Limitations of range estimation in wireless LAN

Hector Velayos, Gunnar Karlsson

KTH, Royal Institute of Technology, Stockholm, Sweden, (hvelayos,gk)@imit.kth.se

Abstract – **Limitations in the range estimation techniques due to the indoor radio propagation prevent a broader spread of WLAN positioning. We analyze in this paper the two more promising range estimation techniques for wireless LANs. Firstly, we examine the predominant option, range estimation based in received signal strength (RSS). Our measurements illustrate its shortcomings: lack of accurate radio propagation models and difficulties to build experimental radio maps. Then, we discuss the problems with range estimation based in time of arrival (TOA): the resolution of the frame timestamp and the need for synchronized clocks between access points and stations. To overcome the last problem, we suggest a novel technique to estimate the increment in propagation time without synchronized clocks.**

1 Introduction

Techniques for range estimation in wireless communications have been studied for several years now. Some of these techniques were successfully applied to existing wireless systems to provide positioning. In particular, positioning is featured in outdoors wireless systems. GPS is been in operation for some years using dedicated satellite receivers, and cellular phones with positioning capabilities will be roll out this year.

However, positioning for wireless LANs (WLAN), the dominating technology in high data-rate indoor wireless systems, is not expected to be widely available in the near future. Several studies have been published, and some companies are offering commercial products [1]. But limitations in the range estimation techniques due to the indoor radio propagation prevent a broader spread of WLAN positioning.

We analyze in this paper the two more promising range estimation techniques for wireless LANs. Firstly, we present the shortcomings of range estimation based in received signal strength (RSS). Then, we discuss the problems with range estimation based in time of arrival (TOA).

2 Limitations of range estimation based on Received Signal Strength

The predominant option for range estimation in WLAN is to leverage the dependence of received signal strength on distance. As the signal propagates from the access point (AP) towards the receiving station, its energy reduces. If a station measures the received signal strength, and it knows the transmitted signal strength and how the signal strength reduces with distance (i.e. the radio propagation model), it can estimate the range to the AP. The technique is simple, but several factors complicate its application to wireless LANs.

In wireless LANs, the transmitter selects the transmitted power depending on the environmental conditions and the receiver does not know the used value. If this information would be necessary at the receiver for range estimation, it should be included in the frame header. While this can be easily done, it is not desirable because it increases the overhead per frame, and thus it reduces the channel capacity for user data.

A more challenging problem is the need for an accurate radio propagation model. The model must predict the RSS as a function of the distance. In case of free space propagation, the model is well known:

$$P(d)[dBm] = P(d_0)[dBm] - 10n\log\left(\frac{d}{d_0}\right) \tag{1}$$

where *P(d)* is the received power at some distance *d*, $P(d_0)$ is the transmitted power measured at a reference distance d_0, and *n* indicates the rate at which the path loss increases with distance. In free space, *n* is 2, but it is a challenging calculation for indoor WLAN because the path loss must account for refraction, reflection, attenuation and the obstacles found in the path. A reasonable approximation for *n* in the 2.4Ghz band is 3.5 [2]. Other researchers found that a static value for *n* cannot accurately model the indoor RSS. They suggest including in the model the actual number and type of relevant obstacles in the path. For instance, Seidel and Rapport proposed including the number of floors in the path [3], while Bahl and Padmanabhan opted for the number of walls [4]. Although these models are more accurate for RSS prediction, they cannot be used for range estimation because the position, and thus the number of obstacles, is unknown a-priori.

Our experiments confirm that the free-space model cannot be accurately adjusted via calculating *n* to describe indoor propagation. Figure 1 presents the result of our measurements. The upper plot shows the received signal strength versus distance for Line-Of-Sight (LOS) propagation in the corridor of an office. The measured RSS values are represented by dots and taken at different distances. Since this situation should be similar to free-space propagation with a different value for *n*, we tried to calculate *n* using a nonlinear least square method to minimize the error of the resulting model to the measured values. The continuous line in the upper plot represents the model. The measured RSS values appear scattered around the model, indicating the model does not fit properly. The lower plot shows what would be the range estimation error when using the model for different distances. This second plot shows that the error can be up to 10 meters, even in short distances.

Our measurements also indicate that a 3 segment piece-wise linear function would fit better the measured points. The RSS seems to decay fast with distance between zero and 12 meters range, and for ranges larger than 28 meters. But it is almost constant between 12 and 28 meters range. However, we have not found any study following this approach.

Bahl and Padmanabhan found similar limitations when using propagation models, so they suggest substituting the general model for an *empirically-built model* [4]. They found that location accuracy improved if a map of the RSS was constructed by measuring the RSS at different points in the area of interest. The mobile station can find its position by comparing the received signal strength with the information in the map.

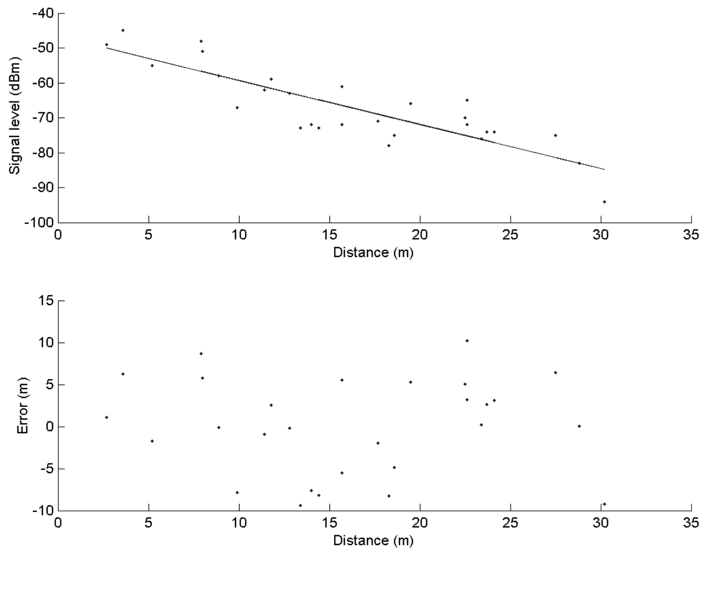

Figure 1: Received signal level versus distance (top) and error versus distance if the linear model is used (bottom)

Figure 2 presents the RSS map for an office floor. It was created by measuring the RSS corresponding to the beacon broadcasted from the access point at position (22,14) (shown by a black dot in the figure). We took measurements at 25 locations distributed around the office. Each measurement is the average of the RSS of 10 consecutive beacons. A linear interpolation was used to calculated values in between measured locations. The figure shows, color-coded, the resulting RSS in dBm.

While creating the map, several limitations of this approach were revealed. First, this map is only valid for a particular WLAN card model. Large differences were observed when using cards from different vendors. Second, the map changes with the orientation and height above the floor of the measuring laptop. Third, there are large connected areas with the same RSS. A laptop could be moved from some offices to the office besides crossing the corridor and still measuring the same RSS. Fourth, there are several unconnected areas with the same RSS. This means that a single reading of the RSS cannot determine the position in the map, but a set of possible locations.

The solution to this last problem is recording the RSS as the mobile station moves. The sequence of RSSs is likely to be unique. This approach has been positively evaluated in [4]. However, recent studies on the usage of WLANs showed that the users do not move when using the WLAN connection [7]. They remain mainly static. Therefore, this scheme can hardly be used in practice.

We can conclude that the lack of good radio propagation models for indoor environments limit the accuracy of range estimation based on RSS. An alternative would be to use empirically-built RSS maps. But they require a non-changing environment (e.g. fixed furniture) and using always the same WLAN devices. So, different range estimators should be researched.

3 Limitations of range estimation based on time of arrival measurement

A promising alternative for range estimation in WLAN is measuring the propagation time. The radio signals propagate at the speed of light, so if a station knows when the signal left from the AP and measures when it arrives (time of arrival), it can calculate the propagation time and convert it to the distance to the AP. This technique presents the following limitations when applied to wireless LANs.

The resolution in the range estimation when using time of arrival is limited by the resolution of the frame timestamp. Since the propagation of the radio signal is approximately the speed of light, a timestamp resolution of 1 ns would yield a position resolution of 30 cm. However, such high resolution cannot be achieved due to the regulatory restrictions in the 2.44 and 5.78 GHz bands used for wireless LANs. A practically reachable resolution is 3.8 meters [5].

The multipath propagation is one of the major sources of error in TOA measurements. Multipath propagation means that the radio signal reaches the receiver via a Non-Line-Of-Sight (NLOS) path when an obstacle blocks the direct path. This makes the receiver appear further away than it actually

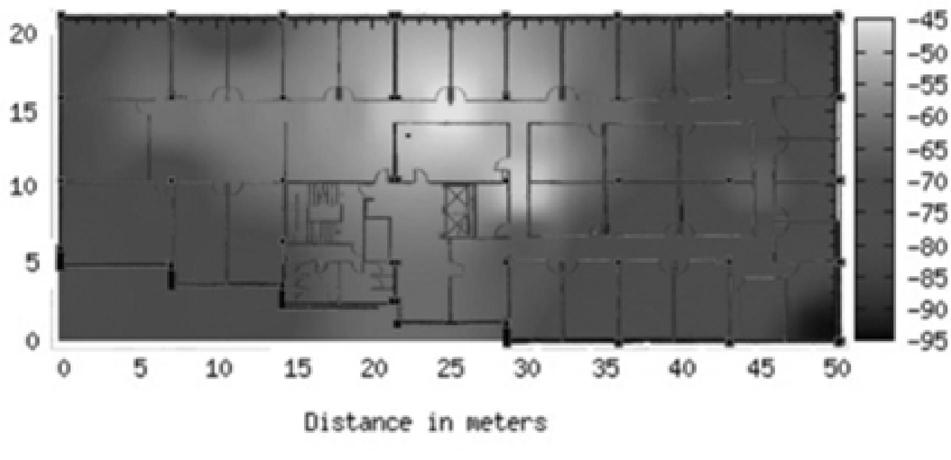

Figure 2: Measured received signal level in dBm (color coded) as a function of position

is. This problem is particularly acute for outdoor wireless positioning. In this area, several models have been proposed to estimate the multipath error (e.g. [6]). However, multipath error is not a mayor concern for TOA measurements for indoor wireless LANs, particularly when the resolution is already limited to roughly 4 meters due to regulation restrictions. The short distance between access point and receivers, the limited transmitted power and the materials typically used inside buildings contribute to minimize the relevance of the multipath error.

On the other hand, an important source of error is the architecture of wireless LAN receivers. A typical receiver runs an operating system (OS) in the main board that interfaces with the wireless LAN card via interruptions. The WLAN card internal processor triggers an interruption upon the reception of a frame. The OS will set the timestamp when the interruption is attended. This scheme cannot guarantee a timestamp with a resolution of few nanoseconds as required for range estimation. The load in the operating system can delay the attention of the interruption up to several microseconds.

Moving the timestamp from the OS to the processor in the WLAN card is not plausible. The OS needs the timestamps in the frames referred to the same clock regardless of their incoming interface. Maintaining synchronized clocks among all interfaces with a resolution of nanoseconds is not feasible to implement.

We find a better approach to have two timestamps per frame. The frame would be stamped firstly by the WLAN interface with very high resolution. Then it would receive a second timestamp indicating its reception by the OS. The first timestamp would be used for range estimation; while the OS kernel would use the second to sort frames by time of arrival. This approach is currently implemented in the Linux beta drivers for Prism-based WLAN cards[1]. Unfortunately, current WLAN chipsets feature a 1-microsecond resolution in the timestamp, which is far from the needs for TOA range estimation. Since this resolution is enough for the operation of the WLAN channel access procedure, it is unlikely that chipset manufacturers will improve the resolution.

Another problem when using time measurements to estimate range is the need for synchronized clocks when using TOA or TDOA. It is not feasible to have a GPS receiver or an atomic clock per access point or mobile station, thus remote synchronization is required. But state of the art remote synchronization protocols, such as Simple Network Time Protocol (SNTP), cannot keep clocks synchronized in a range shorter than microseconds [8].

To overcome the problems with clock synchronization, we have designed a method to measure the increase in propagation time that does not require it. We suggest using the beacon reception time to estimate the increase in distance from the receiving station to the access point. The beacon is a management frame broadcasted at regular intervals. Each beacon includes, among other information, the time interval to wait for the next beacon.

[1] http://www.shaftnet.org/~pizza/software/capturefrm.txt

Figure 3 presents our proposed procedure. It shows the events at the AP and station during the transmission of two consecutive beacons. Firstly, in the AP the first beacon appears on the air after T_{R1}, which is the transmission time for the first beacon. The second beacon is generated after the beacon interval (T_{B1}) and appears on the air after its transmission time T_{R2}. The beacons are received at the station after their corresponding propagation delay T_{P1} and T_{P2}, respectively. The station measures the time between the arrivals of the beacons, shown as T'_{B1}.

After the reception of the second beacon, the station can calculate the increase in propagation delay as follows:

$$T_{B1} - T'_{B1} = (T_{R1} - T_{R2}) + (T_{P1} - T_{P2}) = (T_{R1} - T_{R2}) + \Delta T_P \qquad (3)$$

In Equation (3), the transmission times T_{R1} and T_{R2} are the only unknown. The station measures the time between received beacons T'_{B1}, and the beacon interval T_{B1} appears in the header of the first beacon. The station can calculate the transmission time with some extra information. The transmission time is the time that needed the access point to gain access to the channel for the beacon transmission. It depends on the cell traffic, but the station can calculate it since the WLAN MAC protocol operation mandates a constant monitoring of the channel usage.

The channel access procedure to transmit the beacon is as follows. When the beacon is ready to transmit, the AP waits until the current transmission, if any, finishes. This is the initial waiting time. Then, it randomly chooses a number between 0 and 31. This is the number of 50 microsecond slots that the channel must be idle before the AP can transmit. Since the station monitors the channel, it can calculate the transmission time if the initial waiting time and the number of slots is known. Unfortunately, these values are not included in the beacon information. We suggest including them to permit time-based range estimation in WLANs. This extension of the beacon payload would not noticeably damage the capacity of the radio cell because it only affects to the beacons, not to regular data frames.

We would like to mention that the hidden node problem could not affect the correct calculation of the beacon's transmission time. In a WLAN cell, it is possible that two stations A and B communicate with the AP, but they cannot sense each other. A is said to be a hidden node to B and vice versa. A could temporarily consider the channel idle while B is transmitting to the AP, but it will discover the mistake when the acknowledgement sent from the AP to confirm the reception of B's frame is

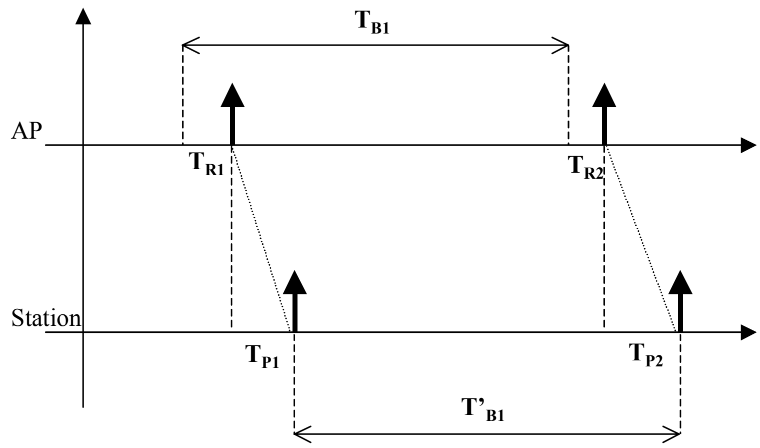

Figure 3: Relation between beacon transmission and reception

received. Thus, A can detect the hidden node problem and discard the incorrect transmission time measurements.

Due to the limited resolution of the frame timestamp mentioned above, the procedure as described in Figure 3 can only detect the movement of the stations if it is larger than 4 meters between consecutive beacons. Since the beacon interval is typically 100 ms, this would mean that the station's speed is at least 144kmh. To be able to detect more realistic station's speeds, we suggest comparing the increase in propagation delay between one reference beacon and later non-consecutive ones until a 4 meters movement is detected. At this time, the last beacon would be the new reference for future comparisons and the range estimation would be increased or decreased by 4 meters.

Figure 4 shows this situation. Propagation delay for beacon 1 can be directly compared to propagation delay for beacon 4 using the following formula:

$$\sum_{i=1}^{3} T_{Bi} - \sum_{i=1}^{3} T'_{Bi} = (T_{R1} - T_{R4}) + (T_{P1} - T_{P4}) = (T_{R1} - T_{R4}) + \Delta T_P \tag{4}$$

Equation 5 shows the general formula to compare the increase in propagation delay between the first beacon and an arbitrary later beacon *n:*

$$\sum_{i=1}^{n-1} T_{Bi} - \sum_{i=1}^{n-1} T'_{Bi} = (T_{R1} - T_{Rn}) + (T_{P1} - T_{Pn}) = (T_{R1} - T_{Rn}) + \Delta T_P \tag{5}$$

Finally, we should indicate that this method measures increases or decreases in the distance between the AP and station in steps of 4 meters. To determine the physical position of the station with respect to some reference system, one initial position of the station must be known.

4 Conclusions

Several research studies and commercial products suggest using the received signal strength (RSS) as the range estimation for positioning in WLANs. We have analyzed its limitations and shown the difficulties to overcome them in practice. We have also looked at a promising alternative, the time of arrival (TOA) range estimation. We found that it could perform better in practice since the impact of

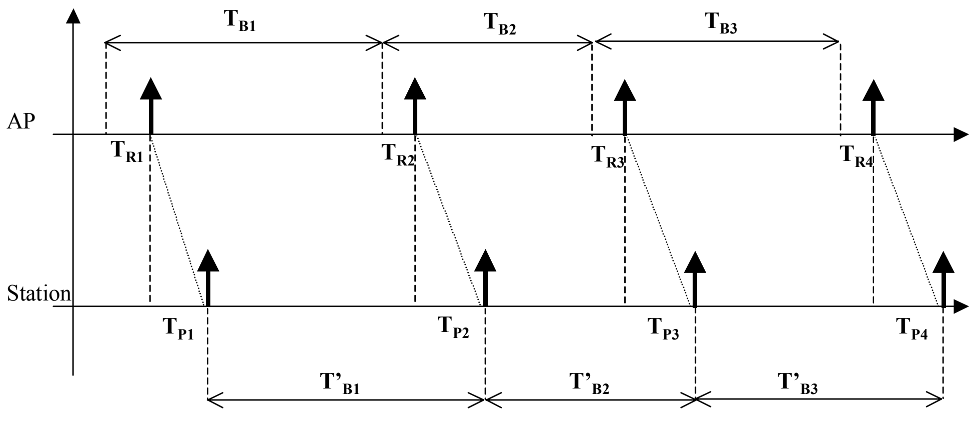

Figure 4: Comparing beacon's propagation delay increase between non-consecutive beacons

the surrounding environment would be less important. But real life experiments are not possible due to the low resolution in the timestamp of the current WLAN chips. Nevertheless, we have suggested a novel approach to measure the variations in range between the AP and the station that does not require synchronized clocks.

References

[1] Ekahau, Inc. Ekahau Positioning Engine, September 2003.
[2] "An Introduction to Indoor Radio Propagation", Spread Spectrum Scene, June 2001, http://www.sss-mag.com/indoor.html
[3] S. Y. Seidel and T. S. Rapport, "914 MHz path loss prediction Model for Indoor Wireless Communications in Multi-floored buildings," IEEE Trans. on Antennas & Propagation, Feb. 1992
[4] Paramvir Bahl and Venkata N. Padmanabhan, "RADAR: An In-Building RF-based User Location and Tracking System", In Proceedings of IEEE Infocom 2000, 2000.
[5] Kaveh Pahlavan, Xinrong Li, Mika Ylianttila, Ranvir Chana, Matti Latva-aho, "An Overview of Wireless Indoor Geolocation Techniques and Systems", In Proceedings of IEEE MWCN 2000, pages 1-13, 2000.
[6] Marilynn P. Wylie-Green and S.S. (Peter) Wang, "Robust Range Estimation in the Presence of the Non-Line-of-Sight Error", In Proceedings of IEEE VTC Fall 2001, volume 1, pages 101-105, 2001.
[7] Anand Balachandran, Geoffrey M. Voelker, Paramvir Bahl, P. Venkat Rangan, "Characterizing User Behavior and Network Performance in A Public Wireless LAN". In Proceedings of ACM SIGMETRICS 2002, 2002.
[8] D. Mills, "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI", IETF RFC 2030, Oct 1996.