TDMA Device Identification Using Continuity of Carrier Phase

Y Pan*, H Peng, T Li and W Wang
Information Engineering University, Zhengzhou 450001, China

*E-mail: novakd@163.com

Abstract. Specific emitter identification provides the capability to distinguish radio emitters with the external features carried by the received waveforms. As existing features are not specific to time-division multiple access (TDMA) devices, it is yet intractable to discern the emitter in the case of low signal-to-noise rates or short durations. In this paper, we propose a novel characteristic based on the continuity of carrier phase and explore its application on TDMA device identification. The characteristic reflects a fact whether adjacent time slots are assigned to the same user terminal, which reveals a potential link between slots even if the protocol is unknown. To apply it to TDMA device identification, we augment the typical SEI scheme with two subsystems, Decision and Correction, in which the recognition results can be corrected to improve the accuracy. Simulation results demonstrate that the characteristic is resilient against the ambient noise, and it evidently improves the recognition accuracy.

1. Introduction

Specific emitter identification (SEI) is a technique to identify the individual emitters by extracting external features from a given signal [1]. Because the external features are unique for each emitter, SEI plays an important role in military and civil fields [2], [3]. A typical SEI system, as shown in figure 1, generally consists of several subsystems: Radio Frequency (RF) System, Signal Processing, Feature Estimation, Identification Classifier, Cluster Management and Database [1].

![Figure 1. Typical SEI system.](image_url)

The key of SEI is a set of features that make identification possible. Features can be inferred or predefined [4]. We say that features are inferred when they are extracted from signals by means of some transformations, without a priori knowledge of a specific signal characteristic. For example, features are extracted using Wavelet Transform to identify the individual RF emitters [5]. Another approach is to exploit bispectrum characteristics with Fast Fourier Transform [6]. Furthermore, Hilbert-Huang Transform is also applied to extract the RF fingerprinting in [7], [8]. Differently from inferred features, the predefined ones relate to well-understood signal characteristics. In [9], Vladimir Brik creatively proposes a passive radiometric device identification system (PARADIS) differentiating 138 wireless
devices with accuracy in excess of 99%. The proposed characteristics are imperfections in modulation domain, such as frequency offset, I/Q origin offset, magnitude and phase errors. Besides, phase noise of the oscillator is used as the device tags to identify individual emitters in [10].

However, the foregoing features are not specific to time-division multiple access (TDMA) devices. Especially, in the case of low signal-to-noise rates (SNRs) or short durations, the features are too unstable to be used for recognition. In this paper, we propose a novel characteristic based on the continuity of carrier phase and augment the typical SEI scheme with two subsystems to identify the TDMA devices. To be specific, the new characteristic reflects a fact whether adjacent time slots are assigned to the same user terminal. In other words, it reveals a potential link between slots, even if the protocol is unknown. Thus, SEI for each slot may be no longer independent. The potential link, as a priori knowledge, can further improve the accuracy by correcting the results. The main contributions are summarized as follows:

- A novel characteristic of TDMA devices is proposed to detect whether the adjacent slots are assigned to the same user. Besides, we not only interpret the fingerprinting in terms of the transmitter structure, but also extract it with a defined metric.
- For TDMA device, the typical SEI system is extended with two subsystems: Decision and Correction. In the Decision subsystem, an adaptive threshold is derived by modelling and analysing the distribution of the novel characteristic. In the Correction subsystem, a maximum-confidence approach is provided to correct the results.

The remainder of this paper is organized as follows. Section 2 gives the background. Section 3 introduces the new characteristic. Section 4 presents the augmented system for TDMA device identification. Section 5 provides the numerical simulations. Finally, Section 6 concludes the paper.

2. Background

2.1. Frame Structure

TDMA is frequently used in the multiuser communication systems. For a TDMA system, each user terminal transmits the information in bursts. As depicted in figure 2, bursts are organized within a periodic structure, called a TDMA frame. Each frame is divided into a number, say \( S \), of non-overlapping time slots. A small time interval is reserved between adjacent slots for protection.

![Figure 2. TDMA frame structure.](image)

2.2. Transmitter Structure

In the TDMA system, each user terminal is equipped with an independent modem and antenna. This implies that each user is an individual radio emitter. Nowadays, direct complex modulation has
increasingly become the architecture of choice for implementing transmitter signal chains for end applications [11]. This technique directly modulates the output I/Q signals of a digital-to-analog converter onto an RF carrier, which eliminates the need for an intermediate frequency stage and the associated filtering. A typical direct conversion transmitter is shown in figure 3.

3. Continuity of carrier phase

RF fingerprinting is possible due to hardware imperfections in the analog circuitry introduced at the manufacturing process. As indicated in figure 3, the reserved time interval is very small. When adjacent slots are assigned to the same user, there is no enough time for local oscillator (LO) in the transmitter to adjust. This means that LO maintains the same operating state during the reserved time interval, which leads to a continuity of carrier phase between the adjacent slots. Obviously, this phenomenon will hardly exist when the adjacent slots are assigned to different users. Therefore, the continuity of carrier phase is a characteristic of TDMA signals, which can be used to detect the assignment of adjacent slots.

We assume that there are $S$ time slots in a frame. Consider slot $i$, the complex envelope of the received waveform can be modelled as:

$$r_i(t) = \exp\left[i(2\pi f t + \theta_i)\right] \sum_k c_k g(t - kT_0 - \tau_i) + \omega_i(t), \quad i = 2, \cdots, S,$$  \hspace{1cm} (1)

Where $f$ is the frequency offset, $\theta$ is the carrier phase, $\tau$ is the timing phase, $\{c_k\}$ are information symbols, $T_0$ is the symbol period, $g(t)$ is the real-valued signalling pulse shape, $\omega_i(t)$ is the complex-valued channel noise which is assumed to be white and Gaussian.

To measure the continuity of carrier phase, a new metric $\phi$ named phase prediction error is defined. We first start with the phase difference $\Delta \theta_i$:

$$\Delta \theta_i = \theta_{i,\text{pre}} - \theta_{i,\text{act}}, \hspace{1cm} \text{(2)}$$

Where $\theta_{i,\text{act}} = \theta_i$ is the actual carrier phase of slot $i$, and $\theta_{i,\text{pre}}$ represents the predicted carrier phase inferred from slot $i - 1$. We consider $f$ as a fixed parameter, and then the predicted carrier phase can be expressed as $\theta_{i,\text{pre}} = 2\pi f_{i-1}\Delta t + \theta_{i-1}$, where $\Delta t$ is the time difference between adjacent slots. Substituting into equation (2) yields:

$$\Delta \theta_i = (2\pi f_{i-1}\Delta t + \theta_{i-1}) - \theta_i.$$

In fact, there are phase ambiguities when estimating carrier phase of I/Q signals. Let $\psi$ represent the minimum phase ambiguity. (e.g. $\psi = 0.5\pi$ with QPSK modulation.) To sidestep its obstacle, we have:

$$\Delta \tilde{\theta}_i = \Delta \theta_i \mod \psi,$$ \hspace{1cm} \text{(4)}

Where $x \mod y$ is the remainder after division of $x$ by $y$. Finally, we derive phase prediction error $\varphi_i$:

$$\varphi_i = \begin{cases} 
\Delta \tilde{\theta}_i, & 0 \leq \Delta \tilde{\theta}_i < 0.5\psi \\
\Delta \tilde{\theta}_i - \psi, & 0.5\psi \leq \Delta \tilde{\theta}_i < \psi.
\end{cases}$$ \hspace{1cm} \text{(5)}

4. TDMA device identification

Differently from the conventional features, the new characteristic seems not to be used to identify the individual radio emitters directly. Here, we propose an augmented system for TDMA device identification, as displayed in figure 4.
In figure 4, \( \mathbf{f} \) refers to the vector of conventional features, and \( \varphi \) is the prediction phase error. In Decision subsystem, it is necessary to determine whether the adjacent slots are assigned to the same user terminal with \( \varphi \). Taking the slots assignment as a priori knowledge, Correction subsystem can correct some wrong results obtained by Identification Classifier.

![Diagram](https://example.com/diagram.png)

**Figure 4.** Augmented system for TDMA device identification.

### 4.1. Decision Subsystem

Assume that \( ID_i \) is the user identity of slot \( i \). Determining whether the adjacent slots are assigned to the same user terminal is a problem of detection, which can be formulated as a binary hypothesis test:

\[
H_0 : ID_i \neq ID_{i-1} \\
H_1 : ID_i = ID_{i-1}.
\]  

(6)

In the test, we consider the detector \( X = \varphi_i \). Now, the issue is how to derive an adaptive threshold.

From the foregoing discussion, it is clear that \( \varphi_i \) is close to zero under \( H_0 \); on the contrary, \( \varphi_i \) is a random value in the range \([-0.5\pi, 0.5\pi)\). Because \( \{\varphi_1, \ldots, \varphi_s\} \) is a set of statistically independent random variables, the distribution of the detector \( X \) can be modelled as:

\[
X \sim \begin{cases} 
U(-0.5\pi, 0.5\pi), & H_0 \\
N(0, \sigma^2), & H_1
\end{cases}.
\]

(7)

As is seen, \( X \) has a uniform distribution under \( H_0 \); whereas \( X \) is Gaussian-distributed with zero mean and variance \( \sigma^2 \) under \( H_1 \). Hence, we produce the probability density function of \( X \):

\[
p(x) = \begin{cases} 
\frac{1}{\psi}, & H_0 \\
\frac{1}{2\pi\sigma^2} \exp \left( -\frac{x^2}{2\sigma^2} \right), & H_1
\end{cases}.
\]

(8)

We notice that \( \sigma^2 \) is unknown in equation (8), which may relate to the characteristics of both channel and transmitter. To proceed, we concentrate on estimating \( \sigma^2 \) using a statistical method. Suppose that the received waveform is observed over \( L \) frames. Let \( \varphi_j^i \) represent the phase prediction error of slot \( i \) in frame \( j \). We organize them into a vector of length \( L(S-1) \), as follows:

\[
\varphi = [\varphi_2, \varphi_3, \ldots, \varphi_j^1, \varphi_3, \ldots, \varphi_j^2, \ldots, \varphi_j^S, \ldots, \varphi_j^{S-1}]^T.
\]

(9)

We compute the absolute value of each element in \( \varphi \), and sort them in ascending order to produce a new vector \( \tilde{\varphi} \). Figure 5 shows the vector \( \tilde{\varphi} \) of an actual signal. As is seen, \( \tilde{\varphi} \) has a length of 976, and takes value in the range \([0, \pi/4)\) with QPSK modulation. Suppose that \((x, y)\) is any point on the...
curve, it can be interpreted that there are \( y \) elements whose values are in the range \([0, x]\). Because \( \varphi_i' \) follows the distribution in equation (7), the curve of \( \Phi \) achieves the cumulative distribution function of \( |X| \) when the vector length is sufficiently large.

![Figure 5. Vector \( \Phi \) of an actual signal.](image)

Furthermore, it is interesting to note that the curve is clearly divided into two parts under the two hypotheses. This reflects the fact that the value of the inflection point can be used as the test threshold. Assume that the inflection point is \( N_0 \), thus, we have the test threshold:

\[
\gamma = \bar{\varphi}_{N_0}, N_0 = 1, \ldots, L(S - 1), \tag{10}
\]

Where \( \bar{\varphi}_{N_0} \) is the \( N_0 \)-th element of vector \( \Phi \).

Now, we focus on locating the inflection point \( N_0 \). Bearing in mind that \( \varphi_i' \) follows the normal distribution under \( H_1 \), the interval \((-3\sigma, 3\sigma)\) contains 99.74% of all the values based on the 3-sigma rule. Thus, it is reasonable to assume that \( 3\sigma \approx \bar{\varphi}_{N_0} \) and the number of adjacent slots satisfying hypothesis \( H_1 \) approximately equals \( N_0 \). Then, the variance can be estimated as \( \hat{\sigma}^2 = (\bar{\varphi}_{N_0}/3)^2 \).

Accordingly, we yield the fitting curve of \( \Phi \ (x \in [0, 3\sigma]) \):

\[
F(x) = \frac{N_0}{(2\pi\hat{\sigma}^2)^{1/2}} \int_{-\infty}^{x} \exp\left(-\frac{t^2}{2\hat{\sigma}^2}\right) dt = \frac{6N_0}{(2\pi)^{1/2}} \bar{\varphi}_{N_0} \int_{-\infty}^{x} \exp\left(-\frac{9t^2}{2\bar{\varphi}_{N_0}^2}\right) dt. \tag{11}
\]

With these results at hand, the normalized mean square error of fitting can be expressed as:

\[
E(N_0) = \frac{1}{N_0} \sum_{k=1}^{N_0} \left( \bar{\varphi}_k - F^{-1}(k) \right)^2. \tag{12}
\]

For the sake of simplicity, \( F^{-1}(N_0) = 3\hat{\sigma} \). Thus, we can get the inflection point by means of a search:

\[
\hat{N}_0 = \arg \left\{ \min_{N_0} E(N_0) \right\}, N_0 = 1, \ldots, L(S - 1). \tag{13}
\]

Once \( N_0 \) is available, threshold \( \gamma \) is eventually derived by equation (10). Finally, our decision rule is:
\[ |X| = |\varphi| \geq \gamma. \quad (14) \]

In addition, the missed probability and the false alarm probability are:

\[
P_m = \Pr(|\varphi| \geq \gamma | H_i) = \left( \frac{2}{\pi \sigma^2} \right)^{\frac{1}{2}} \int_{\frac{\gamma}{\sigma}}^{\infty} \exp \left( -\frac{t^2}{2\sigma^2} \right) dt
\]

\[
P_f = \Pr(|\varphi| < \gamma | H_0) = 2\int_{0}^{\frac{\gamma}{\sigma}} \frac{1}{\psi} dt = \frac{6\sigma}{\psi}
\]

(15)

According to the 3-sigma rule, the detection probability \( P_d \approx 99.74\% \). Hence, \( P_m \approx 0.26\% \). For a specific modulation, \( P_f \) depends only on \( \sigma \) as \( \psi \) is a constant.

4.2. Correction Subsystem

Here, we introduce a maximum-confidence correction approach concentrating on the following case: there are consecutive \( V (V = 2, 3, \ldots, S) \) time slots assigned to the same user in a frame, whereas their original recognition results are not same.

With the incoming features, classifier returns the best-matching identity, along with the similarity of each identity. Here, we name the similarity as ‘confidence’. Suppose that \( U \) user terminals are in a TDMA system. Let \( P \), with the size of \( V \times U \), be the confidence matrix of the \( V \) slots. The \((v, u)\)-th element \( p_{v,u} \) of \( P \) represents the confidence that slot \( v \) is recognized as user \( u \). Clearly, \( \sum_{u=1}^{U} p_{v,u} = 1 \).

Now, the key is to find out the wrong results. Suppose that \( n_r \) is the number of right results, \( n_w = V - n_r \) is the number of wrong ones; \( p_r \) and \( p_w \) are the maximum confidences of right results and wrong ones, respectively. Fortunately, we could have \( n_r \geq n_w \) and \( p_r > p_w \) with a high probability. Bearing these in mind, we sum all \( V \) confidences of user \( u \) and yield:

\[
P_u = \sum_{v=1}^{V} p_{v,u}.
\]

(16)

By summing, the adverse effect of wrong results can be eliminated. Thus, the original recognition results are corrected as:

\[
ID' = \arg \max_{u} P_u, \ u = 1, \ldots, U.
\]

(17)

5. Results

We demonstrate our technique on a collection of five TDMA transmitters with the same manufacturer. All devices operate at the 1.4 GHz center frequency and are digitized at a sampling rate of 800 KHz. Specifically speaking, QPSK modulation, 400 Kbps date rate, \( L = 122 \), \( S = 9 \), \( U = 5 \). Because the SNRs of the received signals are measured to be more than 40 dB, which are considered as ‘noise-free’. We add white Gaussian noise to the noise-free signals to simulate the different SNR scenarios.

5.1. Decision Performance

There are a total of \( L(S - 1) = 976 \) adjacent time slots, 650 of which are under \( H_i \), and the others are under \( H_0 \). The performance of Decision subsystem is assessed by detection accuracy defined as:

\[
P_e = 1 - \frac{n_w + n_f}{L(S - 1)},
\]

(18)
Where \( n_m \) is the missed number, \( n_f \) is the false alarm number.

Figure 6 illustrates the average results obtained by 1 000 Monte-Carlo tests. As shown in figure 6, as \( E_s/N_0 \) increases, \( \tilde{P}_c \) decreases. It is apparent that \( \tilde{P}_c \) is adaptive to the different SNRs. In addition, increasing \( E_s/N_0 \) makes \( \tilde{P}_d \) and \( \tilde{P}_c \) larger. Notice that \( \tilde{P}_c < \tilde{P}_d \), because \( \tilde{P}_c \) depends on both \( n_m \) and \( n_f \) in equation (18). As \( \tilde{P}_c \) keeps on a high level at different SNRs, the performance of Decision subsystem is satisfactory.

![Figure 6](image6.png)

**Figure 6.** Detection performance at different SNRs. (a) threshold, (b) detection probability and detection accuracy.

Figure 7 shows the missed probability and false alarm probability at different SNRs, where the theoretical false alarm probability \( P_f,\text{theo} \) is drawn by substituting \( \tilde{P}_c \) into equation (15) (\( \gamma=\tilde{P}_d/N_0 \approx 3\sigma \)). In figure 7, both \( P_f,\text{simu} \) and \( P_m,\text{simu} \) are quite close to the theoretical probabilities. This corroborates the rationality of equation (15). Besides, notice that as \( E_s/N_0 \) increases, \( P_f \) gradually drops. This is expected, because \( P_f \) is proportional to \( \gamma \), which approaches to zero as \( E_s/N_0 \) increases.

![Figure 7](image7.png)

**Figure 7.** Missed probability and false alarm probability at different SNRs.

![Figure 8](image8.png)

**Figure 8.** Recognition accuracies with and without correction at different SNRs.

5.2. Correction Performance
We investigate the performance of Correction subsystem by comparing the recognition accuracies with and without correction. Figure 8 depicts the recognition accuracies with and without correction at different SNRs. In this simulation, PARADIS in [9] is employed to extract the features. 61 frames (a total of 549 slots) are used to train a support vector machine (SVM), and the remaining 61 frames are used to test. The SVM classifier, with the radial basis function, is implemented by the LIBSVM in [12]. As shown in figure 8, PARADIS with correction outperforms PARADIS without correction. The former achieves about 10% gain in recognition accuracy. The reason is that, SEI for each slot is no longer independent, and wrong results are effectively corrected in Correction subsystem.

6. Conclusion
In this letter, we propose a novel characteristic based on the continuity of carrier phase and explore it application on TDMA devices identification. The characteristic throws a light to the adjacent slots assignment even if the protocol is unknown. Taking it as a priori knowledge of the slot assignment, SEI for each slot may be no longer independent. Recognition accuracy can be improved by corrected the results. Simulation results are provided to demonstrate the effectiveness of our work.

Acknowledgments
This research was supported by the National Natural Science Foundation of China (No. 61401511, and No. U1736107).

References
[1] Kenneth T, Paul D and Martin Hyatt 2003 J. Tech. Review Jan 113-33
[2] Kevin M, Shauna R, George S and Bryan N 2018 J. IEEE J. Sel. Top. Sig. Pro. 12 160-67
[3] Wen J, Ying C, Lin Y and Zichang H 2017 J. Sensors 17 1972
[4] Boris D, Davide Z and Srdjan C 2012 J. ACM Comput. Surv. 45 6
[5] Huanhuan W and Tao Z 2017 Proc. Int. Conf. on Information Technology Electronic Automation Control vol 2 (Chongqing: China/IEEE) p 1613
[6] Jie H, Tao Z, Dongfang R and Xiaoyu Z 2017 J. IET Sci. Meas. Tech. 11 1104-12
[7] Jingwen Z, Fanggang W, Octavia D and Zhangdui Z 2016 J. IEEE Trans. Info. Forensics Secu. 11 160-67
[8] Udit S, Nikita T, Gagarin Biswal and Baratram R 2019 J. IEEE Trans. Info. Forensics Secu. 14 581-91
[9] Vladimir B, Suman B, Marco G and Sangho O 2008 Proc. ACM Mob. Comput. Network. vol 14 (New York: USA/ACM) p 116
[10] Adam P and Dennis G 2015 J. IEEE Trans. Info. Forensics Secu. 10 2492-501
[11] Yi, Z 2010 Wireless transmitter IQ balance and sideband suppression (Norwood: USA/ Analog Devices) [Online]. Available: http://www.analog.com/media/en/technical-documentation/application-notes/AN-1100.pdf
[12] Chih-Chung, C and Chih-Jen, L 2016 LIBSVM: a library for support vector machines Version 3.22 [Online]. Available: http://www.csie.ntu.edu.tw/~cjlin/libsvm