Designing and Implementing an Enhanced Bluetooth Low Energy Scanner with User-Level Channel Awareness and Simultaneous Channel Scanning

Sangwook BAK†a), Student Member and Young-Joo SUH†b), Nonmember

SUMMARY This paper proposes an enhanced BLE scanner with user-level channel awareness and simultaneous channel scanning to increase theoretical scanning capability by up to three times. With better scanning capability, channel analysis quality also has been improved by considering channel-specific signal characteristics, without the need of beacon-side changes.

key words: bluetooth low energy, iBeacon, user-level channel awareness, simultaneous channel scanning, multi-level transmission power

1. Introduction

Bluetooth [1], or more specifically Bluetooth Low Energy (BLE), is the most popular communication technology for wireless personal area network (WPAN). BLE is widely embedded in many IoT and other portable devices, smartphones, tablets and PCs, where many popular services including inter-device file transfer, IoT device control, and wireless audio transmission are relying on BLE. Moreover, BLE is not only limited to personal area; it’s also widely utilized in industrial and commercial area with the applications including asset tracking, indoor positioning and proximity detection.

While there have been many contributions to utilize BLE in industrial and commercial area, iBeacon [2], the most dominant protocol for advertising device identification in BLE network, could be the main contribution. With the advantage of BLE compliance and high usability, iBeacon has been the most dominant advertising protocol for BLE-based beacons, providing the opportunity for BLE to be the one of the main supporting technology for the aforementioned industrial and commercial applications with the advantage of ease of development, inexpensive deployment cost, and low power consumption.

Although BLE-based applications are very popular and promising, narrow channel bandwidth and some standard implementation-related issues are the fundamental and inevitable limitations for providing high precision BLE-based applications. First, BLE uses 40 channels in 2.4 GHz band with the narrow channel width of 2 MHz, when compared to the WiFi with the minimum channel width of 20 MHz. Its narrow channel width makes BLE-based systems severely suffering from signal fading and fluctuation [3], reducing the reliability of the systems. Second, according to Fig. 2, BLE assigns 37 adjacent channels (0–36) as the data channels, whereas three apart channels (37–39) are assigned as the advertising channels to mitigate the interference from IEEE 802.11b/g/n which also occupies same 2.4 GHz band. As the advertising channels are apart each other, each channel has different physical characteristics due to different center frequencies [3], therefore statistics of signal strength distribution including average and its standard deviation become different for each channel. Figure 1 (a) is a graphical representation of signal strength distributions measured from 10 BLE beacons for a second. As seen in the figure, each channel has different distribution pattern with different average and standard deviation: [−67.04, 4.27] for channel 37,
[−70.4, 6.99] for channel 38, and [−66.43, 5.17] for channel 39. However, as most commercial BLE devices hide the incoming channel information to the users, users can only obtain a mixed distribution of all channels, which results in degraded channel analysis quality with higher ambiguity. Lastly, the BLE scanner scans beacon frames in three advertising channels consecutively. Although consecutive scanning can guarantee beacon detection, it might not be the optimal if the scanner desires to collect beacon frames as much as possible. Figure 1 (b) describes the scanning inefficiency caused by advertisement and scan procedure of standard BLE beacons and scanners. Considering the duration of one beacon advertisement is much shorter than an active scan duration of one channel [4], only one out of three beacon frames can be detected in a single beacon advertisement duration, definitely unable to detect other two beacon frames. This behavior becomes a critical obstacle to collect rich channel-specific information, because there is no guarantee that beacon frames are evenly detected in the advertising channels so there exists the possibility of uneven channel information.

To provide high precision BLE-based applications despite of the physical and implementation-related limitations, this paper proposes an enhanced BLE scanner which utilizes channel-specific characteristics and parallel multi-channel scanning approach to maximize beacon frame collection capability without degrading beacon detection quality. With the proposed scanner, problems of degraded channel analysis quality and scanning inefficiency can be fundamentally solved; the proposed BLE scanner can detect all beacon frames from all channels simultaneously, improving theoretical scanning capability up to three times.

Contributions of this paper can be summarized as follows. First, this paper achieves user-level channel awareness with publicly available hardwares. There is a previous study on user-level channel awareness [3], however its implementation has determined to be not publicly available, because the related public API [5] doesn’t provide incoming channel information. In contrast, our proposed system achieves user-level channel awareness with publicly available BLE sniffer and its open source tools. Second, this is the first study as far as we know, to utilize multiple interfaces in BLE for maximizing scanning capability. In most traditional BLE services relying on data channels, scanning capability hasn’t be the interest of research because advertising channels are only used for advertisement. However, commercial and industrial services including asset tracking and indoor positioning are based on beacon frames from advertising channels, which is different from traditional BLE services. With the explosion of commercial and industrial services, scanning capability becomes important as it is closely related to the service quality. This paper is the first research to recognize the importance of and to enhance the scanning capability.

The rest of the paper is organized as follows. Section 2 discusses existing limitations in more detail. In Sect. 3, the description of proposed enhanced BLE scanner is presented, which is followed by the discussion in Sect. 4. Section 5 evaluates the performance of the proposed scanner. Lastly, this paper is concluded in Sect. 6.

2. Detailed Description of Existing Limitations

2.1 User-Level Channel Unawareness

As described in Introduction, most traditional BLE services are served through data channels, which the advertising channels are only used for service information advertisement. A BLE client scans advertising channels to obtain the list of available BLE services, establishes the connection with a desired device, then starts communicating with the device through data channels. When the client receives beacon frames from advertising channels, it discards the incoming channel information and forwards only the frame data to upper layer. The reason of channel information abstraction is not clearly stated, but the most probable reason could be that the channel information is discarded because only the advertisement data is required for connection and communication.

Inspecting the BLE scan library of mobile OSs (iOS [5] and Android [6]) and desktop OSs (Windows [7], Linux [8] and Mac OS [9]), the scan libraries only provide beacon ID and received signal strength (RSS), as summarized in Table 1. All libraries lack incoming channel information, which makes difficult to enhance channel analysis quality by utilizing incoming channels of beacon frames.

2.2 Scanning Inefficiency

Figure 3 describes the timing terms of BLE advertisement and scan procedures. BLE beacons periodically advertise beacon frames to inform their identification with the prede-

| OS         | Provided Information                  |
|------------|---------------------------------------|
| iOS [5]    | iBeacon ID (UUID, Major, Minor), RSS  |
| Android [6]| Advertisement Data, RSS               |
| Windows [7]| Advertisement Data^1, RSS             |
| Linux [8]  | Advertisement Data^1, RSS             |
| Mac OS X [9]| Advertisement Data^1, RSS            |

^1 Advertisement data needs to be parsed to obtain iBeacon ID.
fined advertising interval \( (T_{AdvInt}) \). At each advertising interval, the beacon transmits beacon frames through three advertising channels in sequence with a very short inter-frame delay \( (T_{IFS}) \), which the duration of a single beacon advertisement \( (T_{AdvEvt}) \) takes about 0.7 ms [4]. While beacons are advertising, BLE scanners scan advertising channels during the predefined scan window \( (T_{ScanWin}) \) every scan interval \( (T_{ScanInt}) \) to detect beacon presence, which both \( T_{ScanWin} \) and \( T_{ScanInt} \) have the minimum length of 2.5 ms. Although both BLE beacons and scanners switch channels alternately, channel switching frequency of the beacons is much shorter than the frequency of the scanners. Different from beacons which use all three channels in a single advertising interval, scanners only scan a single channel at each scan interval. Considering the duration of a beacon advertisement \( (T_{AdvEvt}) \) is much shorter than the scan interval \( (T_{ScanInt}) \), only one of three beacon frame can be detected at each scan interval, definitely missing other two beacon frames. As a result, the scanning capability of the scanner are limited to one-third of advertised beacon frames.

3. Proposed System

The proposed BLE scanner solves user-level channel unawareness and scanning inefficiency by specialized BLE hardware and simultaneous multi-channel scanning scheme. A specialized BLE sniffer which provides incoming channel information is utilized to achieve user-level channel awareness. Ubertooth One [10] is determined as the BLE sniffer in the proposed system with the advantage of user-level channel awareness, low cost, high portability, and open source, and high operability in Linux.

To solve the scanning inefficiency problem, the proposed BLE scanner scans multiple BLE channels simultaneously to maximize detection rate of beacon frames. Figure 4 compares scan procedures of traditional and proposed BLE scanners. Traditional scanner scans channels one by one with a single BLE hardware, whereas the proposed scanner performs batch scanning with three BLE hardwares where each BLE hardware scans one dedicated advertising channel.

The proposed BLE scanner has implemented with Raspberry Pi 3 B+ model, the popular small board computer (SBC) which operates on Linux. Three Ubertooth One devices are attached to the Raspberry Pi through USB interfaces, which each device dedicatedly scans one channel. As the Raspberry Pi has no display, an Android smartphone (Samsung Galaxy S7) is used as the controller for the BLE scanner. For the ease of deployment, Raspberry Pi serves as a 5 GHz 802.11a/n Wi-Fi AP so that the smartphone controller can directly communicate with the Raspberry Pi, avoiding the interference with BLE. Figure 5 describes the design and overall workflow of the proposed BLE scanner.

4. Discussion

4.1 Enhancement with Beacons with Multiple Transmission Power Levels

The proposed BLE scanner is able to enhance the scanning capability up to about three times with user-level channel awareness, only with scanner-side modification. The enhanced scanning capability improves channel analysis quality by collecting massive amount of beacon frames with better outlier removal. On the other hand, if beacon side modifications are allowed to add or modify functions, the enhanced scanning capability can be utilized in more ways.

Signal propagation characteristics including signal detection range and signal fading pattern strongly depend on transmission power as shown in Fig. 6 (a). Figure 6 (a) shows distinct signal strength distributions of beacons with the transmission power of \([0, 4, 10]\) dBm, measured with the distance of 1 m to 20 m. To utilize these tx power-specific characteristics, BLE beacons can be modified to adjust their transmission power in a round-robin manner. As an example, the combination of the enhanced BLE scanner...
and the multi-tx powered BLE beacon with three transmission power levels has the effect like there are tripled beacons which have tripled advertising interval. As both the number of beacons and their advertising interval are tripled, total number of transmitted beacon frames are equivalent within same time bound. That is, depending on the number of transmission power levels, the direction to improve channel analysis quality becomes either by accurate outlier removal with massive beacon frame data or by widened spatial dimensions. Figure 6 (b) describes the procedure of the proposed scanner and the beacon with multiple transmission power levels.

4.2 Feasibility and Usefulness of the Proposed System

The proposed system utilizes three BLE hardwares to simultaneously scan three advertising channels. While the proposed system maximizes the scanning capability to enhance service quality, it also has some drawbacks of additional cost, energy, and space consumption caused by two additional BLE hardwares. These two devices cost around $240, consume 0.18 A (idle), and occupy 61.75 mm × 38 mm [10]. With 5V USB power, two additional BLE hardwares consumes 0.9 Wh, which is equivalent to 180 mAh.

Although the proposed system requires additional expenses for using three BLE hardwares, its advantage of user-level channel awareness and enhanced channel scanning capability exceeds the additional cost, energy, and space consumption. User-level channel awareness enables channel-aware analysis from signal strength distributions to provide rich channel-specific information, which helps efficient service management for maintaining and improving service quality. Moreover, enhanced channel scanning capability can improve system responsiveness, as the enhanced scanner is able to collect adequate amount of beacon frames with requiring much shorter scanning time. To summarize, the proposed system provides noticeable benefits both to customers and service providers by faster system responsiveness, as the enhanced scanner is able to collect adequate amount of beacon frames with requiring much shorter scanning time. To summarize, the proposed system provides noticeable benefits both to customers and service providers by faster system responsiveness, and efficient service management.

5. Performance Evaluation

To validate the performance of the proposed BLE scanner, a testbed is constructed in first basement floor of PIRL building in POSTECH. The basement floor has no communication infrastructure including Wi-Fi APs and BLE beacons, therefore the place is ideal for the performance evaluation. For the experiment, a prototype of BLE scanner described in Sect. 3 has used as both traditional and proposed scanners with switching its scanning scheme. A total of 10 Estimote’s Location Beacon [11] are deployed as the BLE beacon for the experiment, which the transmission power is set to the strongest 10 dBm for guaranteeing best detection condition.

Following performance metrics have determined for the performance evaluation: the total number of collected beacon frames, and the frame amount ratio defined as the ratio of collected amount of the proposed scanner (#PSSD) to that of the traditional scanner (#TRAD). Table 2 summarizes the number of collected beacon frames from traditional and proposed scanners for a second, with the number of BLE beacons increasing from 1 to 10. Scan window and scan interval are set to 25 ms, and advertising interval is set to 100 ms. In all cases, the proposed scanner can collect about three times more beacon frames than the traditional one. The average of frame amount ratio is 3.15, indicating the proposed scanner has lower probability of frame detection loss.

6. Conclusion

In this paper, the limitation of current BLE scan procedures are analyzed: user-level channel unawareness and scanning inefficiency due to one-by-one channel scan procedure. To overcome the limitations, the enhanced BLE scanner with user-level channel awareness and simultaneous channel scanning is proposed and implemented with the Raspberry Pi and the specialized BLE sniffer Ubertooth One. Finally, it is validated by the experiment that the proposed scanner has increased the scanning capability by up to about three times, without more beacons or more scanning time.

References

[1] “Bluetooth Core Specification, v5.0,” Bluetooth SIG, https://www.bluetooth.com/specifications/bluetooth-core-specification, accessed Sept. 25 2018.
[2] “iBeacon - Apple Developer,” Apple, https://developer.apple.com/beacon, accessed Sept. 25 2018.
[3] R. Faragher and R. Harle. “Location fingerprinting with Bluetooth low energy beacons,” IEEE J. Sel. Areas Commun., vol.33, no.11, pp.2418–2428, Nov. 2015. DOI: 10.1109/JSAC.2015.2430281
[4] K. Cho, W. Park, M. Hong, G. Park, W. Cho, J. Seo, and K. Han, “Analysis of latency performance of Bluetooth low energy (BLE) Networks,” MDPI Sensors, vol.15, no.1, pp.59–78, Jan. 2015. DOI: 10.3390/s150100059
[5] “CLBeacon - Core Location,” Apple, https://developer.apple.com/documentation/corelocation/clbeacon, accessed Sept. 25 2018.
[6] “BluetoothAdapter.LeScanCallback,” Google, https://developer.android.com/reference/android/bluetooth/BluetoothAdapter.LeScanCallback, accessed Sept. 25 2018.

[7] “BluetoothLEAdvertisement Class (Windows.Devices.Bluetooth.Advertisement),” Microsoft, https://docs.microsoft.com/uwp/api/windows.devices.bluetooth.advertisement.bluetoothleadvertisement, accessed Sept. 25 2018.

[8] “bluez.git - Bluetooth protocol stack for Linux,” BlueZ Project, https://git.kernel.org/pub/scm/bluetooth/bluez.git, accessed Sept. 25 2018.

[9] “centralManager(_:didDiscover:advertisementData:rssi:)- CBCentralManagerDelegate,” Apple, https://developer.apple.com/documentation/corebluetooth/cbcentralmanagerdelegate/1518937-centralmanager, accessed Sept. 25 2018.

[10] “Project Ubertooth - Ubertooth One,” Project Ubertooth, http://ubertooth.sourceforge.net/hardware/one, accessed Sept. 25 2018.

[11] “Technical specification of Estimote Beacons and Stickers,” Estimote, https://community.estimote.com/hc/en-us/articles/204092986-Technical-specification-of-Estimote-Beacons-and-Stickers, accessed Sept. 25 2018.