CV-Track: Leveraging Carrier Frequency Offset Variation for BLE Signal Detection

Weiping Sun
Seoul National University
Department of ECE and INMC
Seoul, Republic of Korea
weiping@mwnl.snu.ac.kr

Jeongyeup Paek
Chung-Ang University
School of CSE
Seoul, Republic of Korea
jpaek@cau.ac.kr

Sunghyun Choi
Seoul National University
Department of ECE and INMC
Seoul, Republic of Korea
schoi@snu.ac.kr

ABSTRACT

We propose CV-Track, a real-time, low-complexity BLE signal detection scheme that leverages carrier frequency offset (CFO) estimation of commodity BLE chipsets to enable detection of the intact part of a partially corrupted BLE packet. It detects BLE signal by observing the variation of the estimated CFO values based on the finding that the CFO values are almost constant for BLE signal while dispersing otherwise. With CV-Track, we can salvage useful information such as received signal strength from an erroneous BLE packet which would otherwise be wasted. We implement a prototype of CV-Track on commodity BLE chipset, and evaluate its performance in an indoor environment. Our results indicate that CV-Track detects significantly more BLE packets compared with legacy BLE receiver under cross-technology interference.

CCS CONCEPTS

• **Networks** → *Network protocol design*; *Cross-layer protocols*; Network measurement;

KEYWORDS

BLE, GFSK, Signal Detection, Carrier Frequency Offset (CFO)

ACM Reference format:
Weiping Sun, Jeongyeup Paek, and Sunghyun Choi. 2017. CV-Track: Leveraging Carrier Frequency Offset Variation for BLE Signal Detection. In *Proceedings of HotWireless'17, October 16, 2017, Snowbird, UT, USA., ,* 5 pages.
DOI: http://dx.doi.org/10.1145/3127882.3127886

1 INTRODUCTION

Bluetooth Low Energy (BLE) [13] is an extension of the Bluetooth standard in version 4.0 that further enhances the energy-efficiency of the underlying Bluetooth technology; operating with just a single coin-cell battery, a BLE beacon can sustain for several months to years. Such aspects make BLE ideal for applications requiring transfers of small amount of data, and BLE has since attracted enormous attention in a wide range of industrial and consumer applications, but especially for its fascination on the indoor context-aware services; For example, Apple announced iBeacon[1] protocol for an industry-wide solution, which can provide context-awareness based on the signal strength of BLE packets transferred between pre-installed BLE beacons and iBeacon-compatible portable devices such as smartphones. These have allowed widespread adoption and deployment of indoor proximity/location enabled applications in our everyday lives [2, 6, 8].

A key challenge that BLE faces is loss of information due to collision and interference. Bit-error occurs when signal-to-interference-and-noise ratio (SINR) is insufficient to decode the bits correctly. Assuming that the receiver is within communication range of the transmitter, bit-error is often due to packet collision or cross-technology interference. For example, on the increasingly crowded 2.4 GHz ISM band, ambient interference is a salient factor that accounts for low SINR, where Wi-Fi, BLE, and Zigbee channels overlap (see Figure 1), implying the existence of cross-technology interference. To address or mitigate this challenge, there needs to be a way to detect the bit-error, and also a way to distinguish the cause of that error. Depending on the cause, the action to be taken, or lack there of, may differ.

As with many wireless technologies, BLE uses cyclic redundancy check (CRC) to detect bit-errors. Since we cannot judge the correctness for every bit of the packet when there is a CRC mismatch, a single bit-error can result in a discarded packet. Note that we will lose all information in that packet (implicit or explicit) if a packet is discarded. This is wasteful since very often, only part of a packet is in error while the rest is correct, especially when the packet is partially corrupted by ambient interference—a common phenomenon on 2.4 GHz ISM band. Said differently, if we can retrieve the intact part of a partially erroneous packet, we may be able to save significant amount of information from a transmission that would otherwise have been wasted.

Although discriminating the intact part of a partially erroneous packet is a challenging task, it can play an enabling role in various applications. For example, received signal strength indicator (RSSI) of an erroneous BLE packet can be retrieved through the intact part of the packet if we can detect it, which is essential for RSSI-based applications such as indoor localization, proximity-aware services, and link control algorithms. Furthermore, it may be possible to recover the original packet from multiple partially erroneous retransmissions by combining the intact parts of the packets [3]. Besides, knowing the existence of BLE signal itself (distinguished from other cross-technology signal) has a meaningful implication for network diagnosis and trouble-shooting, especially in the era of

HotWireless'17, October 16, 2017, Snowbird, UT, USA.

DOI: http://dx.doi.org/10.1145/3127882.3127886

[1] iBeacon for developers, Apple, https://developer.apple.com/ibeacon.

Internet of things (IoT) where finding out the cause of a packet-loss becomes more burdensome due to the massive cross-platform deployments of embedded technologies. If we can detect BLE signal with finer granularity than packet-level, it will be easier to judge whether a packet has (or has not) been transmitted on the BLE link, and whether there were cross-technology interference in the channel, providing opportunity for improved network performance.

Motivated by the above challenge, in this work, we propose CV-Track, a real-time, low-complexity BLE signal detection scheme that detects the intact part of an corrupted BLE packet using commodity BLE chipset. The key distinguishing aspect of CV-Track from any other prior work is that we make novel use of the *carrier frequency offset* (CFO) estimation module in commodity BLE transceivers to detect BLE signal by observing the variation of the estimated CFO values with and without cross-technology interference. CFO is the difference in the frequency between the transmitter and the receiver oscillators. Virtually all BLE chipsets incorporate a CFO estimation module to counteract the frequency mismatch because the underlying modulation scheme, i.e., Gaussian frequency shift keying (GFSK), is vulnerable to CFO. An important characteristics of the CFO is that it is pair-wise (near) constant. That is, for a given pair of BLE transmitter and receiver, their relative difference in the oscillator frequency is near constant. Thus, through the output of the CFO estimation module, it is possible to infer that an incoming signal is BLE signal without disruptive interference when the estimated CFO values are almost constant while dispersing otherwise (as we will later show). We use this feature to detect BLE signal.

The contributions of this paper are as follows;

- We are the first to propose and investigate the use of estimated CFO values in commodity BLE chipset for detecting BLE signal.
- We propose CV-Track, a **C**FO **V**ariation-based BLE signal detection scheme that can detect intact part of corrupted BLE packets and infer the transmitter based on the uniqueness of pair-wise CFO and the timing of the detection.
- We implement a prototype of CV-Track on commodity BLE chipset, and evaluate its performance via experiments in an indoor environment.

2 PRELIMINARY

In this section, we provide brief overview and background on BLE channelization, GFSK modulation, and the CFO estimation.

2.1 Channelization

There are 40 BLE channels defined on 2.4 GHz ISM band, ordered from number 0 to 39 with 2 MHz spacing. The band is shared with other technologies, e.g, Wi-Fi, Zigbee, and microwave oven (MWO), thus introducing cross-technology interference. Figure 1 highlights three BLE *advertising channels*, i.e., channels 37, 38, and 39, where BLE beacons transmit BLE advertising packets for proximity-aware applications. Although the BLE advertising channels are designed to fall in between three non-overlapping Wi-Fi channels 1, 6, and 11 to reduce Wi-Fi interference in the U.S., in many other countries, Wi-Fi channels 1, 5, 9, and 13 are widely used such that the three BLE advertising channels overlap significantly and face the risk of suffering Wi-Fi interference. Furthermore, three Zigbee channels

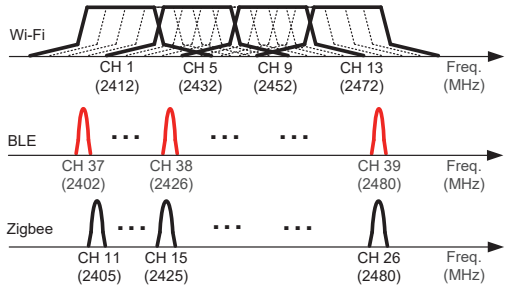


Figure 1: Overlap of frequency usage in Wi-Fi, BLE, and Zigbee channel assignment on 2.4 GHz ISM band.

11, 15, and 26 also overlap with the three BLE advertising channels, respectively.

2.2 GFSK

BLE employs GFSK modulation. A baseband GFSK signal is generated by modulating bit 1 and 0 with *symmetric* positive and negative frequency deviations relative to DC level, respectively, and in demodulation, received signal's frequency component is extracted and compared with the DC level per bit-period to make a decision between the two hypotheses. Specifically, baseband pulses ($\in \{\pm 1\}$) generated from data bit sequence by non-return-to-zero (NRZ) line coding are first passed through the Gaussian filter before modulation to make the pulse transition smoother. The pulse shaping function reduces the modulated signal's spectrum width, thus reducing interference with neighboring channels, but at the cost of increasing inter-symbol interference (ISI)

Modulation: The functional blocks of a typical GFSK transceiver are shown in Figure 2. After modulation, a passband GFSK signal can be represented as

$$s(t) = \sqrt{\frac{2E}{T}} \cos[2\pi f_c t + \theta(t) + \theta_0], \tag{1}$$

where E, T, f_c, and θ_0 are symbol energy, symbol period, carrier frequency, and arbitrary initial phase, respectively. The phase deviation $\theta(t)$ is determined by the original baseband pulse sequence $x[n]$ ($\in \{\pm 1\}$), since

$$\theta(t) = \frac{\pi h}{T} \int_{-\infty}^{t} \sum_{n=-\infty}^{\infty} x[n] r(\tau - nT)\, d\tau, \tag{2}$$

where h and $r(\cdot)$ indicate modulation index[2] and Gaussian pulse shaping function, respectively. The pulse shaping function $r(\cdot)$ is defined as

$$r(t) = Q\left(\sqrt{2}\alpha T\left(-\frac{1}{2} - \frac{t}{T}\right)\right) - Q\left(\sqrt{2}\alpha T\left(\frac{1}{2} - \frac{t}{T}\right)\right), \tag{3}$$

where $Q(\cdot)$ and α are Q-function and $5.336B$, respectively. B is the 3 dB bandwidth of the Gaussian filter. Figure 3 illustrates the pulse shaping function versus t/T for three values of BT product. One observation from these curves is that the ISI introduced by the Gaussian pulse shaping filter extends to one adjacent (on each side) symbol when $BT = 0.5$ which is the case of BLE.

Demodulation: A typical GFSK demodulation utilizes phase detector and frequency discriminator as shown in Figure 2 [1]. If we

[2]BLE standard defines that modulation index is between 0.45 and 0.55.

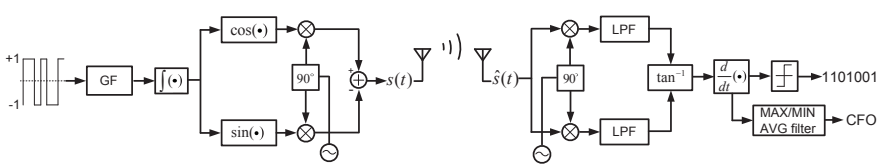


Figure 2: Structure of GFSK transceivers, a transmitter (left) and a receiver (right).

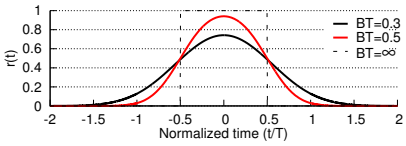


Figure 3: Gaussian pulse shaping function.

ignore the noise term for simplicity, after down-conversion, the two inputs of the phase detector, in-phase (I) and quadrature (Q) components of the baseband signal, can be expressed as

$$I(t) = \cos\left(\frac{\pi h}{T}\int_{-\infty}^{t}\tilde{x}(\tau)d\tau + \theta_0\right) \quad (4)$$

$$Q(t) = \sin\left(\frac{\pi h}{T}\int_{-\infty}^{t}\tilde{x}(\tau)d\tau + \theta_0\right), \quad (5)$$

respectively, where

$$\tilde{x}(t) = \sum_{k=-\infty}^{\infty} x[k]r(t-kT) \quad (6)$$

corresponds to the ISI version of $x[n]$. We can obtain $\tilde{x}(t)$ from the output of the frequency discriminator $\tilde{f}(t)$ since

$$\tilde{f}(t) = \frac{d}{dt}\left(\tan^{-1}\frac{Q(t)}{I(t)}\right) = \frac{\pi h}{T}\sum_{k=-\infty}^{\infty} x[k]r\left(t-kT\right) = \frac{\pi h}{T}\tilde{x}(t). \quad (7)$$

Finally, we can recover $x[n]$ and hence the data bit sequence by comparing $\tilde{x}(t)$ with DC level at the middle of each symbol period.

2.3 CFO Estimation Module

If there is residual CFO in demodulation process, not only does $\tilde{x}(t)$ contain ISI, but it also contains DC offset, which further disrupts demodulation. Accordingly, commodity GFSK transceivers incorporate a CFO estimation module to compensate it, which is always on to cope with sudden BLE packet reception [4].

Typically, CFO is estimated using so-called "MaxMin" algorithm in commodity BLE chipsets [4, 10, 12]; the maximum and the minimum levels of the incoming signal's frequency component are successively identified and then averaged to yield estimated CFO, exploiting the symmetry in the levels of positive and negative frequency deviations of GFSK signal. More specifically, whenever the first derivative of the frequency component turns from positive to negative (negative to positive), the maximum (the minimum) is updated with the current level. In most BLE chipsets, the estimated CFO values are stored in a register, and accessible through an I/O interface. In the following, 'a CFO sample' means an output value of the CFO estimation module with Max/Min algorithm.

3 PROPOSED SCHEME

In this section, we propose CV-Track with the following features.

- **Real-time:** CV-Track detects BLE signal in real-time, which is an indispensable feature for context-aware services.
- **Low-cost:** It is implemented with commodity off-the-shelf BLE chipset without any need for expensive nor specialized hardware.

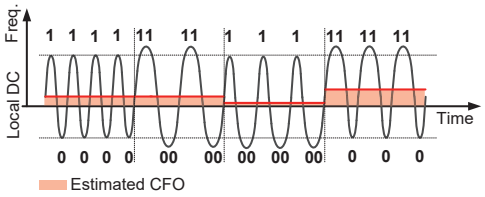


Figure 4: Repetitive bit pattern leads constant CFO samples.

- **Low-complexity:** CV-Track detects BLE signal by simply inspecting whether the stream of CFO samples are within a predefined range without requiring any advanced signal processing.

3.1 CFO Characteristics

CFO is normally caused by 1) frequency mismatch (i.e., the difference in clock drift rates) between the oscillators of transmitter and receiver, and 2) the Doppler effect when transmitter or receiver is moving. In indoor environments where BLE is most likely to be used, the former dominates. It has been shown in [7, 9] that the amount of frequency mismatch are constant for a certain time period (less than 1000 seconds) and changes gradually even with sudden temperature variation. This implies that we can expect constant CFO samples during intact part of a single BLE packet.

However, the ISI introduced by the Gaussian pulse shaping function (cf. Figure 3) makes the levels of the positive and the negative frequency deviations slightly asymmetric as shown in Figure 4; the maximum level of 11 is higher than that of a single 1, and similarly, the minimum level of 00 is lower than that of a single 0. Accordingly, the average of these maximum and minimum levels also fluctuates slightly if random bits are transmitted.

Ideally, the CFO samples obtained from intact BLE signal should be as constant as possible to make it distinct from other types of signals that are unlikely to satisfy the symmetry between maximum and minimum levels of frequency component. We found that even with ISI, as long as the data bits have *repetitive pattern*, i.e., the numbers of consecutive 1s and 0s are constant, respectively, the resultant CFO samples remain constant. Four different repetitive bit patterns are illustrated in Figure 4.

We conduct measurement study with seven different types of wireless signals to verify their CFO characteristics, using an Ubertooth device (http://ubertooth.sourceforge.net/) as BLE receiver, which incorporates a commodity BLE transceiver (CC2400 [4]).

Figure 5 plots the empirical CDF (ECDF) of Δ_{cfo}, defined as the difference between two consecutive CFO samples for each type of signal. We observe that the ECDF curve with BLE signal with repetitive bit pattern is densely concentrated near zero, meaning that the CFO samples are almost constant, while other types of signals make ECDF curves relatively flat, demonstrating the distinctive feature of the BLE signal with repetitive bit pattern, which can be

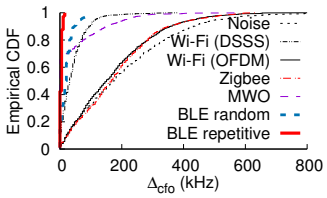


Figure 5: Empirical CDF of Δ_{cfo}.

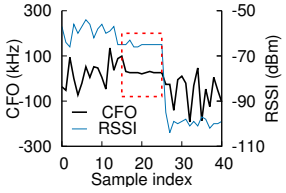


Figure 6: Captured CFO and RSSI samples.

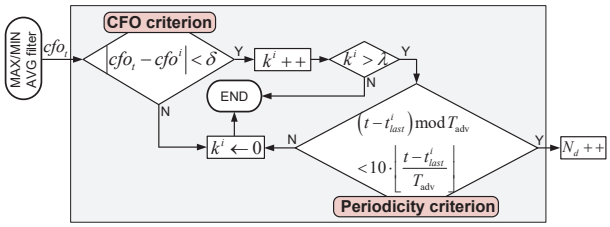


Figure 7: Proposed BLE signal detection and identification algorithm in CV-Track.

used to detect BLE signal. Furthermore, Figure 6 shows a snippet of captured CFO samples along with RSSI measurements. The middle part (in dotted box, samples 15–25) represents the intact part of a BLE signal, whereas the left part (samples 0–15) is a BLE signal corrupted with Wi-Fi interference, and the right part (samples 25–40) is white noise, i.e., no BLE signal. As it can be seen, only the intact part of BLE signal provides stable and near constant CFO (as well as RSSI) values.

3.2 Detection and Identification

Basically, CV-Track deems there is an intact BLE signal, if more than λ CFO samples confined within the range $(-\delta, +\delta)$ are successively observed. However, it is insufficient to just detect the signal; knowing the transmitter of the signal is also very important. To this end, CV-Track uses pair-wise uniqueness of CFO and timing based fingerprinting to identify the transmitter, based on the facts that 1) the amount of frequency mismatch between two independent BLE devices are constant for a time period much longer than BLE packet interval (cf. Section 3.1), and 2) the BLE packets, especially BLE advertising packets used in context-aware services, are periodically transmitted.

The overall operation of the BLE signal detection and identification algorithm used in CV-Track works as follows. First, for each successfully received BLE packet, CV-Track associates the average of the CFO samples observed during the packet reception, denoted as cfo^i, with the device index i. When a new CFO sample cfo_t is generated at time t, CV-Track takes it to conduct the detection and identification algorithm as illustrated in Figure 7, where k^i, T_{adv}, t^i_{last}, and N_d indicate CFO counter for BLE device i, BLE advertising packet interval, the last time a BLE packet from device i was detected by CV-Track or successfully received, and the number of BLE devices identified as the transmitter of the current BLE signal, respectively. The coefficient 10 in the righthand side of the periodicity criterion indicates the 0 to 10 ms randomness introduced in each BLE advertising interval defined in [13]. The algorithm illustrated in Figure 7 is conducted for every previously identified BLE device such that if N_d eventually exceeds one, i.e., there are more than one candidates for current detection, the detection is discarded. If N_d eventually becomes one, i.e., there is only one candidate, we reset the CFO counter for the candidate device and replace the last detection time and the average CFO associated with the candidate device with current time t and the average of the most recently observed λ CFO samples, respectively. After conducting the algorithm for all the previously identified BLE devices, we reset N_d.

4 PERFORMANCE EVALUATION

Implementation: We use Estimote (https://estimote.com/) as the BLE transmitter which supports various types of BLE advertising packets including iBeacon. We employ iBeacon format in the experiments, which provides several configurable fields including UUID (16 bytes), major (2 bytes), and minor (2 bytes). In order to improve detection accuracy, we modify the configurable fields such that they have repetitive bit pattern 1010…1010 after data whitening—the process used to scramble the original bits with a predefined function before modulating them to make them seemingly random—except the minor field, which is used as a beacon identifier.

For the receiver, we implement CV-Track on Ubertooth platform. The microcontroller (MCU) reads CFO samples from CC2400 chipset continuously, and runs the detection and identification algorithm. While doing this, although CC2400 can generate CFO samples every symbol period (1 μs), the read operation at the MCU is much slower, thus limiting the actual CFO sampling rate to around 10^5 Hz. This means that two consecutive CFO samples we observe actually span 10 μs—the time for 10 symbols to pass—such that the performance of the current prototype can be further improved by accelerating the read operation of the MCU. Besides, we set λ and δ to 7 and 10.4 kHz, respectively, which are empirically determined as a condition that guarantees reasonable detection performance with negligible false positive rate.

Packet detection experiment: The experiments were conducted in an office environment where there are three devices; a BLE beacon, a BLE receiver (operating in legacy mode or CV-Track) placed 1 m away from the BLE beacon, and an interferer placed 1 m away from the BLE receiver. The interferer is either a Wi-Fi AP (with 20 dBm tx power), a Zigbee Kmote (with 0 dBm tx power), or an MWO. The interferer is always fully loaded except MWO which conducts frequency sweeping (around 2455 MHz) with ON-OFF pattern as designed by the manufacturer. We conduct the experiments on three BLE advertising channels, 37 (at 2402 MHz), 38 (at 2426 MHz), and 39 (at 2480 MHz), and the BLE channel at 2455 MHz where the MWO signal is mostly concentrated. In each experiment, the interferer's operating channel is set as closely as possible to the corresponding BLE channel except MWO. In the experiments, we consider a BLE packet as detected by CV-Track if the entire packet is successfully received or if an intact BLE signal which satisfies the criteria illustrated in Figure 7 is detected. In the case of legacy scheme, we only count the former case.

Figure 8 shows the packet detection rate (PDR) at the BLE receiver operating with the legacy scheme ('L') or CV-Track ('C') for the cases with three different types of interferer. We observe

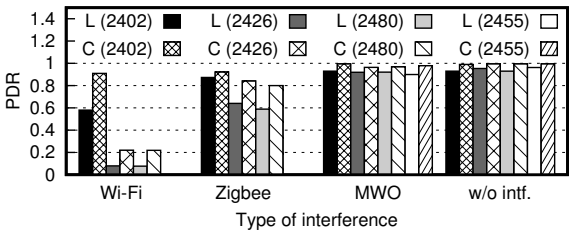
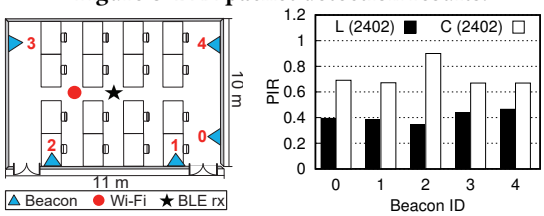


Figure 8: BLE packet detection results.



(a) Topology (b) Result

Figure 9: BLE packet identification results.

that when there is no interference (indicated as 'w/o intf.') or just MWO interference, PDRs are fairly high, while Zigbee or Wi-Fi interference noticeably impose adverse impact on the detection performance. We find CV-Track superior to the legacy scheme in all cases. Note that at 2402 MHz, the detection performance is much better than that in other cases since the BLE channel at 2402 MHz is farther away from the most closely located Wi-Fi or Zigbee channel than the other BLE channels. In real applications, a BLE scanner, the device responsible for receiving BLE advertising packets, is supposed to scan all the BLE advertising channels sequentially as defined in the BLE standard, which means the best performance of the three advertising channels is of significant concern since it determines the actual performance.

Packet identification experiment: We also conduct experiments with five BLE beacons to verify the identification capability of CV-Track. In this experiments, we only count the BLE packet detection when its transmitter is identified correctly. The experiments are conducted with topology shown in Figure 9(a); there is a BLE receiver at 2402 MHz, a Wi-Fi AP with fully loaded traffic at Wi-Fi channel 1 (closest Wi-Fi channel to 2402 MHz), and five BLE beacons deployed in an office environment. Figure 9(b) shows the packet identification rate (PIR) at the BLE receiver with respect to each BLE beacon. We observe that with CV-Track, the BLE receiver detects and identifies incoming BLE packets with much higher probability than with the legacy scheme. Note that with CV-Track, the PIR of beacon 2 is much higher than that of other beacons, which is caused by the distinctive CFO value and the timing of the packet transmission of beacon 2 compared with other beacons.

5 RELATED WORK

Detecting BLE/Bluetooth signal is a challenging task due mainly to its narrow signal bandwidth and frequency hopping operations. So far, there has been several efforts [5, 11, 14] to detect classic Bluetooth signal. RFDump [5] uses timing and phase information to classify various signal types including Bluetooth using expensive USRP platform. Timing analysis is based on detecting the start and end of a Bluetooth packet using energy detection, while phase analysis is based on the statistics of the phases of the received signal. Airshark [11] is another effort which detects Bluetooth signal by exploiting the features related to the duration of a Bluetooth packet, inter-packet time, signal bandwidth, and power versus frequency characteristics using commodity Wi-Fi card. Similarly, ZiSense [14], implemented on TelosB platform, detects Bluetooth signal by inspecting received signal's peak-to-average power ratio (PAPR), signal duration, and interval. However, none of these schemes are completely real-time. CV-Track is real-time, and its identification capabilities via novel use of CFO are noteworthy progress.

6 CONCLUDING REMARKS

In this work, we proposed CV-Track which enables BLE signal detection at a finer granularity than packet-level. Not only does CV-Track detect intact part of an incoming BLE signal in real-time, it also identifies the transmitter using pair-wise uniqueness of CFO and timing-based fingerprinting. We demonstrate the effectiveness of CV-Track via real prototype implementation and experiments. Although the current prototype has room for improvement, our evaluation results show promising potential. As future work, we plan to exploit the information and benefits that CV-Track provides us in many real-world context-aware applications to improve their performance and open new opportunities.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF) grant funded by Korea government (MSIP) (NRF-2015R1A2A2A01006750), and the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B03031348).

REFERENCES

[1] Dah-Chung Chang and Tsung-Hau Shiu. 2006. Digital GFSK carrier synchronization. In *IEEE APCCAS*.
[2] Giorgio Conte, Massimo De Marchi, Alessandro A. Nacci, Vincenzo Rana, and Donatella Sciuto. 2014. BlueSentinel: A first approach using iBeacon for an energy efficient occupancy detection system. In *ACM BuildSys*.
[3] Jeongyoon Heo, Jung Jun Kim, Jeongyeup Paek, and Saewoong Bahk. 2017. Dodge-Jam: Anti-jamming technique for low-power and lossy wireless networks. In *IEEE SECON*.
[4] Texas Instruments. 2007. CC2400: 2.4 GHz low-power RF transceiver. (2007).
[5] Kaushik Lakshminarayanan, Samir Sapra, Srinivasan Seshan, and Peter Steenkiste. 2009. RFDump: An architecture for monitoring the wireless ether. In *ACM CoNEXT*.
[6] Xin-Yu Lin, Te-Wei Ho, Cheng-Chung Fang, Zui-Shen Yen, Bey-Jing Yang, and Feipei Lai. 2015. A mobile indoor positioning system based on iBeacon technology. In *IEEE EMBC*.
[7] Steven J Murdoch. 2006. Hot or not: Revealing hidden services by their clock skew. In *ACM CCS*.
[8] Jeongyeup Paek, JeongGil Ko, and Hyungsik Shin. 2016. A measurement study of BLE iBeacon and geometric adjustment scheme for indoor location-based mobile applications. *Mobile Information Systems*, Article 8367638 (2016).
[9] Attila Pásztor and Darryl Veitch. 2002. PC based precision timing without GPS. *ACM SIGMETRICS Performance Evaluation Review* 30, 1 (2002), 1–10.
[10] Adrian Weston Payne. 2006. DC offset estimation. (Nov. 15 2006). US Patent App. 12/093,991.
[11] Shravan Rayanchu, Ashish Patro, and Suman Banerjee. 2011. Airshark: Detecting non-WiFi RF devices using commodity WiFi hardware. In *ACM IMC*.
[12] Roland Egon Ryter. 2010. Apparatus for determining a frequency offset error and receiver based thereon. (June 8 2010). US Patent 7,733,991.
[13] Bluetooth SIG. 2014. Specification of the Bluetooth system. (Dec. 2014).
[14] Xiaolong Zheng, Zhichao Cao, Jiliang Wang, Yuan He, and Yunhao Liu. 2014. Zisense: Towards interference resilient duty cycling in wireless sensor networks. In *ACM SenSys*.