used to measure how the noise corrupts the signal. The performance assessment of the current transient the proposed method as known would be more reliable, if they were tested under different levels of SNR [17].

To analyze the method's performance under realistic noise conditions the noise signal must be magnified, to reduce the SNR levels to small values. To do this, the proper noise scale factor (NSF) is used to magnify the generalized noise signal. Then, SNR is estimated by dividing the average energy of the noisy signal $E_{noisy\ signal}$ on the average energy of the noise signal E_{noise} [18] :

$$SNR = 10log_{10}\left(\frac{E_{noisy\ signal}}{E_{noise}} - 1\right) \quad dB \qquad (\mathbf{4})$$

The NSF values that would be started from $(1\ to\ 50)$, attaining the level 50 of SNR by reducing the SNR from $(30\ to\ -3\ dB)$ using an increment 1.

Experimental Results and Discussion

It has been mentioned in the previous section that there is a dependency of transient signal's wake up on the used device type. Some of Wi-Fi devices have small amplitude signal at switching on (leading response), and the other devices switch on sharply. However, both these transient starting patterns might affect the detection accuracy. For this reason, the performance of the AIC method must be evaluated according to the type of device in detecting said datasets. Here, the error is estimated as an absolute difference between an actual start point p_a, and estimated point p_e, which it is divided by a sampling frequency f_s as described in the following equation:

$$error = \frac{|p_e - p_a|}{f_s} \qquad (sec.) \qquad (\mathbf{5})$$

Moreover, in this work, the detection error has been located according to variation of SNR values. Then, the number occurrence of detection error could be visualized according to SNR variation. To do this, the bivariate histogram bin counter has been used, to locate the detection error occurrence and corresponding SNR into three dimension bins. So, the number of error occurrence can be observed in each bin according to change the SNR values. Furthermore, the average detection error is computed at every specific level of SNR. In Fig. 6, three levels of SNR are selected as samples of low SNR $(-3dB)$, Medium SNR $(12dB)$, and high SNR $(30dB)$. This technique makes the performance evaluation of the detection method reliable and robust.

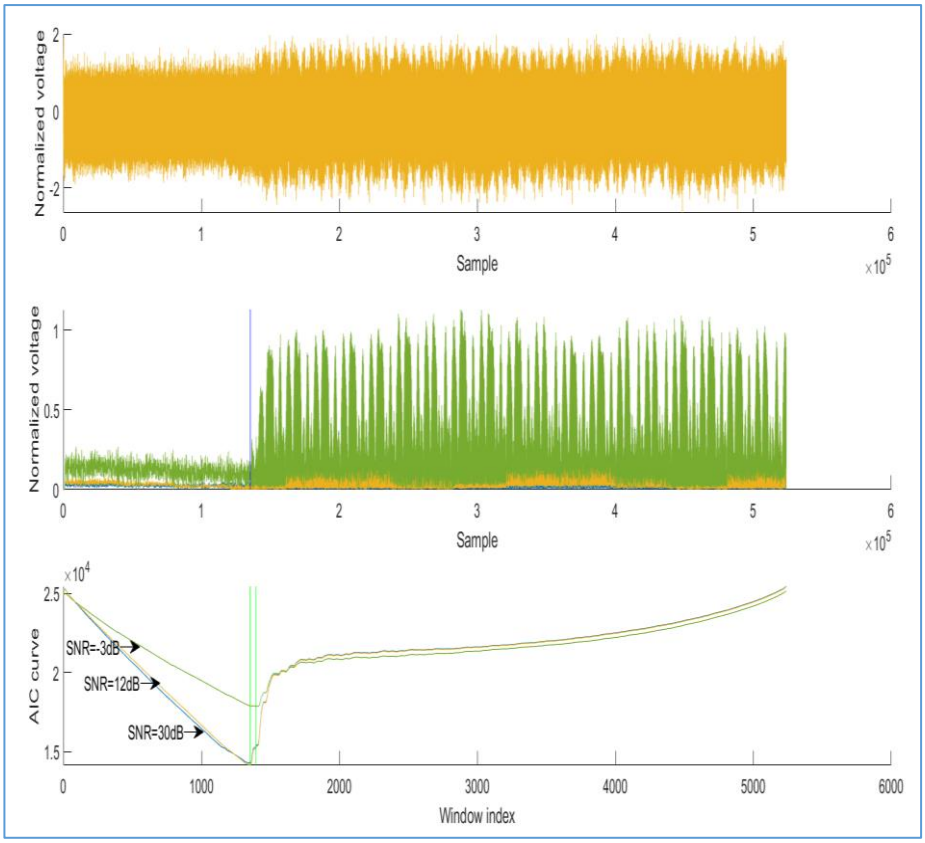
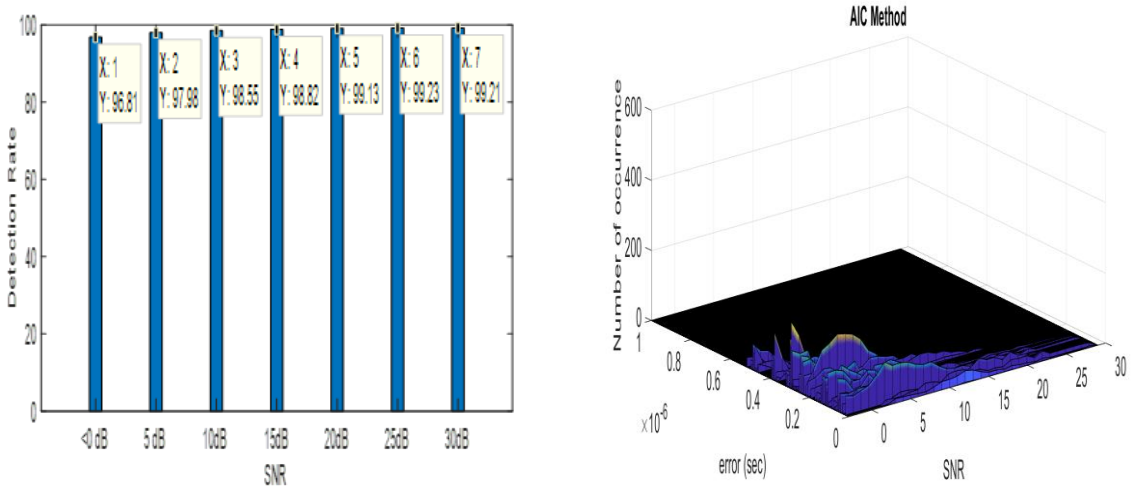


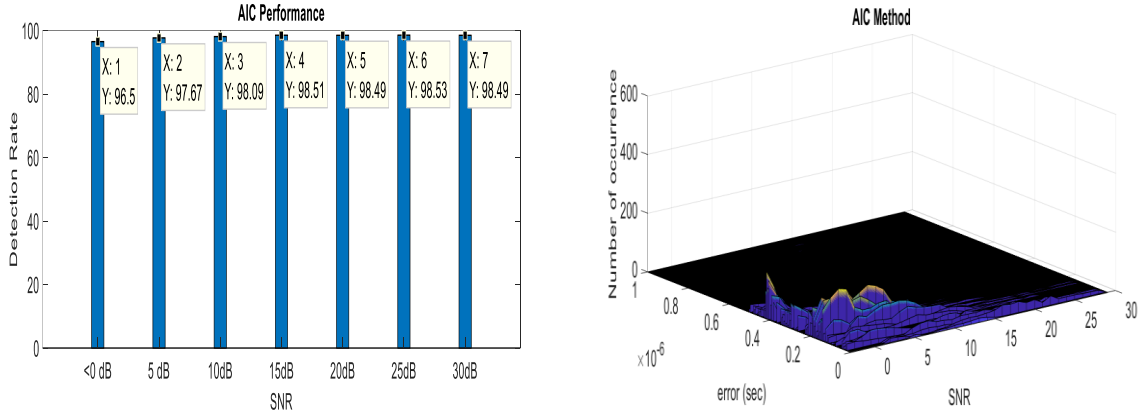
Figure 6. *AIC Method response at decreasing SNR levels.*

The performance evaluation of the studied method for devices (iPhone5, SamsungS8, Huawei P Smart, LeEco Max2, and Xiaomi Mi A1) is shown in the following figures (7-11):



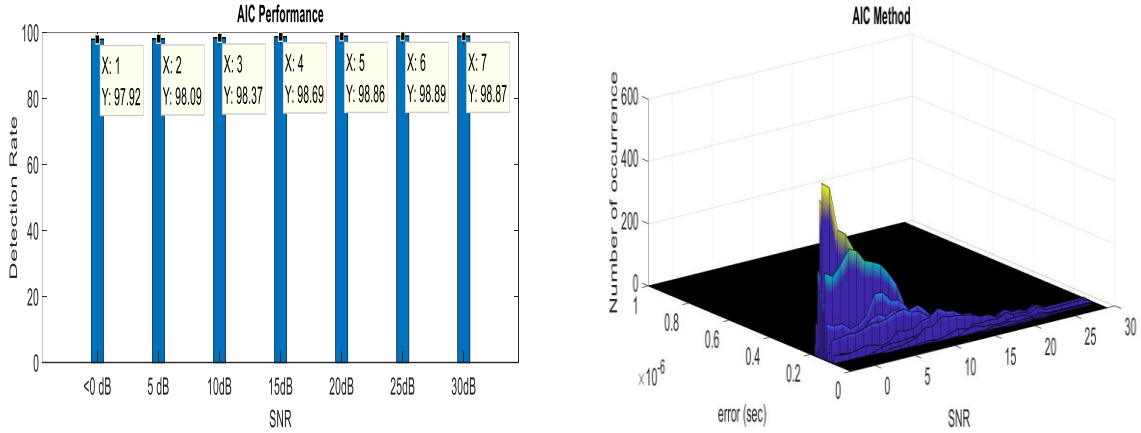
(a) **(b)**

Figure 7. *Performance Assessment for detecting 100 Wi-Fi transient signals-iPhone5 (a) Average Detection Rate (%) (b) Error Distribution*



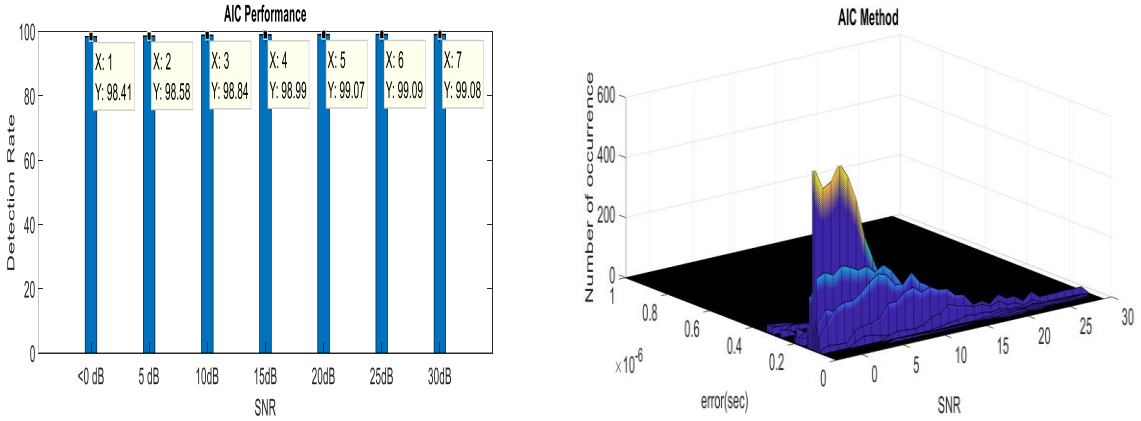
(a) **(b)**

Figure 8. *Performance Assessment for detecting 100 WiFi transient signals-SamsungS8, (a) Average Detection Rate (%) (b) Error Distribution*



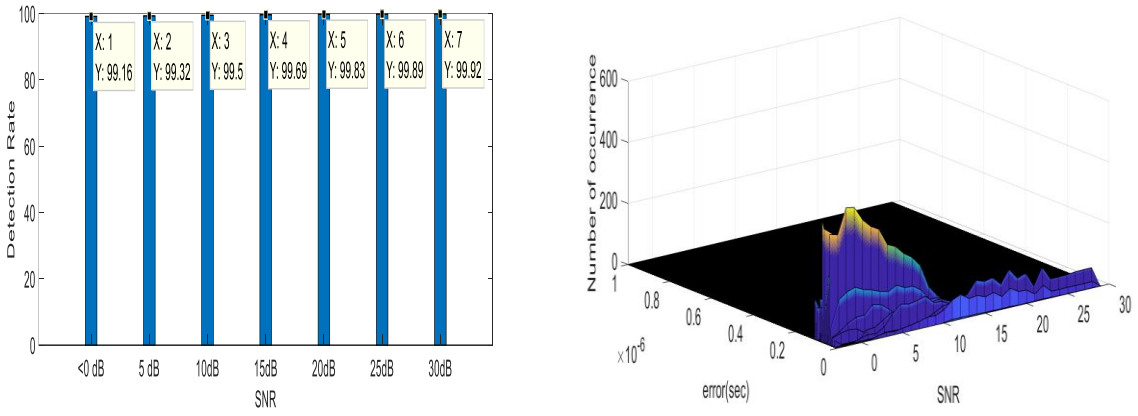
(a) **(b)**

Figure 9. *Performance Assessment for detecting 100 Wi-Fi transient signals-Huawei P Smart (a) Detection Rate(%) (c) Error Distribution.*



(a) **(b)**

Figure 10. *Performance Assessment for detecting 100 WiFi transient signals-LeEco Max2 (a) Detection Rate (%), (b) Error Distribution*



(a) **(b)**

Figure 11. *Performance Assessment for detecting 100 WiFi transient signals-Xiaomi Mi A1 (a) Detection Rate (%) (b) Error Distribution*

In this method, the detection accuracy was high at all SNR levels, and at both transient starting patterns. This accuracy is validated for both dataset's types Wi-Fi devices. For this reason, AIC method will be absolutely useful for the RFF distinguishability stage.

Conclusion

In this project, a novel detection method is applied to detect Wi-Fi transient signal. This method has built on the AIC curve of the signal. The idea behind it, the start of transient signal will be corresponded to the minimum of the AIC curve. Here, the potency is validated, by evaluating the performance of the AIC in terms of detection accuracy. It should be noted that the detection performance of current tentative starting point detection is relatively evaluated using extensive data under realistic noise conditions. For this purpose, this method has been implemented and tested. The results show that the proposed method is a very effective method for detecting the transient onset of Wi-Fi signals at different SNR levels (−3 to 30 dB). Implemented on a comprehensive data set by testing it on 100 registered Wi-Fi signals from each Wi-Fi brand (iPhone 5, Samsung S8, Huawei P smart, LeEco Max2, Xiaomi Mi A1). Due to the effectivenessof using the AIC transient detection method in detection of a transient signal accurately, there are good opportunities to enhance the performance of the RFF system in the future.

REFERENCES

[1] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," in Proceedings of the IEEE, vol. 104, no. 9, pp. 1727-1765, Sept. 2016, doi: 10.1109/JPROC.2016.2558521.

[2] N. Soltanieh, Y. Norouzi, Y. Yang and N. C. Karmakar, "A Review of Radio Frequency Fingerprinting Techniques," in *IEEE Journal of Radio Frequency Identification*, vol. 4, no. 3, pp. 222-233, Sept. 2020, doi: 10.1109/JRFID.2020.2968369.

[3] R. W. Klein, M. A. Temple, and M. J. Mendenhall, "Application of wavelet-based RF fingerprinting to enhance wireless network security." Journal of Communication and Networks, vol. 11, pp. 544–555, Dec. 2009.

[4] Z. Li, Y. Yin, L. Wu, X. Gu, G. Liu, and B. Li, "Radio frequency fingerprint identification method in wireless communication," in *Machine Learning and Intelligent Communications*, Cham: Springer International Publishing, 2018, pp. 195–202, doi: 10.1007/978-3-319-73564-1_19.

[5] O. Ureten and N. Serinken, “Wireless security through RF fingerprinting.” Canadian Journal of Electrical and Computer Engineering, vol. 32, pp. 1–8, Jan. 2007.
[6] M. Kose, S. Tascioglu, Z. Telatar, “The Effect of Transient Detection Errors on RF Fingerprint Classification Performance,” in Proc. Int. Conf. (CSECS), 2015, pp. 89–93.
[7] A. Aghnaiya, Y. Dalveren, and A. Kara, “On the performance of variational mode decomposition-based radio frequency fingerprinting of Bluetooth devices.” Sensors, vol. 20, pp. 1704–1714, Mar. 2020.
[8] Ureten, Oktay & Serinken, Nur. (1999). Bayesian detection of radio transmitter turn-on transients. 830-834.
[9] J. Hall, M. Barbeau, and E. Kranakis, “Detection of transient in radio frequency fingerprinting using signal phase,” in Proc. Int. Conf. Wireless Opt. Commun. (IASTED), 2006, pp. 108–113.
[10] L. Huang, M. Gao, C. Zhao, and X. Wu, “Detection of Wi-Fi transmitter transients using statistical method,” in Proc. IEEE ICSPCC, 2013, pp. 1–5
[11] Yuan, YJ., Wang, X., Huang, ZT. *et al.* Detection of Radio Transient Signal Based on Permutation Entropy and GLRT. *Wireless Pers Commun* **82**, 1047–1057 (2015). https://doi.org/10.1007/s11277-014-2265-2
[12] I. S. Mohamed, Y. Dalveren, and A. Kara, “Performance Assessment of Transient Signal Detection Methods and Superiority of Energy Criterion (EC) Method.” IEEE Access, vol. 8, pp. 115613–115620, June 2020.
[13] AJOUAT S. A., TEZEL N. S., “Radio frequency transient segment detection based on Akaike Information Criterion”, Politeknik Dergisi, 25(4): 1681-1686, (2022). https://doi.org/10.2339/politeknik.967341
[14] K. L. McDonald and A. S. L. de Silva, "Signal Complexity and Transient Behavior in Modern Modulation Schemes," Journal of Wireless Communications and Networking, vol. 2020, Article ID 123456, 2020.
[15] L. Huang, M. Gao, C. Zhao, and X. Wu, “Detection of Wi-Fi transmitter transients using statistical method,” in Proc. IEEE ICSPCC, 2013, pp. 1–5
[16] N. Maeda, “A method for reading and checking phase time in auto-processing system of seismic wave data,” Zisin (Journal of the Seismological Society of Japan. 2nd ser.), vol. 38, (1985).
[17] A. M. Ali, E. Uzundurukan, and A. Kara, “Assessment of Features and Classifiers for Bluetooth RF Fingerprinting.” IEEE Access, vol. 7, pp. 50524–50535, Apr. 2019.
[18] M. Kose, S. Tascioglu, and Z. Telatar, “RF Fingerprinting of IoT Devices Based on Transient Energy Spectrum.” IEEE Access, vol. 7, pp. 18715–18726, Jan. 2019.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.