WIDAR: bistatic WI-fi Detection And Ranging for off-the-shelf devices

Pierluigi Gallo*, Stefano Mangione* and Giampiero Tarantino*
*Universitá di Palermo, Italy Email: {pierluigi.gallo},{stefano.mangione.tlc}@unipa.it

***Abstract*—The huge spread of wireless networks and the success of location-aware applications require novel indoor positioning mechanisms based on existing technologies such as IEEE 802.11. Taking inspiration from the RADAR, we propose WIDAR: a bistatic WI-fi Detection And Ranging system for off-the-shelf devices. WIDAR implementation is based on the USRP2 platform and is able to locate 802.11 stations while they operate in existing legacy networks. No substitution or repositioning of the Access Points is necessary. WIDAR works passively and does not expect any dedicated action from the target WiFi node. No airtime is wasted and the target cannot even detect that it is being ranged. Such features make WIDAR desirable in surveillance and monitoring applications where it can provide real-time tracking functionalities.**

I. Introduction

Last decades have been characterised by a huge and still increasing number of location-aware applications, spanning from commerce to e-health [1]. Nowadays, GPS is considered the privileged outdoor localization solution for positioning and navigation, where the receiver computes its position by measuring delays from different satellites. The RADAR (RAdio Detection And Ranging) is mainly used to localize unaware or not-collaborative objects at long distances. Both techniques, originally developed in the military field, are nowadays employed also in civil applications such as navigation, piloting, flight monitoring and control, etc.. Furthermore, both technologies are deployed in outdoor and use time-of-arrival (ToA) measures: one-way for the GPS and round-trip for RADAR. A RADAR localizes objects in polar coordinates ranging them while scanning all possible directions. It scales worse than GPS, as for the number of localized targets, because the computation is centrally done by the RADAR. On the other hand, it does not require any collaboration from the target, that is generally unaware that someone is localizing it[1]. Currently, indoor ranging techniques suffer a trade-off between high accuracy, using dedicated devices, and low accuracy, using legacy ones. On the one hand, RADAR-like solutions use UWB dedicated devices obtaining millimetric accuracy in indoor ranging [2]. On the other hand, legacy 802.11 devices can be ranged with an error lower than 2 m in 90% of the cases, and with a maximum error of 16 m in real-time ranging of a target moving at pedestrian speed [3]. In the present work we provide a novel ranging system based on software defined radio devices, namely WIDAR. The adaptation of selected RADAR solutions to the WiFi field yields an improvement in ranging accuracy. Our system can range off-the-shelf IEEE 802.11b devices in real-time, while operating in legacy networks and without an explicit intervention from the target. WIDAR works also in outdoor, even if, the pervasive indoor deployment of 802.11 access networks and the obtained accuracy with a maximum error of 1.8 m, make it specially valuable for indoor applications. WIDAR is an intermediate solution between two opposites: ranging with dedicated hardware and ranging using only current 802.11 legacy devices. WIDAR performs a passive ranging of existing hardware (WiFi handsets, laptops, etc.); it does not need neither substitution, nor repositioning of the existing access points. Ranging requirements are the same for all technologies [3], [4]: (i) maximum accuracy; (ii) energy efficiency; (iii) minimum packet overhead, (iv) maximum scalability; (v) maximum working range; (vi) low convergence time; (vii) no calibration demanded to the end user; (viii) end-user unawareness. Ranging solutions entail a trade-off among the above conflicting requirements. ToA-based ranging methods share the same basic idea: correlate propagation delays at a known speed with distances. Propagation time measures strongly depend on the triggering events that are chosen to activate/deactivate the stopwatch. As for example, the most intuitive way to measure an inter-packet time is to consider the end of the first packet and the beginning of the second one; we will discuss later on that it is not the best solution. The example above introduces the first problem to solve: the selection of proper events that trigger actions on the stopwatch. These events can be chosen among those available in the MAC/PHY APIs, being the latter more appropriate for fine-grained time measurements. ToA-based ranging accuracy and precision is influenced by: (i) *internal factors* depending on the ranging system and its way to grab time measurements, e.g. choice of triggering events, frequency shift among TX/RX, extra latency introduced by the hardware; (ii) *external environmental factors* such as interferences, multipath and fading.

A. Justifying the SDR approach

WIDAR employes a USRP2 [5] software defined radio (SDR) platform equipped with the GnuRadio software development toolkit. SDR platforms are generally used by researchers because of their costs and their learning curve. Despite such cons, the SDR choice is justified in WIDAR because of two reasons: (i) money are saved because targets are off-the-shelf devices and a good accuracy is obtained; (ii) one USRP2 is sufficient to range all nodes in its coverage area. These two aspects make the investment affordable. USRP2

[1]In legacy RADARs, target can detect impulses; we instead focus on passive RADARS, which are completely non-detectable.

978-1-4673-5828-6/13/$31.00 2013 IEEE

permits the application layer to know the instant of detection of the starting frame delimiter (SFD), impossible to be obtained with the monolithic PHY of the current WiFi cards. WiFi commercial receivers are designed neither for ranging nor for localization; time and frequency shifts are compensated with a precision that is enough for demodulation but too rough for ranging. Borrowing some well known tools from the RADAR technology, we are able to refine the estimation of time and frequency offsets by leveraging the USRP2 flexible PHY. The main advantage of using the SDR approach is its measuring instrumentation capability, although it is more than a measuring instrument. A WiFi RF front-end and baseband are engineered to meet the minimum required sensitivity with minimum area/power consumption constraints. The USRP can represent the signal in a predetermined bandwidth via its complex envelope and with an high dynamic range (more than 12 bits per sample for the USRP2).

II. Related work

In the present section we focus on time-of-arrival based solutions in 802.11 networks. Active and passive ranging approaches are described in [6] for RSSI fingerprinting; those considerations can be applied also to ToA-based ranging. Active ranging technologies introduce dedicated transmissions/packets for ranging purposes. This approach is potentially detectable by the target node and, specifically in 802.11 systems, it consumes airtime otherwise used for data transmissions over the shared channel. Ranging passively is not detectable by the target, the counterpart is that quasi-silent nodes cannot be ranged. In [7], [8], [3], ranging is performed by measuring propagation delay at MAC level. Propagation is affected by multi-path reflections, they influence ranging accuracy and precision. In [1], multi-path effects were combated with diversity performing antenna or frequency switching. Spacial diversity is considered in case of moving targets, thanks to their motion model. In [1] an analogy between a ToA-based ranging system and a RADAR is drawn. The authors describe how the SIFS interval is not deterministic and they introduce a mechanism to compute the mis-synchronization time among independent unsynchronized nodes. They also introduce a timestamp in their packets, and modify the transceiver of the WiFi card in order to receive also while transmitting (bypassing the low-noise amplifiers). The authors used a testing device from Intel with customized PHY and firmware. In [9], the author classifies ranging techniques with hardware enhancements and purely software ones. He designed an external hardware to improve resolution in measuring the propagation delay, using RTT measurements in order to avoid the need for time synchronization. ToA measurements at MAC level can be obtained using the flexible MAC programmability of the Wireless MAC Processor proposed in [10], [11], but no flexibility on the PHY is provided. Software Defined Radio approaches are described in [12], using $5.8\ GHz$ ISM band. The authors measure both the amplitude and phase of the channel frequency response and the ideal time of arrival for the direct path signal. Multi-path components are recognized via complex sinusoids appearing in the channel frequency response. In the project report [13], the authors use the USRP2 in order to build a localization system using specially configured USRP2 transmitters and receivers, so they can range only special targets, not off-the-shelf ones. In [7] it is proposed a ranging solution based on commercial Atheros cards, equipped with a 44 MHz internal clock. The implementation, based on the open-source driver, polls card registers at regular time intervals. Reading the cumulative durations in which the medium has been sensed idle and busy, the authors compute the time of flight of packets. [16] proposed an hybrid solution that using both angle of arrival and ranging. Having 5 base stations they obtained $3\ m$ accuracy in 50% of cases. In [14], the authors analyze the impact of the IEEE 802.11v standard, lately included in [17], on TOA-based positioning systems. The authors compare a commonly adopted RTT TOA-based positioning in two conditions: with and without incorporating the IEEE 802.11v capabilities. Since authentication and association are no more necessary, scalability lightly improves. The novel processing time computation performed at the AP does not improves ranging accuracy but eliminates the need for manual pre-calibration. Further enhancements are expected to come thanks to the timing measurements mechanism.

Algorithm 1 Ranging algorithm

```
while true do
  TOBERANGED ← load list of targets MAC address
  while NOT RECORDTIMEOUT do
    record trace
  end while
  for frame in trace do
    if (frame is DATAFRAME) AND (MACSRC OR
    MACDST is in TOBERANGED) then
      compensate frequency offset
      detect start of frame delimiter
      compute frame length
    end if
    if nextframe is ACK then
      frequency offset
      detect start of frame delimiter
    end if
  end for
  compute A to B and B to A ranges
  evaluate target possible positions
end while
```

III. WIDAR ToA based ranging

Ranging can be performed using the propagation time which depends on the measured round trip time (RTT). It is the time elapsed between the transmission of a DATA frame and the consequent reception of the ACK frame. Accordingly to the IEEE 802.11 standard, if a station receives a DATA frame it has to reply with an ACK in a short inter-frame space (SIFS). By considering a couple of DATA/ACK frames, $RTT = 2 \cdot t_p + SIFS$, where SIFS is computed from the end of the last symbol of the DATA frame to the beginning of the first

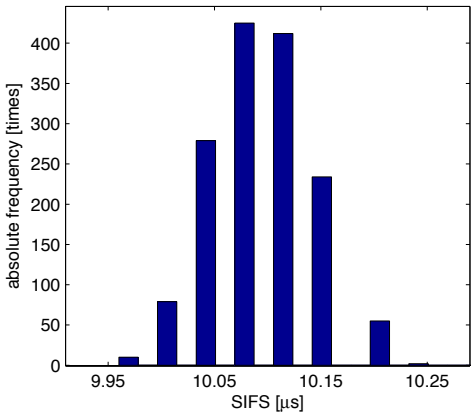


Fig. 1. SIFS distribution

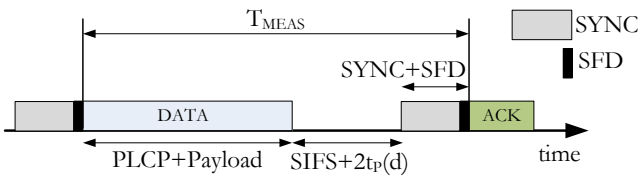


Fig. 2. Reference points used to activate and deactivate the stopwatch.

symbol of the preamble of the ACK frame, as seen at the air interface [17]. Nominal SIFS duration is 10 μs long, with allowed variations below $\pm 10\%$ of $aSlotTime$ for the PHY in use. For 802.11b, aSlotTime is 20 μs; it means an allowed SIFS range of ± 2 μs which results, by multiplying for the speed of light, in an ugly ranging precision of ± 600 m. Our SIFS measurements, taken from cards from different vendors, show that SIFS variance is much lower than the value allowed by the standard, although its shape and variance depend on manufacturer. As example, in fig. 1, a SIFS delay distribution is gathered from Broadcom cards. WIDAR operates ranging of targets in an endless loop, as reported in algorithm 1.

A. Methodology

1) Triggering events: Although the most intuitive manner to determine the propagation time t_p is to have a direct measure of the RTT, we found this not the best way to do it. Time measurements from the end of a frame to the beginning of the next one are affected by uncertainty on *transmit power-on ramp* and *transmit power-down ramp*. Frame timing cannot be taken from its power envelope because the standard gives only maximum duration for ramps: 2 μs in rising/falling between 10% and 90% of maximum TX power [17]. To reduce the uncertainty in determining trigger events, we decided to use the Start of Frame Delimiter, as shown in fig. 2, instead of frame edges. The propagation time is then computed from this formula (in case of long preamble): $t_{MEAS}(d) = t_{PLCP} + t_{PAYLOAD} + SIFS + 2 \cdot t_p + t_{SYNC} + t_{SFD}$. PLCP preamble is made by 128 bit (SYNC) + 16 bit (SFD) and PLCP header is 48 bit long which sum 192 bit that means 192 μs at basic rate.

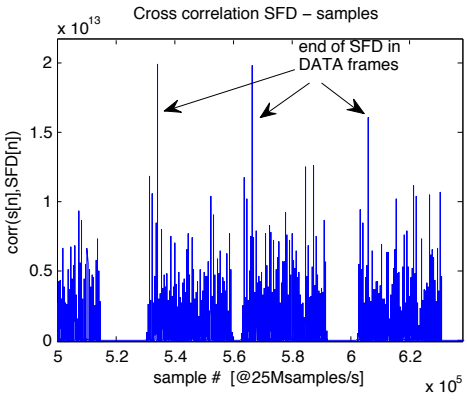


Fig. 3. Cross-correlation peaks (received samples - SFD sequence).

2) SFD and frame edge detection: Abandoning the edges of frames as triggering events comes with a cost; start/end of a frame are MAC events that are signaled by MAC implementation while SFD detection needs PHY flexibility, currently obtainable only with the SDR approach. To detect the SFD we use a well known method borrowed from the RADAR technology: the matched filter [18]. It is used to correlate a known signal, or template (in our case the SFD sequence), with an unknown signal (the received samples) to detect the presence of the template in the unknown signal. The correlation between the SFD and the received sequence cannot be done as they are, because 802.11b uses Direct Sequence Spread Spectrum (DSSS). It means that sequences are spread with an 11-chip Barker sequence, hence the received sequence has to be correlated with the SFD sequence after it is spread with the Barker code and resampled at 25 $Mbit/s$. This correlation will provide several peaks, because the Barker sequence will be recognized as many times as the number of bits in the preamble. The highest peak will delimit the end of the SFD because it is the case where the whole SFD matches. In fig. 3 is shown correlation between SFD sequence, spread with Barker code, and sequence captured by WIDAR. The end of the SFD of DATA frames is pointed by the highest correlation peak in each block, as pointed by arrows on the figure. Each block of correlation peaks represents a DATA/ACK couple. Blue blocks are separated by the backoff, since the transmitting station is competing for using the channel. To distinguish the SFD of ACKs in fig. 3, the frequency shift between ACK sender and WIDAR have to be compensated.

3) Bistatic ranging: As shown in fig. 4, our system has a strong analogy with bistatic radars. Bistatic radars are made by transmitter and receiver which are separated by a distance that is comparable to the expected ranging distance. This kind of radars use the target as a mirror that reflects electromagnetic waves. On the contrary, in 802.11 systems, the node under ranging (the STA), alternatively sends DATA and receives ACK, (as depicted in fig. 4-(a)), then receives DATA and sends ACK (as in fig. 4-(b)). Single arrows represent propagation of DATA packets, while double arrows indicate ACKs. Fig. 5 depicts, in space and time, the topology described in fig. 4-(a) and (b) respectively. Also the single/double arrow convention

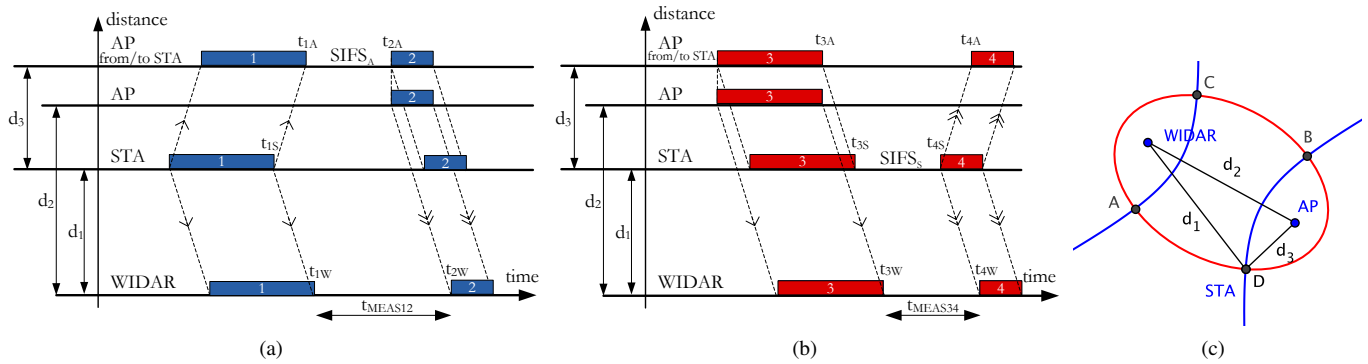


Fig. 5. Bistatic ranging in time and space: STA sends DATA to the AP (a) the AP sends DATA to the STA (b), ranging loci defined by equations (c).

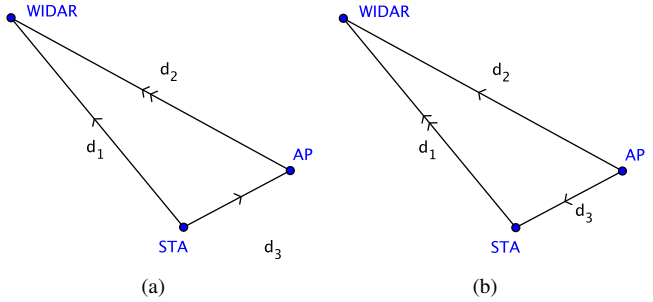


Fig. 4. Reciprocal bistatic ranging topology: STA transmits data to the AP (a) the AP transmits data to the STA (b).

for DATA/ACK is adopted. Horizontal lines represent the position of AP, STA, and WIDAR. In order to squeeze on a single axis information of the triangular topology, the AP appears represented by two horizontal lines. The lower line defines the AP position considering its distance from WIDAR; the upper line describes the AP considering its distance from the STA. When the AP communicates with STA, the higher line is considered, otherwise the lower line is used (propagation till WIDAR). Such representation clarifies the reciprocal distances, with no impact on timing computation. The picture confirms that WIDAR acts passively: only entering arrows towards WIDAR are depicted. All dashed lines have the same slope, that represents the speed of light. 5-(a) shows two frames: 1 is a DATA frame sent by the STA, 2 is and ACK frame sent by the AP. They both are listened by the WIDAR, which evaluates t_{MEAS12}. Key time values are indicated with a naming convention where first subscript is tied to the frame id (1 or 2) and the second one represents the node, e.g. t_{1A} delineates the end of frame 1 as seen by the AP, t_{1S} regards frame 1 as seen by the STA, t_{1W} represent the same event as seen by WIDAR. t_{MEAS12} is the time interval between DATA and ACK, as measured in WIDAR. We recall the use of SFD as triggering event, however the begin and the end of frames is computed by considering headers and payload duration. With $t(d_i)$ we indicate the time spent by the electromagnetic wave to propagate along distance d_i with $i = 1, 2, 3$, therefore $t(d_i) = d_i/c$. Furthermore, distances and consequently times are subject to $d_i < d_j + d_k$ due to the triangle inequality. Furthermore, we use different colors, blue to indicate DATA sent from STA to AP (fig. 5-(a)) and red to indicate DATA sent from AP to STA (fig. 5-(b)). The same colors are used to draw the ranging loci obtained by the corresponding equations (fig. 5-(c)). Looking at fig. 5-(a), we can write the following system:

$$\begin{cases} t_{MEAS12} = t_{2W} - t_{1W} \\ t_{2W} = t_{2A} + t(d_2) \\ t_{2A} = t_{1A} + SIFS_A \\ t_{1A} = t_{1S} + t(d_3) \\ t_{1W} = t_{1S} + t(d_1) \end{cases}$$

from which derives:

$$t_{MEAS12} = t(d_3) + SIFS_A + t(d_2) - t(d_1) \quad (1)$$

Since $t(d_2)$ and SIFS are known, t_{MEAS12} is measured, so eq. 1 can be written as:

$$t(d_3) - t(d_1) = \alpha \quad (2)$$

where α is a known constant. Eq. 2 represents an hyperbola having foci in WIDAR and the AP, whose positions are known. By considering fig. 5-(b). we can derive the following system:

$$\begin{cases} t_{MEAS34} = t_{4W} - t_{3W} \\ t_{4W} = t_{4S} + t(d_1) \\ t_{4S} = t_{3S} + SIFS_S \\ t_{3S} = t_{3A} + t(d_3) \\ t_{3W} = t_{3A} + t(d_2) \end{cases}$$

from which derives:

$$t_{MEAS34} = t(d_3) + t(d_1) - t(d_2) + SIFS_S \quad (3)$$

Here, as before, $t(d_2)$ and SIFS are known, t_{MEAS34} is measured, hence we obtain:

$$t(d_3) + t(d_1) = \beta \quad (4)$$

where β is a known constant, whose value is the bistatic range. Eq. 4 represents an ellipses having foci in WIDAR and the AP, whose positions are known. Bistatic range β corresponds to the length of the major axis of the ellipse. Loci defined by eq. 2 and 4 are painted in fig. 5-(c), which can be read as follows: given the positions of the AP and the WIDAR, the STA lays on the ellipses whose foci are the AP and the WIDAR

and contemporary lays on the hyperbola with the same foci. Reciprocal bistatic ranging has a twofold pro: (i) introduces path diversity, useful to combat multi-path effects (ii) defines an ellipses and an hyperbola that intercept in four points. The STA location is one of these points so WIDAR provides an enhanced ranging: it provides a quasi-localization, i.e. the target can be in one of these four possible points. Special cases are when the loci becomes degenerates (the ellipses in a segment and the hyperbola in two rays). A single AP has usually N associated STAs; in this case WIDAR acts as a multi-static ranging system, providing an ellipse and a hyperbola for each STA. However, in our implemented algorithm, we perform an easier interception between circles.

4) Frequency offset: The WIDAR has a frequency offset towards both the STA and the AP, due to the low quality quartz oscillators in wireless cards. Their frequency tolerance is about $10\ ppm$, meaning that the frequency offset can be dozens of kHz. In order to have a successful communication, the offset must be roughly compensated for; to have an accurate ranging, the frequency offset has to be finely corrected. In [13], the authors use USRP both as ranging device and target ones, so they transmit a signal at a known frequency from a device and analyze the FFT in the other one, to evaluate the offset. We cannot apply this method because we range legacy 802.11 nodes, so we compute frequency offset using the ambiguity function, a standard mathematical tool in RADAR defined as $\chi(\tau, f_d) = \int_{-\infty}^{+\infty} s(t)s^*(t-\tau)e^{-j2\pi f_d t}dt$ [15]. The ambiguity function permits a joint estimation of time and frequency offsets. It is generally used to evaluate the Doppler frequency shift due to relative motion among nodes; in indoor scenarios, at pedestrian speed, the Doppler shift is negligible so the ambiguity function helps in evaluating receiver tuning offset.

IV. Testbed setup

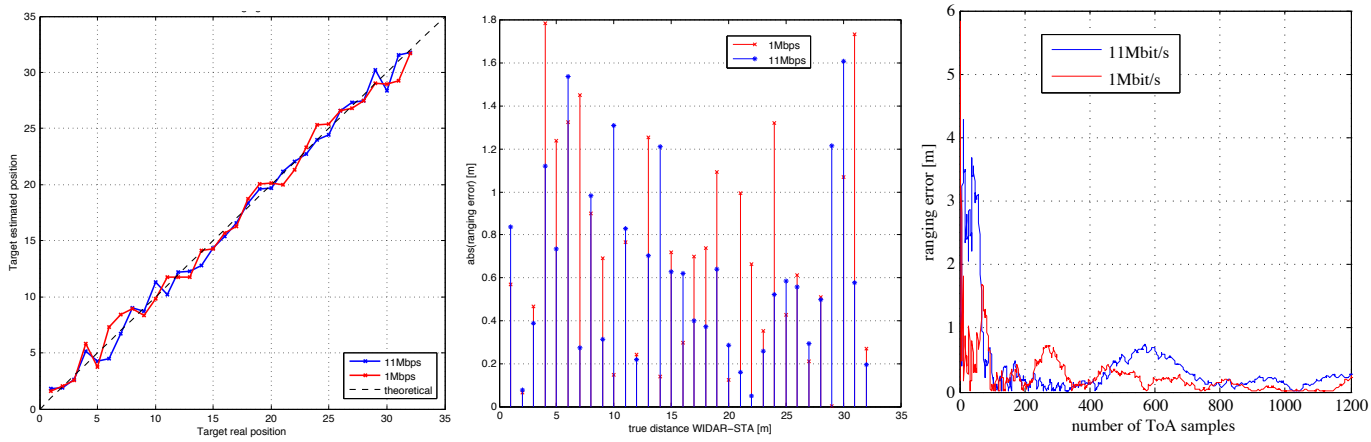
WIDAR is composed by a USRP2 platform which includes a Gigabit Ethernet interface, a Xilinx Spartan FPGA and RF transceiver, two input channels and two output channels. It receives I/Q samples from the ADC, at a sampling rate that we fixed at $25\ MS/s$. The maximum sampling rate obtainable from the USRP2 is $50\ MS/s$, however we opted to sample at $25\ MS/s$ because the dynamic range at $50\ MS/s$ is very small, about six bits per sample, so the choice of amplifier gain becomes very critical. The host is equipped with GNU Radio 3.6, and UHD 3.4 running on Linux. Using the USRP2, computation on samples are done in a regular PC, being possible to elaborate at any OSI level, PHY included. The STA is a notebook running Linux 2.6; the wireless card is an Intel WiFi Link 5100. The AP is a PCEngine Alix2 vers. 0.99h including a Broadcom B4318 card running Linux 2.6. Ranging tests have been performed both in the corridor on third floor of the authors' department and on the adjacent terrace. In both cases the radio environment has revealed crowded and noisy and some metallic shelves where positioned along the walls.

V. Experimental results

In this section we report experimental results for both ranging (fig. 6-(a-b-c)) and localization (fig. 7). To validate the true WIDAR potentials in ranging, we employed a scenario where it was positioned close to the transmitter (both fixed) measuring round-trip time of flight towards the STA. The distance between the station and the AP spans from 1 to $32\ m$ along the same direction (1-D localization). Results are shown in fig. 6-(a), where the true position of the target is compared with the estimated one. Points fit extremely well the first theoretical line. At $11\ Mbps$ the error keeps lower than $1\ m$ for 26 times out of 30, and 23 times out of 30 at 1Mbps, as shown in fig. 6-(b). Ranging distances are obtained with a sampling rate at the USRP2 of $25\ MS/s$, which results in $40\ ns$ sampling period. The reason why we obtain better-than-nominal accuracy lays on interpolation; in facts, at $25\ MS/s$ the WiFi signal can be fully represented. To evaluate the time needed by WIDAR in order to estimate a single position of a WiFi node, we show the ranging error vs the number of computed samples. From fig. 6-(c), it appears that for more than 100 samples, the error keeps lower than $1\ m$. Quasi-localization brings to the position estimation in two possible locations, as explained in Sect. III-A3. The two possible points present a reflection symmetry along the segment WIDAR-AP. In fig. 7 it is shown the topology used for the quasi-localization testbed; the blue quads indicate the true station positions, while the blue crosses depict the estimated ones. Green arrows represent the quasi-localization estimation error. The position of the AP is represented by the red circle, while WIDAR is identified by a red square marker. For sake of figure readability, only one estimated point is shown for each position (the closest one). It is evident that because of topological constraints (walls, floor delimitation, etc.), only a single estimation, of the possible two, can be taken into account. In the present paper we do not claim to provide any contribution on the localization algorithm, in fact we use a legacy trilateration algorithm. Although localization results can be improved by considering multiple WIDARs acting cooperatively and by applying optimized localization algorithms, the main strength of WIDAR is the ability to localize nodes using a *single device* and without focusing on localization algorithms. Figure 7 shows that WIDAR is able to detect the station position without the use of multiple anchors. The use of a single localizing device comes with a side-effect on accuracy, being higher than the accuracy obtained with localization systems based on multiple anchors.

VI. Conclusions and future work

WIDAR leverages both MAC and PHY peculiarities of the 802.11b standard and employs RADAR-specific tools for precise frame timing. This paper introduces the use of a bidirectional and bistatic ranging technique; it allows a quasi-localization using a single WIDAR device. As a future work, the system can be expanded taking into account not only the DATA/ACK couple but also the RTS/CTS one and the presence of multiple WIDARs will be evaluated, as well as the effects of NLOS. The limitation to 802.11b can be lifted, our approach can be easily generalized to 802.11g signals. Furthermore, the effects of a precise localization will be evaluated to increase the awareness of cognitive wireless networks.



(a) (b) (c)

Fig. 6. Estimated distances over true distances at different rates (a); ranging error by distance (b); ranging error vs number of samples (c).

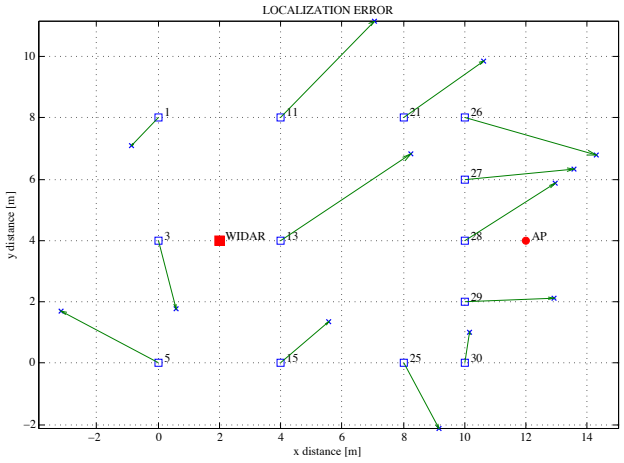


Fig. 7. Position estimation error using WIDAR with 802.11b at 2 $Mbps$ rate.

ACKNOWLEDGMENT

This work is partially supported by the EU under projects FP7-257263 (FLAVIA) and FP7-258301 (CABIN-CREW).

REFERENCES

[1] S. A. Golden, and S. S. Bateman, *Sensor measurements for Wi-Fi location with emphasis on time-of-arrival ranging*, Transactions on Mobile Computing, vol. 6, no. 10.

[2] C. Zhang, M. Kuhn, B. Merkl, M. Mahfouz, and A.E. Fathy, *Development of an UWB Indoor 3D Positioning Radar with Millimeter Accuracy*, Microwave Symposium Digest, 2006. IEEE MTT-S International , vol., no., pp.106-109, 11-16 June 2006.

[3] D. Giustiniano, and S. Mangold *CAESAR: Carrier Sense-Based Ranging in Off-The-Shelf 802.11 Wireless LAN*. In Proceedings of CoNEXT '11.

[4] T. C. Karalar *Implementation of a Localization System for Sensor Networks*. PhD Thesis, University of California, Berkeley, Spring 2006.

[5] Ettus Research *Universal Software Radio Peripheral*, http://www.ettus.com/

[6] B. Sieka, *Active Fingerprinting of 802.11 Devices by Timing Analysis*, Consumer Communications and Networking Conference, 2006.

[7] A. Gunther and C. Hoene, *Measuring round trip times to determine the distance between WLAN nodes*, in Proc. of Networking 2005, Waterloo, Canada, 2005. pp.768-779,

[8] K. I. Ahmed and G. Heidari-Bateni, *Improving two-way ranging precision with phase-offset measurements*, in IEEE Global Telecommunications Conference (GLOBECOM), 2006.

[9] M. C. Adell, *Contributions to TOA-based location with WLAN*, Ph.D. dissertation, Universitat Politecnica de Catalunya, Departament dEnginyeria Telematica, Barcelona, Spain, Apr. 2010.

[10] I. Tinnirello, G. Bianchi, P. Gallo, D. Garlisi, F. Giuliano, F. Gringoli, *Wireless MAC Processors: Programming MAC Protocols on Commodity Hardware*, Proc. of IEEE INFOCOM, March 2012.

[11] P. Gallo, D. Garlisi, F. Giuliano, F. Gringoli, and I. Tinnirello, *WMPS: A Positioning System for Localizing Legacy 802.11 Devices*, IEEK Transactions on Smart Processing and Computing.

[12] D. Humprey and M. Hedley, *Super-Resolution Time of Arrival for Indoor Localization*, IEEE International Conference on Communications ICC, 2008. Sydney, Australia, 2008.

[13] R. Dobbins, S. Garcia, and B. Shaw, *Software Defined Radio Localization Using 802.11-style Communications*, Worcester Polytechnic Institute

[14] M. Ciurana, F. Barcel-Arroyo, and I. Martn-Escalona, *Comparative performance evaluation of IEEE 802.11v for positioning with time of arrival*, Computer Standards & Interfaces, Volume 33, Issue 3, March 2011, pp. 344-349

[15] S. Stein, *Algorithms for Ambiguity FunctionProcessing*, IEEE Transactions on acoustics, speech, and signal processing, VOL. ASSP-29, N. 3, June 1981

[16] D. Niculescu and B. Nath, *VOR Base Stations for Indoor 802.11 Positioning*, Proceedings of the 10th annual international conference on Mobile computing and networking, MobiCom 2004.

[17] IEEE Standard for Information technology *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. 6 February 2012

[18] B. R. Mahafza, *Radar Systems Analysis and Design Using MATLAB, Chapter 6, Matched filter and Radar ambiguity function*, edited by Chapman and Hall/CRC - 552 Pages, 2000