TKN Telecommunication Networks Group

Technical University Berlin

Telecommunication Networks Group

# Measuring Round Trip Times to Determine the Distance between WLAN Nodes

André Günther, Christian Hoene

anguenther@gmx.de, hoene@ieee.org

Berlin, 18. December 2004

TKN Technical Report TKN-04-16

TKN Technical Reports Series

Editor: Prof. Dr.-Ing. Adam Wolisz

## Abstract

This technical report explores the degree of accuracy to which the propagation delay of WLAN packets can be measured using today's commercial, inexpensive equipment. The aim is to determine the distance between two wireless nodes for location sensing applications. We conducted experiments and measured the time difference between sending a data packet and receiving the corresponding immediate acknowledgement. We found the propagation delays correlate closely with the distance, having only a measurement error of a few meters. Furthermore, they are more precise than the received signal strength indications.

To overcome the low time resolution of the given hardware timers, various statistical methods are applied, developed and analyzed. For example, we take advantage of drifting clocks to determine propagation delays that are forty times smaller than the clocks' quantization resolution. Our approach also determines the frequency offset between remote and local crystal clocks.

# Contents

# Chapter 1

# Introduction

Knowing the distance between wireless nodes is required for location-aware services and applications. The distance helps to calculate the position of wireless nodes, to decide the time of handovers, or to find the optimal routing path throughout an ad-hoc network.

A couple of approaches for in- and outdoor location sensing techniques have been presented [1]. In this paper we focus on locating techniques which use the intrinsic features of WIFI based wireless access. The RADAR system [2] has been one of the first approaches presenting an indoor positing system based on WLAN components – others have followed ( [3–9] and the references therein). An essential part of location sensing algorithms is a method to determine the distance between two wireless nodes. In general, three methods have been considered:

1. The information, which nodes are within transmission range, is used to estimate the distance. This approach benefits from densely populated networks such as sensor networks [10].

2. The received signal strength indication (RSSI) of data packets is considered as it decays with distance. Actually, the RADAR system and most other proposals are based on RSSI. Because RSSI decreases sharply in a non-linear fashion with distance, signal strength maps have to be gathered to relate the RSSI values with positions. Generating these maps is time-consuming and it has to be redone if the environment changes.

3. The propagation time of radio signals can be used because in free air it linearly increases with the distance. Such an approach is usually considered to be impossible without the help of special signal processing hardware [11].

In this paper we show that precise location positioning based on round trip time measurements of WLAN packets is indeed possible even with low-cost, commercial WLAN hardware. We developed the algorithms to determine indirectly the air propagation time and to improve the accuracy and resolution of the time measurements. We validated our approach with two independent experimental measurement campaigns and with an analytical explanation.

We take advantage of an intrinsic feature of IEEE 802.11: Each data packet is immediately acknowledged by its receiver (Figure 1.1). We measure the time between starting the transmission of a data packet and receiving the corresponding immediate acknowledgement. We will refer to this as remote delay ($t_{remote}$). We also measure the duration of receiving one data packet and sending out the

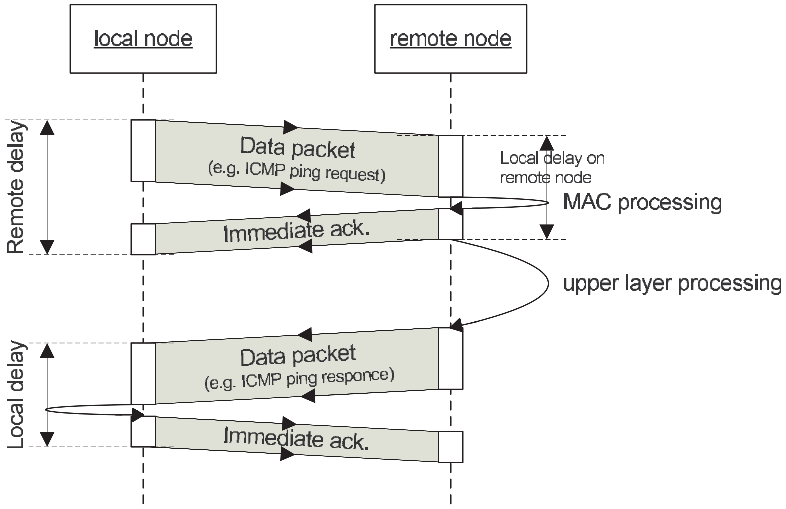


Figure 1.1: Distance Measurement: ICMP Ping sequence diagram.

immediate acknowledgement. We will call this duration local delay ($t_{local}$). The overall propagation time is then estimated by subtracting the local time from the remote delay (1.1).

$$c = \frac{2 \cdot distance}{t_{remote} - t_{local}} \text{where } c \approx 3 \cdot 10^8 \frac{\mathrm{m}}{\mathrm{s}} \text{ being the speed of light.} \qquad (1.1)$$

The most difficult part of this work was to cope with the low resolution of the clocks: If the operating system records the time stamps of outgoing and incoming packets, the variable interrupt latency falsifies the results. Most WLAN solutions allow to record time stamps at a resolution of 1 $\mu$s. However, packets travel a distance of 300 m in 1 $\mu$s, which usually exceeds the range of WLAN transmission. We achieve a more precise resolution by using multiple delay observations and applying statistical methods to enhance the accuracy.

We take advantage of the fact that both local and remote clocks are drifting and interfere. The interference is caused by the data-acknowledgement sequence. As a result the observations contain a beat frequency that is equal to the frequency offset of local and remote clock crystals. The beat frequency introduces measurement noise, which we utilize to identify a weak signal below the timers' quantization resolution. The weak signal is the propagation delay.

This paper is structured as follows: In chapter 2 we refer to the state of the art. Then we explain our approaches to enhance the measurement resolution. In chapter 4 and 5 we describe our experimental measurement campaigns. Finally, we briefly summarize the results and contributions of this paper.

# Chapter 2

# Related Work

In the realm of Information Technology, the classic approach estimates the time of arrival (TOA) of pure radio signals (instead of WLAN packets) for position location purposes. This is conducted by applying signal processing algorithms based on cross-correlation techniques [12]. The received signal resembles the initial transmitted signal delayed by propagation delay. The autocorrelation function for the transmitted signal accounting shows its maximum peak for a certain shift in time ($\tau$ = time lag). TOA based time measurements require synchronised clocks. Although TOA as a ranging metric is considered to be the most popular technique for accurate indoor positioning [13], the method suffers from multi-path conditions. The difficulty is to determine the autocorrelation peak referring to signal travelling along the direct line of sight (DLOS). The problem can be encountered with a wider frequency band, e.g. ultra-wide band.

TOA measurement is being employed both outdoors for GPS-positioning [14] and indoors to find things and people marked by a tag [15]. In the latter paper, the author gives an appraisal of the achievable accuracy when measuring the round trip TOA within the 2.44 GHz and 5.78 GHz bands. For a signal bandwidth of 40 MHz, the accuracy of 3.8 m can be an achievable resolution limit unless further signal processing techniques are applied. Those might enhance the resolution up to 1 m.

The only paper focussing on measuring pure packet propagation delays is [16]. It has actually inspired this work. The objective is to determine the speed of light using the averaged measured round trip propagation delay of many ping packets and the known distance between the sender and receiver. The measurements were conducted in a wired Ethernet infrastructure. Estimating the propagation delay which ranges below the clock resolution was facilitated by employing the concept of noise-assisted sub-threshold signal detection. The aim of this work is to teach students the effect of stochastic resonance [17] and to explain how to enhance the resolution. For measurements in an IEEE 802.11b wireless environment the round trip times were too variable and noisy to be used.

# Chapter 3

# Approach

The presented approach is based on the ideas of [16]. We use the round trip time delay of packets to determine the distance as given in (1.1). In order to further enhance the measurement resolution, we utilize the IEEE 802.11 data/acknowledgement sequence instead of the ICMP-Ping request/response packet sequence. Also, we measure the time stamps not in the operating systems but on the WLAN card, which is not subject to variable interrupt latencies. Let us explain these enhancements:

The ping response is generated by operation systems and thus subject to a highly variable delay. In contrast, the immediate acknowledgements are handled by the hardware of the WLAN radio and highly predictable: On standardized IEEE 802.11 the MAC processing time (SIFS interval) is 10 $\mu$s (802.11b) or 16 $\mu$s (802.11a) with a tolerance up ±25 ppm resp. ±20 ppm. Acknowledgements are valid only if they are received after the SIFS interval with a tolerance of ±2 $\mu$s resp. ±0.9 $\mu$s. Thus, if the WLAN card is implemented according to the standard, the transmission delays are highly deterministic. We can also assume that the MAC processing times on both nodes are identical. However, in this paper, we will prove that not all WLAN cards operate in compliance with the standard.

Ping round trip times are measured in the operating system's kernel, for example during an interrupt. In [18] we showed that OS time measurements are quite imprecise due to variable interrupt latency. In our experiments, about 5% of the time stamps have an error of more than 2 ms. Also, in our experiments OS time measurements did not work if applied for distance measurements. Instead, we utilized the WLAN cards to record the transmission and arrival times of packets. These time measurements are not falsified by interrupt latency, because they are conducted by the hardware. The resolution of these hardware time stamps implemented in most current WLAN products is 1 $\mu$s, which is still not precise enough because it is equal to 300 m.

The accuracy of delay measurements is hampered by a discrete time resolution. The resolution increases with multiple observations being combined and smoothened. This has the drawback that the determination of changes over time – e.g. due to node movement – is slower. In the following we discuss, which phenomena are considered to achieve a higher resolution using the mean of multiple observations.

## 3.1 Gaussian noise

The presence of measurement noise is assumed. Thus, the delay values are not limited to only one value. (In Figure 3.1 not only 323 $\mu$s can be observed but also other values). If one assumes a

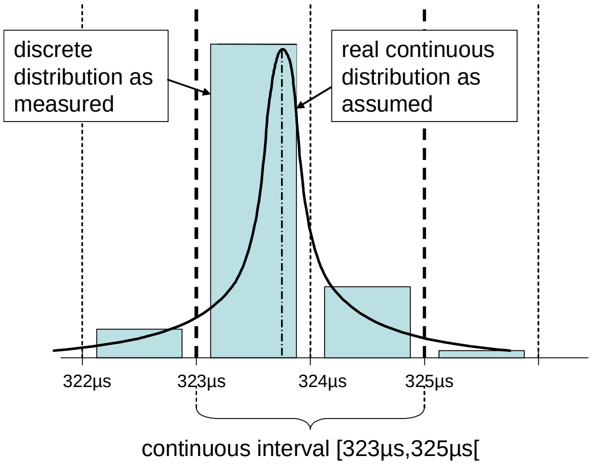


Figure 3.1: Discrete distribution of noisy delay measurements.

Gaussian noise distribution with a suitable strength, we can simply take the sample mean to enhance the resolution [19]. Also, it can be expected that different discrete delay values occur entirely random.

But which effects introduce noise? The measurement noise can be caused by thermal noise present in the received radio signal. Thus, the synchronization to the modulation symbols might vary. In the presence of a multi-path environment, the dominant propagation path might vary leading changes in the propagation delay. Also, the crystal clocks of the WLAN equipment are subject to a constant clock drift and variable clock noise.

## 3.2 Stochastic Resonance

Instead of the explanation above the authors of [16] suggested another statistic effect called stochastic resonance. The concept of stochastic resonance was originally introduced as an explanation for the periodically recurrent ice ages. In the last two decades, it has been applied to explain many physical phenomena [17, 20]. In the realm of signal detecting [21] stochastic resonance allows for detecting signals below the resolution of the measuring units because the signal becomes detectable with the help of noise. Noise adds to the signal so that it eventually exceeds the threshold given by the resolution of the detecting device.

For example, in a bi-stable system a state change occurs only if the weak signal added to the noise signal is higher than a barrier between both states. The length of the period that the system stays in one state is random. If one measures discrete values, the probability is high, that one value remains the same for the next observation. This effect results in blocks of the same values and these blocks have random lengths.

## 3.3 Beat Frequencies

In our experiments (Figure 4.3) it can be observed that the occurrence of 323 and 324 values occur in block of regular patterns. But this effect cannot be explained with the effect of stochastic resonance.

Another effect can also entail resolution enhancement even if measurement noise is missing: Both WLAN cards are driven by built-in crystal oscillators that have nearly the same frequency. Due to tolerances, there is a slight drift between both clocks. If two frequencies interfere, a so called beat frequency is produced. The beat frequency is the difference of both frequencies.

$$f_{beat} = |f_1 - f_2| \tag{3.1}$$

Let us consider the impact of discrete time resolution on the measurement error. First, we construct a model of the experiment setups. Instead of using packets we assume that a delta pulse is sent from the local to the remote node. After the delta pulse's arrival another delta pulse is sent from the remote to the local node representing an acknowledgement. The local node can process the impulses only in discrete time steps $loc \in \mathbf{N}$ described with natural numbers.The remote node also reacts only in discrete time steps, which are $rem = \delta + n$ where $n \in \mathbf{N}$ and phase offset of $\delta \in [0; 1[$. We assume that the clocks work at the same speed but a phase offset is present. The phase offset changes over time but not for the duration of a round trip. The transmission of a delta impulse from one node to the other takes the time of $dist \in \mathbf{R}^+$, which is equal to the propagation time.

Let us assume that a delta impulse is sent out from the local node at time $loc_{out}$. It arrives at the remote node $dist$ times later. Due to the discrete MAC processing, the delta impulse is only identified at the next clock impulse, which is:

$$rem = \lceil (loc_{out} + dist) - \delta \rceil + \delta \tag{3.2}$$

At the same time, the remote node sends back a delta impulse representing the acknowledgement. It arrives at the local node $dist$ times later, but is again recognized only at the next clock, which is

$$loc_{in} = \lceil rem + dist \rceil \tag{3.3}$$

Then, the observed round trip time *rtt* is (3.4). It is display in Figure 3.2.

$$\begin{aligned} &rtt = loc_{in} - loc_{out} \\ &= \lceil \lceil loc_{out} + dist - \delta \rceil + \delta + dist \rceil - loc_{out} \\ &= \lceil dist + \delta \rceil + \lceil dist - \delta \rceil \end{aligned} \tag{3.4}$$

Next, we assume that the phase changes during the measurement. The change is constant and repeats after each phase period starting at zero again. In the following, we only consider one phase period and assume that round trip times are measured at all times. Thus, the number of observations is infinite. The mean $rtt$ over all phase offsets is calculated as follows.

$$\begin{aligned} &\overline{rtt} = \int_0^1 rtt \, d\delta \\ &= \int_0^1 \lceil dist + \delta \rceil + \lceil dist - \delta \rceil \; d\delta \\ &= \; 2 \cdot dist + 1 \end{aligned} \tag{3.5}$$

The variance of the quantization error is calculated as followed and is simplified to a cubic function of the fractional part of the round trip distance. Both the mean and variance are displayed in Figure 3.3.

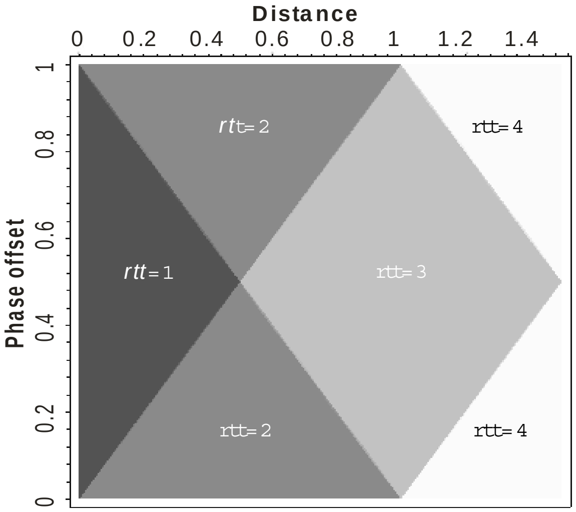


Figure 3.2: Round trip time versus distance and phase offsets

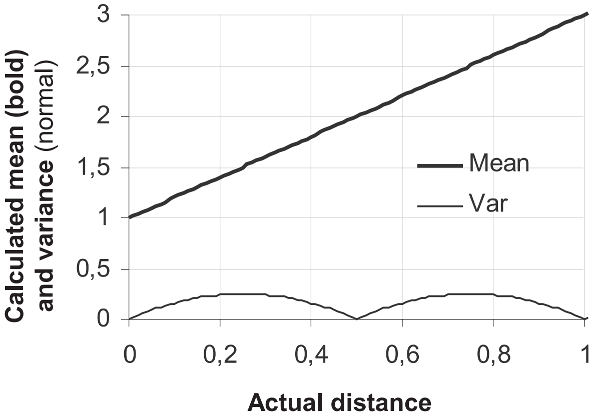


Figure 3.3: Theoretical mean distance and variance of distance.

$$\begin{aligned}\sigma^2 &= \int_0^1 \left(\overline{rtt} - rtt\right)^2 \, d\delta \\ &= \{2dist\} - \{2dist\}^2 \\ &= \tfrac{1}{4} - \left(\{2dist\} - \tfrac{1}{2}\right)^2\end{aligned} \tag{3.6}$$

The $rtt$ function produces a pattern repeating every phase period. This reoccurrence introduces a frequency component to be present in the observations. If two clocks interfere, their phases are equal every beat period (the reciprocal of the beat frequency). Thus, the impact of quantization errors causes a similar effect as the two interfering waves – namely a beat frequency.

## 3.4 Limits and Verification

The accuracy of location and distance sensing algorithms have fundamental limits [22–26]. For example, the analytic calculations above do not take into account the clock drift during one RTT observation. Assuming a frequency stability of ±25 ppm and a length of a transmission sequence of 60 $\mu$s and 320 $\mu$s, the maximal error could be up to 0.9 m and 4.8 m respectively.

Furthermore, one should note that only in vacuum light travels at the speed of light $c$. In materials the propagation speed depends on the square root of the dielectric constant $\varepsilon$. For example, dry ferroconcrete has an $\varepsilon$ of about 9 and electromagnetic waves traverse through ferroconcrete 3 times slower than in vacuum. Most other materials used in buildings have lower dielectric constants.

Another source of possible errors is due to non-line-of-sight conditions. This results in an overestimation of the distance between the two nodes [27]. Multipath propagation might introduce measurement errors because the dominant path can vary depending on the current transmission conditions. Multipath propagation is present only if reflections are given. Reflections can have large impact on signal strength but only a low one on propagation delay. Thus, in the presence of multipath propagation or reflections, we assume time delay measurement as being more precise than those based on the RSSI.

In order to check these hypotheses and identify the real measurement resolution, we conducted experiments. The first measurement campaign was conducted to study the impact of slow-user motion on packet loss and delay as described in [18]. At the same time, we also measured the impact of distance on the round trip times. One year later, we embarked on a second measurement campaign. We altered the radio modem technology, the location, the analysis software, and the staff. Thus, we proved the reliability and correctness of our approach.

# Chapter 4

# Measurements: First campaign

## 4.1 Experimental setup

The measurement was done in a gymnasium (Figure 4.1 and 7.6) [18]. The data communication takes place between the local and the remote node. ICMP ping packets were transmitted each 20 ms. The measurements of RTT were conducted for several distances (5, 10, 15, 20, 25, 30, 35, 40 m). At each distance, we measured for about 15 minutes. One should note that in this first campaign, the wireless LAN cards were close to the ground. Also, the directions of the antennas were selected at random and were not recorded. This is important to know, because it explains some of the results presented later.

## 4.2 Equipment

All PCs were running a Suse 6.4 Linux system with a 2.4.17 kernel. D-Link cards featuring an Intersil's (now Conexant) Prism2 chipset were employed as a wireless interface. Packets were directly sniffed on the MAC layer by the measurement tool 'Snuffle' [28].

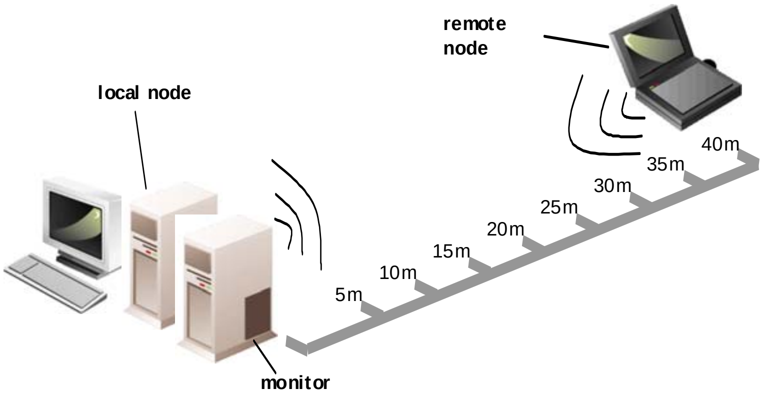


Figure 4.1: First measurements: schematic experimental setup.

## 4.3 Configuration

WLAN networking technologies based on the IEEE 802.11 standards transmit data packets via air. Each data packet that is addressed to only one receiver is immediately acknowledged if it is received without errors. The receiver must send the acknowledgement instantaneously after data packet's arrival. Thus, the sender knows whether the transmission has been successful or whether it has to be redone. To avoid potential packet delay effects, in this experiments the maximal number of retransmissions (transmission type) was set to zero.

The data packet and the acknowledgement start with a preamble followed by a Physical Layer Convergence Procedure (PLCP) header which contains the length and modulation type. The length of the preamble and header are 144+48 $\mu$s (802.11). After the PLCP header, the actually MAC frame body is sent immediately at the selected modulation type. In case of the data packets, the speed of the transmission (modulation type) was set to 11 Mbit/s. The MAC frame contains the header of MAC (24 b), IP (20 b), UDP (8 b), RTP (16 b), Voice (20 b) and the frame check sequence (4 b). Overall the MAC PDU has a length of 92 b, which takes 66.91 $\mu$s to transmit. Thus, the overall length of the data packet is 258.91 $\mu$s. The acknowledgement is shorter. The ACK frame has a length of only 10 b plus the CRC (4 b). At 2 Mbit/s it has a transmittion time of 192+56=248 $\mu$s. Between the data packet and the acknowledgement the receiver waits of the Short Interframe Space (SIFS), which has a length of 10 $\mu$s.

## 4.4 Time measurements

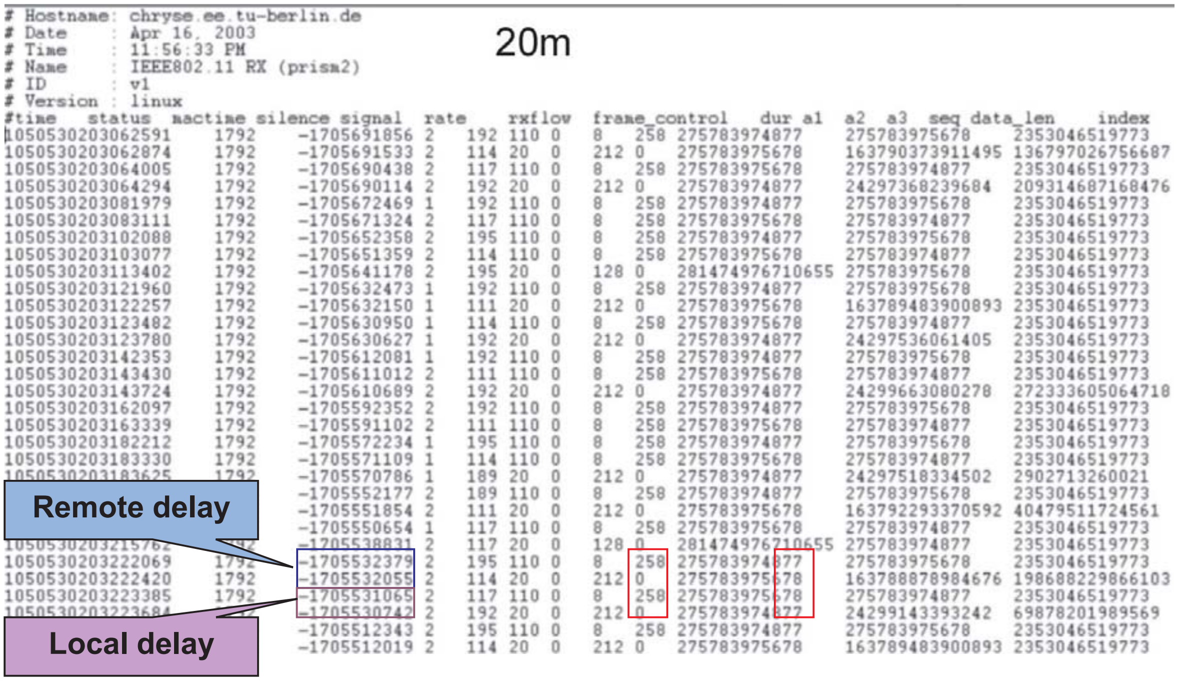
The WLAN card recorded the arrival time of packets at a resolution of 1 $\mu$s without any variable latency. The precise point of time, at which the time stamp is recorded, is not documented. In case of the data packet, we assume that the arrival time is recorded at the start of the MAC packet. In case of the acknowledgement, it might be recorded after the MAC header. Thus, the local delay for the given configuration is about 66.91+10+192+56=324.91 $\mu$s. This value closely fits the measured delay.

The Prism2 cards implement only the recording time stamps of incoming packets. But we needed both sending and receiving time stamps. Therefore, we decided to use a third PC to monitor the packets which the local node sends and receives. The monitor PC was placed close-by the sender to avoid any additional propagation delays that could falsify the measurements.

It will be straight forward to alter software and firmware of WLAN cards to record transmission time stamps, too. Due to legal constraints, we were not able to implement these changes by ourselves. We expect that WLAN chipset manufactures will provide firmware updates to support precise time stamps because they will benefit from customers using WLAN for location-aware services. Until then, we are required to use the third monitoring node.

## 4.5 Data collection & processing

Snuffle provides the packet traces of all 802.11 packets received at the monitoring node. We filtered-out only the successful ping sequences which consist of an ICMP request, an acknowledgement, an ICMP response and again an acknowledgement (Figure 4.2). Other packets like erroneous transmissions, beacons, ARQ messages etc. are dropped. Due to hardware limitations of the WLAN card only a fraction of observations were recorded (Table 4.1).



```
# Hostname: chryse.ee.tu-berlin.de
# Date    : Apr 16, 2003
# Time    : 11:56:33 PM
# Name    : IEEE802.11 RX (prism2)
# ID      : v1
# Version : linux
#time    status  mactime silence signal  rate    rxflow   frame_control   dur a1  a2  a3  seq data_len     index
1050530203062591     1792     -1705691856 2   192 110 0   8   258 275783974877      275783975678      2353046519773
1050530203062874     1792     -1705691533 2   114 20  0   212 0   275783975678      163790373911495 136797026756687
1050530203064005     1792     -1705690438 2   117 110 0   8   258 275783975678      275783974877      2353046519773
1050530203064294     1792     -1705690114 2   192 20  0   212 0   275783974877      24297368239684   209314687168476
1050530203081979     1792     -1705672469 1   192 110 0   8   258 275783974877      275783975678      2353046519773
1050530203083111     1792     -1705671324 2   117 110 0   8   258 275783975678      275783974877      2353046519773
1050530203102088     1792     -1705652358 2   195 110 0   8   258 275783974877      275783975678      2353046519773
1050530203103077     1792     -1705651359 2   114 110 0   8   258 275783975678      275783974877      2353046519773
1050530203113402     1792     -1705641178 2   195 20  0   128 0   281474976710655 275783975678      2353046519773
1050530203121960     1792     -1705632473 1   192 110 0   8   258 275783974877      275783975678      2353046519773
1050530203122257     1792     -1705632150 1   111 20  0   212 0   275783975678      163789483900893 2353046519773
1050530203123482     1792     -1705630950 1   114 110 0   8   258 275783975678      275783974877      2353046519773
1050530203123780     1792     -1705630627 1   192 20  0   212 0   275783974877      24297536061405   2353046519773
1050530203142353     1792     -1705612081 1   192 110 0   8   258 275783974877      275783975678      2353046519773
1050530203143430     1792     -1705611012 2   111 110 0   8   258 275783975678      275783974877      2353046519773
1050530203143724     1792     -1705610689 2   192 20  0   212 0   275783974877      24299663080278   272333605064718
1050530203162097     1792     -1705592352 2   192 110 0   8   258 275783974877      275783975678      2353046519773
1050530203163339     1792     -1705591102 2   111 110 0   8   258 275783975678      275783974877      2353046519773
1050530203182212     1792     -1705572234 1   195 110 0   8   258 275783974877      275783975678      2353046519773
1050530203183330     1792     -1705571109 1   114 110 0   8   258 275783975678      275783974877      2353046519773
1050530203183625     1792     -1705570786 1   189 20  0   212 0   275783974877      24297518334502   2902713260021
                              -1705552177 2   189 110 0   8   258 275783974877      275783975678      2353046519773
                              -1705551854 2   111 20  0   212 0   275783975678      163792293370592 40479511724561
                              -1705550654 1   117 110 0   8   258 275783975678      275783974877      2353046519773
1050530203215762              -1705538831 2   117 20  0   128 0   281474976710655 275783974877      2353046519773
1050530203222069     1792     -1705532379 2   195 110 0   8   258 275783974877      275783975678      2353046519773
1050530203222420     1792     -1705532055 2   114 20  0   212 0   275783975678      163788878984676 198688229866103
1050530203223385     1792     -1705531065 2   117 110 0   8   258 275783975678      275783974877      2353046519773
1050530203223684              -1705530742 2   192 20  0   212 0   275783974877      24299143393242   69878201989569
                              -1705512343 2   195 110 0   8   258 275783974877      275783975678      2353046519773
                              -1705512019 2   114 20  0   212 0   275783975678      163789483900893 2353046519773
```

Figure 4.2: Snuffle trace file showing recorded data traffic (20 m measurement)

Table 4.1: Numbers of missing, invalid and valid observations.

| distance | trace file entries | ‚good' entries | corrupted entries | share of corrupted entries |
|---:|---:|---:|---:|---:|
| 5 m | 14371 | 12722 | 1649 | 11.5% |
| 10 m | 21256 | 18450 | 2806 | 13.2% |
| 15 m | 89877 | 77440 | 12437 | 3.8% |
| 20 m | 10316 | 9344 | 972 | 9.4% |
| 25 m | 9864 | 8822 | 1042 | 10.6% |
| 30 m | 20095 | 18124 | 1971 | 9.8% |
| 35 m | 40776 | 35682 | 5094 | 12.5% |
| 40 m | 32750 | 29216 | 3534 | 10.8% |

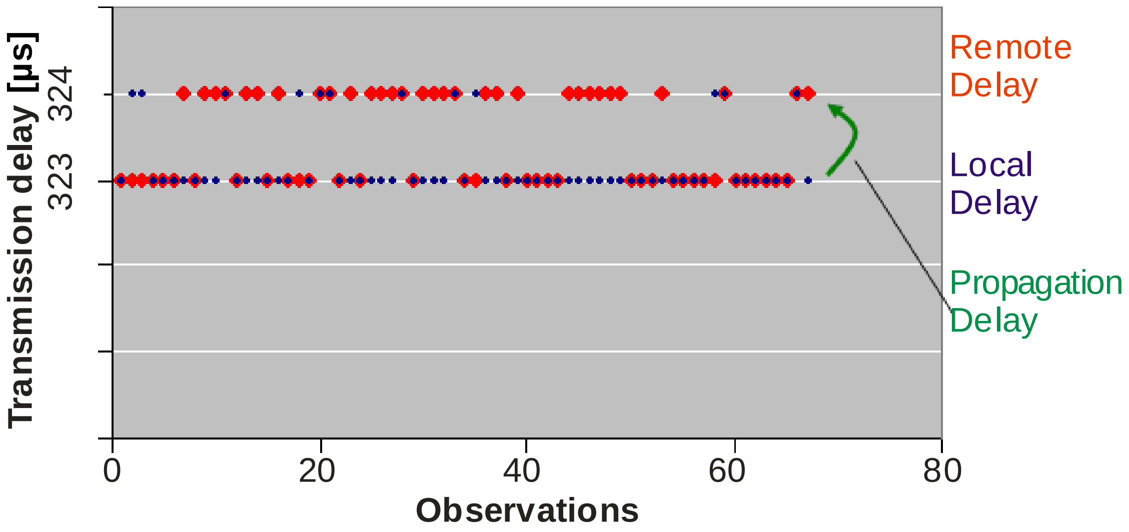


Figure 4.3: Remote and local delay observations over time.

Only the delays fitting in the interval [323 $\mu$s, 324 $\mu$s] are considered in further calculations (Figure 4.3. Only a very few delay measurements were observed with the value of 322 and 325 $\mu$s. These and all other delays were considered as measurement errors. Taken these packet sequences, the mean and variance of the remote delay and local delay were calculated. To check for stationary process properties, the autocorrelation function was calculated. The screening of data entries and the subsequent calculations were executed by a self-created C-program [29].

## 4.6 Results

The distance was directly derived from the measured propagation delay using equation (1.1). Assuming a Gaussian error distribution, we also plotted the confidence intervals in Figure 4.4 and Table 4.2. Usually, the calculated distances were always higher than the real distances. Also, in some measurements (e.g. 35 m) the air propagation time was significantly higher. Due to the experimental setup, we could not ensure that the direct line-of-sight path was taken. The remote node was placed directly on the ground. Thus, the Fresnel zone was violated and the direct transmission path was hampered. In radio communications, a Fresnel zone is a concentric ellipsoid, covering the radiation path. Fresnel zones result from diffraction by the circular aperture.

In Figure 4.5 the signal strength is displayed over the distance. Theoretically, the signal strength should decrease with distance. In this measurement campaign other factors, such as reflection, seem to be dominant. If one compares Figure 4.4 and Figure 4.5, it seems time measurements reflect the distance more precisely than RSSI but they have a higher variance and a larger confidence interval.

## 4.7 Analysis

In [29] we show that the measurements follow a weak stationary process, with a constant mean, variance and covariance (for a constant lag) (Figure 4.6). Thus, further statistical methods are applicable.

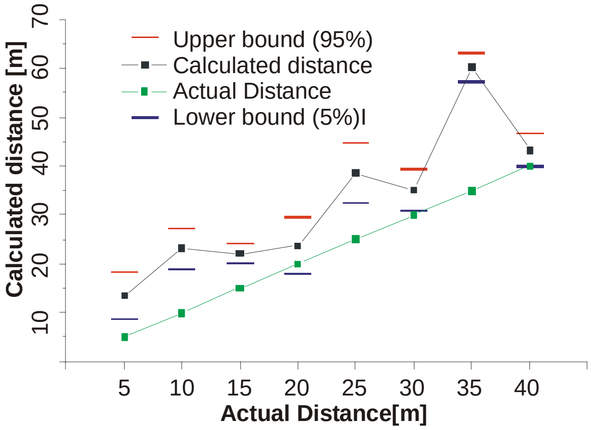


Figure 4.4: Distance as calculated from RTT versus actual distance between both nodes. 95% confidence levels are given.

Table 4.2: Delays, calculated distance and deviation versus real distance.

| actual distance [m] | remote delay [$\mu$s] | local delay [$\mu$s] | one-way delay [ns] | calculated distance [m] | standard deviation [m] |
|---|---|---|---|---|---|
| 5 | 323.297 | 323.207 | 45.0 | 13.44 | 8.4400 |
| 10 | 323.359 | 323.205 | 77.0 | 23.12 | 13.1125 |
| 15 | 323.377 | 323.230 | 73.5 | 22.07 | 7.0690 |
| 20 | 323.396 | 323.238 | 79.0 | 23.74 | 3.7395 |
| 25 | 323.465 | 323.208 | 128.5 | 38.62 | 13.6165 |
| 30 | 323.450 | 323.216 | 117.0 | 35.11 | 5.1105 |
| 35 | 323.567 | 323.166 | 200.5 | 60.21 | 25.2050 |
| 40 | 323.481 | 323.192 | 144.5 | 43.31 | 3.3090 |

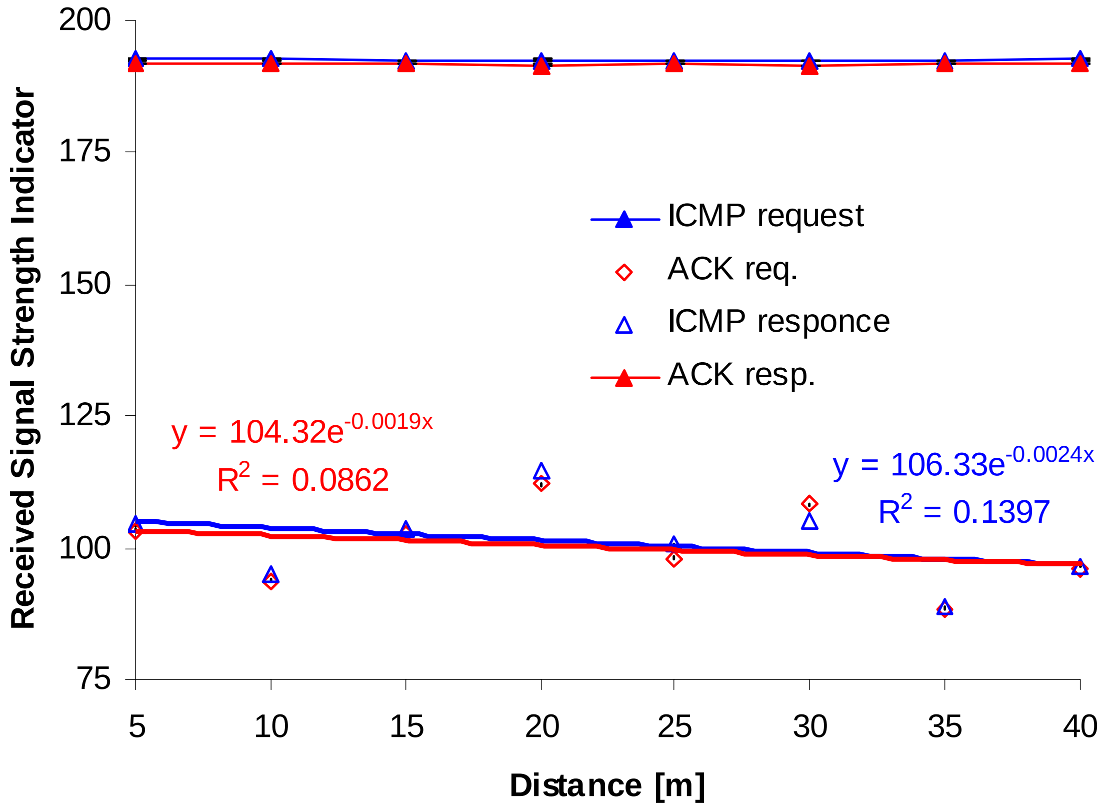
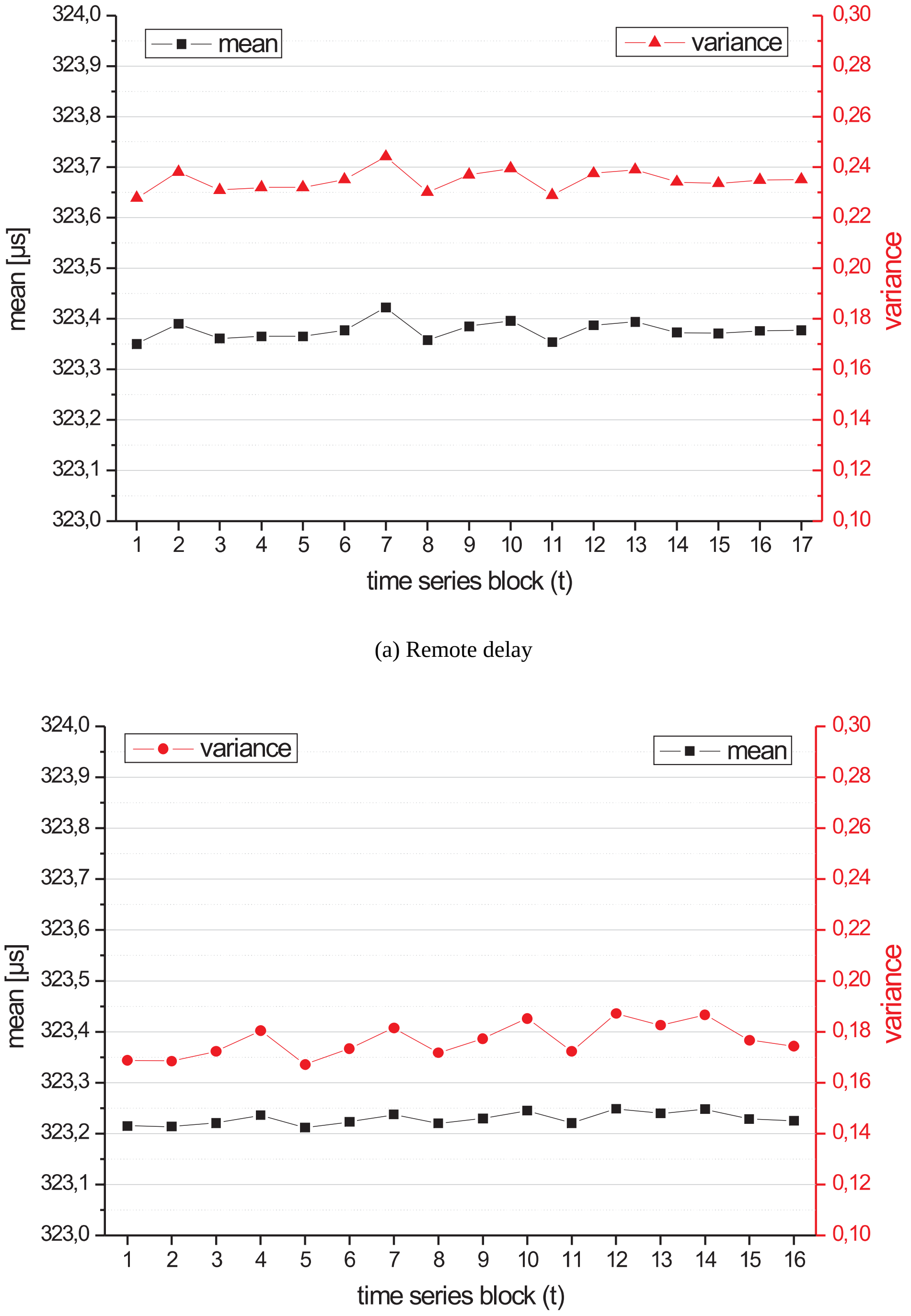


Figure 4.5: Received signal strength indication versus distance. Confidence intervals are too small to be shown.



(a) Remote delay

(b) Local delay

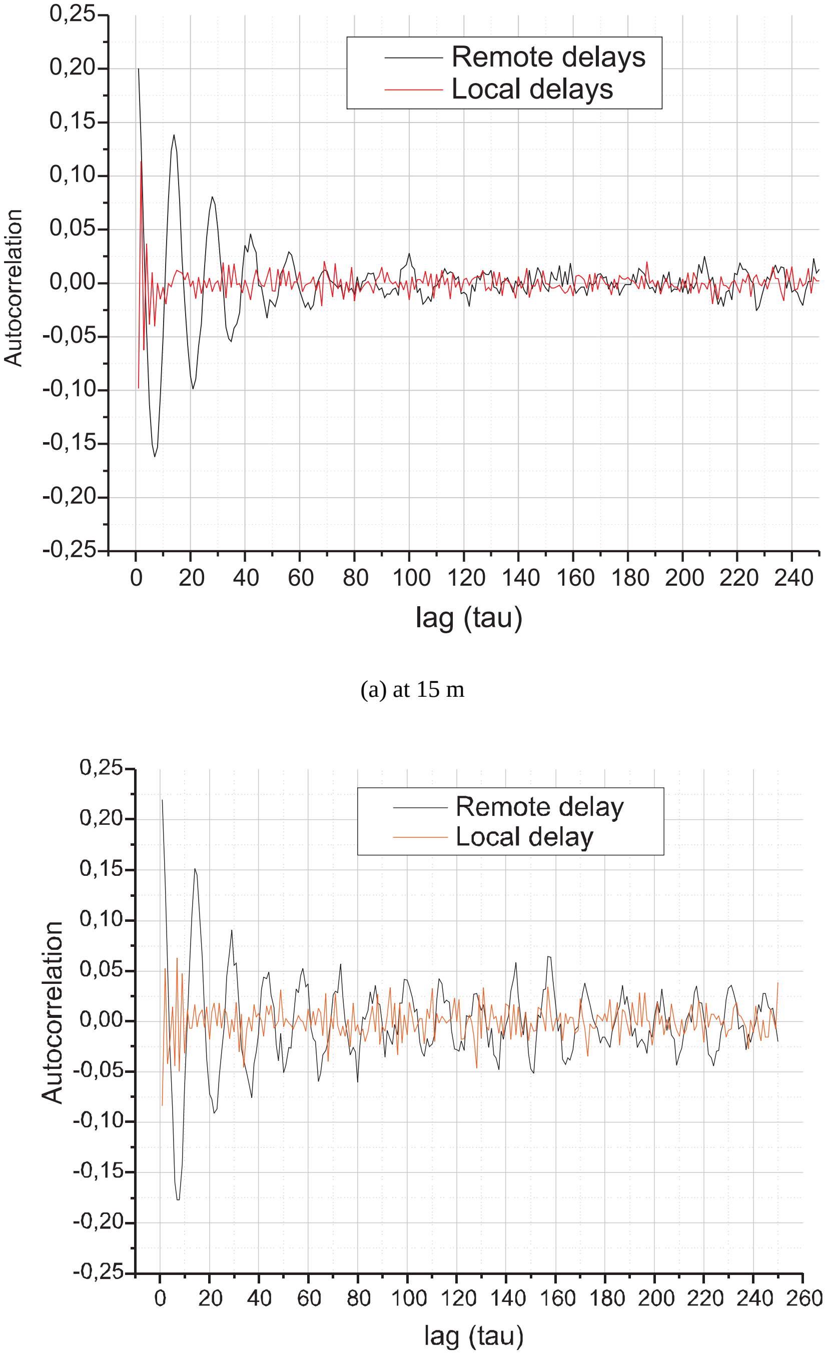
Figure 4.6: Mean and variance over time at 15 m. The mean varies by ±36 ns resp. ±18 ns around its average. The variance varies by ±0.008 resp. ±0.01 around its average.

Confidence intervals are meaningful only if the observations are independent. This assumption can be verified by the autocorrelation function. The time-lag dependent autocorrelation coefficients are presented as a graph in Figure 4.7. The 15 m and 40 m results are shown as an example. The graphs at other distances look similar. The autocorrelation for the local delay is low. It is smaller than $\rho$=0.05. Thus, the local delay measurements can be seen as independent. The autocorrelation of remote delay values has the form of a decaying cosinus wave. This kind of autocorrelation curve is found if the observations feature a constant frequency component. Indeed, this pattern manifests in the delay traces. The values of 323 and 324 occur block-wise in bursts. We also calculated an FFT over the packet delays. Assuming that each observation follows the previous after 20 ms, we identified a dominant frequency at about 3.5 Hz independent of the distance (Figure 4.8). However, the lower the packet error rate, the stronger this effect is.

We explain the effect displayed in Figure 4.7 with interference of both remote and local crystal clocks. Taken this explanation of quantization errors we can calculate the clock drift between both signals. Assuming a clocking of the MAC protocol at 1 MHz, the drift between both clocks is approximately $drift = \frac{f_{beat}}{f_1} = \frac{3.5Hz}{1MHz} = 3.5$ppm. Usually, the tolerance of consumer grade quartz clocks is up to 25 ppm. Thus, we consider this explanation to be plausible.

Interestingly, the MAC processing is conducted in steps of 1 $\mu$s. Thus, the MAC processing time is not precisely the SIFS interval but is rounded up to the next 1 $\mu$s. However, the error is small so that receivers tolerate it.

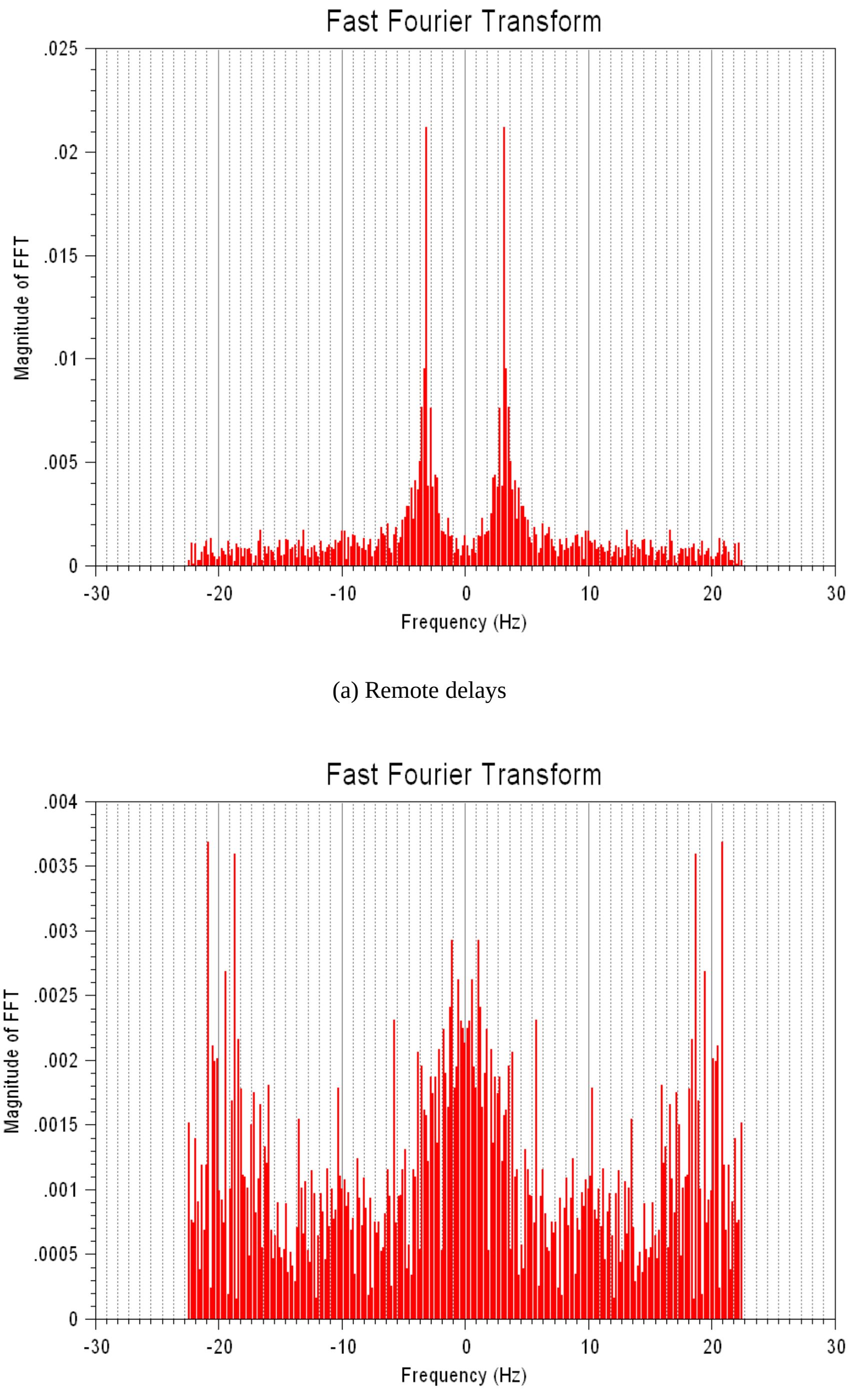
In our quantization error analysis we calculated the variance which is up to$^1/_4$. A distance of one and a time unit of one in the analysis refer to 300 m or 1 $\mu$s in the experiments. Then, the standard deviation would be 18.75 m or 62.5 ns at most. The standard deviation is between 3.3 and 25 m. Thus, the quantization error is not the only dominant effect and others such as thermal noise are important too.



(a) at 15 m

(b) at 40 m

Figure 4.7: Autocorrelation (=cross correlation of itself) is oscillating for remote delays – indicating a fundamental frequency component in observations.



(a) Remote delays

(b) Local delays

Figure 4.8: The fourier transformation of the observations shows a dominant frequency at 3.5 Hz, which is only present in the remote delays. Taken from the 40 m measurements.

# Chapter 5

# Measurements: Second Round

## 5.1 Experimental setup

The measurements were conducted outside in the countryside where one could expect the channel to be free of disturbing noise coming from other radiating devices. The measurements were extended to the maximal transmission range of 100 m. The sender was placed on a table, whereas the receiver was installed on top of a 1.5 m ladder. This was to guarantee that a large percentage of the Fresnel-zone, an elliptic space around the direct line-of-sight between both nodes is free of any obstacles harming the transmission. This time, the antennas were directed at each other. The schematic setup is displayed in Figure 5.1 and 7.7. A notebook acting as local node was sending out ICMP request packets. An access point was used as a remote node. Again, a monitoring PC close to the local node was required. Ping packets were sent every 10 ms until the monitor received up to 20.000 packets.

## 5.2 Equipment

We used an access point (Netgear FWAG114) supporting 802.11b/g and as remote node. The PCs were running under Linux, Suse 9.1, with a special 2.6 kernel. We used two different WLAN cards containing chip sets from Atheros and Conexant implementing IEEE 802.11 a,b and g. The Atheros cards (brand Netgear WAG-511, contained an AR5212 chip) are supported by the Madwifi device driver. We used the software version downloaded from the CVS server on the August 30th, 2004. The Conexant cards (brand: Longshine LCS-8531G containing Prism-GT chipset with an ISL3890 as MAC-Controller) are controlled by the prism54.org device driver (date 28-06-2004, firmware 1.0.4.3.arm). During each measurement both the sender and monitor were equipped with cards of the same brand. We also altered the notebook to study the impact of the CPU speed: An Asus Centrino 1.5 GHz and an Amilo Celeron 850 MHz notebook were used. To gather the packet traces, we used tcpdump and libpcap instead of Snuffle.

## 5.3 Configuration

The measurements were conducted in seven different configurations to study the impact of the WLAN card, CPU clock and modulation type. We used the default configuration of WLAN cards and access point but changed the supported standard to 802.11g and set the modulation type to either 36 or

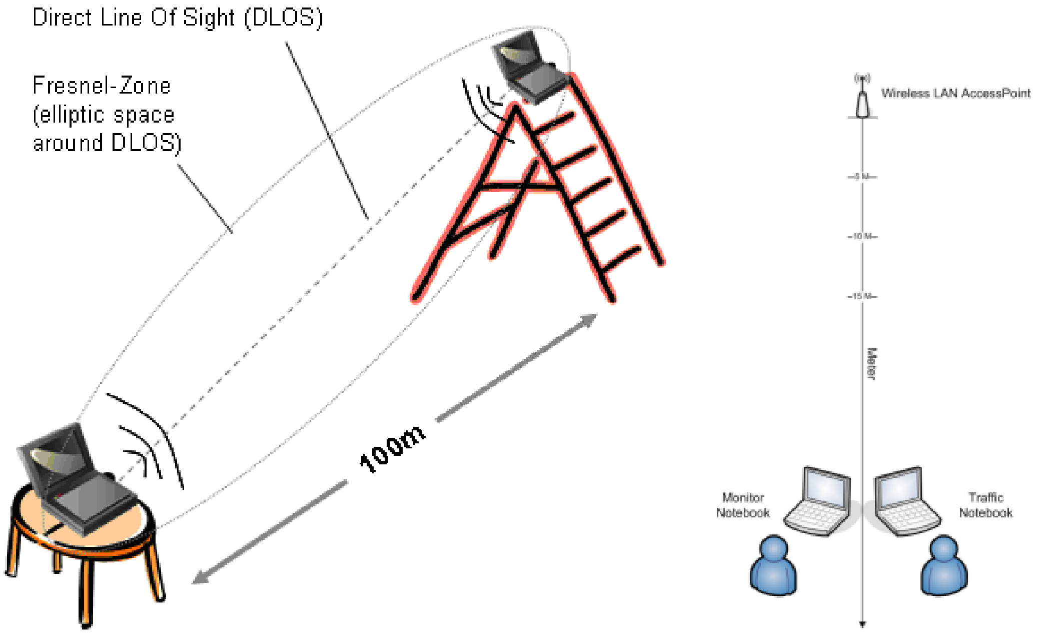


Figure 5.1: Setup of the second campaign

54 Mbit/s (Table 5.1 and 5.2). The frame length of the data packets are 65 bytes and of the acknowledgements 14 bytes.

In case of the IEEE 802.11g transmission mode, a packet starts with a preamble and PLCP header of 48+4 $\mu$s. After the PLCP header, the MAC frame body is sent. Beside the MAC PDU is contains a minimum of 22 bits of the PLCP header and padding bits. The pad bit round up the data packet length because it can be only a multiple of 4 $\mu$s. (An OFDM symbol has the length of 4 $\mu$s.) In case of the OFDM modulation mode, the SIFS has a length of 16 $\mu$s. All other values are similar to the 802.11b mode.

The transmission time for a data packet is 64 and 68 $\mu$s respective the modulation rate of 54 and 36 Mbit/s. The length of the acknowledgement is 60, 56, 56 $\mu$s for a transmission mode of 24, 36, and 56 Mbit/s.

## 5.4 Time measurements

The Atheros and Prism54 chipsets support time stamps of received packets with a resolution of 1 $\mu$s similar to the Prism II chip set. Thus, again, a second notebook near the sender is required to measure both sending and receiving time stamp. Also, we modified the device drivers to record the reception of a packet. After each interrupt, which is generated to notify the operating system about the received or transmitted packets, the current time stamps are saved. The time was measured with a libpcap time stamp. We also used a feature of Intel CPUs, which counts the CPU clock cycles. Linux supports reading the time stamp counter (TSC) with the rdtsc(. . . ) function if the OS kernel has proper support included.

Table 5.1: Configuration: Modulation speed of MAC packets depending on direction and type.

| Mode | Chipset | Monitor | Request | Ack. | Responce | Ack. |
|---|---|---|---|---|---|---|
| | | CPU | l→r | r→l | r→l | l→r |
| amilo_ath_36m | Atheros | 850 MHz | 54 | 24 | 36 | 24 |
| amilo_ath_54m | Atheros | 850 MHz | 54 | 24 | 54 | 24 |
| asus_ath 36m | Atheros | 1.5 GHz | 54 | 24 | 36 | 24 |
| asus_ath_54m | Atheros | 1.5 GHz | 54 | 24 | 54 | 24 |
| asus_prism_36-54m | PrismGT | 1.5 GHz | 54 | 24 | 36 | 24 |
| asus_prism_36m | PrismGT | 1.5 GHz | 36 | 24 | 36 | 36 |
| asus_prism_54m | PrismGT | 1.5 GHz | 54 | 54 | 54 | 54 |

Table 5.2: Configuration of the WLAN cards on a Linux system.

**Sender configuration:**

```
> iwpriv ath0|eth0 mode 3            # 802.11g mode
> iwconfig ath0 rate 36M             # (or 54M) set a fix tx rate (Atheros)
> iwpriv eth0 rate 36M               # (or 54M) set a fix tx rate (Prism54)
> ping -i 0.01 -s 1 $IPADDR          # send pings each 10 ms
```

**Monitor configuration:**

```
> iwconfig ath0|eth0 mode monitor    # Monitormodus
> sysctl -w devath.ctlpkt=-2         # trace all headers (Atheros)
> iwpriv eth0 set_prismhdr 1         # trace all headers (Prism54)
> tcpdump -i ath0|eth0 -c 20000
-n -e -s 231 -tt -w trace_filename   # trace 20000 packets including link layer header
```

## 5.5 Data collection & processing

Tcpdump recorded the packet trace and wrotes them to files. After the measurements we used an tcpdump to convert these files to plain text files (refer 7). Tcpdump had to been modified in order to print out the prism link-layer headers.

For statistical analysis the R project software turned out to be quite efficient. Thus, this time we applied R programs to calculate the data's analyse mean, variance and autocorrelation.

## 5.6 Results

Similar to the first campaign we calculated the distance from the time delay measurements. Figure 5.2 displays the remote (blue) and local delay (red) measurements, the number of overall observations (#) and the correlation coefficient (R) for the given configuration. A clear correlation between actual distance and calculated distance can be identified. In the middle graph, one can see that the larger the distance (and the worse the link quality), the larger the confidence interval becomes.

Figure 5.3 and 5.4 show the relation between distance and signal strength. The received signal strength (blue lines) decreases with distance. The correlation coefficient (R) is also given but one should consider that signal strength usually decays exponentially. Thus, the correlation coefficient should not be compared directly with Figure 5.2. Our measurement data also show, that the signal strength of received data packets and received acknowledgement packets are nearly the same regardless of the packet length.

We also calculated the distances with time measurements in the interrupt routine. We could not identify which time gathering method (jiffies or TSC) is better. There was a slightly better result using a faster CPU. However, measuring the propagation time with the interrupt routine seems to be far too imprecise.

## 5.7 Analysis

We also calculated the autocorrelation of local and remote delays (Figure 5.5, 7.8, 7.9 and 7.10). Interestingly, high and alternating correlation coefficients were only present, if we used the prism chipsets. With increasing distance and increasing error rate, the pattern vanishes. At farer distances the observations, which are based only on successful transmission, might follow each other not after exactly 20 ms but after a multiple of 20 ms. Thus, we can conclude that the effect is rather due to the elapsed time than to the number of successful transmissions.

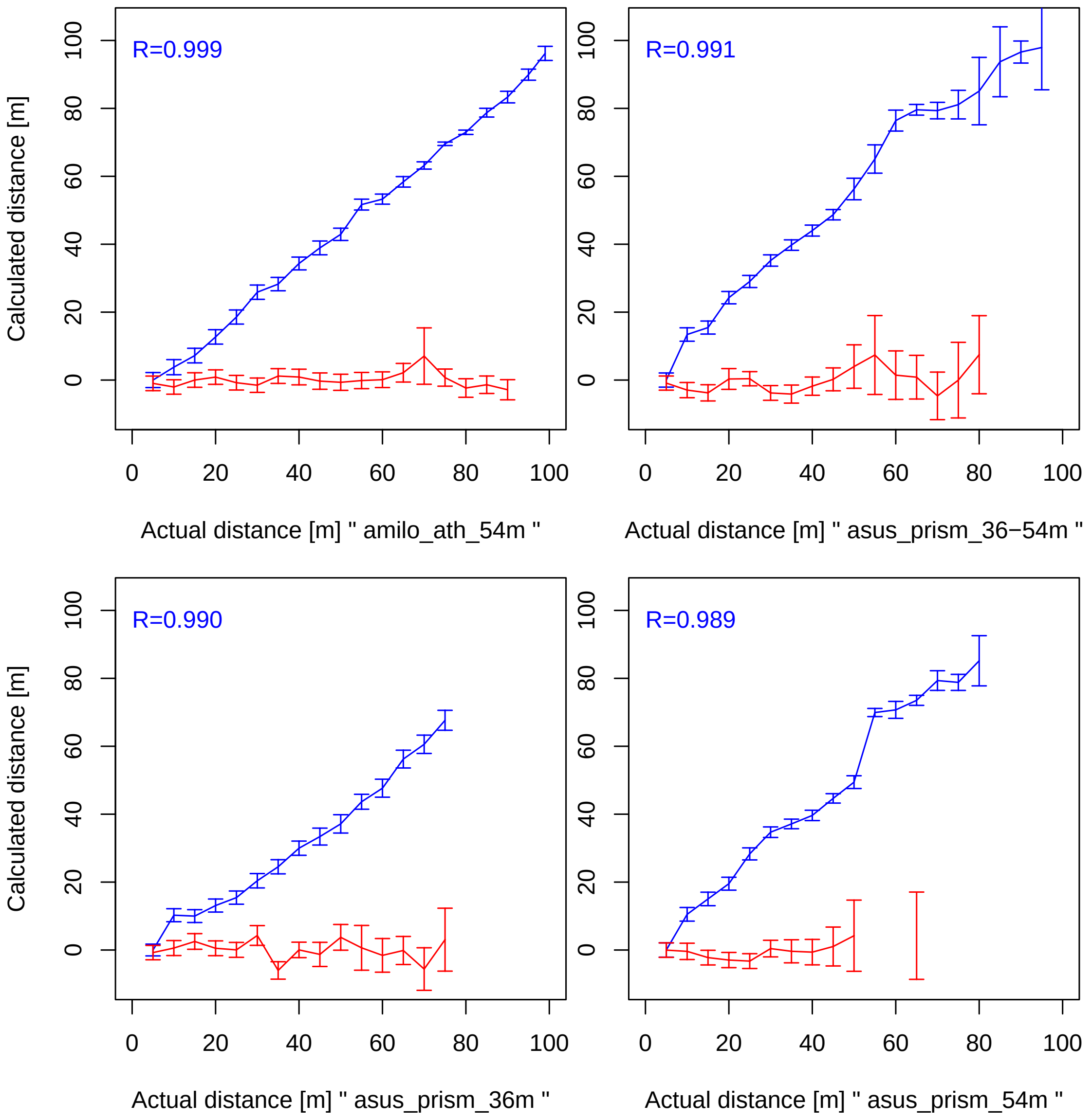


Figure 5.2: Propagation delay (=calculated distance) vs. actual distance (plus 95% conf. intervals). (blue/upper lines=biased remote delay, red/lower lines=biased local delays). Each value is based on at least 1000 observations.

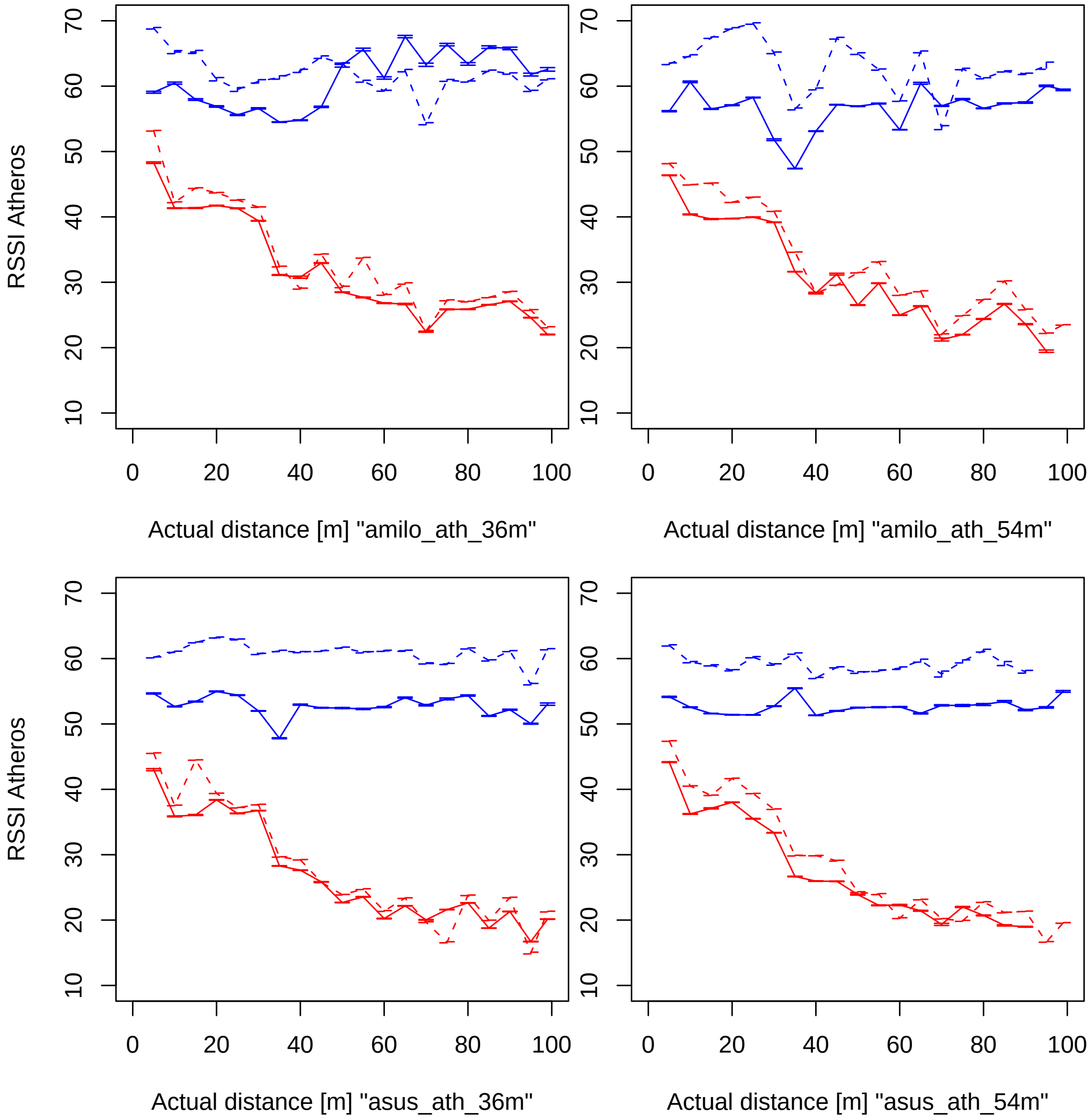


Figure 5.3: Atheros: Received signal strength indication (RSSI) vs. actual distance (plus 95% confidence intervals). Blue=remote packets' RSSI; red=local packets' RSSI; lines=data packets; dotted=acknowledgements

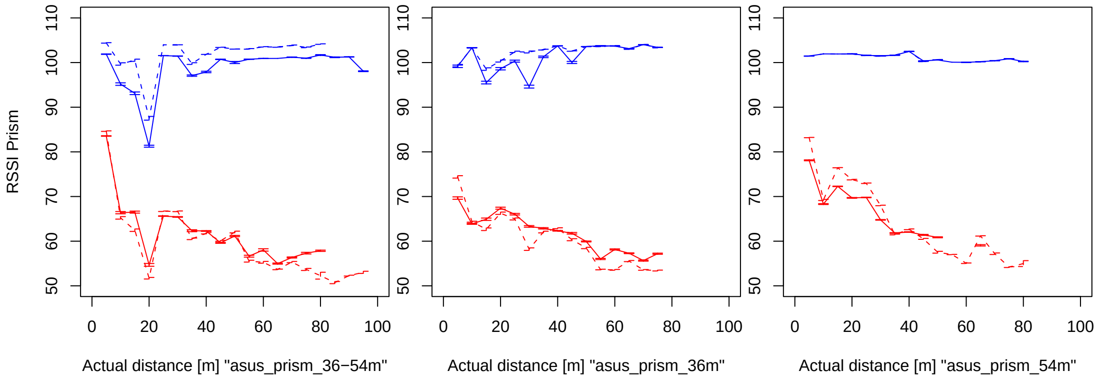


Figure 5.4: PrismGT: Received signal strength indication (RSSI) vs. actual distance (plus 95% confidence intervals). Blue=remote packets' RSSI; red=local packets' RSSI; lines=data packets; dotted=acknowledgements

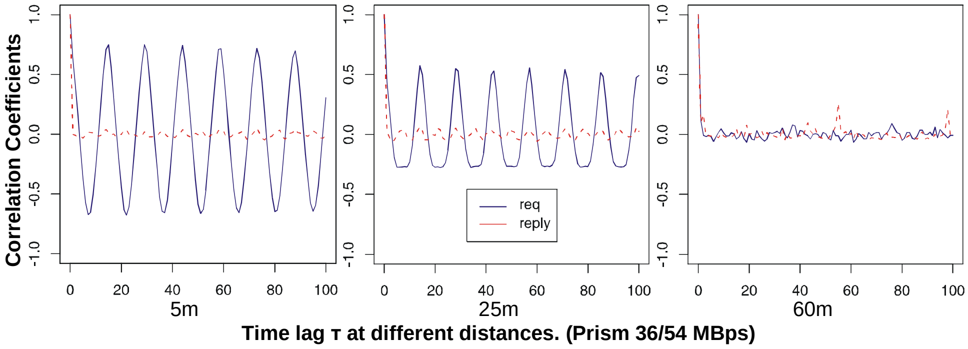


Figure 5.5: Autocorrelation of local and remote delay. Between two observations a delay of at minimal 20 ms is present.

# Chapter 6

# Conclusion

We have presented an algorithm on how to measure the air propagation time of IEEE 802.11 packets with a higher accuracy. Using two different experimental setups, we determined the precision of round trip time measurements. We use commercial WLAN cards, supporting IEEE 802.11b and 802.11g, implemented with three different WIFI chip sets. We have shown that such time measurements are possible even with off-the-shelf, commercial WLAN equipment and without additional signal processing.

To overcome the low resolution of the clocks, multiple observations have to be combined and smoothened. This can be done best during an ongoing data transmission at no additional cost. Otherwise, ICMP pings have to be sent for a few seconds to achieve a proper resolution.

The duration of distance determination is short enough to follow nodes moving at pedestrian speed. The tracking of faster nodes will require additional algorithms such as Kalman filters.

We explained why smoothing indeed helps to enhance the resolution of the time difference measurement so that distance measurements become possible. This effect can be due to the presence of measurement noise and to the beat frequency resulting from drifting clocks. To the best of our knowledge, especially the latter explanation is novel.

Our finding suggests that instead of RSSI the round trip time should be measured because it is correlated with the distance more strongly. In our gymnasium measurement the RSSI has not been useful to identify the distance because – due to reflections – the attenuation varied largely.

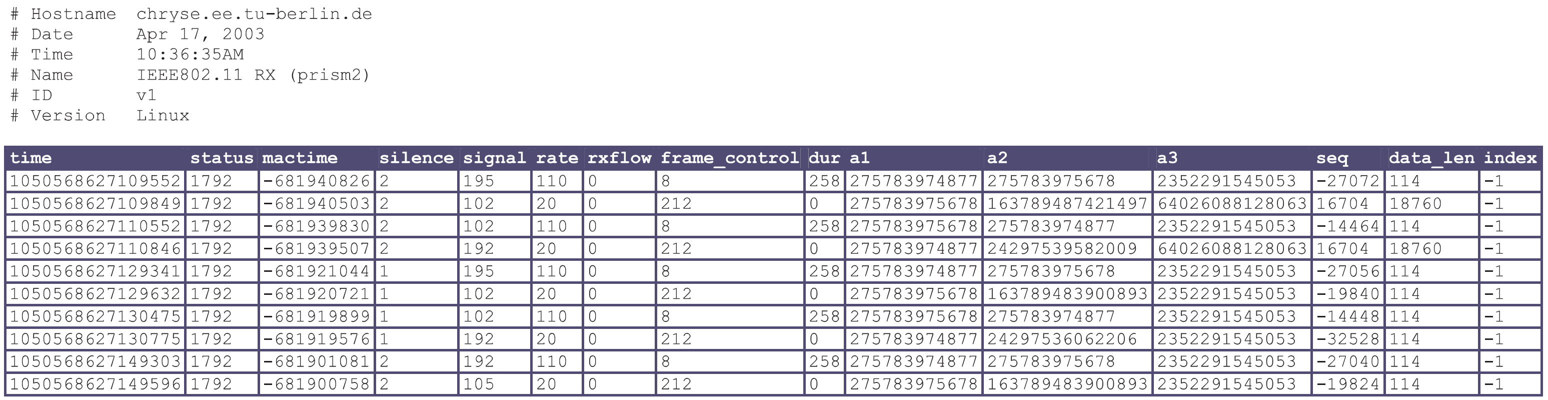
The contribution of this work is to show that neither synchronized, precise clocks nor special hardware is required if the propagation delay between two WLAN nodes is to be measured. This allows the implementation of easy-to-use, cheap and precise indoor positioning systems, which do not require maps containing signal strength distributions.

# Acknowledgements

This work has been supported by the Deutsche Forschungsgemeinschaft (DFG) via the priority program AKOM. We like to thank Prof. Wolisz for his support, E.-L. Hoene for the revision, and Sven Lamprecht and David Hundenborn for conducting the second measurements.

# Chapter 7

# Appendix



```
# Hostname  chryse.ee.tu-berlin.de
# Date      Apr 17, 2003
# Time      10:36:35AM
# Name      IEEE802.11 RX (prism2)
# ID        v1
# Version   Linux
```

| time | status | mactime | silence | signal | rate | rxflow | frame_control | dur | a1 | a2 | a3 | seq | data_len | index |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1050568627109552 | 1792 | -681940826 | 2 | 195 | 110 | 0 | 8 | 258 | 275783974877 | 275783975678 | 2352291545053 | -27072 | 114 | -1 |
| 1050568627109849 | 1792 | -681940503 | 2 | 102 | 20 | 0 | 212 | 0 | 275783975678 | 163789487421497 | 64026088128063 | 16704 | 18760 | -1 |
| 1050568627110552 | 1792 | -681939830 | 2 | 102 | 110 | 0 | 8 | 258 | 275783975678 | 275783974877 | 2352291545053 | -14464 | 114 | -1 |
| 1050568627110846 | 1792 | -681939507 | 2 | 192 | 20 | 0 | 212 | 0 | 275783974877 | 24297539582009 | 64026088128063 | 16704 | 18760 | -1 |
| 1050568627129341 | 1792 | -681921044 | 1 | 195 | 110 | 0 | 8 | 258 | 275783974877 | 275783975678 | 2352291545053 | -27056 | 114 | -1 |
| 1050568627129632 | 1792 | -681920721 | 1 | 102 | 20 | 0 | 212 | 0 | 275783975678 | 163789483900893 | 2352291545053 | -19840 | 114 | -1 |
| 1050568627130475 | 1792 | -681919899 | 1 | 102 | 110 | 0 | 8 | 258 | 275783975678 | 275783974877 | 2352291545053 | -14448 | 114 | -1 |
| 1050568627130775 | 1792 | -681919576 | 1 | 192 | 20 | 0 | 212 | 0 | 275783974877 | 24297536062206 | 2352291545053 | -32528 | 114 | -1 |
| 1050568627149303 | 1792 | -681901081 | 2 | 192 | 110 | 0 | 8 | 258 | 275783974877 | 275783975678 | 2352291545053 | -27040 | 114 | -1 |
| 1050568627149596 | 1792 | -681900758 | 2 | 105 | 20 | 0 | 212 | 0 | 275783975678 | 163789483900893 | 2352291545053 | -19824 | 114 | -1 |

Figure 7.1: Tracefile from the first experiment, Snuffle output

```
> cd amilo/ath_dump/ap36-INT36/
> tcpdump-3.8.3tkn/tcpdump -tt -n -ee -r 36M-05m-a-am-1.dmp
```

| | Msg | Len | Dev | Th | Tm | Ch | RSSI | Sq | Sig | Noise | Rate | Ist | Frmlen | Fc | Dur | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1088864798.516164 | 68 | 144 | "ath0" | 2916315546 | 1445536891 | 6 | 9180 | 0 | 56 | 56 | 54 | 0 | 65 | 0108 | 40 | 00095B6625F4 | 00095B432E15 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.52 > 192.168.127.1: icmp 9: echo request seq 3889 |
| 1088864798.516178 | 68 | 144 | "ath0" | 0 | 1445536908 | 6 | 9219 | 0 | 52 | 52 | 24 | 0 | 14 | 00D4 | 0 | 00095B432E15 | C9736AB02E15 | Acknowledgment |
| 1088864798.518392 | 68 | 144 | "ath0" | 4294967295 | 1445539112 | 6 | 11491 | 0 | 50 | 50 | 36 | 0 | 65 | 0208 | 44 | 00095B432E15 | 00095B6625F4 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.1 > 192.168.127.52: icmp 9: echo reply seq 3889 |
| 1088864798.518404 | 68 | 144 | "ath0" | 0 | 1445539125 | 6 | 11530 | 0 | 69 | 69 | 24 | 0 | 14 | 00D4 | 0 | 00095B6625F4 | E7FC15BA25F4 | Acknowledgment |

```
> cd amilo/ath_dump/ap54-INT54/
> tcpdump-3.8.3tkn/tcpdump -tt -n -ee -r 54M-05m-a-am-1.dmp
```

| | Msg | Len | Dev | Th | Tm | Ch | RSSI | Sq | Sig | Noise | Rate | Ist | Frmlen | Fc | Dur | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1088874574.262585 | 68 | 144- | "ath0" | 1768296129 | 2539960779 | 6 | 14638 | 0 | 58 | 58 | 54 | 0 | 65 | 0908 | 40 | 00095B6625F4 | 00095B432E15 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.52 > 192.168.127.1: icmp 9: echo request seq 494 |
| 1088874574.262595 | 68 | 144 | "ath0" | 0 | 2539960789 | 6 | 14677 | 0 | 48 | 48 | 24 | 0 | 14 | 00D4 | 0 | 00095B432E15 | C9736AB02E15 | Acknowledgment |
| 1088874574.264561 | 68 | 144 | "ath0" | 1769141286 | 2539962756 | 6 | 16734 | 0 | 44 | 44 | 54 | 0 | 65 | 0208 | 44 | 00095B432E15 | 00095B6625F4 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.1 > 192.168.127.52: icmp 9: echo reply seq 494 |
| 1088874574.264601 | 68 | 144 | "ath0" | 1769171071 | 2539962797 | 6 | 16773 | 0 | 58 | 58 | 24 | 0 | 14 | 00D4 | 0 | 00095B6625F4 | E7FC15BA25F4 | Acknowledgment |

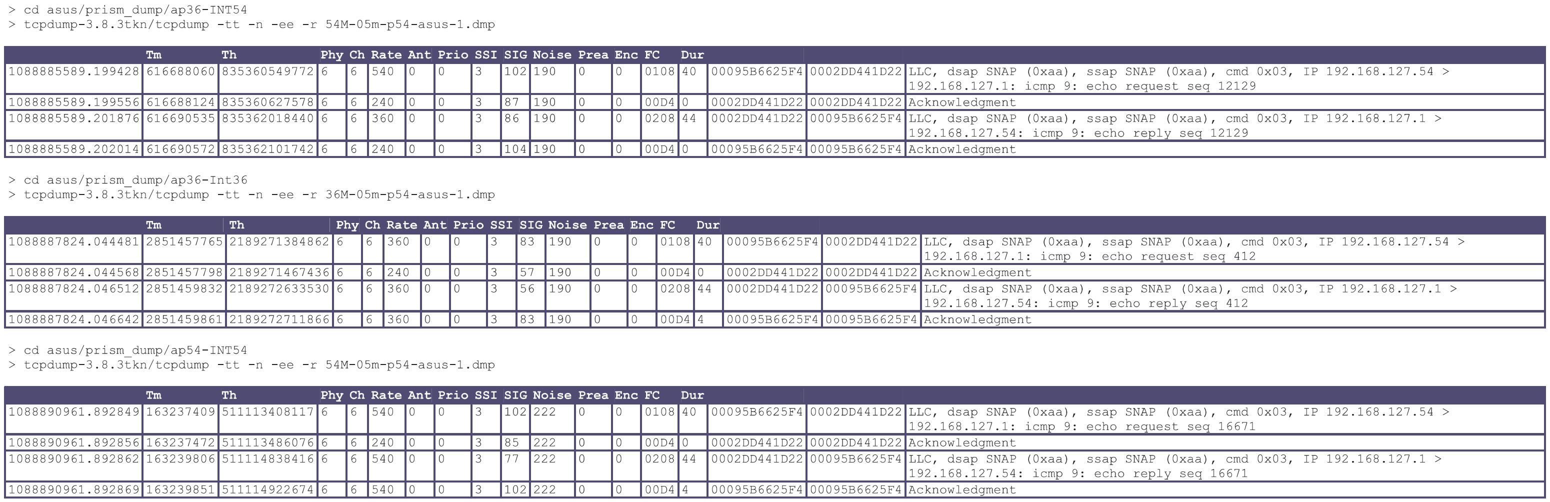
```
> cd asus/ath_dump/ap36-INT36
> tcpdump-3.8.3tkn/tcpdump -tt -n -ee -r 36M-05m-ath-asus-1.dmp
```

| | Msg | Len | Dev | Th | Tm | Ch | RSSI | Sq | Sig | Noise | Rate | Ist | Frmlen | Fc | Dur | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | 65 | 0108 | 40 | 00095B6625F4 | 00095B432E1A | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.50 > 192.168.127.1: icmp 9: echo request seq 24997 |
| 1088881085.079462 | 68 | 144 | "ath0" | 3969266142 | 268510561 | 6 | 0 | 0 | 45 | 45 | 24 | 0 | 14 | 00D4 | 0 | 00095B432E1A | 586ED5202E1A | Acknowledgment |
| 1088881085.081750 | 68 | 144 | "ath0" | 3970642008 | 268512850 | 6 | 0 | 0 | 42 | 42 | 36 | 0 | 65 | 0208 | 44 | 00095B432E1A | 00095B6625F4 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.1 > 192.168.127.50: icmp 9: echo reply seq 24997 |
| 1088881085.081790 | 68 | 144 | "ath0" | 3970664292 | 268512890 | 6 | 0 | 0 | 65 | 65 | 24 | 0 | 14 | 00D4 | 0 | 00095B6625F4 | E7FC15BA25F4 | Acknowledgment |

```
> cd asus/ath_dump/ap54-INT54
> tcpdump-3.8.3tkn/tcpdump -tt -n -ee -r 54M-05m-ath-asus-1.dmp
```

| | Msg | Len | Dev | Th | Tm | Ch | RSSI | Sq | Sig | Noise | Rate | Ist | Frmlen | Fc | Dur | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1088878655.863312 | 68 | 144 | "ath0" | 3997372611 | 2341831993 | 6 | 0 | 0 | 54 | 54 | 54 | 0 | 65 | 0108 | 40 | 00095B6625F4 | 00095B432E1A | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.50 > 192.168.127.1: icmp 9: echo request seq 8517 |
| 1088878655.863319 | 68 | 144 | "ath0" | 3997394358 | 2341832033 | 6 | 0 | 0 | 43 | 43 | 24 | 0 | 14 | 00D4 | 0 | 00095B432E1A | 586ED5202E1A | Acknowledgment |
| 1088878655.863325 | 68 | 144 | "ath0" | 3998836695 | 2341834421 | 6 | 0 | 0 | 41 | 41 | 54 | 0 | 65 | 0208 | 44 | 00095B432E1A | 00095B6625F4 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.1 > 192.168.127.50: icmp 9: echo reply seq 8517 |
| 1088878655.863332 | 68 | 144 | "ath0" | 3998858832 | 2341834460 | 6 | 0 | 0 | 67 | 67 | 24 | 0 | 14 | 00D4 | 0 | 00095B6625F4 | E7FC15BA25F4 | Acknowledgment |

Figure 7.2: Tracefile from the second experiment, modified tcpdump output for Atheros chipsets



```
> cd asus/prism_dump/ap36-INT54
> tcpdump-3.8.3tkn/tcpdump -tt -n -ee -r 54M-05m-p54-asus-1.dmp
```

| | Tm | Th | Phy | Ch | Rate | Ant | Prio | SSI | SIG | Noise | Prea | Enc | FC | Dur | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1088885589.199428 | 616688060 | 835360549772 | 6 | 6 | 540 | 0 | 0 | 3 | 102 | 190 | 0 | 0 | 0108 | 40 | 00095B6625F4 | 0002DD441D22 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.54 > 192.168.127.1: icmp 9: echo request seq 12129 |
| 1088885589.199556 | 616688124 | 835360627578 | 6 | 6 | 240 | 0 | 0 | 3 | 87 | 190 | 0 | 0 | 00D4 | 0 | 0002DD441D22 | 0002DD441D22 | Acknowledgment |
| 1088885589.201876 | 616690535 | 835362018440 | 6 | 6 | 360 | 0 | 0 | 3 | 86 | 190 | 0 | 0 | 0208 | 44 | 0002DD441D22 | 00095B6625F4 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.1 > 192.168.127.54: icmp 9: echo reply seq 12129 |
| 1088885589.202014 | 616690572 | 835362101742 | 6 | 6 | 240 | 0 | 0 | 3 | 104 | 190 | 0 | 0 | 00D4 | 0 | 00095B6625F4 | 00095B6625F4 | Acknowledgment |

```
> cd asus/prism_dump/ap36-Int36
> tcpdump-3.8.3tkn/tcpdump -tt -n -ee -r 36M-05m-p54-asus-1.dmp
```

| | Tm | Th | Phy | Ch | Rate | Ant | Prio | SSI | SIG | Noise | Prea | Enc | FC | Dur | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1088887824.044481 | 2851457765 | 2189271384862 | 6 | 6 | 360 | 0 | 0 | 3 | 83 | 190 | 0 | 0 | 0108 | 40 | 00095B6625F4 | 0002DD441D22 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.54 > 192.168.127.1: icmp 9: echo request seq 412 |
| 1088887824.044568 | 2851457798 | 2189271467436 | 6 | 6 | 240 | 0 | 0 | 3 | 57 | 190 | 0 | 0 | 00D4 | 0 | 0002DD441D22 | 0002DD441D22 | Acknowledgment |
| 1088887824.046512 | 2851459832 | 2189272633530 | 6 | 6 | 360 | 0 | 0 | 3 | 56 | 190 | 0 | 0 | 0208 | 44 | 0002DD441D22 | 00095B6625F4 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.1 > 192.168.127.54: icmp 9: echo reply seq 412 |
| 1088887824.046642 | 2851459861 | 2189272711866 | 6 | 6 | 360 | 0 | 0 | 3 | 83 | 190 | 0 | 0 | 00D4 | 4 | 00095B6625F4 | 00095B6625F4 | Acknowledgment |

```
> cd asus/prism_dump/ap54-INT54
> tcpdump-3.8.3tkn/tcpdump -tt -n -ee -r 54M-05m-p54-asus-1.dmp
```

| | Tm | Th | Phy | Ch | Rate | Ant | Prio | SSI | SIG | Noise | Prea | Enc | FC | Dur | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1088890961.892849 | 163237409 | 511113408117 | 6 | 6 | 540 | 0 | 0 | 3 | 102 | 222 | 0 | 0 | 0108 | 40 | 00095B6625F4 | 0002DD441D22 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.54 > 192.168.127.1: icmp 9: echo request seq 16671 |
| 1088890961.892856 | 163237472 | 511113486076 | 6 | 6 | 240 | 0 | 0 | 3 | 85 | 222 | 0 | 0 | 00D4 | 0 | 0002DD441D22 | 0002DD441D22 | Acknowledgment |
| 1088890961.892862 | 163239806 | 511114838416 | 6 | 6 | 540 | 0 | 0 | 3 | 77 | 222 | 0 | 0 | 0208 | 44 | 0002DD441D22 | 00095B6625F4 | LLC, dsap SNAP (0xaa), ssap SNAP (0xaa), cmd 0x03, IP 192.168.127.1 > 192.168.127.54: icmp 9: echo reply seq 16671 |
| 1088890961.892869 | 163239851 | 511114922674 | 6 | 6 | 540 | 0 | 0 | 3 | 102 | 222 | 0 | 0 | 00D4 | 4 | 00095B6625F4 | 00095B6625F4 | Acknowledgment |

Figure 7.3: Tracefile from the second experiment, modified tcpdump output for Prism chipsets

Table 7.1: Second Campaign: Distance vs. round trip time

| **Configuration: amilo_ath_54m** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Act. | **Remote delays** | | | | | **Local delays** | | | | |
| dist. | mean | var | min | max | # | mean | var | min | max | # |
| [m] | [μs] | | [μs] | [μs] | | [μs] | | [μs] | [μs] | |
| 5 | 39.531 | 0.249 | 39 | 40 | 4415 | 39.499 | 0.250 | 39 | 40 | 4681 |
| 10 | 39.556 | 0.247 | 39 | 40 | 4306 | 39.492 | 0.250 | 39 | 40 | 4785 |
| 15 | 39.579 | 0.244 | 39 | 40 | 4553 | 39.506 | 0.250 | 39 | 40 | 4721 |
| 20 | 39.616 | 0.237 | 39 | 40 | 4553 | 39.512 | 0.250 | 39 | 40 | 4746 |
| 25 | 39.655 | 0.226 | 39 | 40 | 4529 | 39.501 | 0.250 | 39 | 40 | 4683 |
| 30 | 39.703 | 0.209 | 39 | 40 | 4073 | 39.496 | 0.250 | 39 | 40 | 4830 |
| 35 | 39.719 | 0.202 | 39 | 40 | 4521 | 39.514 | 0.250 | 39 | 40 | 4585 |
| 40 | 39.760 | 0.183 | 39 | 40 | 4437 | 39.512 | 0.250 | 39 | 40 | 4071 |
| 45 | 39.790 | 0.166 | 39 | 40 | 3473 | 39.504 | 0.250 | 39 | 40 | 3727 |
| 50 | 39.817 | 0.150 | 39 | 40 | 3962 | 39.502 | 0.250 | 39 | 40 | 3844 |
| 55 | 39.875 | 0.109 | 39 | 40 | 3691 | 39.505 | 0.250 | 39 | 40 | 3794 |
| 60 | 39.886 | 0.101 | 39 | 40 | 3969 | 39.507 | 0.250 | 39 | 40 | 4058 |
| 65 | 39.920 | 0.074 | 39 | 40 | 2664 | 39.520 | 0.250 | 39 | 40 | 2873 |
| 70 | 39.952 | 0.046 | 39 | 40 | 3429 | 39.553 | 0.248 | 39 | 40 | 311 |
| 75 | 39.995 | 0.010 | 39 | 41 | 3237 | 39.511 | 0.250 | 39 | 40 | 3393 |
| 80 | 40.017 | 0.018 | 39 | 41 | 3687 | 39.490 | 0.250 | 39 | 40 | 2900 |
| 85 | 40.056 | 0.053 | 40 | 41 | 2741 | 39.497 | 0.250 | 39 | 40 | 3265 |
| 90 | 40.086 | 0.079 | 40 | 41 | 2348 | 39.487 | 0.250 | 39 | 40 | 2456 |
| 95 | 40.130 | 0.113 | 40 | 41 | 3688 | 39.429 | 0.247 | 39 | 40 | 98 |
| 99 | 40.172 | 0.143 | 40 | 41 | 2857 | 39.500 | 0.258 | 39 | 40 | 32 |

| **Configuration: asus_prism_36-54m** | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| Act. | **Remote delays** | | | | | **Local delays** | | | | |
| dist. | mean | var | min | max | # | mean | var | min | max | # |
| [m] | [μs] | | [μs] | [μs] | | [μs] | | [μs] | [μs] | |
| 5 | 63.578 | 0.244 | 63 | 64 | 4841 | 36.582 | 0.243 | 36 | 37 | 4850 |
| 10 | 63.668 | 0.222 | 63 | 64 | 4913 | 36.569 | 0.249 | 33 | 38 | 4280 |
| 15 | 63.681 | 0.217 | 63 | 64 | 5101 | 36.563 | 0.250 | 33 | 38 | 3790 |
| 20 | 63.740 | 0.194 | 63 | 65 | 5084 | 36.591 | 0.251 | 32 | 37 | 2320 |
| 25 | 63.772 | 0.177 | 63 | 65 | 4836 | 36.591 | 0.242 | 36 | 38 | 4817 |
| 30 | 63.813 | 0.153 | 63 | 65 | 4740 | 36.563 | 0.251 | 32 | 37 | 4612 |
| 35 | 63.843 | 0.134 | 63 | 65 | 4884 | 36.561 | 0.248 | 36 | 38 | 3022 |
| 40 | 63.872 | 0.116 | 63 | 65 | 3832 | 36.576 | 0.253 | 32 | 38 | 3029 |
| 45 | 63.903 | 0.090 | 63 | 65 | 3373 | 36.590 | 0.248 | 33 | 37 | 1887 |
| 50 | 63.953 | 0.105 | 63 | 65 | 899 | 36.615 | 0.241 | 36 | 38 | 509 |
| 55 | 64.012 | 0.116 | 63 | 65 | 577 | 36.638 | 0.233 | 36 | 37 | 149 |
| 60 | 64.088 | 0.113 | 63 | 65 | 1028 | 36.598 | 0.241 | 36 | 37 | 408 |
| 65 | 64.109 | 0.109 | 63 | 65 | 3779 | 36.594 | 0.242 | 36 | 37 | 505 |
| 70 | 64.107 | 0.106 | 63 | 65 | 1558 | 36.557 | 0.247 | 36 | 37 | 436 |
| 75 | 64.119 | 0.105 | 64 | 65 | 513 | 36.588 | 0.244 | 36 | 37 | 170 |
| 80 | 64.145 | 0.125 | 64 | 65 | 110 | 36.638 | 0.232 | 36 | 37 | 152 |
| 85 | 64.203 | 0.163 | 64 | 65 | 133 | 36.600 | 0.300 | 36 | 37 | 5 |
| 90 | 64.222 | 0.173 | 64 | 65 | 1418 | 36.639 | 0.237 | 36 | 37 | 36 |
| 95 | 64.231 | 0.450 | 57 | 65 | 251 | 37.357 | 3.786 | 36 | 44 | 14 |

**Configuration: asus_prism_36m**

| Act. | Remote delays | | | | | Local delays | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| dist. | mean | var | min | max | # | mean | var | min | max | # |
| [m] | [$\mu$s] | | [$\mu$s] | [$\mu$s] | | [$\mu$s] | | [$\mu$s] | [$\mu$s] | |
| 5 | 32.215 | 0.170 | 31 | 33 | 4871 | 28.556 | 0.250 | 25 | 30 | 4826 |
| 10 | 32.283 | 0.203 | 32 | 33 | 4787 | 28.565 | 0.249 | 25 | 29 | 4410 |
| 15 | 32.282 | 0.202 | 32 | 33 | 4891 | 28.578 | 0.245 | 28 | 30 | 3979 |
| 20 | 32.302 | 0.211 | 31 | 33 | 4956 | 28.564 | 0.246 | 27 | 29 | 4479 |
| 25 | 32.318 | 0.217 | 32 | 33 | 4965 | 28.561 | 0.247 | 28 | 30 | 4429 |
| 30 | 32.351 | 0.228 | 32 | 33 | 4411 | 28.590 | 0.247 | 25 | 29 | 2524 |
| 35 | 32.378 | 0.235 | 32 | 33 | 4678 | 28.521 | 0.250 | 28 | 29 | 3275 |
| 40 | 32.415 | 0.243 | 32 | 33 | 4802 | 28.561 | 0.248 | 28 | 30 | 4132 |
| 45 | 32.438 | 0.246 | 32 | 33 | 3439 | 28.552 | 0.247 | 28 | 29 | 1689 |
| 50 | 32.463 | 0.249 | 32 | 33 | 2953 | 28.586 | 0.243 | 28 | 29 | 1461 |
| 55 | 32.506 | 0.250 | 32 | 34 | 4490 | 28.565 | 0.246 | 28 | 29 | 490 |
| 60 | 32.533 | 0.250 | 32 | 34 | 3079 | 28.551 | 0.250 | 28 | 30 | 881 |
| 65 | 32.590 | 0.242 | 32 | 33 | 3052 | 28.560 | 0.256 | 25 | 29 | 1298 |
| 70 | 32.619 | 0.236 | 32 | 33 | 2799 | 28.524 | 0.250 | 28 | 29 | 550 |
| 75 | 32.666 | 0.223 | 32 | 34 | 2236 | 28.581 | 0.244 | 28 | 29 | 246 |

**Configuration: asus_prism_54m**

| Act. | Remote delays | | | | | Local delays | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| dist. | mean | var | min | max | # | mean | var | min | max | # |
| [m] | [$\mu$s] | | [$\mu$s] | [$\mu$s] | | [$\mu$s] | | [$\mu$s] | [$\mu$s] | |
| Act. | Remote delays | | | | | Local delays | | | | |
| dist. | mean | var | min | max | # | mean | var | min | max | # |
| [m] | [$\mu$s] | | [$\mu$s] | [$\mu$s] | | [$\mu$s] | | [$\mu$s] | [$\mu$s] | |
| 5 | 63.602 | 0.240 | 63 | 64 | 4681 | 44.622 | 0.240 | 44 | 49 | 4552 |
| 10 | 63.672 | 0.221 | 63 | 64 | 4730 | 44.619 | 0.237 | 44 | 46 | 3551 |
| 15 | 63.702 | 0.210 | 63 | 65 | 4588 | 44.607 | 0.240 | 44 | 46 | 4448 |
| 20 | 63.732 | 0.197 | 63 | 65 | 4716 | 44.602 | 0.241 | 44 | 46 | 4158 |
| 25 | 63.791 | 0.166 | 63 | 65 | 4549 | 44.600 | 0.241 | 44 | 46 | 4354 |
| 30 | 63.833 | 0.140 | 63 | 65 | 5051 | 44.625 | 0.240 | 44 | 48 | 3472 |
| 35 | 63.849 | 0.130 | 63 | 65 | 5634 | 44.619 | 0.238 | 44 | 46 | 1784 |
| 40 | 63.866 | 0.118 | 63 | 65 | 4412 | 44.618 | 0.238 | 44 | 46 | 1465 |
| 45 | 63.899 | 0.101 | 63 | 65 | 4556 | 44.629 | 0.237 | 44 | 46 | 625 |
| 50 | 63.931 | 0.100 | 63 | 65 | 2448 | 44.650 | 0.229 | 44 | 45 | 180 |
| 55 | 64.068 | 0.113 | 63 | 65 | 6805 | 44.333 | 0.333 | 44 | 45 | 3 |
| 60 | 64.073 | 0.109 | 63 | 65 | 1516 | NA | NA | NA | NA | 0 |
| 65 | 64.092 | 0.108 | 63 | 65 | 4264 | 44.650 | 0.229 | 44 | 45 | 120 |
| 70 | 64.131 | 0.122 | 63 | 65 | 1254 | NA | NA | NA | NA | 0 |
| 75 | 64.127 | 0.118 | 63 | 65 | 1824 | NA | NA | NA | NA | 0 |
| 80 | 64.170 | 0.141 | 64 | 65 | 224 | NA | NA | NA | NA | 0 |

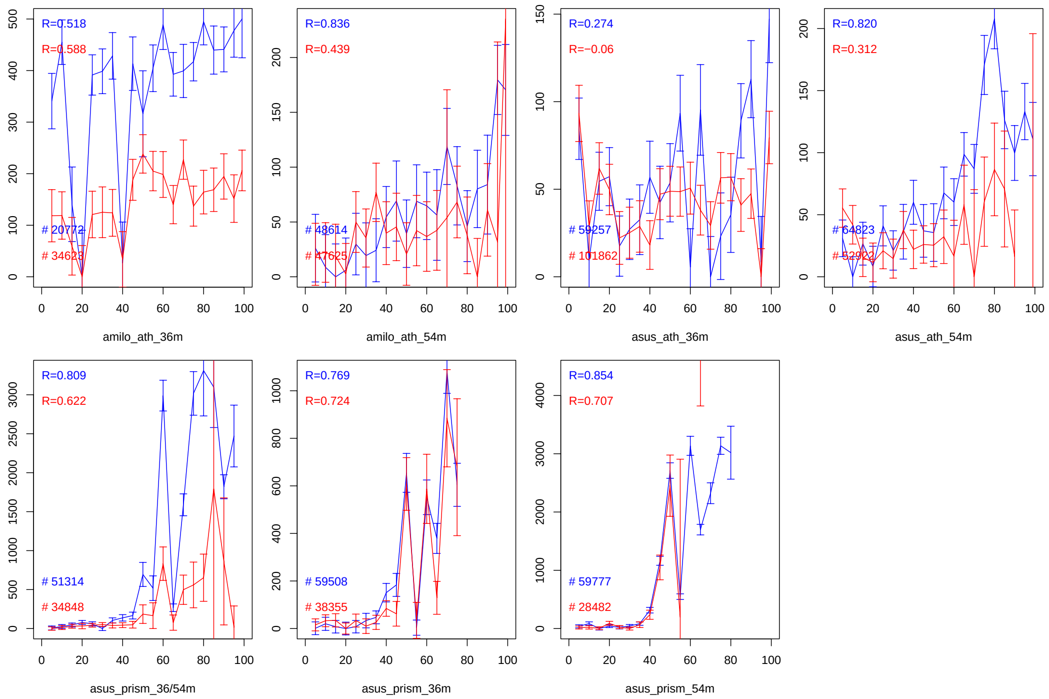


Figure 7.4: Distance vs. delay using libpcap time stamps.

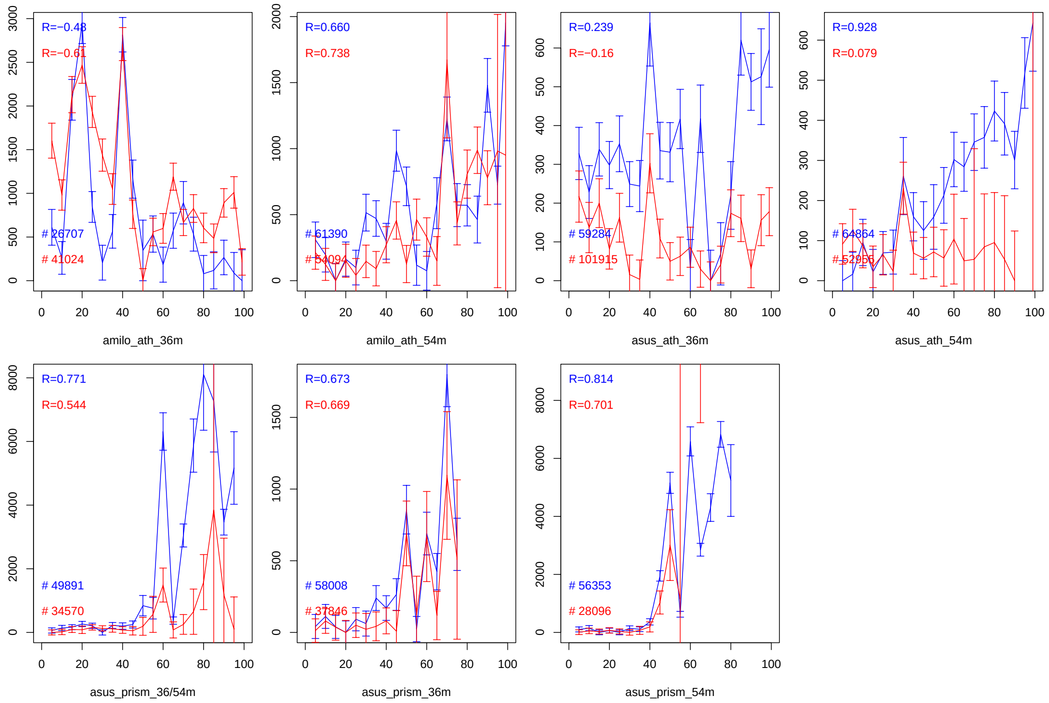
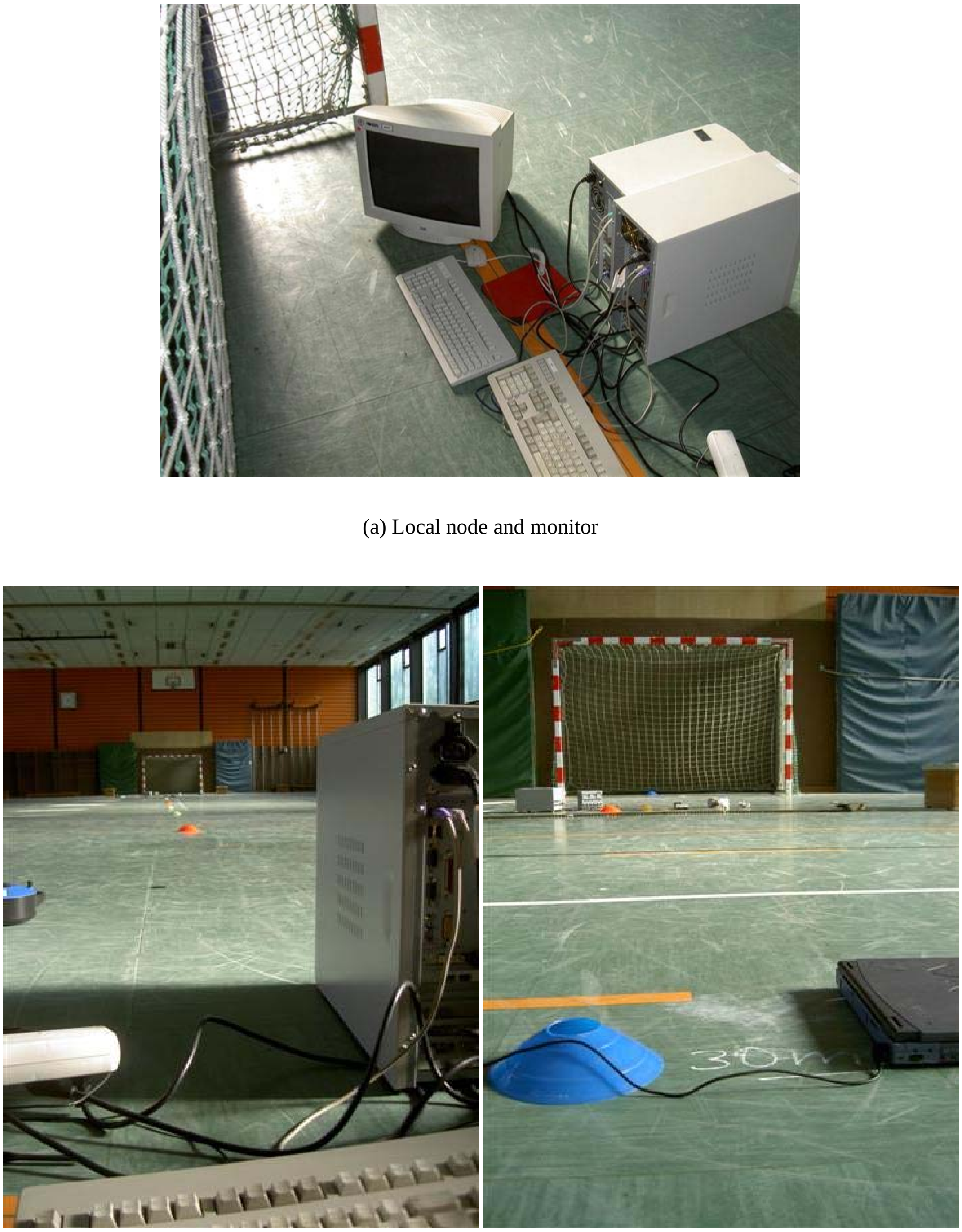


Figure 7.5: Distance vs. delay using the CPU's time stamp counter (TSC)

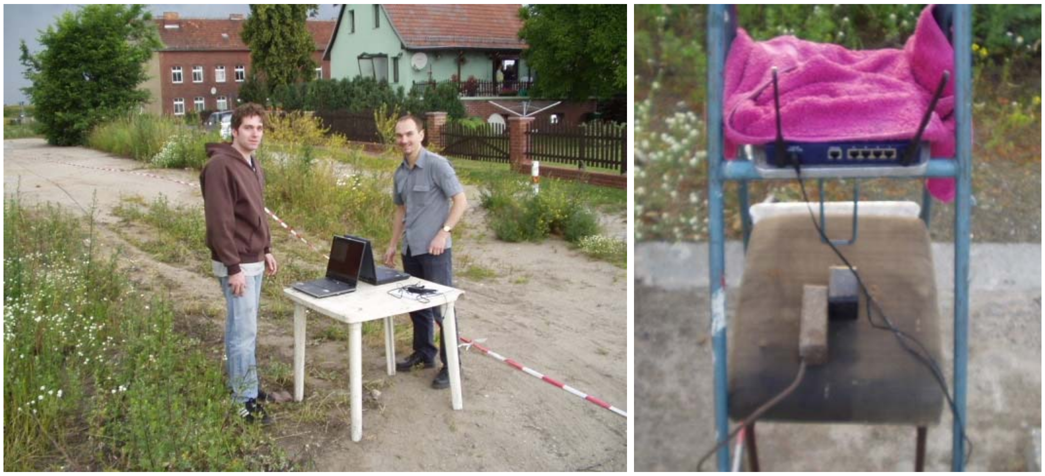


(a) Local node and monitor

(b) Direct line of sight

(c) Notebook at 30m

Figure 7.6: First measurements: experimental setup.



(a) Local and monitor node

(b) Remote node

Figure 7.7: Photos from the second campaign

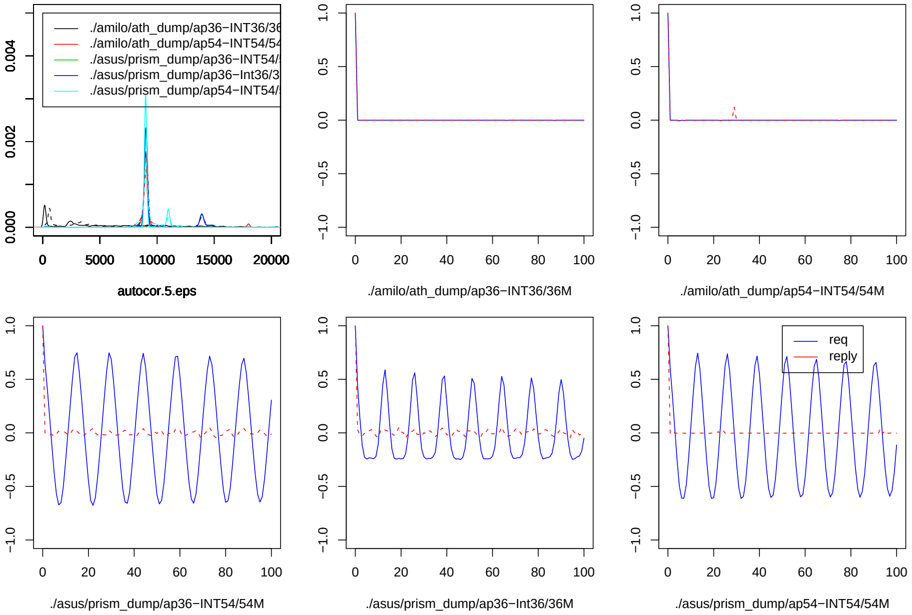


Figure 7.8: Autocorrelation of local and remote delay. Between two observations a delay of at minimal 20 ms is present. Distance is 5 m.

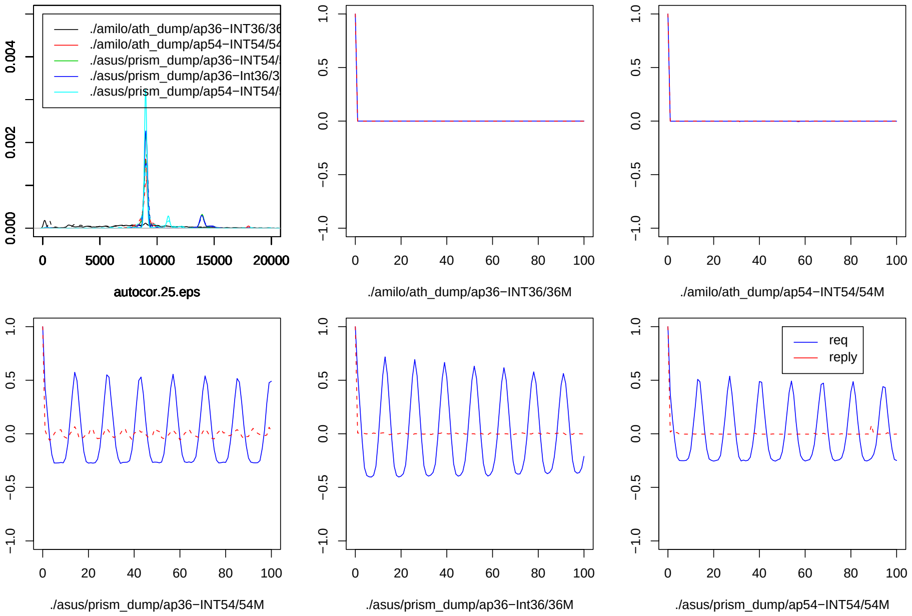


Figure 7.9: Autocorrelation of local and remote delay. Between two observations a delay of at minimal 20 ms is present. Distance is 25 m.

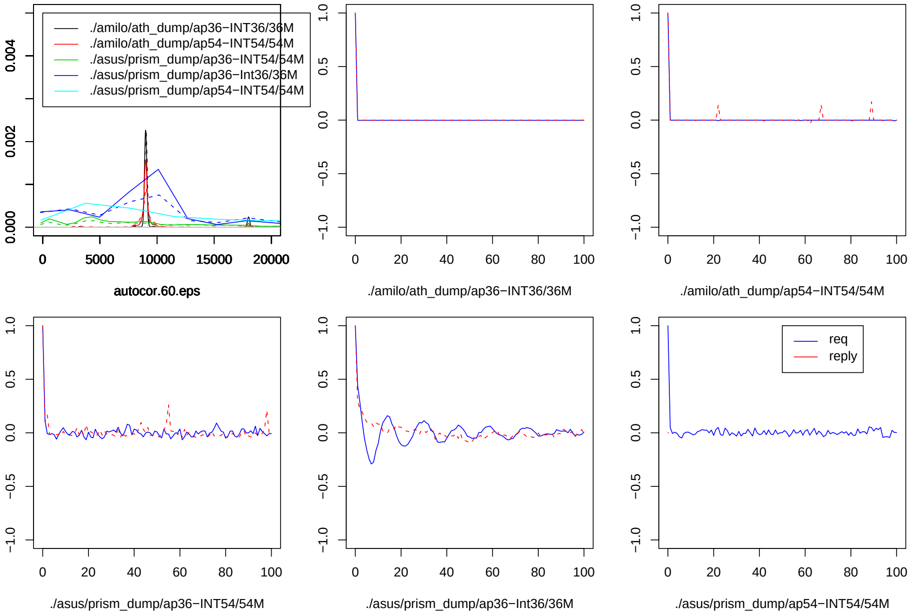


Figure 7.10: Autocorrelation of local and remote delay. Between two observations a delay of at minimal 20 ms is present. Distance is 60 m.

# Bibliography

[1] Jeffrey Hightower and Gaetano Borriello. Location systems for ubiquitous computing. *IEEE Computer*, 34(8):57–66, August 2001.

[2] Paramvir Bahl and Venkata N. Padmanabhan. RADAR: An In-Building RF-Based User Location and Tracking System. In *Infocom 2000*, pages 775–784, Tel-Aviv, Israel, March 2000.

[3] Ming-Hui Jin, Eric Hsiao-Kuang Wu, Yun-Bin Liao, and Hui-Chun Liao. 802.11-based positioning system for context aware applications. In *GLOBECOM 2003 - IEEE Global Telecommunications Conference*, volume 22, pages 929–933, December 2003.

[4] Moustafa Youssef, Ashok Agrawala, and Udaya Shankar. WLAN location determination via clustering and probability distributions. In *IEEE PerCom 2003*, March 2003.

[5] P. Krishnan, A.S. Krishnakumar, Wen-Hua Ju, Colin Mallows, and Sachin Ganu. A system for LEASE: Location estimation assisted by stationary emitters for indoor RF wireless networks page(s): 1001- 1011. In *Infocom 2004*, pages 1001– 1011, Hong Kong, March 2004.

[6] Kamol Kaemarungsi and Prashant Krishnamurthy. Modeling of indoor positioning systems based on location fingerprinting. In *Infocom 2004*, pages 1012– 1022, Hong Kong, March 2004.

[7] Youngjune Gwon, Ravi Jain, and Toshiro Kawahara. Robust indoor location estimation of stationary and mobile users. In *Infocom 2004*, pages 1032– 1043, Hong Kong, March 2004.

[8] David Moore, John Leonard, Daniela Rus, and Seth Teller. Robust distributed network localization with noisy range measurements. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 50–61. ACM Press, 2004.

[9] Andreas Haeberlen, Eliot Flannery, Andrew M. Ladd, Algis Rudys, Dan S. Wallach, and Lydia E. Kavraki. Practical robust localization over large-scale 802.11 wireless networks. In *Proceedings of the 10th annual international conference on Mobile computing and networking (MOBICOM)*, pages 70–84, Philadelphia, PA, September 2004. ACM Press.

[10] Tian He, Chengdu Huang, Brian M. Blum, John A. Stankovic, and Tarek Abdelzaher. Range-free localization schemes for large scale sensor networks. In *Proceedings of the 9th annual international conference on Mobile computing and networking (MOBICOM)*, pages 81–95, San Diego, CA, September 2003. ACM Press.

[11] Hector Velayos and Gunnar Karlsson. Limitations in range estimation for wireless LAN. In *Proc. 1st Workshop on Positioning, Navigation and Communication (WPNC'04)*, Hannover, Germany, March 2004.

[12] X. Li, K. Pahlavan, and J. Beneat. Performance of TOA estimation techniques in indoor multipath channels. In *The 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, volume 2, pages 911–915, September 2002.

[13] N. Alsindi, X. Li, and K. Pahlavan. Performance of TOA estimation algorithms in different indoor multipath conditions. In *IEEE Wireless Communications and Networking Conference (WCNC)*, volume 1, pages 495–500, March 2004.

[14] P. Enge and P. Misra, editors. *Special issue on GPS: The Global Positioning System*. IEEE, January 1999.

[15] J. Werb and C. Lanzl. Designing a positioning system for finding things and people indoors. *IEEE Spectrum*, 35(9):71–78, September 1998.

[16] J. Lepak and M. Crescimanno. Speed of light measurement using ping. *American Physical Society - Meeting Abstracts*, April 2002. abstract B2.009+.

[17] L. Gammaitoni, P. Hanggi, P. Jung, and F. Marchesoni. Stochastic resonance. *Reviews of Modern Physics*, 70(1):223–287, 1998.

[18] C. Hoene, A. Günther, and A. Wolisz. Measuring the impact of slow user motion on packet loss and delay over IEEE 802.11b wireless links. In *Proc. of Workshop on Wireless Local Networks (WLN) 2003*, Bonn, Germany, October 2003.

[19] R. W. Potter. *The Art of Measurements*. Prentice Hall PTR, New Jersey, USA, 2000.

[20] F. Moss. Stochastic resonance: a signal+noise in a two state system. In *Proceedings of the 45th Annual Symposium on Frequency Control*, pages 649–658, May 1991.

[21] G.P. Harmer, B.R. Davis, and D. Abbott. A review of stochastic resonance: circuits and measurement. *IEEE Transactions on Instrumentation and Measurement*, 51(2):299–309, April 2002.

[22] Tolga Eren, David Goldenberg, Walter Whiteley, Yang Richard Yang, A. Stephen Morse, Brian Anderson, and Peter Belhumeu. Rigidity, computation, and randomization in network localization. In *INFOCOM 2004*, pages 2673– 2684, Hong Kong, March 2004.

[23] Dragos Niculescu and Badri Nath. Error characteristics of ad hoc positioning systems (aps). In *Proceedings of the 5th ACM international symposium on Mobile ad hoc networking and computing (MobiHoc'04)*, pages 20–30. ACM Press, 2004.

[24] F. Bouchereau and D. Brady. Bounds on range-resolution degradation using RSSI measurements. In *IEEE International Conference on Communications*, volume 6, pages 3246– 3250, June 2004.

[25] Eiman Elnahrawy, Xiaoyan Li, and Richard P. Martin. The limits of localization using signal strength: A comparative study. In *The First IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON 2004)*, Santa Clara, CA, October 2004.

[26] C. Chang and A. Sahai. Estimation bounds for localization. In *The First IEEE International Conference on Sensor and Ad hoc Communications and Networks (SECON 2004)*, Santa Clara, CA, October 2004.

[27] Li Cong and Weihua Zhuang. Non-line-of-sight error mitigation in mobile location. In *Infocom 2004*, pages 650– 659, Hong Kong, March 2004.

[28] C. Hoene. Easysnuffle - a tool to measure the performance of multimedia flows over ieee 802.11b. URL: ¡a href=”http://www.tkn.tu-berlin.de/research/easysnuffle/”¿http://www.tkn.tu-berlin.de/research/easysnuffle/¡/a¿, March 2001.

[29] A. Günther. Accuracy of propagation delay measurements in wireless LANs. Intermediate thesis, Technical University of Berlin, August 2004.