Dead on Arrival: An Empirical Study of The Bluetooth 5.1 Positioning System

Dead on Arrival: An Empirical Study of The Bluetooth 5.1 Positioning System

Marco Cominelli
University of Brescia
Italy
marco.cominelli@unibs.it

Paul Patras
The University of Edinburgh
Scotland, UK
ppatras@inf.ed.ac.uk

Francesco Gringoli
CNIT/University of Brescia
Italy
francesco.gringoli@unibs.it

ABSTRACT

The recently released Bluetooth 5.1 specification introduces fine-grained positioning capabilities in this wireless technology, which is deemed essential to context-/location-based Internet of Things (IoT) applications. In this paper, we evaluate experimentally, for the first time, the accuracy of a positioning system based on the Angle of Arrival (AoA) mechanism adopted by the Bluetooth standard. We first scrutinize the fidelity of angular detection and then assess the feasibility of using angle information from multiple fixed receivers to determine the position of a device. Our results reveal that angular detection is limited to a restricted range. On the other hand, even in a simple deployment with only two antennas per receiver, the AoA-based positioning technique can achieve sub-meter accuracy; yet attaining localization within a few centimeters remains a difficult endeavor. We then demonstrate that a malicious device may be able to easily alter the truthfulness of the measured AoA, by tampering with the packet structure. To counter this protocol weakness, we propose simple remedies that are missing in the standard, but which can be adopted with little effort by manufacturers, to secure the Bluetooth 5.1 positioning system.

ACM Reference Format:
Marco Cominelli, Paul Patras, and Francesco Gringoli. 2019. Dead on Arrival: An Empirical Study of The Bluetooth 5.1 Positioning System. In *13th International Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization (WiNTECH'19), October 25, 2019, Los Cabos, Mexico.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3349623.3355475

WiNTECH'19, October 25, 2019, Los Cabos, Mexico

ACM ISBN 978-1-4503-6931-2/19/10…$15.00
https://doi.org/10.1145/3349623.3355475

1 INTRODUCTION

Indoor localization of user devices is a critical research topic that has been attracting increasing interest from vendors [1], app developers [2], and the researcher community at large [3]. Localization is also a key application on the 5G mobile technology roadmap [4]. To date, however, a positioning solution as widespread as GPS and usable when satellite signals cannot be received has not been available.

To address this problem in IoT scenarios, the Bluetooth Special Interest Group (Bluetooth SIG) introduced a set of features in the latest Bluetooth Core Specification v5.1 [5], which are specifically aimed at determining the location of a device with high accuracy. In particular, the standard adopts two signal processing techniques for identifying the Angle-of-Arrival (AoA) and Angle-of-Departure (AoD) of a transmitted signal. AoA enables a receiver to determine the angular position of a transmitter by measuring the phase-delay at multiple antennas. With AoD, a transmitter having multiple antennas can send a signal that allows receivers equipped with a single antenna to detect their angular position with respect to the transmitter. Combined with distance estimation [6, 7], these techniques aim to help pinpoint the precise location of a device.

Numerous systems based on different technologies have been proposed to date to tackle indoor localization, ranging from those whereby users carry smart tags, to systems that opportunistically use signals transmitted by mobile devices/smartphones to infer their position. Naturally, previous solutions build upon wireless communications systems commonly embedded into mobile devices, including Wi-Fi [8, 9], Bluetooth [10, 11], and ultra-wideband (UWB) [12, 13] transceivers. Nevertheless, even if some of these solutions demonstrated remarkable performance in terms of positioning accuracy, none of them gained enough traction to witness wide adoption. With the growing adoption of IoT technology and the emergence of standardized methods for positioning, the situation is bound to change. In 2018, nearly 4 billion devices were shipped with Bluetooth technology and, thanks to its low energy capability, the Bluetooth SIG forecasts that the location services domain will encompass over 400 million products per year by 2022 [14], with applications spanning

supply chain asset tracking, customized visitor experience in museums through proximity detection, smart homes, healthcare, and many more.

Contributions. In this paper we test the market readiness of the Bluetooth 5.1 positioning capability by experimentally evaluating the performance of the adopted AoA mechanism from two perspectives: that of pure angular measurement accuracy and the ability to correlate two or more angular measurements in order to estimate a device's position in a 2D plane. To this end, we use a software-defined radio (SDR) testbed and deploy the BLE 5.1 positioning technique in its simplest form, i.e., with only two antennas at the receiver.[1] We report results that offer a first glimpse into the performance of this localization solution, and a primer for more complex implementations that are yet to appear.

Through our study, we first reveal severe limitations that affect angular measurements and which restrict the applicability of the AoA technique within a specific circular sector centered at the receiver. Secondly, we show that positioning based on AoA measurements, although offering sub-meter accuracy, is far from achieving centimetre-level precision. Our findings should prove useful to system and app developers who aim to build upon this feature. We then provide a preliminary assessment of the (in)security of the AoA-based positioning mechanism, laying out guidelines on antenna switching patterns that manufacturers could follow to prevent attackers from compromising position truthfulness. Finally, we release the tool opensource, interested readers can download and test it from https://github.com/bsnet/bleaoa.

2 RELATED WORK

Determining a wireless device's position should be strictly a matter of signal direction (angle) finding. The problem of estimating the Angle-of-Arrival (AoA) of a signal has been extensively studied. In general, an antenna array is required in order to measure the phase-delay between the replicas of the signal received by each element of the array. The most common approach to determine the AoA based on the measured phase-delay is the multiple signal classification (MUSIC) [15], which achieves excellent angular resolution.

In commodity wireless systems, however, estimating the position of a transmitter has been largely based on measuring the power of the received packets (RSSI). With respect to Bluetooth Low Energy (BLE), the accuracy of positioning frameworks based on iBeacon technology has been studied in [10] and [11]. In the former, an average localization error of 4 m was achieved by installing 36 beacons. The latter divided a testbed into 12 subareas and obtained localization errors within 5 m of adjacent subareas. An analysis of how positioning accuracy depends on the number of BLE beacons has been carried out in [16]. More recently, De Blasio et al. examined the positioning accuracy of BLE 5.0 in a deployment with 12 beacons in a 168 m^2 area, reporting accuracy within 2.5 m [17]. The key limitation of existing methods for estimating indoor position is that they assume an accurate channel model, which is very difficult to build. Moreover, different BLE channels may exhibit different characteristics, leading to modest positioning accuracy when relying on RSSI [18]. To circumvent these problems, MUSIC has been applied recently to determine the position of BLE transmitters based on the AoA estimated by multiple nodes [19].

The decision made by the Bluetooth SIG to include the direction finding feature in the new BLE standard reshapes the positioning problem. In particular, in order to apply MUSIC, multiple coherent RF channels would be required. Instead, the AoA feature in BLE 5.1 uses only one channel connected to the different elements of an antenna array and an RF switch to select among them [5]. The sequence transmitted to perform AoA measurements is assumed to be known (as described in the next sections). Luo et al. have conducted simulations to assess the performance of AoA estimation in the case of known transmit sequences [20]. However, a thorough characterization of the positioning accuracy of BLE 5.1 in real deployments has not been reported yet. This is mainly due to the lack of commercial hardware supporting this feature. To the best of our knowledge, our work is the first to conduct an experimental study of the BLE 5.1 positioning system and document its performance and vulnerabilities.

3 BLUETOOTH LOW ENERGY (BLE)

BLE is a wireless standard designed for inexpensive personal area networks that require low power consumption and low data rates. BLE has been integrated into version 4.0 of the Bluetooth Core specification in 2010 and has been also marketed as Bluetooth Smart.

At the physical layer (PHY), BLE operates in the 2.4 GHz ISM Band. The access to the medium is regulated by a hybrid time-frequency division multiplexing scheme. In particular, the assigned 80 MHz bandwidth is divided into 40 orthogonal channels with central frequencies equally spaced by 2 MHz. Two types of BLE channels exist: 3 *advertising* channels are used for enabling device discovery, connection setup, and broadcasting messages; the other 37 *data* channels are used to exchange data. When a connection is established between a pair of devices, an Adaptive Frequency Hopping (AFH) technique is used to combat interference: connected devices switch rapidly between channels according to a pseudo-random sequence that is known by both transmitter and receiver. Channels can be dynamically removed from the hopping sequence depending on external conditions (e.g.,

[1] At the time of writing, commercial devices implementing Bluetooth 5.1 positioning were not launched to market. We thus resort to SDR hardware.

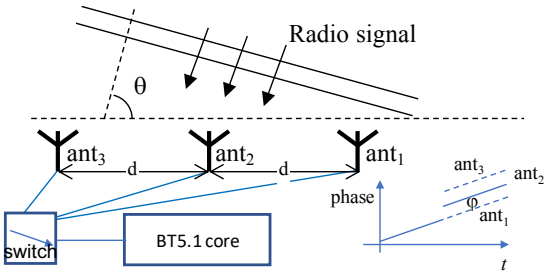

Figure 1: The AoA mechanism needs to estimate phase-delay φ between antennas to compute angle θ: multiple antennas are connected to a single radio transceiver using an RF switch.

strong narrow-band interference). The communication between devices happens at specific time intervals. A channel access policy is defined based on time slots and intervals that depend on the role of a BLE device (master/slave).

For transmission, BLE employs binary Gaussian Frequency Shift Keying (GFSK) modulation with a bandwidth-bit period product of 0.5 and two possible symbol rates: 1 Msym/s and 2 Msym/s. Even if four different PHY modes build on these modulation schemes, in version 5.1 of the BLE standard the AoA mechanism can be used only with the Uncoded PHYs. In the rest of the paper we confine consideration to the mandatory LE 1M PHY with 1 Mb/s data rate.

3.1 Direction Finding in BLE 5.1

According to the standard, a device equipped with an antenna array of M elements can determine the AoA of signals from a transmitter using simple geometric calculations. The documentation considers the scenario illustrated in Fig. 1. Assuming the radio signal is a plane wave with constant frequency impinging on the antenna array of the receiver, the phase difference φ between the signals received at each pair of adjacent antennas is expressed as

$$\varphi = 2\pi(d/\lambda)\cos\theta, \tag{1}$$

where λ is the wavelength of the signal, d the distance between the antennas, and θ the angle of arrival. Therefore,

$$\theta = \arccos\left(\frac{\lambda\varphi}{2\pi d}\right). \tag{2}$$

By measuring the phase-delay φ and knowing both λ and d, computing θ is straightforward. Fusing θ values computed at different antenna pairs is left to the manufacturer.

From Eq. 1 it is clear that all the angles θ from 0° to 180° can be determined from the phase-delay φ only if $d < \lambda/2$. If this condition is not met, then an aliasing phenomenon appears, whereby it is not possible to uniquely map a value of φ to an angle θ. Further, how to evaluate the phase-delay φ is unclear, because the standard requires a single radio in the chipset to be connected to the different antennas using a RF switch (as in Fig. 1) and a procedure for inferring the phase-delay is not specified in the official documentation. Instead, manufacturers can develop their own algorithms to estimate φ. We explain in the next section how we implemented this feature on our SDR platform. On the other hand, the standard specifies *(i)* the format of the field inside a packet that should be used to evaluate the phase-delay and *(ii)* the timing for performing antenna switching over this field. We discuss these features next.

3.2 Direction Finding Packets and Antenna Switching Timings

BLE packets supporting the direction finding capability embed an additional field called Constant Tone Extension (CTE) that follows the CRC coefficient as we show in Fig. 2. The CTE consists of a constantly modulated sequence of unwhitened 1-valued bits, i.e., a constant tone signal with variable length, which can last between 16–160 μs. This is divided into different subfields: a **reference period** (8 μs) is sent first, after a guard interval; then, an alternating sequence of **switch slots** and **sample slots** follows. Slots of 2 μs must be implemented by all the devices that support the direction finding features, whereas slots of 1 μs can be optionally supported.

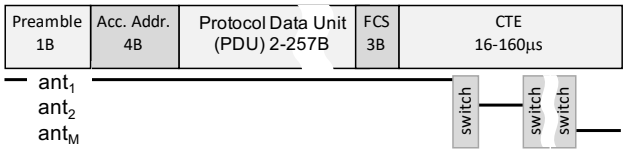

Figure 2: The format of a packet supporting AoA detection, and corresponding switching timing.

A receiver uses one antenna to receive a BLE packet (from preamble to the CRC field) and relies on the same antenna to collect 8 IQ samples during the reference period (8 μs sampled at 1 MS/s). It then switches among the available antennas during switch slots, taking one IQ sample per sample slot (even if the sample slot is 2 μs-long). The switching pattern is defined by the BLE host. The shortest possible switching pattern lasts 16 μs and uses only two antennas. This is also the pattern with which we work in our study. We leave investigating the impact of the length of the switching pattern on positioning accuracy for future work.

4 BLE 5.1 TESTBED DEPLOYMENT

We implement Software-Defined Radio (SDR) prototypes to replicate the behavior of BLE transceivers supporting the AoA detection mechanism as defined by the Bluetooth 5.1 Specification. Our setup consists of two USRP Ettus B210

boards that we use for receiving, and a USRP Ettus N200 that we use for transmitting. The receiver is connected to a laptop powered by an Intel i5 CPU clocked at 2.7GHz with 8GB of RAM, which has enough power to run our software receiver in real-time. We manufactured a plastic support to place two half-wavelength dipole antennas at a distance of 6 cm from each other; each antenna is connected to a TX/RX port of the USRP B210 using a rigid coaxial cable. The transmitter is driven by a Chromebook powered by an Intel Core M CPU clocked at 2GHz with 2 GB of RAM. All computers run Ubuntu 18.04. Next, we describe our implementation of the BLE AoA detection mechanism, introducing first the real-time BLE software transmitter/receiver developed, then explaining how we customize this to emulate the AoA detection feature.

4.1 Emulating BLE 5.1 Connections

For our experiments we do not setup a real BLE FH data connection; we rather emulate it by continuously transmitting packets and tuning all nodes simultaneously on the same channels. We program the software transmitter to generate BLE packets, which we encode as LE 1M PHY and send at the rate of 100 packets per second, using a fixed Access Address. Inside the payload we embed a sequence number that we use for debugging purposes and for matching the same packet at multiple receivers. To emulate the CTE, we add a sequence of binary ones at the end of each packet.

The software receiver acquires IQ samples with a sampling frequency of 2 MS/s. It then decodes bits at 1 Mb/s by operating a phase-discrimination procedure on consecutive pairs of samples. Finally, it detects valid packets starting from every preamble found and checking the validity of the CRC.

It is important to notice that in BLE 5.1 the CTE is not subject to error checking and that in the packet format (Fig. 2) it comes right after the CRC field. In addition, AoA measurements can be performed by BLE devices even if errors occurred while receiving the packet.

To achieve FH and ensure the transmitter and receivers are on the same physical channel, we rely on out-of-band signalling performed via a wired network that connects all nodes and distributes information generated by a controller. The controller provides to all nodes a deterministic hopping sequence spanning all the available BLE channels. Each receiver can adjust the gain dynamically by measuring the amplitude of the IQ samples in the received BLE packets, so that it can use the entire dynamic range of the Analog-to-Digital Converters of the USRP B210.

4.2 Implementing AoA Detection

As described before, BLE devices supporting the AoA mechanism have only one receiving radio chain that is connected to the different elements of the antenna array using an RF switch. This means that only one antenna can be active at any given time and that phase-delay φ must be inferred from IQ samples captured during the reference period in the CTE and in the following sample slot. We explain here the algorithm that we implemented for inferring the phase-delay and how we emulated it over USRP B210 boards. Hereafter we consider the case with $M = 2$ antennas.

As the CTE is a sequence of unwhitened ones, the signal appears as a constant frequency tone and as such its phase increases linearly. During the CTE reference period, we collect 8 IQ samples from antenna 1 and we build a linear model of its phase evolution. The AoA antenna switching takes place during the switch slot, after which we collect an IQ sample from antenna 2 exactly at the next sample slot. We then compare the phase of this IQ sample with the instantaneous phase of the signal on antenna 1 that we estimate using the linear model built during the reference period, as shown in Fig. 3. The phase difference estimated with this method corresponds to φ in Eq. 1, and the angle of arrival θ is found with Eq. 2.

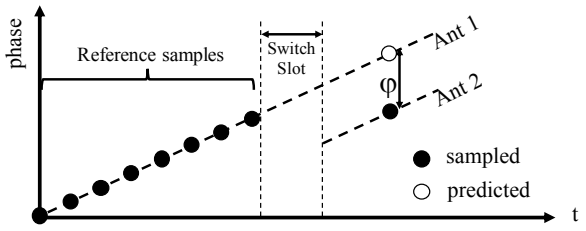

Figure 3: The phase difference is computed by subtracting the phase sampled on antenna 2 from the phase predicted on antenna 1 according to the samples it received during the reference period.

Emulating the algorithm over the B210 boards is straightforward: we continuously look for valid packets received at one antenna and, once we detect one, we process the reference period of the CTE, we predict the value of the phase on this antenna in the following sample slot, and we finally subtract from it the value of the phase sampled on the other antenna at that same moment in time.

In our setup, we account for a constant phase offset between the two receiving chains of each B210 board. This delay can result from path differences between the two receiving chains due to the specific manufacturing of the boards and the antennas used. Before deploying the boards in the testbed, we execute a calibration procedure by connecting both input ports of a USRP to the same source with a splitter, using good quality cables of the same length.

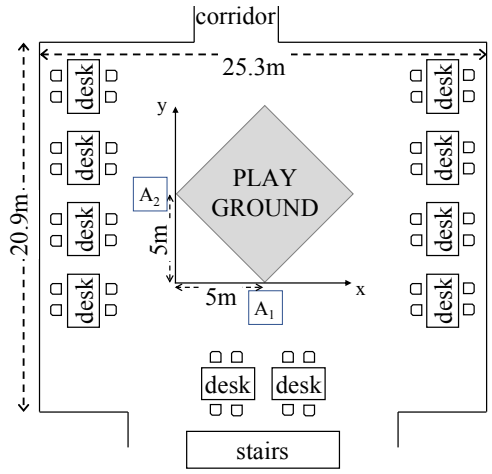

Figure 4: Indoor testbed used for evaluating the AoA-based positioning mechanism. Two receivers (anchors) A_1 and A_2 determine the position of target transmitter in the "playground".

4.3 Positioning Using BLE 5.1

To estimate the position of the transmitter, instead of ranging, we use an additional USRP B210 connected to a different laptop with same specification as before. The two software receivers perform the steps described before to determine AoAs independently. The receivers are connected in a network, so that it is possible to collect all the AoA measurements and use simple geometric operations to convert the two angles into the 2D coordinates of the target device. The configuration we used for positioning experiments is the indoor scenario shown in Fig. 4. The two receivers (*anchors*) A_1 and A_2 are placed at equal distance from the origin of the reference frame. The linear antenna array of each receiver is aligned with the x and y axes of the reference frame respectively.

5 EXPERIMENTAL RESULTS

We test the viability of the positioning mechanism adopted by BLE 5.1 by conducting two sets of experiments: one focusing on assessing the accuracy of the determined AoAs, the other on quantifying positioning errors when employing 2 anchors.

5.1 Angular Accuracy

We begin by evaluating the angular accuracy in the simplest configuration, i.e., a device running our software receiver with two dipole antennas, and another running our software transmitter. To isolate the impact of reflections and multipath-induced errors, we ran these experiments in an outdoor scenario, on a flat court far away from obstacles, with both the receiver and transmitter placed at 0.5 m above the ground and all antennas of the same type, i.e., dipoles positioned vertically.

We measure the angle θ between the axis of the antenna array and the propagation direction of the signal, starting with $\theta = 90°$, which corresponds to ideal no-phase-delay. We progressively reduce the angle to 0°, in 5° steps. For all angles we collect 30 correctly received packets with CTE extension, on each of the 40 BLE channels, which corresponds to a total of 1,200 phase-delay measurements per angle. As the two antennas are spaced less than half of the wavelength for all the BLE channels, and given the position of the reference antenna, by reducing θ we expect to observe the phase-delay decreasing monotonically.

First of all, we note that, when the propagation direction of the signal is close to the axis of the antenna array, the collected phase-delays are almost random. Hence we do not report data for the range $0° \leq \theta \leq 10°$. We then check the accuracy of the estimated angle within each of the 40 BLE channels, for all the remaining 16 values, i.e., $\theta \in \{15°, 20°, \ldots, 90°\}$. The four bitmaps in Fig. 5 demonstrate that the estimated angle is relatively stable over different packets received on the same channel/angle. For instance (bottom maps), only 1.5% of the explored configurations exceed a standard deviation of 5°, and only 4% exceed 2° (this happens almost only for $\theta = 15°$). More than 65% of the configurations exhibit a standard deviation below 0.2° (top-left map) and it is interesting to notice that estimation over higher frequency channels seems to be more accurate.

Looking more closely at the data collected, even though the qualitative variation with θ is correct, we observe two issues: *(i)* angle estimation depends on the channel, this becoming more noticeable at lower frequencies, i.e., estimations spread more; and *(ii)* because of spreading, for angles close to zero there is a higher chance the phase-delay wraps around and the estimated angle bounces up to 180°. Interestingly, for $60° \leq \theta \leq 90°$ the dependency with channel seems *random* rather than deterministic: lower frequency channels, in fact, spread similarly to higher frequency channels, suggesting there is some residual multipath effect affecting the estimation on all channels in the same way. Instead, for the $40° \leq \theta \leq 55°$ range, estimations spread much less. This is somewhat expected, since for such angles the size of the antenna array seen by the incident wave is much smaller than in the $\theta = 90°$ case and waves with higher frequency and smaller wavelength can be more accurate. To avoid wrap-around phenomena on the phase difference that greatly affects the angle error, we exclude from the rest of the analysis situations where θ can be small: hence, we limit the "cone" by considering only $\theta \geq 35°$. The *random dependency* with the frequency suggests that averaging estimations obtained on different channels would be appropriate, to reject the uncertainty due to multipath. This would come at no cost,

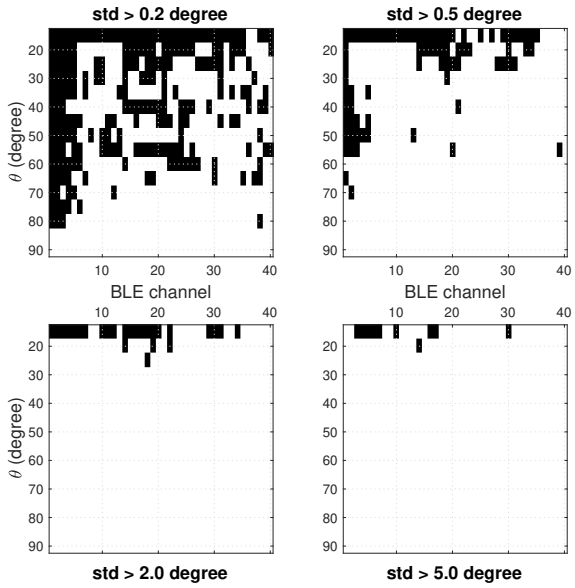

Figure 5: Channel (x-axis) and angle (y-axis) combinations for which the standard deviation of the estimated angle over 30 measurements is below (white) or exceeds (black) the standard deviation threshold indicated in the sub-plot title.

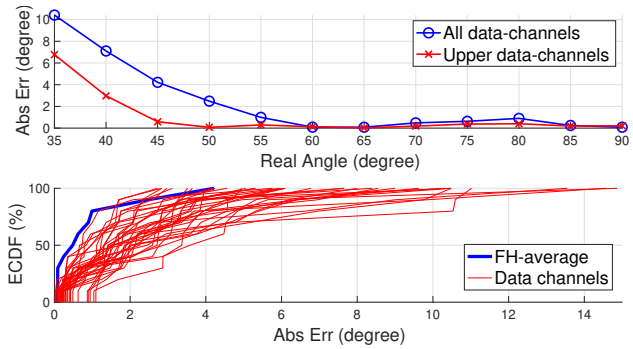

Figure 6: Estimation errors in outdoor settings. Top: absolute error after averaging over all data channels (blue) and over upper-frequency half (red); bottom: ECDF of error after averaging over all data channels and for each channel; angles of 35° and 40° removed.

given that AoA should be used within connection events, i.e., when the two AoA nodes are hopping over the channel sequence that was decided during the connection establishment phase. For this reason in the following we consider only data channels, excluding those dedicated to advertising.

Fig. 6-top, where we report the absolute estimation error after averaging over different sets of data channels, confirms our finding: while for $60° \leq \theta \leq 90°$ restricting the average over the upper half of the set of data channels does not

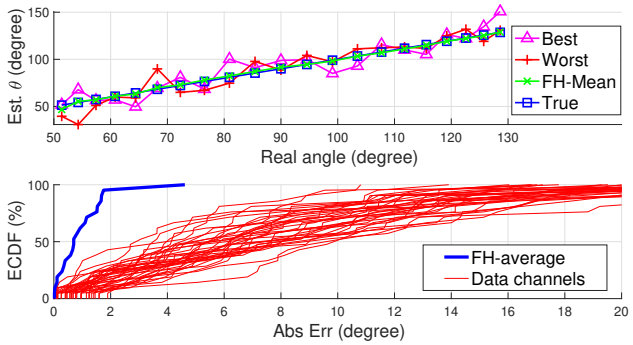

Figure 7: Indoor results for angular accuracy: top, qualitative match of average estimation to *True* angle; bottom, ECDF of absolute error.

bring any advantage, using only higher frequencies would be beneficial for higher rotations, i.e., for $\theta \leq 55°$. However, nodes may exclude upper channels from the FH sequence and for this reason in the following we will always consider all data channels. We will instead limit further the maximum rotation by restricting even more the "cone", setting $\theta \geq 45°$, to contain the maximum error within 4°. In the bottom part of the figure, we show the ECDF of the absolute error within this new cone. To this end, we consider the estimation after averaging over all data channels (thick blue line) and that of every data channel considered alone (thinner red lines). It can be noticed that apart from very few cases (some red lines above the average ECDF close to 100%) averaging over all data channels is always beneficial. We also note that 80% of the averaged estimations are affected by error below 1°.

Before moving to *positioning*, we repeat this experiment in the indoor scenario. This time however we keep the receiver fixed and we move the transmitter along a straight line placed at 4 m from the receiver, in 40 cm steps. This measurement procedure is much more similar to what we will consider next, i.e., it faces different propagation issues at different positions of the transmitter because of the stronger multipath effects inherent to indoor environments as that in Fig. 4. As this environment is not symmetric and there are plenty of objects around, we reduce the cone to $50° < \theta < 130°$.

We report the obtained estimation results in Fig. 7. In the top part we emphasize the very good qualitative match between the *True* angle and the one estimated after averaging over all data channels. We also show the estimations obtained on selected channels, respectively the one with the minimum and maximum root-mean-square error computed over all the considered angles. The benefit of averaging over channels becomes evident. In the bottom part we give a comparison of the ECDF after averaging and for every channel. Wrt. the outdoor case, we note a much worse estimation on each

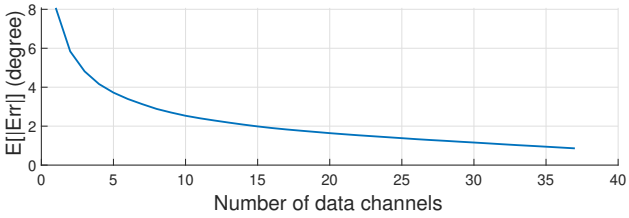

Figure 8: The effect of number of channels used for AoA estimation on the average absolute error.

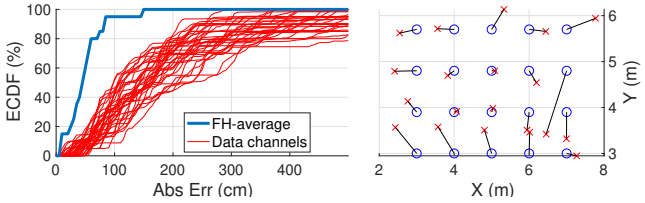

Figure 9: ECDF of indoor position estimation error (left). Qualitative estimation, real (circles) vs estimated (crosses) positions.

separate channel, which however reduces to similar results when averaging is performed.

We complete our AoA analysis by examining the average absolute error that we may obtain with the same dataset in case we limit the average to a restricted number of data channels. For each number we compute the average error by considering all possible FH sequences with a different starting channel and different hop value. We depict the obtained results in Fig. 8. We observe that starting with 15 channels, the average estimation error is well below 2°.

5.2 Positioning Accuracy

To evaluate the accuracy of 2D positioning based on AoA detection, we conduct experiments using the playground area shown in Fig. 4. We use the two receivers A_1 and A_2 placed in the bottom and left corners of the shaded area, within which we constrain the position of the transmitter according to the angular accuracy limitations identified and discussed in the previous subsection. We consider a four by five position grid spanning 4 m over the x- and 2.7 m over the y-axis. The system operates as before, by receiving 30 packets per channel and hopping over all data channels. After collecting the angular data generated by each receiver, we apply the methodology described in Sec. 4.3 to compute positions (x, y) of the target.

We quantify the positioning accuracy in Fig. 9 (left), where we report the ECDF of the absolute estimation error. Observe that (thick blue line) the error is below 85 cm for more than 95% of the positions. However, this is far from meeting the centimetre level accuracy expected by IoT applications, since the absolute positioning error is <10 cm only in 15% of cases. We report on the right a qualitative evaluation: we show with blue circles and red crosses the real and estimated positions.

6 COMPROMISING AOA ESTIMATION

At this early *development stage*, the AoA mechanism in the BLE 5.1 standard does not enforce any security provisions. Surprisingly, no procedure for detecting whether interference affects the transmission of the CTE is considered. Indeed, this follows the CRC that protects the packet, thus there is no way of checking CTE correctness. This offers attackers opportunities to exploit the AoA based positioning capability for malicious purposes, as we explain next.

As we show in Fig. 10, in our implementation we compute a single value for φ by subtracting the phase on antenna 2 (filled circle) from that predicted on antenna 1 (empty circle). Despite the very low level of complexity – in a real device this technique requires just one integrated Single-Pole Double Throw circuit switch (SPDT) – we showed in the previous section some good results that could attract manufacturers. However, we will demonstrate a simple attack on this procedure and propose simple countermeasures. To this end, we change the code of the transmitter to artificially modify the phase of the CTE during the switch slot: here we anticipate the phase of a constant term Ω.

The value predicted by the AoA method on antenna 1 does not change, since the receiver keeps assuming its value corresponds to the top empty circle in Fig. 10 ("Normal" case). However, the value sampled on antenna 2 is different and corresponds to the bottom filled circle ("Hacking" case). The computed phase-delay is hence $\varphi + \Omega$. This gives the transmitter the ability to modify the detected angle over time by properly choosing Ω.

To demonstrate the feasibility of this attack, we run an experiment with the transmitter placed in front of the AoA receiver sweeping Ω linearly over time, between $-\pi/6$ and $\pi/6$, which corresponds to a rotation of approximately 60°

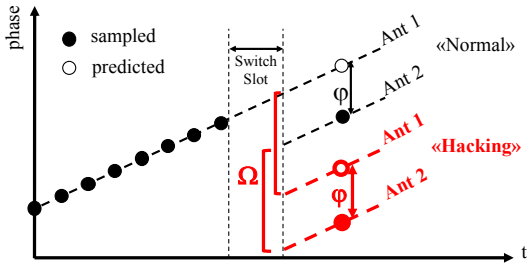

Figure 10: The transmitter can control the phase-delay computed at receiver by modifying phase after switching time, thus compromising correct AoA detection.

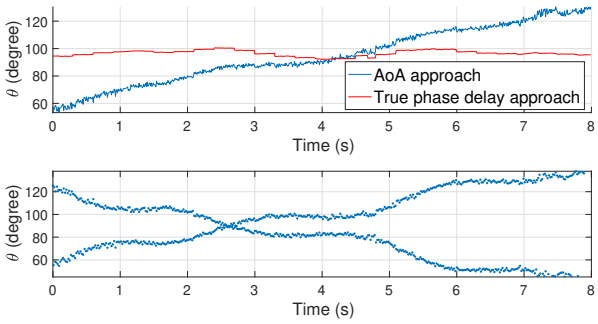

Figure 11: By artificially modifying the signal phase, a transmitter can trick a BLE 5.1 receiver into measuring an arbitrary crafted angle even if not moving (top). A simple approach to detect misleading devices involves changing antenna switching pattern (bottom).

around the receiver. We report the detected angle θ with the blue line in Fig. 11-top. We want to underline that the same procedure can be adopted to trick more complex receivers using multiple antennas, by modifying the signal phase multiple times during the transmission of the CTE. For comparison we also show in the figure with a red line the angle that would be measured by a *classic* approach that receives the signals at the two antennas with two coherent radio chains active at the same time. Since no prediction is involved in this case, the receiver would not be tricked by any artificial modification of the signal phase.

As a simple countermeasure, we can slightly change the behavior of the receiver, so that instead of using one main antenna and switching to the other only for measuring the phase-delay, it keeps the other antenna active for the next packet to be received. In this case, the resulting angle θ appears instead as in Fig. 11-bottom and an untruthful transmitter would be immediately discovered. Needless to say that should the transmitter know the switching pattern, it would always be able to properly craft the phase. To prevent this, keeping the switching pattern hidden to the transmitter and not deterministic would be an effective way of detecting such positioning attacks.

7 SUMMARY & CONCLUSIONS

In this paper, we performed an empirical evaluation of the AoA based positioning mechanism incorporated in the BLE 5.1 standard. We revealed that angular detection accuracy is limited to a constrained range and localization within few centimeters remains difficult. We further showed that an attacker may tamper with the BLE packet structure to mislead the positioning system, and we proposed simple guidelines that manufactures can implement to guarantee the truthfulness of this feature.

REFERENCES

[1] Cisco Meraki. Real-Time Location Services (RTLS). Accessed: June 2019.

[2] Apple Developer. https://developer.apple.com/ibeacon/. Accessed: June 2019.

[3] F. Zafari, A. Gkelias, and K. K. Leung. A survey of indoor localization systems and technologies. *IEEE Comms Surveys & Tutorials*, 2019.

[4] K. Witrisal, P. Meissner, E. Leitinger, Y. Shen, C. Gustafson, F. Tufvesson, K. Haneda, D. Dardari, A. F. Molisch, A. Conti, and M. Z. Win. High-accuracy localization for assisted living: 5G systems will turn multipath channels from foe to friend. *IEEE Signal Processing Magazine*, 33(2):59–70, March 2016.

[5] Bluetooth SIG. Core specification v5.1, Jan 2019.

[6] T. I. Chowdhury, M. M. Rahman, S. Parvez, A. K. M. M. Alam, A. Basher, A. Alam, and S. Rizwan. A multi-step approach for RSSi-based distance estimation using smartphones. In *Intl Conference on Networking Systems and Security (NSysS)*, pages 1–5, Jan 2015.

[7] S. Bertuletti, A. Cereatti, U. Della, M. Caldara, and M. Galizzi. Indoor distance estimated from Bluetooth Low Energy signal strength: Comparison of regression models. In *Proc. IEEE Sensors Applications Symposium*, pages 1–5, April 2016.

[8] C. Luo, L. Cheng, M. C. Chan, Y. Gu, J. Li, and Z. Ming. Pallas: Self-bootstrapping fine-grained passive indoor localization using wifi monitors. *IEEE Trans. Mobile Computing*, 16(2):466–481, Feb 2017.

[9] Deepak Vasisht, Swarun Kumar, and Dina Katabi. Decimeter-level localization with a single wifi access point. In *Proc USENIX NSDI*, 2016.

[10] X. Li, D. Xu, X. Wang, and R. Muhammad. Design and implementation of indoor positioning system based on ibeacon. In *International Conference on Audio, Language and Image Processing (ICALIP)*, pages 126–130, July 2016.

[11] X. Lin, T. Ho, C. Fang, Z. Yen, B. Yang, and F. Lai. A mobile indoor positioning system based on ibeacon technology. In *International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, pages 4970–4973, Aug 2015.

[12] B. Kempke, P. Pannuto, and P. Dutta. Polypoint: Guiding indoor quadrotors with ultra-wideband localization. In *Proc. ACM Hot Wireless*, pages 16–20, 2015.

[13] B. Kempke, P. Pannuto, B. Campbell, and P. Dutta. Surepoint: Exploiting ultra wideband flooding and diversity to provide robust, scalable, high-fidelity indoor localization. In *Proc. ACM SenSys*, 2016.

[14] Bluetooth SIG. Press release: Bluetooth enhances support for location services with new direction finding feature, Jan 2019.

[15] R. Schmidt. Multiple emitter location and signal parameter estimation. *IEEE Trans. Antennas and Propagation*, 34(3):276–280, March 1986.

[16] M. Ji, J. Kim, J. Jeon, and Y. Cho. Analysis of positioning accuracy corresponding to the number of ble beacons in indoor positioning system. In *International Conference on Advanced Communication Technology (ICACT)*, pages 92–95, July 2015.

[17] G. De Blasio, A. Quesada-Arencibia, C. R. García, J. C. Rodríguez-Rodríguez, and R. Moreno-Díaz. A protocol-channel-based indoor positioning performance study for bluetooth low energy. *IEEE Access*, 6:33440–33450, 2018.

[18] J. Powar, C. Gao, and R. Harle. Assessing the impact of multi-channel BLE beacons on fingerprint-based positioning. In *Proc. IPIN*, Sep. 2017.

[19] S. Monfared, T. Nguyen, L. Petrillo, P. De Doncker, and F. Horlin. Experimental demonstration of ble transmitter positioning based on aoa estimation. In *Proc. IEEE PIMRC*.

[20] Z. Zhu and M. Z. Bocus. A computationally efficient method for direction finding with known transmit sequence. In *Proc. IPIN*, Sep. 2018.