electronics

MDPI

Article

Sequential Transient Detection for RF Fingerprinting

Selçuk Taşcıoğlu [1,*], Memduh Köse [2] and Gökhan Soysal [1]

[1] Department of Electrical and Electronics Engineering, Ankara University, Ankara 06830, Turkey
[2] Department of Electrical and Electronics Engineering, Kırşehir Ahi Evran University, Kırşehir 40100, Turkey
* Correspondence: selcuk.tascioglu@eng.ankara.edu.tr

Abstract: In this paper, a sequential transient detection method for radio frequency (RF) fingerprinting used in the identification of wireless devices is proposed. To the best knowledge of the authors, sequential detection of transient signals for RF fingerprinting has not been considered in the literature. The proposed method is based on an approximate implementation of the generalized likelihood ratio algorithm. The method can be implemented online in a recursive manner with low computational and memory requirements. The transients of wireless transmitters are detected by using the likelihood ratio of the observations without the requirement of any a priori knowledge about the transmitted signals. The performance of the method was evaluated using experimental data collected from 16 Wi-Fi transmitters and compared to those of two existing methods. The experimental test results showed that the proposed method can be used to detect the transient signals with a low detection delay. Our proposed method estimates transient starting points 20-times faster compared to an existing robust method, as well as providing a classification performance of a mean accuracy close to 95%.

Keywords: generalized likelihood ratio; RF fingerprinting; sequential change point detection; transient signal; wireless security

check for updates

Citation: Taşcıoğlu, S.; Köse, M.; Soysal, G. Sequential Transient Detection for RF Fingerprinting. *Electronics* **2022**, *11*, 3333. https://doi.org/10.3390/electronics11203333

Academic Editor: Athanasios Kanatas

Received: 17 September 2022
Accepted: 13 October 2022
Published: 16 October 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Radio frequency (RF) fingerprints carrying information about the unique hardware characteristics of transmitters can be used for wireless device identification. The process of identifying wireless devices by using these fingerprints is referred to as RF fingerprinting. In order to enhance the wireless security, RF fingerprints have been used for the identification of various wireless devices so far, e.g., VHF [1,2], Wi-Fi [3–8], Bluetooth [9,10], and ZigBee [11–13] transmitters. Employing RF fingerprinting for the security of systems employing multiple antennas is also discussed in the literature. For instance, in [14], the identification of Wi-Fi transmitters based on the IEEE 802.11n multiple-input multiple-output protocol was considered in an experimental study. More recent studies in [15,16] also discussed an authentication scheme based on RF fingerprints for massive multiple-input multiple-output uplink systems. Unlike traditional cryptographic methods, the RF fingerprinting-based device identification approach does not require additional computational resources at the transmitter [17,18]. This feature makes the RF fingerprinting approach a potential candidate for enhancing wireless security, especially in mobile applications such as Wi-Fi-based healthcare services. In addition to the security, high throughput is an essential requirement for next-generation wireless networks [19]. RF fingerprinting-based techniques can be employed to enhance wireless security without throughput degradation since they do not rely on introducing additional overhead for security [20].

An RF fingerprinting-based device identification system has three main stages, namely; detection, feature extraction, and classification. The RF fingerprinting-based device identification system block diagram is given in Figure 1. RF fingerprints are obtained by extracting characteristic features from different parts of the transmissions such as transient, preamble,

and data regions and then classified using a classifier [21]. In order to obtain distinctive characteristic features, the signal parts used for feature extraction must be accurately detected. In this work, the detection stage of the RF fingerprinting system is discussed and the problem of detecting the transient signals of Wi-Fi transmitters in a sequential framework is considered.

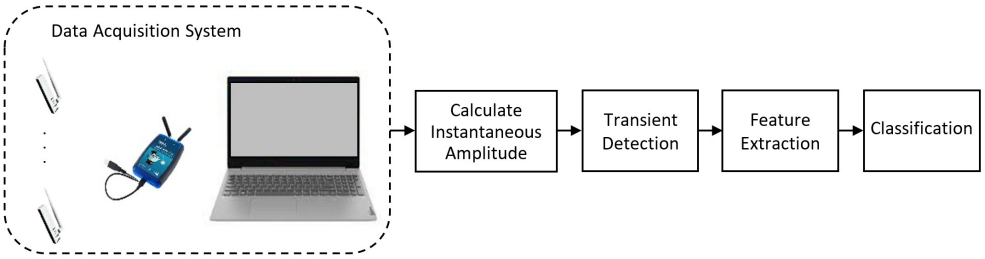

Figure 1. RF fingerprinting-based device identification system block diagram.

One of the detection approaches is to use the correlation properties of the preamble signals. Using this approach, high detection performance can be achieved. However, the requirement of receiving the preamble signal part for detection increases the latency. On the other hand, transient detection methods have potential to achieve low latency since transients are emitted before wireless devices transmit steady-state signal parts such as preambles. However, detecting the transient signals following the channel noise is a challenging problem. One approach to this problem is to characterize the degree of irregularity of the transmitted signals by using a multifractal analysis and finding a change within this characterization [1]. The authors showed that a change can be detected by setting a threshold on the fractal trajectory obtained from the variance of the signal amplitude. Transients of radio transmitters were separated from the channel noise by using this approach. In [22], a method based on permutation entropy was proposed for the detection of transients of wireless transmitters. The idea in the method is to use the difference of the complexity of noise and signals, which was obtained by permutation entropy. This method can achieve high performance; however, it has high computational complexity. A detection technique based on the instantaneous phase characteristics of the received signals was proposed in [9]. Transients of wireless transceivers were obtained by comparing the difference in the variance of the phase characteristics with a threshold. A similar approach was used in [23] to find the starting and end points of the transients of wireless sensor nodes. The variance of the signal values was calculated to measure the deviation of the signal values from the average, and a cumulative sum algorithm was applied to the variance trajectory.

Transient detection has also been considered as a Bayesian change point detection problem. For example, in [24,25], a robust Bayesian approach was proposed based on step and linear ramp data models, respectively. In this approach, the detection is carried out by obtaining the a posteriori probability distribution of the change point in a retrospective manner. These two Bayesian methods have robust detection capability; however, they cannot be implemented for all practical applications due to their high computational complexity.

In a recent study [26], a transient detection approach based on the energy criterion technique was introduced. The basic idea in the method is to characterize the received signals by a variation of their energy content. The performance of the method was assessed using Wi-Fi signals collected from a particular smartphone and compared to those of existing methods. In [27], an extensive performance evaluation of this method was carried out using Wi-Fi signals captured from smartphones of five brands under different SNR conditions. The common transient detection techniques were reviewed in [28,29], and their performances were analyzed using experimental data captured from various wireless transmitters in [4,9,26,27,30,31]. Moreover, the effect of transient detection errors on device identification performance was investigated for IEEE 802.11 transmitters in [4,31].

RF fingerprinting, which is considered as a potential candidate to enhance wireless security, should satisfy the requirements of emerging wireless technologies. In this context, wireless security solutions are required to be implemented online with low latency, as well as to be more robust. In order to exploit the latency advantage of the transient-based systems in online applications, the transient is required to be detected in sequentially observed data.

To the best of our knowledge, the problem of transient detection for RF fingerprinting has not been considered in a sequential framework so far. The main contribution of this paper is to present for the first time a sequential transient detection method for RF fingerprinting. The proposed method is based on a sequential change point detection (also referred to as online change point detection) approach. The method can be implemented online in a recursive manner with low computational and memory requirements, as well as low detection delay. The experimental test results showed that similar performance in estimating the transient starting points can be achieved 20-times faster than a robust Bayesian method [24]. Using the RF fingerprints detected by the proposed method, device classification performance with a mean accuracy close to 95% was achieved.

The outline of the paper is as follows. In Section 2, the transient detection problem is formulated as a sequential change point detection problem. The proposed method based on an approximate generalized likelihood ratio algorithm is presented in Section 3. The experimental setup for data acquisition is described in Section 4. Test results for the transient detection and classification performance are presented in Section 5, and lastly, Section 6 concludes the paper.

2. Problem Definition

The detection of the transients of wireless transmitters is considered as a sequential change point detection problem. When a wireless transmission following the channel noise is received, a change occurs in the parameter set of the instantaneous amplitude samples of the received signal (see Figure 2). For a received complex baseband signal of the form $r[k]{=}r_I[k] + jr_Q[k]$, the instantaneous amplitude values are calculated as

$$x[k] = \sqrt{{r_I}^2[k] + {r_Q}^2[k]} \tag{1}$$

where $r_I[k]$ and $r_Q[k]$ are the real and imaginary parts of the received signal, respectively.

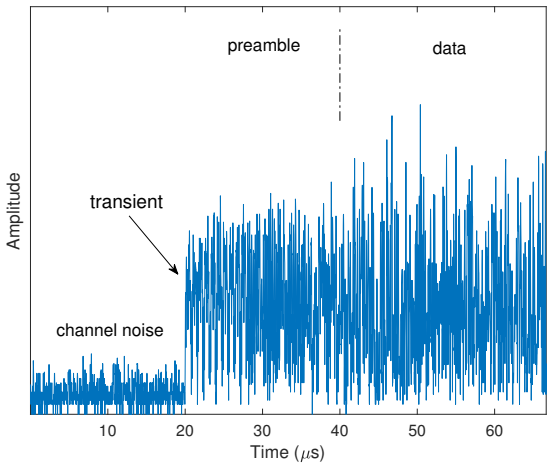

Figure 2. Instantaneous amplitude of a captured IEEE 802.11n signal collected at the 2.4 GHz ISM band.

The change in the parameter set of the instantaneous amplitude samples for the transient region following the channel noise is considered as an abrupt change since the change occurs very fast considering the sampling rate of the receiver, as shown in Figure 2. Let the

instantaneous amplitude samples $\{x[k]\}_{1\leq k\leq n}$ be a sequence of independent Gaussian random variables whose distribution is based on the parameters $\theta_0{=}(\mu_0, \sigma_0^2)$ and $\theta_1{=}(\mu_1, \sigma_1^2)$, which are defined as the parameters before and after the unknown change point m, respectively. A standard approach for sequential change point detection is to define a decision function $g[k]$ based on the observations up to the current time k and compare it with a threshold. This approach, first introduced in [32], is called the cumulative sum (CUSUM) algorithm. In this algorithm, the alarm time at which the change is detected is defined as

$$N_a = \min\{k : g[k] \geq \gamma\} \tag{2}$$

where γ is a predefined threshold. As a function of the log-likelihood ratio for the parameters before and after the change point, the decision function is defined as [33]

$$g[k] = S[k] - \min_{1\leq j\leq k} \left\{ \sum_{i=1}^{j} \ln\left(\frac{p(x[i];\theta_1)}{p(x[i];\theta_0)}\right) \right\} \tag{3}$$

where j denotes the possible change point and $S[k]$ is the cumulative sum of log-likelihood ratios:

$$S[k] = \sum_{i=1}^{k} \ln\left(\frac{p(x[i];\theta_1)}{p(x[i];\theta_0)}\right) \tag{4}$$

Note that the ratio in (4) is calculated at each time instant; therefore, it may be referred to as the instantaneous log-likelihood ratio. In order to reduce the computational cost and memory requirements, the decision function may also be rewritten in a recursive manner as [33]

$$g[k] = \left\{ g[k-1] + \ln\left(\frac{p(x[k];\theta_1)}{p(x[k];\theta_0)}\right) \right\}^{+} \tag{5}$$

where $\{v\}^{+}{=}\sup(0, v)$.

The decision function is compared with the threshold γ for each new observation for online detection of a change in a stochastic process. A detailed review of sequential change point detection methods for various applications can be found in [33–35]. This problem may also be considered in the sequential hypothesis testing framework, in which the null hypothesis $H_0 : \theta{=}\theta_0$ is tested against the alternative hypothesis $H_1 : \theta{=}\theta_1$ by comparing the decision function with a threshold. A detailed analysis of the relationship between these two problems was presented in [36], where the problem of sequential detection of parameter changes in stochastic systems was considered by relating it to sequential hypothesis testing.

For the known model parameters before and after the change, the decision function in (3) or (5) is calculated directly, which is known as Page's CUSUM algorithm [32]. However, in practice, these parameters are generally unknown. In such cases, the parameters may be defined by using a priori information, which results in suboptimal CUSUM algorithms [37]. When a priori information cannot be provided in a practical application, the parameters have to be estimated.

In our work, considering the fact that transmission powers can be at different levels and change randomly due to the nature of the wireless channel, it is obvious that defining a priori information is not a practical solution for the parameter after change (θ_1). For this type of problem, Lorden [38] introduced the generalized likelihood ratio (GLR) algorithm, in which the CUSUM method is generalized. In the standard GLR algorithm, the parameter θ_0 is assumed to be known or estimated from the available observations, whereas the change point and the unknown parameter θ_1 are estimated using the maximum likelihood principle in the following double-maximization form [33]:

$$g[k] = \max_{1 \le j \le k} \sup_{\theta_1} \sum_{i=j}^{k} \ln\left(\frac{p(x[i];\theta_1)}{p(x[i];\theta_0)}\right) \tag{6}$$

Since the maximum likelihood estimation of parameter θ_1 is obtained for each possible change point j, the GLR algorithm has a high computational burden. Therefore, it is not always possible to implement this algorithm in practice [36]. Several approaches, e.g., [39–41], have been introduced to simplify this algorithm while preserving the performance, some of which were reviewed in [33,36,42].

3. Sequential Transient Detection for RF Fingerprinting

We introduce a sequential transient detection method based on an approximate implementation of the GLR algorithm. In this implementation, considering the transient characteristics of wireless devices and the requirements of RF fingerprinting, the main principle of the two-model approach introduced in [40,41] was used. This approach has been used for implementing the GLR algorithm in sequential segmentation of signals using spectral analysis for speech, electroencephalogram, and electrocardiogram data. To the best of our knowledge, this is the first study in which an approximate GLR algorithm based on the two-model approach is used for the detection of the RF fingerprints.

In the proposed GLR-based sequential transient detection method, two time windows called the reference and test window are defined in order to estimate the model parameters. These windows are represented for a captured Wi-Fi signal following the channel noise in Figure 3. The reference window is taken as a growing time window so that it includes all the information about the channel noise, whereas the test window is a sliding window with fixed size W. Model parameters before and after change, i.e., $\theta_0{=}(\mu_0, \sigma_0^2)$ and $\theta_1{=}(\mu_1, \sigma_1^2)$, are estimated by using the samples within the reference and test windows, respectively. At the current time k, the sample being tested as a change point is the one that is received at time $k{-}W{+}1$ (see Figure 3). When a new sample is received, in order to include this sample in the time windows, the fixed-size test window is shifted, whereas the reference window is enlarged. Therefore, at each time instant, the current sample is the end point of both time windows, as shown in Figure 3. The parameter estimates are updated at each time instant using the current sample included within the time windows.

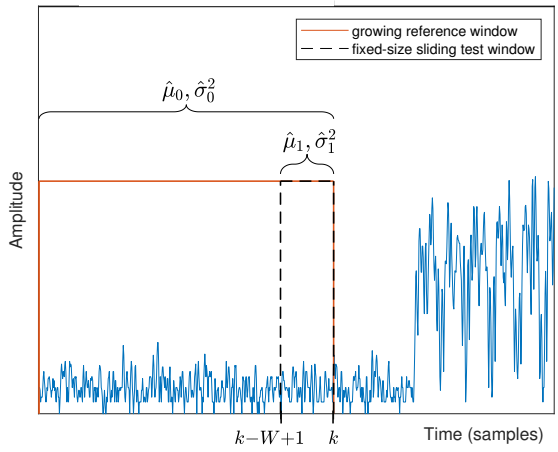

Figure 3. Reference and test windows.

The details of the method including the estimation of the parameters, detection of the transient, and estimation of the transient starting point are presented in the following subsections, respectively.

3.1. Parameter Estimation

The parameters before and after the change are estimated by calculating the sample mean and variance of the samples within the reference and test windows, respectively. The estimates of the parameters are updated at each time instant when a new observation is received. The parameter estimates are obtained as

$$\hat{\mu}_0[k] = \frac{1}{k}\sum_{i=1}^{k} x[i] \tag{7}$$

$$\hat{\sigma}_0^2[k] = \frac{1}{k}\sum_{i=1}^{k} (x[i]-\hat{\mu}_0[i])^2 \tag{8}$$

$$\hat{\mu}_1[k] = \frac{1}{W}\sum_{i=k-W+1}^{k} x[i] \tag{9}$$

$$\hat{\sigma}_1^2[k] = \frac{1}{W}\sum_{i=k-W+1}^{k} (x[i]-\hat{\mu}_1[i])^2 \tag{10}$$

where W is the size of the sliding test window and $k > W$ by definition.

The estimations defined in (7)–(10) are carried out in recursive forms as follows:

$$\hat{\mu}_0[k] = \frac{k-1}{k}\hat{\mu}_0[k-1] + \frac{1}{k}x[k] \tag{11}$$

$$\hat{\sigma}_0^2[k] = \frac{k-1}{k}\hat{\sigma}_0^2[k-1] + \frac{1}{k}(x[k] - \hat{\mu}_0[k])^2 \tag{12}$$

$$\hat{\mu}_1[k] = \hat{\mu}_1[k-1] + \frac{(x[k]-x[k-W])}{W} \tag{13}$$

$$\hat{\sigma}_1^2[k]=\hat{\sigma}_1^2[k-1]+\frac{(x[k]-\hat{\mu}_1[k])^2-(x[k-W]-\hat{\mu}_1[k-1])^2}{W} \tag{14}$$

where $k > W$ by definition. In this work, for $1 \leq k \leq W$, the initial values of the parameters were taken as zero without using any a priori information. If a priori information about the channel noise is provided, the initial values of $\hat{\mu}_0$ and $\hat{\sigma}_0^2$ may also be determined based on this information.

In this work, we updated the estimate of the parameter before change (θ_0) for each new observation, instead of assuming that this parameter is known and remains constant throughout the analysis, which is one of the approaches for implementing the GLR algorithm. By doing so, we aimed to take into account the instantaneous variations of the noise floor and, therefore, achieve high detection and estimation accuracy.

In the standard GLR algorithm, as can be seen from the decision function calculation in (6), the number of maximizations of the log-likelihood over the parameter after change (θ_1) at time k grows to infinity with k [34,36]. That means the number of computations grows to infinity with k. On the other hand, in the proposed transient detection method, which is a simplified implementation of the GLR algorithm, the second maximization over θ_1 is canceled and the parameters are estimated using (11)–(14). Therefore, the proposed method can be implemented with low computational complexity. The complexity evaluation of the proposed method was performed in terms of the computation time by using simulation and experimental data in Section 5.3.

3.2. Transient Detection

Transient detection was carried out by detecting a change in the mean and variance of the instantaneous amplitude samples of the received signals. The decision function is formed by using the estimates of the model parameters which were obtained as explained

in the previous subsection. In this case, the recursive decision function in (5) can be rewritten as

$$g[k] = \max\{0, g[k-1]+L[k]\}, \quad k > W \tag{15}$$

where $L[k]$ represents the log-likelihood ratio and $g[k]=0$ for $1 \leq k \leq W$ by definition. Using the parameter estimates, the log-likelihood ratio for Gaussian random variables with different means and variances is given as

$$\begin{aligned} L[k] &= \ln \frac{p\left(x[k-W+1]; \hat{\theta}_1[k]\right)}{p\left(x[k-W+1]; \hat{\theta}_0[k]\right)} \\ &= \ln \frac{\hat{\sigma}_0[k]}{\hat{\sigma}_1[k]} + \frac{\left(x[k-W+1]-\hat{\mu}_0[k]\right)^2}{2\hat{\sigma}_0^2[k]} \\ &\quad - \frac{\left(x[k-W+1]-\hat{\mu}_1[k]\right)^2}{2\hat{\sigma}_1^2[k]} \end{aligned} \tag{16}$$

For the derivation of this equation, see Appendix A. Since the sample being tested as a change point at the current time k is the one that is received at time $k-W+1$ (see Figure 3), the sample $x[k-W+1]$ is used in (16). The decision function is calculated after receiving samples with a size of W in this method. For the time interval with a length of sliding window size W, which is referred to as the dead zone [33], the decision function is not calculated and taken as zero. The size of the sliding test window was taken as 50 samples, which corresponds approximately to 0.8 µs.

The transient detection was performed by comparing the decision function $g[k]$ with a threshold γ, as given in (2). Detection occurs at the alarm time N_a at which $g[k]$ exceeds the threshold value. For a captured Wi-Fi signal, the decision function $g[k]$ obtained by using (15) and the alarm time N_a are given in Figure 4.

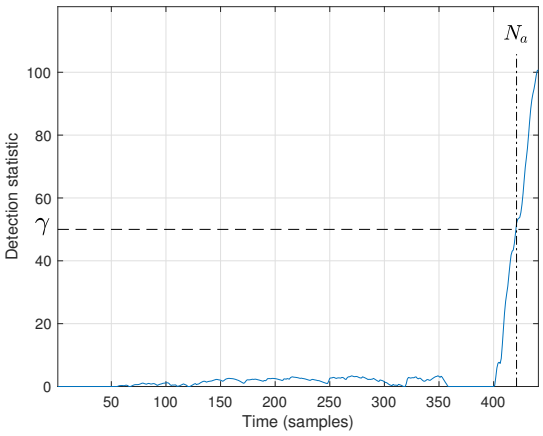

Figure 4. Decision function.

3.3. Estimation of Transient Starting Point

Once a transient is detected, the transient starting point considered as a change point can be estimated by using the observations up to alarm time N_a. Maximum likelihood estimation of the change point is obtained by finding the time index where the cumulative sum of log-likelihood ratios takes its minimum value [33]. In the formulation of this work, the current sample is the end point of the test window, whereas the sample being tested as a possible change point is the starting point of this window (see Figure 3). Therefore, using the observations up to the alarm time N_a, transient starting point estimation is defined as

$$\hat{m} = \underset{W+1<j\leq N_a}{\arg\min} \{S[j-1]\} - W + 1 \tag{17}$$

The estimation defined in (17) may be performed by recording all cumulative sum values, which requires additional memory. Considering the typical behavior of the cumulative sum $S[k]$ given in Figure 5, we propose to perform this task in a recursive manner, which reduces the memory requirement. In this recursive procedure, the current value of the cumulative sum is compared with its minimum value up to the current time. Once the current value of the cumulative sum is lower than the minimum value, the minimum value and its index are updated. The memory requirement is reduced since only the minimum value and its index are held in the memory instead of all cumulative sum values.

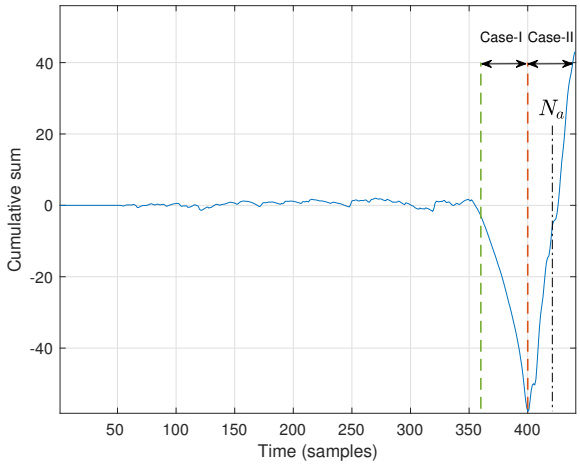

Figure 5. Cumulative sum of log-likelihood ratios.

The underlying reason for the typical behavior of the cumulative sum observed for Wi-Fi signals can be explained as follows. Until the transient signal enters the test window, the estimates of θ_0 and θ_1 are close to each other since both the test and reference windows include only noise samples. Therefore, the log-likelihood ratios defined in (16) take values close to zero and their cumulative sum $S[k]$ fluctuates around zero, as shown in Figure 5. When the change point is between the start and end points of the test window, the estimates of θ_1 increase due to the samples of the transient signal within the test window. We refer to this case as Case-I, for which an example representation of the reference and test windows is shown in Figure 6. In this case, since the sample being tested as a possible change point is a noise sample with parameter θ_0, the log-likelihood ratios take values lower than one, and therefore, the cumulative sum exhibits a negative drift (Figure 5). After the change point leaves the test window, the sample being tested as a possible change point is a transient sample with parameter θ_1, as shown in Figure 6. We refer to this case as Case-II, where the log-likelihood ratios take values greater than one, and therefore, their cumulative sum exhibits a positive drift (Figure 5).

For a captured Wi-Fi signal, the estimated transient starting point $\hat{m}$ obtained by using (17) is represented in Figure 7. The difference between time instants at which the alarm and change occur $(N_a - \hat{m})$ is referred to as detection delay and desired to be small for online implementations. The detection delay for the signal in Figure 7 is 68 samples, which corresponds approximately to 1.1 µs. In order to provide a visual comparison with the IEEE 802.11n preamble with a length of 20 µs, $\hat{m}$ and N_a are represented on a long part of a captured Wi-Fi waveform in Figure 8.

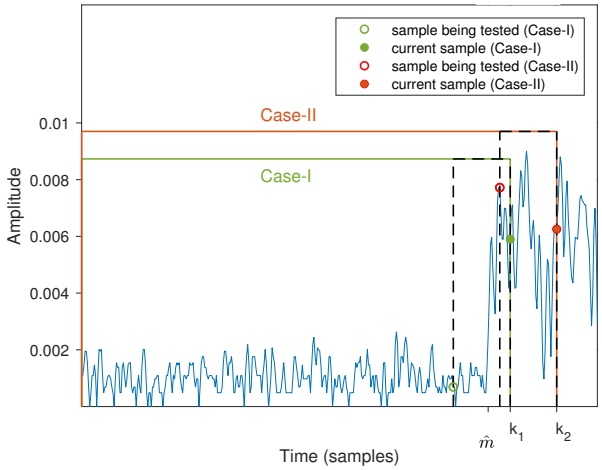

Figure 6. Growing reference window (solid lines) and sliding test window (dashed lines) for two different time instants k_1 (Case-I) and k_2 (Case-II).

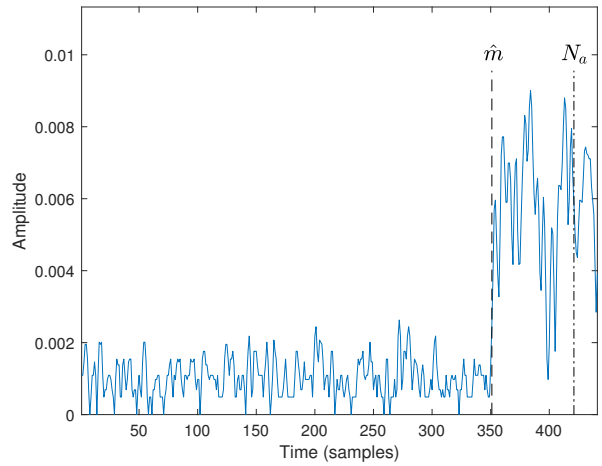

Figure 7. Estimated transient starting point $\hat{m}$ and alarm time N_a.

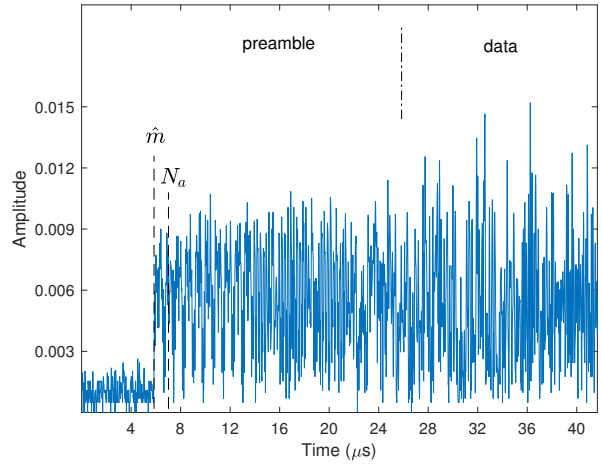

Figure 8. Estimated transient starting point $\hat{m}$ and alarm time N_a over a long part of a captured Wi-Fi waveform.

The memory requirement of the proposed method at time k does not increase with k since the calculation of the decision function, as well as the estimation of the parameters

and change point are performed in a recursive manner. At each time instant, only the current data value, the last values of the parameters, the minimum cumulative sum value, and its index are held in the memory. This demonstrates the advantage of the method in terms of memory requirements compared to the standard [38] and window-limited [39] GLR algorithms, which require the full dataset and the data values within the window, respectively, at every time instant.

4. Experimental Setup

An experimental setup consisting of wireless USB adapters, an access point, and a software-defined radio (SDR) was designed to collect Wi-Fi signals. These devices were located 3 m apart from each other with a line-of-sight between them, as shown in Figure 9. Sixteen wireless USB adapters of three different models from two different brands were used as the Wi-Fi transmitters. The chipsets and supported Wi-Fi standards of these adapters are given in Table 1. They were connected to a computer via USB hubs and configured to transmit data through a wireless network.

A wireless local area network (WLAN) was designed for wireless communication between the access point and Wi-Fi transmitters. The WLAN was managed by an access point that was configured to communicate over the IEEE 802.11n standard with a 20 MHz bandwidth. The Wi-Fi channel was set to 12 with a center frequency of 2.467 GHz. IEEE 802.11n signals with a 20 MHz bandwidth were captured from the Wi-Fi transmitters using an SDR, Analog Devices ADALM Pluto [43]. This SDR has a direct conversion transceiver chip operating in a 325 MHz to 3.8 GHz frequency range and supports up to a 20 MHz channel bandwidth. Captured signals were sampled at 60 MSamples/s with 12-bit resolution. Three-hundred fifty transmissions were collected from each of the 16 Wi-Fi transmitters, resulting in a dataset of 5600 transmissions.

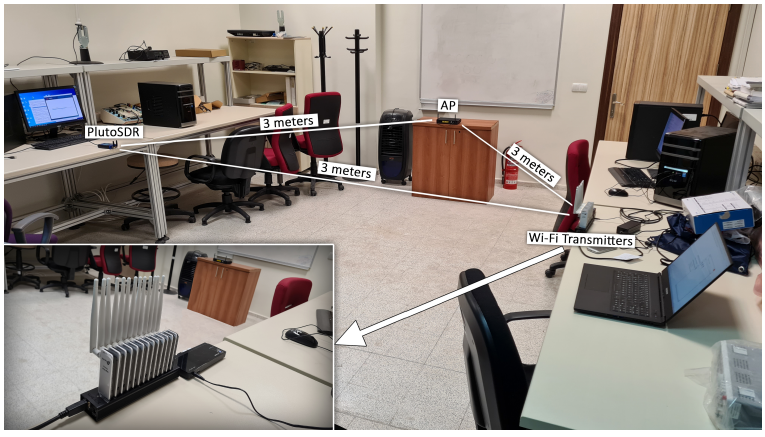

Figure 9. Experimental setup for data acquisition.

In order to obtain the received signals with different signal-to-noise ratio (SNR) values, the gain of the SDR receiver was set to two different levels. Average SNR levels over all transmissions were calculated to be 25 dB and 37 dB for low and high receiver gain values, respectively. These receiver gains and corresponding SNR values were selected considering the fact that the minimum SNR value recommended for most applications in IEEE 802.11 wireless local area networks is around 20 dB in practice [44].

Table 1. Wi-Fi transmitters used in the experiments.

Model	Standards	Quantity	Chipset
TP-Link WN722N	802.11 b/g/n	13	Realtek RTL8188EUS
TP-Link WN725N	802.11 b/g/n	2	Realtek RTL8188EUS
Mercusys MW150US	802.11 b/g/n	1	Realtek RTL8188EU

5. Experimental Performance Evaluation

The performance of the proposed method was assessed using experimental data collected from 16 Wi-Fi transmitters. The performance evaluation was performed in terms of detection delay, estimation error, and computation time. Besides, to demonstrate the usability of the proposed transient detection method in an RF fingerprinting system, the classification performance for the RF fingerprints detected by the proposed method was analyzed.

In order to provide a baseline comparison, the estimation performance of the standard threshold detector was examined, which can be used for the detection of the transients of wireless transmitters [5]. The main idea of this detector is to compare the raw data values with a threshold. The threshold detector can easily be applied to sequentially observed data; however, it is highly prone to errors due to measurement noise.

We also compared the estimation performance of the proposed method with a robust Bayesian approach [24,25]. It was reported in [25] that a Bayesian ramp detector has high performance for IEEE 802.11b signals sampled at 5 GSamples/s. However, when the sampling rate is at lower levels, as in the case of our work where the sampling rate was 60 MSamples/s, the change in the parameter of the random process can be considered as an abrupt change [33]. In this case, the change occurs very fast considering the sampling period of the receiver. That means the step model is more accurate for the instantaneous amplitudes of transmissions considered herein. Therefore, we analyzed the performance of a Bayesian step detector [24] and compared its performance with that of the proposed method. Test results for performance analysis are presented in the following subsections.

5.1. Detection Performance

In the sequential change point analysis, the aim was to perform the change point detection as soon as possible under a false alarm constraint. A test was performed to calculate the false alarms and detection delays for different threshold values for two different SNR levels. According to the test results presented in Table 2, the false alarm rate was reduced substantially for the threshold values above 30. Since the increase in detection delay was not high above this value, the threshold was set to $\gamma = 50$, for which the false alarm did not occur and the average detection delay was approximately 1 μs. This is less than the power-on duration of 2 μs defined for Wi-Fi transmitters in the IEEE standard [45]. This means that the transients of Wi-Fi transmitters can be detected by the proposed method within the duration that is defined for Wi-Fi transmitters to increase their power to a predefined level. Furthermore, when compared to the IEEE 802.11n preamble, which has a length of 20 μs, this delay is very small, as shown in Figure 8.

Table 2. Average detection delay and number of false alarms for different threshold values.

Threshold	Average Detection Delay (μs)		Number of False Alarms	
	25 dB	**37 dB**	**25 dB**	**37 dB**
10	0.88	0.88	1538	1240
20	0.92	0.91	48	67
30	0.95	0.95	2	11
40	0.98	0.97	1	4
50	1.03	1.01	0	0

The histograms of the detection delay values obtained for the experimental data at two different SNR levels for the threshold value of 50 are given in Figure 10. As can be seen from this figure, detection delays had small standard deviations at both SNR levels.

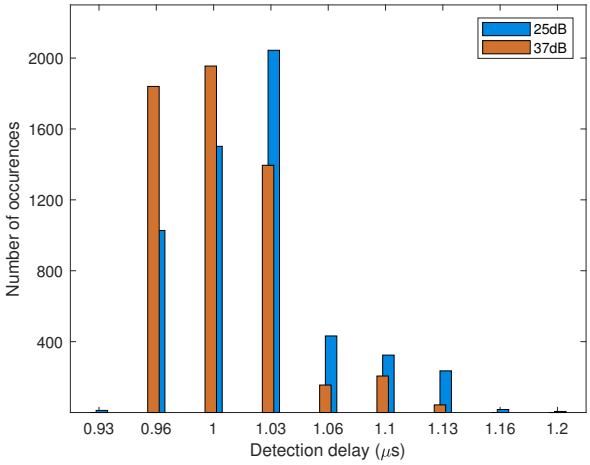

Figure 10. Histogram of detection delay values.

5.2. Estimation Performance

The performance of the estimation stage was evaluated by calculating the estimation error for each transmission. Starting points of Wi-Fi signals, which were obtained using a symbol timing synchronization scheme given in [46], were used as reference starting points for performance evaluation. This synchronization scheme requires the demodulation and decoding of the short and long training fields of the IEEE 802.11 preamble defined in [45]. Estimation error is defined as the difference between the estimated transient starting point obtained by a transient detection method and the reference starting point.

Estimation errors obtained over 5600 transmissions from the Wi-Fi transmitters are summarized in the form of boxplots in Figure 11. This figure demonstrates that the Bayesian step detector had an estimation error distribution with a mean close to zero and a small standard deviation at both SNR levels. A similar estimation performance can be achieved by the proposed GLR-based detector for both SNR values, as shown in Figure 11.

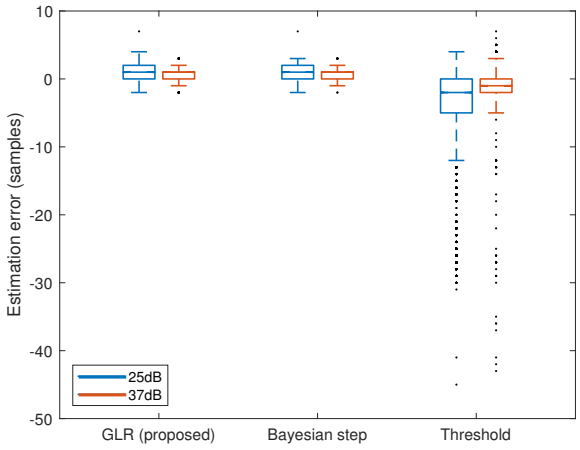

Figure 11. Boxplots of the estimation errors for two different average SNR values. The line in the center of a box is the median; the box edges indicate the 25th and 75th percentiles; the whiskers represent the lowest and highest values without considering outliers; the outliers are represented by the point "·" marker symbol.

Compared to these two detectors, the threshold detector had lower performance with large estimation errors (Figure 11). In addition, the estimation bias of the threshold detector increased as the SNR level decreased. In order to avoid reducing the clarity of visualization,

estimation errors below −50 samples occurred in the threshold detector, i.e., 70 and 73 error values at 25 dB and 37 dB SNR, respectively, are not represented in Figure 11.

5.3. Computation Time

The main aim of this test was to compare the computational performance of the detectors for processing data with a fixed length. The proposed GLR-based detector was compared with the threshold detector and Bayesian step detector in terms of computation time using experimental data. The results achieved by averaging over 5600 transmissions are given in Table 3. As can be seen from this table, the fastest detector was the threshold detector, as expected, in which the raw data samples were compared with a threshold. The proposed method was 20-times faster than the Bayesian step detector. This advantage was due to the recursive and simplified implementation structure of the proposed method.

In order to evaluate the computation performance of the proposed method for larger data sizes, the proposed method was also applied to the simulated data in addition to the experimental data. Compared to the Bayesian step detector, the proposed GLR method was approximately 30- and 230-times faster for the simulated data with sizes of 1K and 10K samples, respectively. The mean squared estimation error for the proposed GLR and Bayesian step detectors were found to be 0.33 and 0.46, respectively. These results showed that the proposed method had a significant complexity advantage while maintaining high performance, especially when the data size was large.

Table 3. Computation time.

Detector	Computation Time (μs)
Proposed GLR detector	84.33
Bayesian step detector	1694.71
Threshold detector	13.57

5.4. Classification Performance

Device classification performance for the RF fingerprints detected by the proposed method was assessed using experimental data. The instantaneous amplitude characteristics of the identification signals were used as features in the classification system. In this work, the identification signals were taken as the signal parts starting from the estimated transient starting points. Therefore, the estimation performance significantly affected the overall performance of the classification system. If the estimation performance was low, the alignment accuracy would decrease, resulting in a classification performance loss. The instantaneous amplitude characteristics of the identification signals obtained by the proposed method from four different Wi-Fi transmitters are represented in Figure 12, where an overlay of 50 signals for each transmitter is shown. This figure shows that the identification signals obtained by the proposed method were properly aligned. From this figure, it can also be seen that the instantaneous amplitude characteristics can be used to represent the characteristic differences between measurements from different Wi-Fi devices and the similarities of different measurements from a fixed device. In order to avoid using the transmission power level as a feature in the classification system, transmission signals were normalized so that their average power was equal to one.

In order to classify the instantaneous amplitude features, a probabilistic-neural-network (PNN)-based [47] classifier was used. In this classifier, the distribution of each class is estimated based on the Parzen window approach using the training data. In the testing stage, the class with maximum posterior probability was assigned to new input data. A detailed description of PNN classifier can be found in [48].

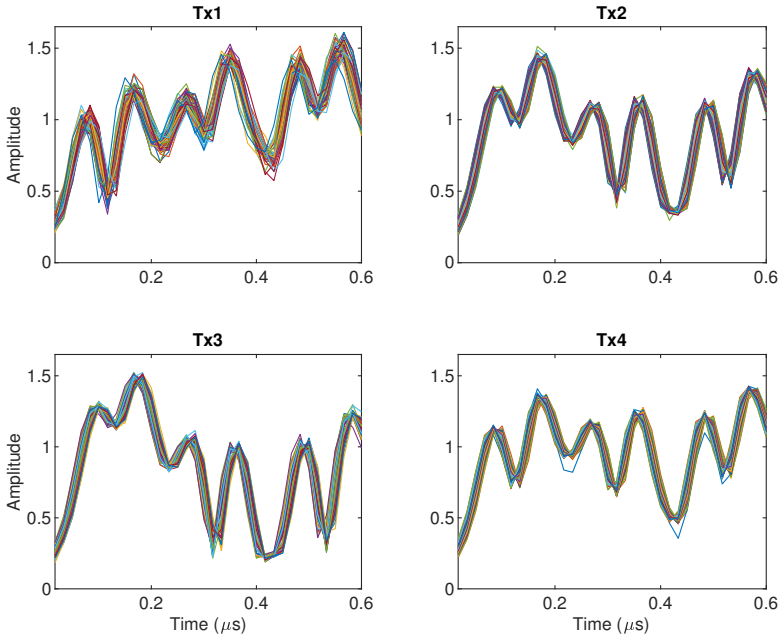

Figure 12. Instantaneous amplitude characteristics obtained from four different Wi-Fi transmitters.

The classification performance evaluation was carried out through Monte Carlo cross-validation in order to accurately measure the performance. In each Monte Carlo trial, half of the signals from each transmitter were randomly selected and used in the training. The first classification test was performed to analyze the effect of the identification signal duration on classification accuracy. The results of one hundred trials for each duration value are represented in Figure 13. This figure demonstrates that the classification accuracy increased as the signal duration increased up to approximately 600 ns at both SNR levels. Increasing the duration beyond this value did not yield substantial performance improvement. Therefore, the identification signal duration was taken as 600 ns for the classification tests, which corresponds to 36 samples for the sampling rate of 60 MSamples/s. As can be seen from Figure 13, shortening the signal duration had a more detrimental effect on the classification performance for the signals with lower SNR values.

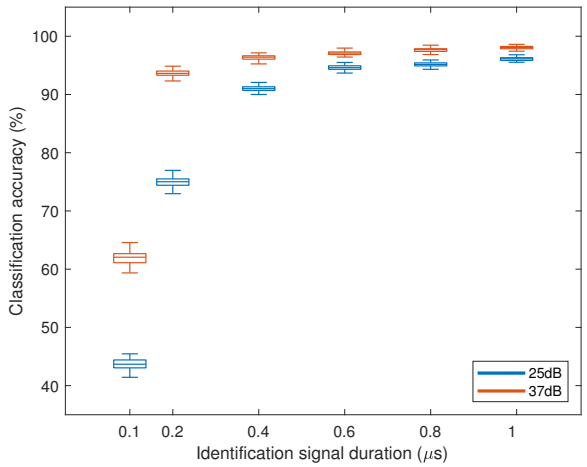

Figure 13. Classification accuracy versus identification signal duration.

Once the identification signal duration was determined, classification tests were run to compare the performance of the RF fingerprints detected by the proposed and two existing

methods. Confusion matrices were obtained for each classification test at two different SNR levels, and the average values over trials are presented in Figure 14. The classification results of one-hundred trials obtained at 25 dB and 37 dB average SNR levels are given in Figure 15 and Figure 16, respectively. Furthermore, the classification performance was assessed in terms of average accuracy, precision, recall, and F1 score, and the results are given in Table 4. From these figures and tables, the effect of the transient detection method on classification performance can be observed. The RF fingerprints obtained by the proposed GLR-based detector achieved a classification performance close to 95% at 25 dB and slightly higher than 97% at 37 dB in terms of all the metrics given in Table 4. The proposed method provided classification performance improvement of approximately 16% compared to the threshold detector at 25 dB. A similar classification performance can be achieved with the Bayesian step detector; however, it required a higher computation time.

When the classification accuracies at two different SNR levels were compared, it can be seen from Figures 15 and 16 that the classification performances degraded at lower SNR values. The performance loss was caused by both the detection and classification stages since the decrease in SNR not only degraded the detection performance, but also made the classification task difficult. A high performance loss was observed for the threshold detector. On the other hand, the performance loss due to SNR degradation was negligible for the proposed detector and Bayesian detector since they had high estimation performance at both SNR levels, as shown in Figure 11.

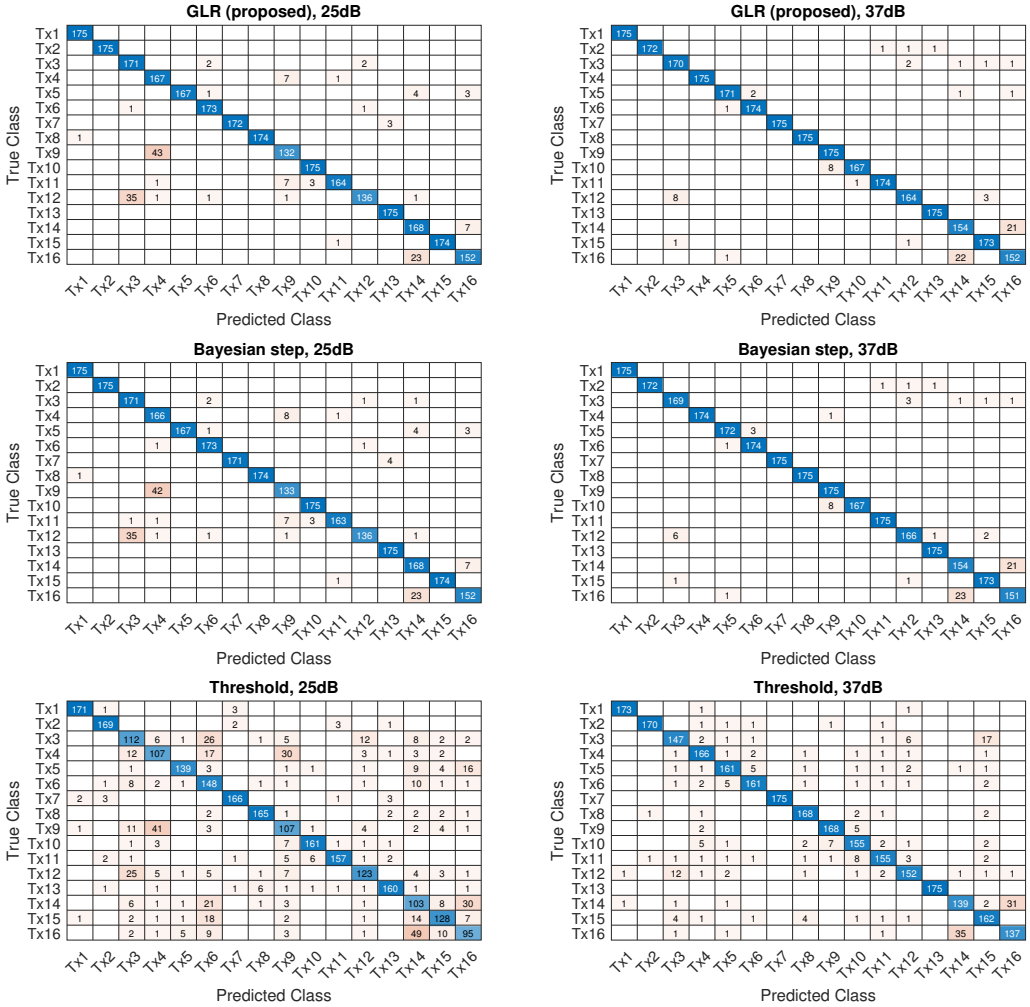

Figure 14. Confusion matrices for device classification using the RF fingerprints detected by three different detection methods at 25 dB (**left panel**) and 37 dB (**right panel**) SNR.

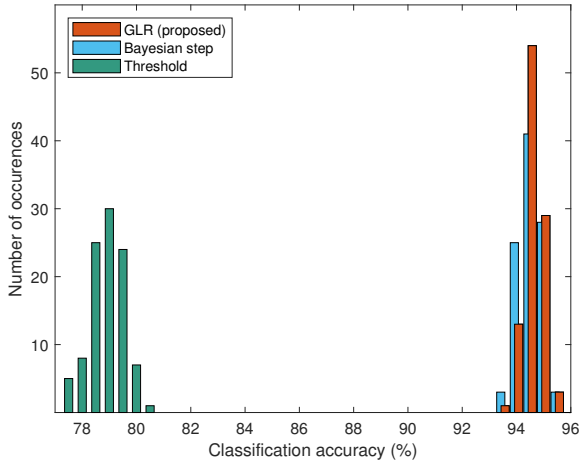

Figure 15. Histogram of classification accuracy at 25 dB SNR.

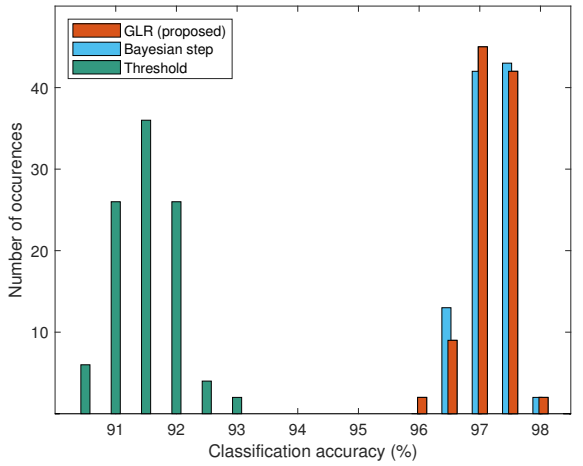

Figure 16. Histogram of classification accuracy at 37 dB SNR.

Table 4. Classification metrics for three different methods at 25 dB and 37 dB SNR.

	SNR 25 dB			SNR 37 dB		
	GLR (Proposed)	**Bayesian Step**	**Threshold**	**GLR (Proposed)**	**Bayesian Step**	**Threshold**
Accuracy	0.9464	0.9457	0.7896	0.9718	0.9721	0.9157
Precision	0.9507	0.9502	0.7997	0.9721	0.9724	0.9160
Recall	0.9464	0.9457	0.7896	0.9718	0.9721	0.9157
F1 score	0.9462	0.9456	0.7921	0.9718	0.9721	0.9156

6. Conclusions

This paper proposed a GLR-based sequential transient detection method, which can be implemented online for RF fingerprinting. The performance of the method was evaluated using experimental data collected from Wi-Fi transmitters that are widely used in wireless networks. The experimental results showed that the proposed method can achieve similar performance in estimating the transient starting points 20-times faster than an existing robust method. A Wi-Fi transmitter classification performance with a mean accuracy close to 95% was achieved using the RF fingerprints detected by the proposed method. Since the detection was performed using transients that were emitted before the wireless devices transmitted any information, the proposed method can be used to detect

the RF fingerprints as soon as possible when the data transmission starts. This feature is particularly desirable in wireless applications that demand low latency. Besides, the method has low detection delay, as well as low computation time, which are desirable properties for online implementations. In this study, the experimental results were obtained from 16 Wi-Fi transmitters operating in the 2.4 GHz ISM band. The performance evaluation of the proposed transient detection method for Wi-Fi transmitters operating at different frequency bands, as well as the impact of the number of Wi-Fi transmitters on the performance will be considered in future work.

Author Contributions: Conceptualization, S.T., M.K., and G.S.; methodology, S.T.; software, G.S., M.K., and S.T.; investigation, S.T.; data curation, M.K., G.S., and S.T.; writing—original draft preparation, S.T. and M.K.; writing—review and editing, M.K., G.S., and S.T.; supervision, S.T. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Scientific and Technological Research Council of Turkey (TUBITAK) under Grant 119E598.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

The likelihood ratio for two Gaussian random variables with different parameter values can be obtained as follows:

$$\begin{aligned} L[k] &= \ln \frac{p\left(x[k-W+1];\hat{\theta}_1[k]\right)}{p\left(x[k-W+1];\hat{\theta}_0[k]\right)} \\ &= \ln \frac{\frac{1}{\sqrt{2\pi\hat{\sigma}_1^2[k]}}\exp\left(-\frac{(x[k-W+1]-\hat{\mu}_1[k])^2}{2\hat{\sigma}_1^2[k]}\right)}{\frac{1}{\sqrt{2\pi\hat{\sigma}_0^2[k]}}\exp\left(-\frac{(x[k-W+1]-\hat{\mu}_0[k])^2}{2\hat{\sigma}_0^2[k]}\right)} \\ &= \ln \frac{\hat{\sigma}_0[k]}{\hat{\sigma}_1[k]} + \frac{(x[k-W+1]-\hat{\mu}_0[k])^2}{2\hat{\sigma}_0^2[k]} \\ &\quad - \frac{(x[k-W+1]-\hat{\mu}_1[k])^2}{2\hat{\sigma}_1^2[k]} \end{aligned} \tag{A1}$$

References

1. Shaw, D.; Kinsner, W. Multifractal modelling of radio transmitter transients for classification. In Proceedings of the IEEE WESCANEX 97 Communications, Power and Computing, Conference Proceedings, Winnipeg, MB, Canada, 22–23 May 1997; pp. 306–312.
2. Serinken, N.; Ureten, O. Generalised dimension characterisation of radio transmitter turn-on transients. *Electron. Lett.* **2000**, *36*, 1064–1066. [CrossRef]
3. Ureten, O.; Serinken, N. Wireless security through RF fingerprinting. *Can. J. Electr. Comput. Eng.* **2007**, *32*, 27–33. [CrossRef]
4. Klein, R.; Temple, M.A.; Mendenhall, M.J.; Reising, D.R. Sensitivity analysis of burst detection and RF fingerprinting classification performance. In Proceedings of the 2009 IEEE International Conference on Communications, Dresden, Germany, 14–18 June 2009; pp. 1–5.
5. Yuan, H.L.; Hu, A.Q. Preamble-based detection of Wi-Fi transmitter RF fingerprints. *Electron. Lett.* **2010**, *46*, 1165–1166. [CrossRef]
6. Vo-Huu, T.D.; Vo-Huu, T.D.; Noubir, G. Fingerprinting Wi-Fi devices using software defined radios. In Proceedings of the 9th ACM Conference on Security Privacy in Wireless and Mobile Networks, Darmstadt, Germany, 18–20 July 2016; pp. 3–14.
7. Li, G.; Yu, J.; Xing, Y.; Hu, A. Location-invariant physical layer identification approach for WiFi devices. *IEEE Access* **2019**, *7*, 106974–106986. [CrossRef]

8. Kose, M.; Tascioglu, S.; Telatar, Z. RF fingerprinting of IoT devices based on transient energy spectrum. *IEEE Access* **2019**, *7*, 18715–18726. [CrossRef]
9. Hall, J.; Barbeau, M.; Kranakis, E. Detection of transient in radio frequency fingerprinting using signal phase. *Wirel. Opt. Commun.* **2003**, 13–18.
10. Aghnaiya, A.; Dalveren, Y.; Kara, A. On the performance of variational mode decomposition-based radio frequency fingerprinting of bluetooth devices. *Sensors* **2020**, *20*, 1704. [CrossRef] [PubMed]
11. Bihl, T.J.; Bauer, K.W.; Temple, M.A. Feature selection for RF fingerprinting with multiple discriminant analysis and using ZigBee device emissions. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 1862–1874. [CrossRef]
12. Peng, L.; Hu, A.; Zhang, J.; Jiang, Y.; Yu, J.; Yan, Y. Design of a hybrid RF fingerprint extraction and device classification scheme. *IEEE Internet Things J.* **2019**, *6*, 349–360. [CrossRef]
13. Zhou, X.; Hu, A.; Li, G.; Peng, L.; Xing, Y.; Yu, J. A robust radio-frequency fingerprint extraction scheme for practical device recognition. *IEEE Internet Things J.* **2021**, *8*, 11276–11289. [CrossRef]
14. Shi, Y.; Jensen, M.A. Improved radiometric identification of wireless devices using MIMO transmission. *IEEE Trans. Inf. Forensics Secur.* **2011**, 6, 1346–1354. [CrossRef]
15. Zhang, P.; Shen, Y.; Jiang, X.; Wu, B. Physical layer authentication jointly utilizing channel and phase noise in MIMO systems. *IEEE Trans. Commun.* **2020**, *68*, 2446–2458. [CrossRef]
16. Zhang, P.; Liu, J.; Shen, Y.; Jiang, X. Exploiting channel gain and phase noise for PHY-layer authentication in massive MIMO systems. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 4265–4279. [CrossRef]
17. Reising, D.; Cancelleri, J.; Loveless, T.D.; Kandah, F.; Skjellum, A. Radio identity verification-based IoT security using RF-DNA fingerprints and SVM. *IEEE Internet Things J.* **2021**, *8*, 8356–8371. [CrossRef]
18. Liu, Y.; Wang, J.; Li, J.; Niu, S.; Song, H. Machine learning for the detection and identification of Internet of Things devices: A survey. *IEEE Internet Things J.* **2022**, *9*, 298–320. [CrossRef]
19. Sangaiah, A.K.; Javadpour, A.; Pinto, P.; Ja'fari, F.; Zhang, W. Improving quality of service in 5G resilient communication with the cellular structure of smartphones. *ACM Trans. Sen. Netw.* **2022**, *18*, 1–23. [CrossRef]
20. Wang, X.; Hao, P.; Hanzo, L. Physical-layer authentication for wireless security enhancement: Current challenges and future developments. *IEEE Commun. Mag. 2016*, *54*, 152–158. [CrossRef]
21. Danev, B.; Zanetti, D.; Capkun, S. On physical-layer identification of wireless devices. *ACM Comput. Surv.* **2012**, *45*, 1–29. [CrossRef]
22. Yuan, Y.-J.; Wang, X.; Huang, Z.-T.; Sha, Z.-C. Detection of radio transient signal based on permutation entropy and GLRT. *Wirel. Pers. Commun.* **2015**, *82*, 1047–1057. [CrossRef]
23. Rasmussen, K.B.; Capkun, S. Implications of radio fingerprinting on the security of sensor networks. In Proceedings of the 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops—SecureComm 2007, Nice, France, 17–21 September 2007; pp. 331–340.
24. Ureten, O.; Serinken, N. Detection of radio transmitter turn-on transients. *Electron. Lett.* **1999**, *35*, 1996–1997. [CrossRef]
25. Ureten, O.; Serinken, N. Bayesian detection of Wi-Fi transmitter RF fingerprints. *Electron. Lett.* **2005**, *41*, 373–374. [CrossRef]
26. Mohamed, I.S.; Dalveren, Y.; Kara, A. Performance assessment of transient signal detection methods and superiority of energy criterion (EC) method. *IEEE Access* **2020**, *8*, 115613–115620. [CrossRef]
27. Mohamed, I.; Dalveren, Y.; Catak, F.O.; Kara, A. On the performance of energy criterion method in Wi-Fi transient signal detection. *Electronics* **2022**, *11*, 269. [CrossRef]
28. Soltanieh, N.; Norouzi, Y.; Yang, Y.; Karmakar, N.C. A review of radio frequency fingerprinting techniques. *IEEE J. Radio Freq. Identif.* **2020**, *4*, 222–233. [CrossRef]
29. Bai, L.; Zhu, L.; Liu, J.; Choi, J.; Zhang, W. Physical layer authentication in wireless communication networks: A survey. *J. Commun. Inf. Netw.* **2020**, *5*, 237–264. [CrossRef]
30. Huang, L.; Gao, M.; Zhao, C.; Wu, X. Detection of Wi-Fi transmitter transients using statistical method. In Proceedings of the 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC 2013), Kunming, China, 5–8 August 2013; pp. 1–5.
31. Kose, M.; Tascioglu, S.; Telatar, Z. The effect of transient detection errors on RF fingerprint classification performance. In Proceedings of the 14th International Conference on Circuits, Systems, Control, Signal Processing (CSECS), Konya, Turkey, 20–22 May 2015; pp. 89–93.
32. Page, E.S. Continuous inspection schemes. *Biometrika* **1954**, *41*, 100–115. [CrossRef]
33. Basseville, M.; Nikiforov, I.V. *Detection of Abrupt Changes: Theory and Application*; Prentice Hall: Hoboken, NJ, USA, 1993.
34. Tartakovsky, A.; Nikiforov, I.; Basseville, M. *Sequential Analysis: Hypothesis Testing and Changepoint Detection*; Chapman & Hall: London, UK, 2014.
35. Xie, L.; Zou, S.; Xie, Y.; Veeravalli, V.V. Sequential (quickest) change detection: Classical results and new directions. *IEEE J. Sel. Areas Inf. Theory* **2021**, *2*, 494–514. [CrossRef]
36. Lai, T.L. Sequential changepoint detection in quality control and dynamical systems. *J. R. Stat. Soc.* **1995**, *57*, 613–658. [CrossRef]
37. Granjon, P. The CUSUM algorithm—A small review. Tech. Rep. 2013. Available online: https://hal.archives-ouvertes.fr/hal-00914697 (accessed on 1 September 2022).
38. Lorden, G. Procedures for reacting to a change in distribution. *Ann. Math. Stat* **1971**, *42*, 1897–1908. [CrossRef]

39. Willsky, A.; Jones, H. A generalized likelihood ratio approach to the detection and estimation of jumps in linear systems. *IEEE Trans. Autom. Control* **1976**, *21*, 108–112. [CrossRef]
40. Appel, U.; Brandt, A.V. Adaptive sequential segmentation of piecewise stationary time series. *Inf. Sci.* **1983**, *29*, 27–56. [CrossRef]
41. Basseville, M.; Benveniste, A. Sequential detection of abrupt changes in spectral characteristics of digital signals. *IEEE Trans. Inf. Theory* **1983**, *29*, 709–724. [CrossRef]
42. Basseville, M. Detecting changes in signals and systems—A survey. *Automatica* **1988**, *24*, 309–326. [CrossRef]
43. ADALM Pluto Software Defined Radio. Analog Devices. 2022. Available online: https://www.analog.com/en/design-center/evaluation-hardware-and-software/evaluation-boards-kits/adalm-pluto.html (accessed on 10 August 2022).
44. Geier, J. *Designing and Deploying 802.11 Wireless Networks: A Practical Guide to Implementing 802.11n and 802.11ac Wireless Networks for Enterprise-Based Applications*; Cisco Press Networking Technology Series; Cisco Press: Indianapolis, IN, USA, 2015.
45. *IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012)*; IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE: Piscataway Township, NJ, USA, 2016; pp. 1–3534.
46. Terry, J.; Heiskala, J. *OFDM Wireless LANs: A Theoretical and Practical Guide*; Sams: Indianapolis, IN, USA, 2002.
47. Specht, D.F. Probabilistic neural networks. *Neural Netw.* **1990**, *3*, 109–118. [CrossRef]
48. Duda, R.O.; Hart, P.E.; Stork, D.G. *Pattern Classification*, 2nd ed.; Wiley-Interscience: New York, NY, USA, 2001.