A Measurement-Referenced Error Vector Magnitude for Counterfeit Cellular Device Detection

Améya S Ramadurgakar*†, Kate A Remley†, Dylan F Williams†, Jacob D Rezac†,
Melinda Piket-May*, Robert D Horansky†
*Department of Electrical, Computer and Energy Engineering
University of Colorado Boulder
Email: {ameya.ramadurgakar, melinda.piket-may}@colorado.edu
†Communications Technology Laboratory
National Institute of Standards and Technology
Email: {ameya.ramadurgakar, kate.remley, dylan.williams, jacob.rezac, robert.horansky}@nist.gov

2023 101st ARFTG Microwave Measurement Conference (ARFTG) | 979-8-3503-2345-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/ARFTG57476.2023.10279175

***Abstract*—Standard formulations of error vector magnitude compare a wireless device's symbol constellation to an ideal reference constellation. In this work, we utilize the residual error vector magnitude, which uses measurements of a wireless device to define a reference constellation. We apply this formulation to the problem of identifying a device's manufacturer from over-the-air measurements of the wireless device and show that the residual error vector magnitude outperforms standard error vector magnitude formulation in this task.**

***Index Terms*—error vector magnitude (EVM), long term evolution (LTE), over-the-Air (OTA), residual EVM, user equipment (UE), vector signal analyzer (VSA), wireless system**

I. Introduction

Error vector magnitude (EVM) is a typical performance metric used in determining the quality of the wireless communication system such as channel impairments and communication hardware. Therefore, it is extensively applied across testing of different wireless networks and devices. EVM is the root-mean-squared distance between the ideal symbol location and the measured locations of the same symbols in the complex coordinate system representing a modulated waveform.

While standard EVM [1] is useful for comparing ideal and measured symbol locations, EVM can also be used to compare measured symbol locations to measured reference locations. Previous work has investigated two definitions of EVM that address this. The first is differential EVM. In [2], differential EVM is defined as the magnitude of the normalized difference between the vectors representing consecutive symbols of the transmitted signals in IEEE 802.15 radio networks. Those formulations focus on applying differential EVM to a single wireless device, whereas in this work we focus on identifying differences between multiple devices. The second definition, known as Residual EVM, is found in the IEEE 1765 standard [3]. Residual EVM compares the symbol positions between a reference-lab receiver and a user-lab receiver. We apply a similar residual formulation to counterfeit detection of wireless cellular devices through a measurement-based reference in the residual EVM formulation.

The motivation for this work is to use over-the-air (OTA) radio-frequency (RF) measurements of cellular user equipment (UE) to identify distinctive characteristics that are unique to the same model of UE. This process, sometimes called RF fingerprinting, is often performed to assess if a UE has been tampered with or is a counterfeit. The RF fingerprinting problem has been studied previously in many contexts. See [4] and its references for an overview as well as [5] - [8]. Conducted methods such as those presented in [9] involve non-destructive techniques that provide over 95% accuracy in identification of counterfeit or cloned hardware.

More recent advancements have leveraged statistical learning techniques in the application of RF fingerprinting. Statistical learning has been used to authenticate UEs by quantifying radiated waveform similarities [10] - [11]. A symbol-based RF fingerprinting technique for identifying counterfeit base station was discussed in [12], where a UE measured the EVM of a counterfeit base station. Our proposed technique adds to previous work by showing the application of residual EVM as a metric that may be applied to the problem of counterfeit UE identification.

II. Experimental Set-Up

We used a fixed measurement setup to determine a UE's residual EVM in this work. Figure 1 shows the components of the setup. A base station emulator (BSE) is used to generate modulated communications signals that are received by a UE under test. The UE then transmits a fixed length modulated symbol stream back to the BSE. A sniffer antenna, which is connected to the vector signal analyzer (VSA), measures radiated signal at the uplink frequency of the UE. Our experimental design relies on the UE consistently transmitting the same modulated symbol stream across observations, which we achieve with the BSE's standardized test modes [13]. This is important in our experiment as it establishes a reference symbol stream that is repetitively measured by the VSA. The reference symbol stream is generated by holding the uplink waveform constant, which helps in detecting subtle differences when the same waveform is emitted from various devices. The conditions that are held constant in the measurements shown in this work are:

- Up-link center frequency = 1950 MHz (LTE Band 1)

- Frame duration = 10 ms (1 Frame)
- LTE Resource Blocks = 50 per sub-frame
- Modulation Depth (uplink) = 16 QAM
- Modulation Coding Scheme index value (uplink) = 20
- Distance of BSE and sniffer antenna from center of the UE inside the chamber
- Observation interval and number of observations
- Fixed length UE uplink symbol stream
- Channel bandwidth = 10 MHz

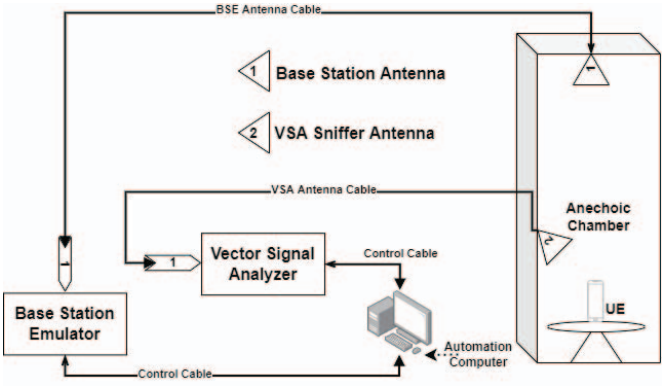

Fig. 1: Block diagram of the measurement set-up

A ranging process is performed at the intermediate frequency (IF) to ensure maximum digitization of the measured waveform by the analog-to-digital (ADC) converter inside the VSA. The UE uplink power is set to a constant value by the BSE after the attach procedure is completed between the BSE and UE.

Each test UE is placed flat with the screen facing up to the BSE antenna and in the same orientation relative to the BSE antenna inside the anechoic chamber and a wireless link established to the BSE. Inside the anechoic chamber, the base station antenna and the VSA sniffer antenna are positioned in a way that minimizes coupling between them. Coupling between the antennas makes the reproducibility of the set-up more difficult. After the UE attaches to the BSE, the BSE instructs the UE to uplink transmit waveforms that match a specific symbol-constellation stream. If this stream is not detected by the VSA, the UE is made to reattach. This specific symbol-constellation stream is used as a reference stream for this device. Additionally, we ensure the downlink between the UE and BSE is error free.

Figure 2 shows a top level block diagram of the measurement and analysis processes involved. The first four steps of Figure 2 are measurement processes. We perform 100 observations in Step 4 of the process, with a delay time of 1 minute between each observation. This 1 minute delay was experimentally chosen to reduce auto-correlation between measurements within a set of observations. A high auto-correlation of the median of each measured signal,taken across measurement observations, would suggest a statistical dependence between observations. A delay of 1 minute was sufficient to ensure small values of the auto-correlation function across all lags for each measurement. The last two steps are part of the analysis process.

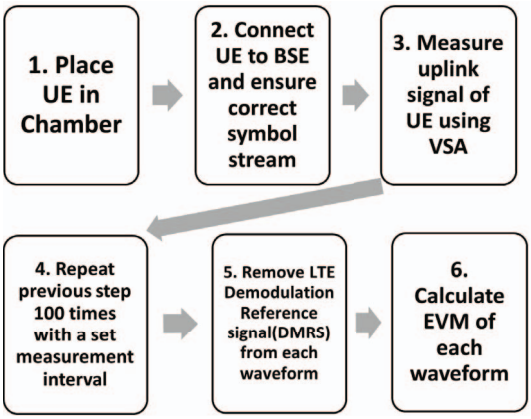

Fig. 2: Measurement and analysis process

III. Residual EVM

The EVM of a measurement as defined in [1] is

$$\mathrm{EVM}(S_{\mathrm{ideal}}, S_{\mathrm{meas}}) = \left(\frac{\frac{1}{N}\sum_{n=1}^{N} |S_{\mathrm{ideal,n}} - S_{\mathrm{meas,n}}|^2}{\frac{1}{N}\sum_{n=1}^{N} |S_{\mathrm{ideal,n}}|^2} \right)^{1/2}, \tag{1}$$

where S_{ideal} and S_{meas} are vectors of length N containing, respectively, the ideal symbol-constellation points and the measured symbol-constellation points. The subscript n indicates the nth symbol's constellation point in each vector; we ensure that the nth element of both the ideal and measured vectors are matched to the same symbol-constellation point. In this paper we present EVM as a percentage.

In counterfeit detection, we are not interested in the transmission quality of a UE but rather how repeatable a fingerprint measurement is, and how unique it is to a specific UE. This is difficult to perform with the standard definition of EVM introduced in (1) because S_{ideal} is a repeatable vector containing the symbol pattern which is independent of the UE. To this end, we apply the residual EVM, which we define as

$$\mathrm{EVM}_{\Delta}(S_{\mathrm{ref}}, S_{\mathrm{meas}}) = \left(\frac{\frac{1}{N}\sum_{n=1}^{N} |S_{\mathrm{ref,n}} - S_{\mathrm{meas,n}}|^2}{\frac{1}{N}\sum_{n=1}^{N} |S_{\mathrm{ref,n}}|^2} \right)^{1/2}, \tag{2}$$

where N is again the number of symbols measured in an experiment. The value $S_{\mathrm{ref,n}}$ determines the reference symbol stream to which measurements, $S_{\mathrm{meas,n}}$, are compared at nth symbol.

We consider two forms of residual EVM in this work, both of which are based on measurements of the symbol-constellation streams. Assume we measure T observations of a fixed symbol stream from the same UE and store these values in a set of vectors $S^{(t)}_{\mathrm{meas}}$, $t = 1, \ldots, T$. Both forms of residual EVM take $S_{\mathrm{ref}} = \overline{S}_{\mathrm{meas}}$, the average over observations of each symbol stream. However, the forms differ from each other in terms of S_{meas}.

The first residual EVM form we consider takes the form $EVM_{\Delta}(\overline{S}_n, \overline{S}_{n,t})$, where n refers to the model of the UE and t refers to the t^{th} measurement of the waveform generated by that UE. The quantity $EVM_{\Delta}(\overline{S}_n, \overline{S}_{n,t})$, which we refer to as the "Deviation EVM," describes the deviation of a measurement of a single waveform in a set of repeated waveforms from the mean of all the measured waveforms generated by the same UE. These deviations could be due to noise in the receivers, which we minimized by adjusting power levels in the setup to be well above the noise floor of the receivers. These deviations may also have components due to noise in the UE, drift in the receivers and measurement setup. We used the Deviation EVM to investigate stability across the measurement time interval and to capture any temporal drift in the measurements. The Deviation EVM establishes a baseline for how much deviation in the measured signals we expect due to noise and drift and helps to identify any errors that occur abruptly during a single measurement.

The second form of residual EVM, which we call Fingerprint EVM, compares measured symbol streams that have been averaged over the T observation sets. The two symbol streams could either be from different UEs or from the same UE measured at different times. The averaging process reduces the noise in each set of data.

IV. Results

In this section, we present the results of experiments that illustrate the noise and other errors in individual measurements with Deviation EVM and demonstrate the efficacy of Fingerprint EVM for identifying UEs and differences between them. We measured three different UE models, each model from a different manufacturer and each having a different RF chipset. For each of these three UEs, we performed $T = 100$ observation measurements in the manner described in Section II. We use the same measurement set of 100 observations for the calculations shown in this section, except for when comparing two measurements of the same UE to each other, in which case, we used a second set of measurements performed in the same way. Prior to calculating the residual EVM formulations described in Section III, we applied the VSA software's internal time and phase alignment procedures to measurements for comparing waveforms. We additionally removed all elements of a LTE-specific reference signal, the Demodulation Reference Signal (DMRS), to ensure we calculated EVM on the known symbol set of transmitted symbols by the UE.

Figure 3 (Top) was generated using (1), the standard EVM formulation. We generated S_{ideal} for this figure with the software package MATLAB,[1] ensuring that the value of each symbol on the constellation diagram was the same as in our measurements. The EVM calculated for all three UEs for each observation t is shown in Figure 3 (Top). The EVM of each UE stays between approximately 1.0% and 1.45% over 100 observations, where UE2 is differentiable but not UE1 and UE3. Figure 3 (Middle) captures the noise and other errors

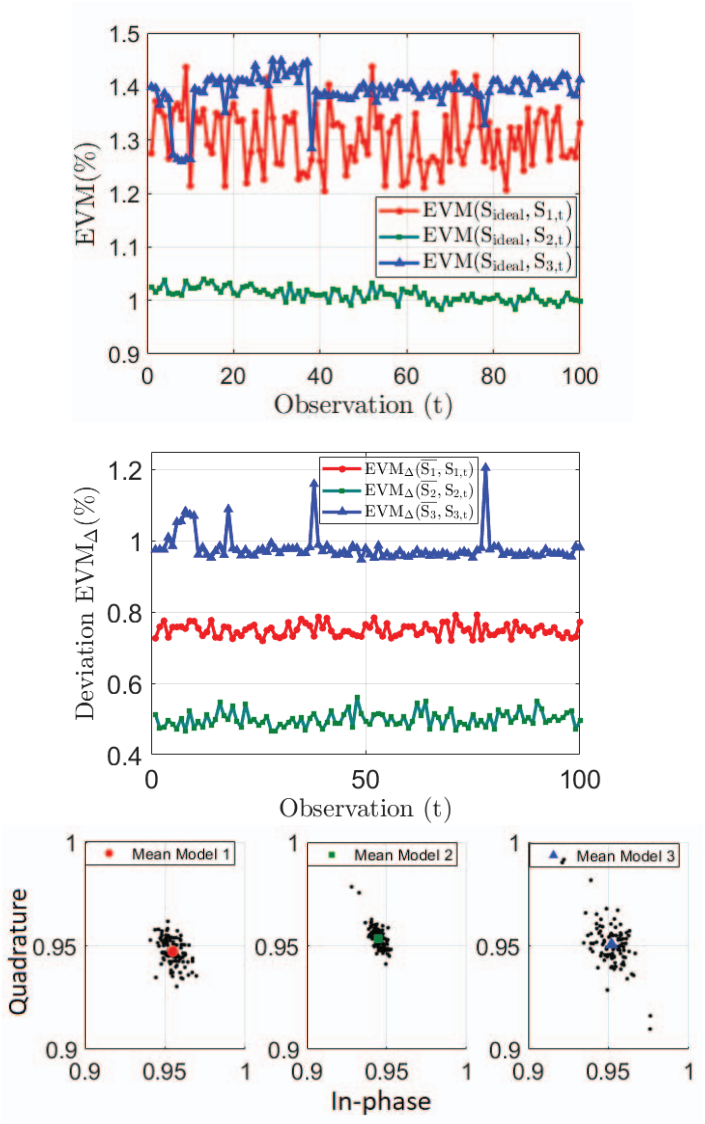

Fig. 3: (Top) EVM using (1) for devices from three manufacturers. (Middle) Deviation EVM. (Bottom) First symbol instance constellation plot.

of each UE measurement for each observation t, which is not clearly conveyed in the plot in Figure 3 (Top). The flatness of the Deviation EVM shown in Figure 3 (Middle) indicate that the noise levels are fairly consistent between 0.07% to 0.25% across the three UEs from observation to observation, while the high level of the deviation of the EVM for each UE illustrate why it is difficult to compare UEs without averaging the observations. Thus, Deviation EVM is used to check the measurement set, while Fingerprint EVM is used to identify UEs.

The curves for each UE model in Figure 3 (Middle) differ from each other because of the size of the symbol cloud on the constellation diagram. Figure 3 (Bottom) exemplifies this,

[1]The National Institute of Standards and Technology does not endorse commercial products. Other products may work as well or better.

where the three plots show the spread of the first symbol instance of a symbol on the outer edge of the constellation diagram "Symbol 12", across 100 observations for each UE Model respectively. The first symbol instance is the first occurrence of a symbol in the measured LTE frame. The mean values depicted in Figure 3 (Bottom) indicate the differences in the waveforms emanating from the UE.

The bigger the size of the Symbol 12 clouds in Figure 3 (Bottom), the higher the Deviation EVM seen in Figure 3 (Middle) and higher the variability of some UEs than others. We next apply Fingerprint EVM, a more robust metric for device identification, having more degrees of freedom than simple noise levels.

We used the Fingerprint EVM to compare different UE models. We make this comparison with $EVM_{\Delta}(\overline{S}_i, \overline{S}_j)$ for each $i, j = 1, 2, 3$. By comparing the average over T observations of these models, we reduce the effect of variability in the Fingerprint EVM. Since the residual EVM of a UE model with itself is zero, we used a second measurement set of each UE to obtain $EVM_{\Delta}(\overline{S}_i, \overline{S}_{i'})$, where $\cdot'$ indicates the second measurement set $(i = 1, 2, 3)$. We summarize this information with the matrix.

$$\begin{bmatrix} EVM_{\Delta}(\overline{S}_1, \overline{S}_{1'}) & EVM_{\Delta}(\overline{S}_1, \overline{S}_2) & EVM_{\Delta}(\overline{S}_1, \overline{S}_3) \\ EVM_{\Delta}(\overline{S}_2, \overline{S}_1) & EVM_{\Delta}(\overline{S}_2, \overline{S}_{2'}) & EVM_{\Delta}(\overline{S}_2, \overline{S}_3) \\ EVM_{\Delta}(\overline{S}_3, \overline{S}_1) & EVM_{\Delta}(\overline{S}_3, \overline{S}_2) & EVM_{\Delta}(\overline{S}_3, \overline{S}_{3'}) \end{bmatrix} \tag{3}$$

$$= \begin{bmatrix} 0.11 & 1.03 & 0.75 \\ 1.03 & 0.08 & 0.76 \\ 0.75 & 1.03 & 0.13 \end{bmatrix}.$$

The diagonal entries of (3) compare measurements of the same UE model taken from different measurement sets while the off-diagonal elements compare different UE models taken from the same measurement set. This matrix is not symmetric because $EVM_{\Delta}(\overline{S}_i, \overline{S}_j)$ and $EVM_{\Delta}(\overline{S}_j, \overline{S}_i)$ have different denominators for each $i, j = 1, 2, 3$.

The values of Fingerprint EVM in (3) show differences in the mean of two sets of measurements of a single UE are small (the diagonal is always less than 0.15%), while the differences of measurement means are nearly an order of magnitude larger (the off-diagonal parts are between 0.75% and 1.03%). This illustrates the importance of phase aligning and averaging measurement sets before calculating residual EVM. This large contrast between residual Fingerprint EVMs suggests that residual Fingerprint EVM deserves further study in the context of UE identification.

V. Conclusion

This work shows that Fingerprint EVM has potential for fingerprinting and identifying cellular devices. The Deviation EVM can additionally be utilized to investigate the noise and stability of the UE's performance in a given setup. Both the Deviation and Fingerprint EVM formulations convey information not conveyed with the traditional EVM definition.

Our future work is aimed at improving OTA fingerprinting with a focus on improving the sensitivity of the EVM formulations to the measurement set-up through improvements in positioning of the UE and antennas and the choice of modulation scheme and frequency bands. Additionally, we will be exploring the uncertainties involved in such measurements. Finding the uncertainties involved will be important in providing confidence we can differentiate between genuine and counterfeit devices. Finally, we are looking into ways where Fingerprint EVM approach can be scaled to identify counterfeit devices at a much larger scale with regard to both both models made by different manufacturers and seperate devices of a single model made by the same manufacturer.

References

[1] S. Forestier, P. Bouysse, R. Quere, A. Mallet, J. . -M. Nebus and L. Lapierre, "Joint optimization of the power-added efficiency and the error-vector measurement of 20-GHz pHEMT amplifier through a new dynamic bias-control method," in IEEE Transactions on Microwave Theory and Techniques, vol. 52, no. 4, pp. 1132-1141, April 2004, doi: 10.1109/TMTT.2004.825745.

[2] "Product Documentation - NI", www.ni.com. https://www.ni.com/docs/en-US/bundle/rfmx-for-bluetooth-test/page/rfmxbt/edr differential evm.html (accessed Nov. 1, 2022).

[3] "IEEE Recommended Practice for Estimating the Uncertainty in Error Vector Magnitude of Measured Digitally Modulated Signals for Wireless Communications," in IEEE Std 1765-2022 , vol., no., pp.1-105, 11 Nov. 2022, doi: 10.1109/IEEESTD.2022.9942923.

[4] G. Baldini and G. Steri, "A Survey of Techniques for the Identification of Mobile Phones Using the Physical Fingerprints of the Built-In Components," in IEEE Communications Surveys Tutorials, vol. 19, no. 3, pp. 1761-1789, 2017, doi: 10.1109/COMST.2017.2694487.

[5] H. P. Romero, K. A. Remley, D. F. Williams and C. Wang, "Electromagnetic Measurements for Counterfeit Detection of Radio Frequency Identification Cards," in IEEE Transactions on Microwave Theory and Techniques, vol. 57, no. 5, pp. 1383-1387, May 2009, doi: 10.1109/TMTT.2009.2017318.

[6] B.B. Yilmaz, E.M. Ugurlu, A. Zajić and M. Prvulovic, "Detecting Cellphone Camera Status at Distance by Exploiting Electromagnetic Emanations," MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), 2019, doi: 10.1109/MILCOM47813.2019.9021060

[7] N. Soltanieh, Y. Norouzi, Y. Yang, and N. C. Karmakar, "A Review of Radio Frequency Fingerprinting Techniques", IEEE J. Radio Freq. Identif., vol. 4, no. 3, pp. 222–233, Sep. 2020, doi: 10.1109/JRFID.2020.2968369.

[8] J. Balasch, B. Gierlichs, and I. Verbauwhede, "Electromagnetic circuit fingerprints for Hardware Trojan detection", in 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), Dresden, Germany, Aug. 2015, pp. 246–251. doi: 10.1109/ISEMC.2015.7256167.

[9] T. D. Bergman, C. P. Manager, and K. T. Liszewski, "Battelle barricade: A nondestructive electronic component authentication and counterfeit detection technology", in 2016 IEEE Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, May 2016, pp. 1–6. doi: 10.1109/THS.2016.7568901.

[10] P. Robyns, E. Marin, W. Lamotte, P. Quax, D. Singelée, and B. Preneel, "Physical-layer fingerprinting of LoRa devices using supervised and zero-shot learning", in Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks, Boston Massachusetts, Jul. 2017, pp. 58–63. doi: 10.1145/3098243.3098267.

[11] M. Cekic, S. Gopalakrishnan, and U. Madhow, "Wireless Fingerprinting via Deep Learning: The Impact of Confounding Factors", 2020, doi: 10.48550/ARXIV.2002.10791.

[12] A.Ali, G. Fischer, "Symbol Based Statistical RF Fingerprinting for Fake Base Station Identification," in 2019 29th International Conference Radioelektronika (RADIOELEKTRONIKA), Pardubice, Czech Republic, Apr. 2019, pp. 1–5. doi: 10.1109/RADIOELEK.2019.8733585.

[13] "3GPP Portal gt; Home," Specification : 36.508. [Online]. Available: https://portal.3gpp.org/desktopmodules/ Specifications/SpecificationDetails.aspx?specificationId=2467. [Accessed: 26-Jan-2023].