University of Paderborn

Computer Networks Group

Experimental evaluation of IEEE 802.11a-based WLANs for medium range communication

Falk Eitzen, Stefan Valentin, Kai Gossens,
Holger Karl, and Oliver Rolfes

{folk|stefan.valentin|gossens|holger.karl}@upb.de,
o.rolfes@eggenet.de

February 2007

Technical Report TR-RI-07-281

The research project *Experimentelle Bewertung neuer WLAN/WMAN-Standards zur Kommunikation über mittlere Reichweite* is a cooperation between the *Eggenet GmbH* and the *Computer networks group, University of Paderborn*. This technical report is based on the final project report submitted on 22 December 2006.

Technical report

Abstract

IEEE 802.11a-based Wireless Local Area Networks (WLANs) provide high data rates, are widely adopted, cheap, easy to use and to deploy. It seems natural to use this technique in scenarios other than for an office or home WLAN, for example, to provide wireless Internet access via the "last mile", to establish fast Wireless Metropolitan Area Networks (WMANs), or for wireless backup links. Since IEEE 802.11a-based WLANs were originally not designed for such *outdoor scenarios*, these applications require careful performance and parameter studies. In this technical report we present an extensive experimental study based on 4 months of measurement in a peer-to-peer medium-range scenario under outdoor conditions. In this scenario we study the performance, system stability, and error characteristics of an IEEE 802.11a-based WLAN. Our measurements show that in such scenarios high average on-air rates of 36 MBit/s can be reached. This leads to high average UDP data rates of 17 MBit/s at sufficient data rate stability. We further discuss system stability and precisely examine transmission error statistics.

1 Introduction

Wireless Local Area Networks (WLANs) enable cheap and easy communication in home and office scenarios. In these indoor scenarios typically devices are used which comply to the IEEE standards 802.11, 802.11a, and 802.11g [1, 2, 3, 4]. Communication systems based on these devices and standards provide the following benefits:

- **Widely adopted:** IEEE 802.11a/g compliant WLAN chip sets have become a standard component of today's Notebooks and hand-held computers. Typically, customers used to indoor WLAN do not understand why *outside* they have to use a different technology, e.g. cellular-based GSM or UMTS. Hence, the number of possible customers for public WLAN/WMAN access continuously grows.
- **Low device costs:** Standardization enables interoperability and, thus, ensures an open market for all manufacturers' WLAN devices, e.g. chip sets, network cards or integrated WLAN-Routers. This, finally, enables competition and ensures low device costs.
- **Ease of deployment:** WLAN devices are specified and built for the end-user. Thus, they include many functions to ensure easy deployment, e.g. automatic channel selection and Medium Access Control (MAC), as well as suitable pre-configuration. In combination with unlicensed frequency bands, this avoids extensive *manual* setup and calibration procedures, e.g. as required in cellular systems.
- **Continuous improvement:** Based on the above standards the IEEE 802.11 working group continuously proposes standard improvements, e.g. the current IEEE 802.11n draft for high data rate communication [5, 6]. These extensions enable to use up-to-date communication techniques, e.g. multiple antenna systems, while providing legacy support.

Although several approaches and devices for outdoor usage exist, they typically do not provide all of these benefits. For example, currently, UMTS base stations and end-user terminals are neither cheap nor world-wide adopted. Using this technology requires a complex infrastructure resulting in extensive connection fees. Since these additional techniques significantly increase cost and complexity, e.g. due to additional hardware and connection fees, many customers do not accept their usage. This situation may change with new approaches, such as the IEEE 802.16 standards [7, 8, 9], called WiMAX [10]. However, as long as these devices are not included in a typical mobile computer, only a few early users might adopt them. Furthermore, a fully deployed cellular or even WiMAX infrastructure makes it difficult to integrate new, improved wireless network transmission techniques.

This raises the question whether it is possible to exploit all of the above mentioned benefits by employing cheap and widely adopted WLAN techniques in outdoor scenarios. In this technical report we study this question *experimentally*. By measurements we show whether it is suitable to employ IEEE 802.11a compliant WLAN devices even in outdoor scenarios for which they are neither specified nor commonly used. We focus on a direct Line Of Sight (LOS), medium-range connection and stationary devices. This setup provides results suitable for several application scenarios such as the last mile access ("wireless DSL"),

WMANs, or the usage of wireless backup links in addition to cable connections. To analyze whether the usage of WLAN techniques in such scenarios is suitable, we perform experiments to characterize the following aspects:

- **Channel conditions and physical layer performance:** In every wireless communication system the state of the wireless channel and the performance of basic communication functions at the physical layer finally limit the achievable performance of the overall system. In WLAN systems, physical layer functions are typically adjusted for wireless indoor channels. Since it is unclear how these functions perform in outdoor scenarios a careful performance and parameter study at the physical layer is crucial to analyze which performance is possible at the application layer.

- **Application layer performance:** Since the application layer, e.g. as a web browser, is directly seen by the user, measuring the systems performance at the application layer includes the effects introduced by communication functions between the wireless channel and the user. Hence, the performance at this layer is finally relevant for the user's impression of the provided service.

- **System stability:** Even if a communication system provides high performance at the Application layer its usage may become unacceptable if this performance highly fluctuates or is not reliably available. While this may have technical causes, e.g. soft- or hardware errors, the unstable nature of the wireless channels may introduce further performance variations. For this reason we, firstly, evaluate the stability of the employed hard- and software and, secondly, carefully study the variation of our performance metrics. Furthermore, we analyze the characteristics of the introduced transmission errors which, as in reference [11], enables to rate the link quality more precisely.

We evaluate the above characteristics for an IEEE 802.11a-based WLAN scenario by defining suitable performance metrics, performing extensive measurements, and by analyzing the obtained statistics. This procedure basically follows standard approaches, e.g. as in reference [12].

This technical report, firstly, provides a detailed description of the scenario and measurement setup and discusses the applied methodology, performance metrics, and studied factors (Section 2). Second, the measurement results are shown and interpreted in Section 3. We, finally, conclude this report in Section4.

2 Measurement setup and scenario

This section introduces the setup of the wireless link. It consists of the basic setup, the measurement system and the methodology, including all metrics, factors and parameters that were used during the measurement.

2.1 Basic scenario

The established connection directly links two devices based on the IEEE 802.11a standard over a distance of 2.3 km. To establish the link typical hardware and antennas were used. Both

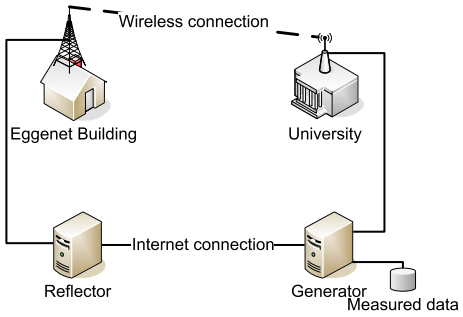


Figure 1: Setup of the established measurement scenario.

antennas are in Line Of Sight (LOS) and, although the antennas do not move, mobility may occur within the propagation environment. Figure 1 shows an overview of the system setup. Each of the shown stations is connected via 100 Mbit/s Ethernet to a computer that controls the measurements and stores the measured data. On the the sender's side this computer is called "Generator", on the receiver's side it is called "Reflector". The computers are out-of-the-box Intel Pentium III machines running at 800 MHz with 256 Mb system memory; the operating system is Microsoft Windows XP Professional. Both computers hold a connection to the Internet which is used for controlling the measurement and collecting the data.

The hardware used to establish the wireless link is made by Proxim Inc. As sender of the measurement data stream a Tsunami MP.11a 5054 BSU (Base Station Unit) is used, and a Tsunami MP.11a 5054 SU (Subscriber Unit) receives this data and sends acknowledgments and management data vice versa. The base station unit provides the services of a standard access point; the subscriber unit registers to it. Both devices automatically establish a IEEE 802.11a-based connection. They also support some extensions to the standard IEEE 802.11a protocol. These extensions pertain to the management of multiple wireless connections between a base station unit and a couple of subscriber units (Wireless Outdoor Routing Protocol WORP) as well as some security enhancements [13] [14]. The security enhancements prevent normal IEEE 802.11a devices from registering to the base station unit. Neither the WORP extensions nor the security enhancements did affect our measurements since we were only using a connection between *one* subscriber unit and base station unit.

The security enhancements are transparent to the user. All other parameters of the devices match with a typical IEEE 802.11a system. For this reason, we treat the connection between the devices as a standard IEEE 802.11a connection [13].

Standard directed antennas made by Proxim were used. Placing at the top of the buildings results in a direct line of sight connection of approximately 2.3 km. The technical data of the antennas is shown in Table 1. The antennas are connected to the sender and receiver using a cable with attenuation 3 dB.

2.2 Measurement system

The used hardware is not the sole part of the setup. There is also the software running on the sender and the receiver and its configuration. The firmware running on both MP.11a devices

Table 1: Technical data of the antennas[15][16]

	Sender (University)	Receiver (Eggenet building)
Type	Proxim 5054-SA-60-17	Proxim 5054-PA-18
Frequency	5.150 - 5.875 GHz	5.250 - 5.785 GHz
Antenna gain	16.5dBi	18 dBi
Beam width	60 °V / 6 °H	18 °V / 18 °H
Polarization	vertical	vertical

is Version 2.3. This firmware was used during the whole measurement period. Most of the provided settings of the internal software were left to factory defaults. Only the encryption keys, passwords for management access, and regional settings were changed. The regional settings were set to German not to violate German frequency regulations[17].

We also enabled the dynamic data rate selection. Without enabling dynamic data rate selection, the devices run at a fixed data rate of 36 Mbit/s, else devices support physical data rates up to 54 Mbit/s.

There are some other features supported by the base station unit. These features (e.g. Network Address Translation, NAT) were not used during our measurement.

The HF output power of the MP.11a devices is fixed to 0 dBm which does not include antenna gain and cable loss. With cable loss and antenna gain this results to a transmission power of 22.4 mW (EIRP) at the antenna of the BSU and to 31.6 mW (EIRP) at the SU antenna. Both values comply with the German frequency regulations [17]. The TX frequency range (IEEE 802.11a channel) is chosen by the devices automatically.

2.3 Measurement methodology

The Tsunami MP.11 base station provides system statistics. This data is accessible via the Simple Network Management Protocol SNMP. The software used to collect data via the SNMP interface was developed for this study and written in Java. It cyclical reads the values from the sender and stores them on the generator. The metrics on the physical layer are:

- Signal and noise from SU and BSU.
- Actual on-air transmission rate between the physical layers at SU and BSU.
- Number of frames that had transmission errors.

Values for signal, noise, and data rate were collected every second. Data about the number of failures and retransmissions are collected every two seconds. The reason for this is that the base station refreshes its internal data record in these intervals.

In addition to the collection of data from the SNMP, a constant data stream of UDP datagrams was sent over the wireless link from the generator to the reflector. Every frame of this data stream contained a sequential number that was stored at the reflector. With a packet size of 1400 Bytes and 100 transmitted frames per second, the data rate of the stream was about 1 Mbit/s.

Weather data was recorded to examine the influence of weather on the wireless connection. The data was provided by the weather observation station of the university [18]. The data was collected every 10 minutes via the web interface of the weather station.

The above described physical layer metrics examine the theoretically achievable data rate due to physical properties. We studied application layer performance via the following metrics:

- Effective data rate (e.g. the data rate between two applications) [Bits/s]
- Latency of the data packets on application level [s]
- Jitter of the data packets [s]
- Packet failures of a data stream

To collect the data for this metrics the network performance software IPERF [19] from the University of Illinois was used. IPERF provides the metrics effective data rate, jitter, and packet failures for an UDP stream for a given input data rate. For a TCP stream it provides only the output data rate. The input data rate of a TCP stream is handled by TCP itself, since TCP automatically adjusts the input data rate . IPERF runs on the generator and the reflector station. It is embedded in a Perl-written test bench. This test bench controls all measurements on the application layer. Each measurement contains of 2 intervals: During the first interval IPERF runs configured with the current metric for a period of 15 seconds. The gathered data is stored on the generator. After this an idle period of 5 second follows. In this period no data is transmitted between the generator and the reflector. This is required to flush the transmit queues and buffers on each side and to set up the system for the next measurement.

The latency on the application layer is measured with the ICMP protocol in parallel to all IPERF measurements. Every second an ICMP packet with a payload of 1024 bytes is transmitted from the generator to the reflector.

3 Measurement results

This chapter presents the results of the performed measurements. It starts with the physical layer and goes on to the application layer and the availability. At last a small analysis of the runlength distribution is presented.

There are no results concerning the influence of weather to the quality of the connection. The reason is that we could not see an evident correlation between the weather and the channel quality.

3.1 Physical layer measurements

The Tsunami MP.11 5054 devices measure the signal to noise ratio. The data rate chosen on the physical layer depends on these measured values. They are stored in the devices and can be read out using SNMP. The values stored in the devices are already time averages of 2 values calculated as

$$\text{value}_{\text{avg}} = \frac{3}{4}\text{value}_{\text{old}} + \frac{1}{4}\text{value}_{\text{new}} \tag{1}$$

Table 2: Thresholds for data rates[14]

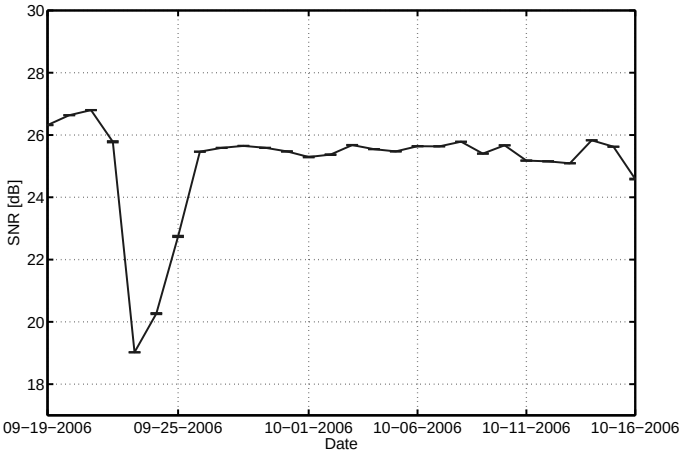
Data rate	SNR threshold
6 Mbit/s	6 dB
9 Mbit/s	7 dB
12 Mbit/s	9 dB
18 Mbit/s	11 dB
24 Mbit/s	14 dB
36 Mbit/s	18 dB
48 Mbit/s	22 dB
54 Mbit/s	25 dB

The signal strength and the noise is measured for each transmitted frame. For our measurement the values were read out every second since the devices update their internal values in this interval. The measurement started on September the 19th and stopped on October the 26th. During this period the measurement was only interrupted by device resets due to firmware crashes.

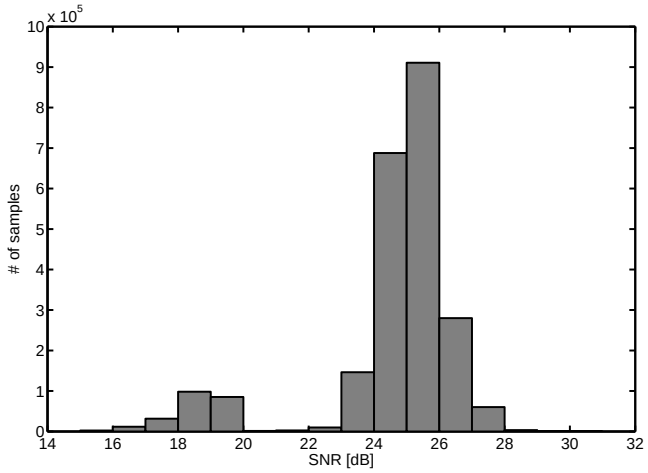
Figure 2(a) shows the characteristics of the measured SNR values. Each point in the figure represents means of all values per day. Confidence intervals are shown for a 95% confidence level. As shown, the SNR values mostly vary slightly in the interval 25 to 26 dB. The histogram of the measured values is shown in Figure 2(b). It confirms that the values are mostly in the interval mentioned before. Only a few values are higher than 27 dB. The histogram shows two peaks. One at the values around 26 dB and one around 18 dB. The highest peak corresponds to the SNR values that were mostly measured. The other, at 18 dB, corresponds to the low SNR ratio measured from September the 23th to September the 25th. We do not know the reason for the sudden decrease of the SNR. On the other hand, the increase of the values on September the 25th happened after a reset of the base station unit; so this may result from a system anomaly.

The next metric that was measured was the on-air physical data rate chosen by the devices. It depends on the measured SNR values. For choosing the data rate the devices take the measured SNR values and compare it with threshold values shown in Table 2. This leads to the data rate that will be used. Note that the SNR is not the only parameter that is used for choosing the data rate. It is also affected by the current amount of transmission failures and retransmissions. This mechanism provides a fall back if the chosen data rate is too high and would lead to frequent transmission failures and retransmissions. Figure 3 shows the characteristics of the chosen on air data rate as well as its histogram. The data rate of the BSU mostly fluctuates between 36 and 48 Mbit/s. This leads to the conclusion that one can expect a minimum data rate of 36 Mbit/s on the physical layer in this scenario. The impact of the period with low SNR values can be seen also in the data rate characteristics of the base station unit. During these days the data rate decreased with the SNR. The mean of the data rate is less than 36 Mbit/s during this period, which means that the data rate fluctuates between 24 and 36 Mbit/s. The histogram of the values confirms this observation.

On the other hand, the SU data rate shows strongly fluctuates between 24 and 48 Mbit/s.

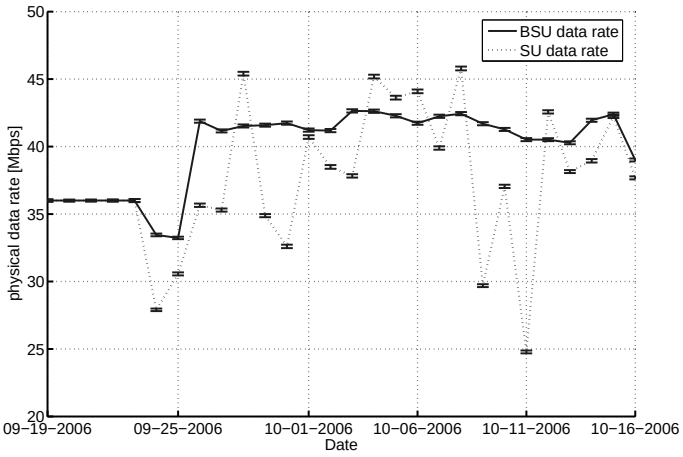


(a) Signal to noise ratio (SNR) vs. time. Confidence intervals are shown for a confidence level of 95%.

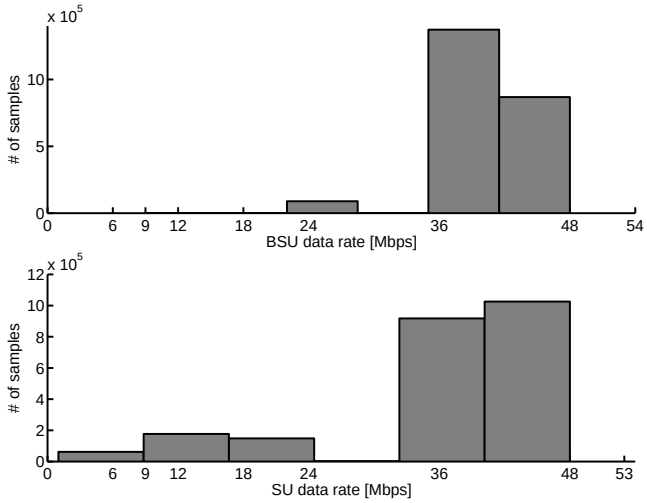


(b) Histogram of the signal to noise ratio values. Mean is 25.1 dB, standard deviation is 2.2 dB.

Figure 2: Signal to noise ratio (SNR) measured over a period of 28 days (19th of September 2006 to the 16th of October 2006).



(a) On-air data rate at the physical layer of BSU and SU. The solid line represents the data rate of the BSU, the dotted line represents the data rate of the SU. Confidence intervals are shown for a confidence level of 95%.



(b) Histogram of the chosen on-air data rates of BSU and SU. The mean of the measured values is 40 Mbit/s for the BSU and 37.5 Mbit/s for the SU. Standard deviations are 6.6 Mbit/s (BSU) and 6.3 Mbit/s (SU).

Figure 3: Characteristics of the on-air data rate at the physical layer of the SU and BSU. The measurements were performed in parallel to the SNR measurements shown in Figure 2.

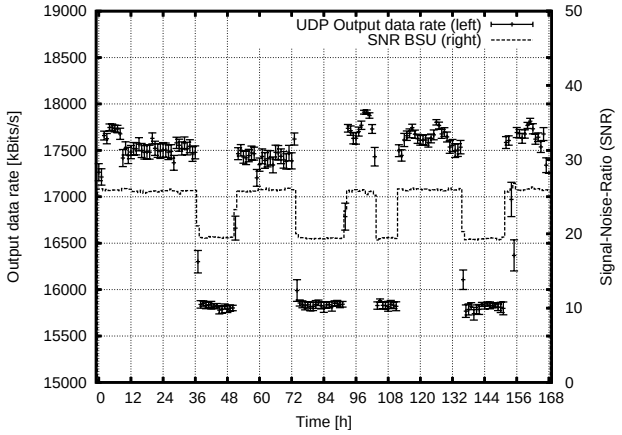


Figure 4: UDP data rate compared to the SNR, measured for 7 days from the 25th of November 2006 to the 1st of December 2006. Confidence intervals are shown for a confidence level of 95%. The input data rate of the UDP stream was 18 Mbit/s.

However, since there was no constant data stream from SU to BSU these results are not relevant. Since the SNR is measured over the incoming frames and there was no data stream sent from the SU to the BSU, it could be difficult to determine the correct data rate for the SU.

3.2 Application layer measurements

The generator and the reflector runs the software IPERF to collect the data from the measurements. The test bench executed the following measurements:

- UDP performance measurement with a fixed input data rate over a period of 7 Days
- TCP maximum performance measurement with a fixed TCP window size over a period of 7 Days
- UDP measurement with an increasing input data rate
- Time of failures and a time between failures measurement over a period of 28 days.

The first measurement describes the effect of the SNR on the UDP output data rate. This measurement started on November the 25th and stopped on December the 1st. The UDP input data rate was set to 18 Mbit/s. The SNR values were measured as described in Section 3.1.

Figure 4 shows the effect of SNR on, respectively, the chosen data rate of the SU and BSU and the UDP input data rate for a period of seven days. Confidence intervals are shown for 95% confidence level in this figure and in Figures 5 to 8. The figure shows the variation of the SNR value and the corresponding changes of the output data rate. With a mean SNR value of 19.5 dB the output data rate reduces to a mean of 15.8 Mbit/s. On the higher mean SNR value the output data rate rises to a mean value of 17.5 Mbit/s. The maximum output data

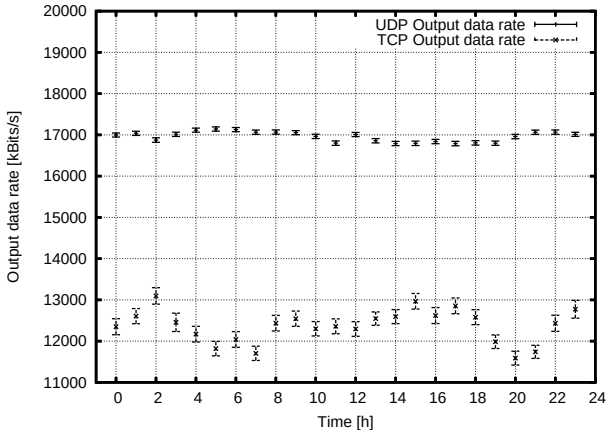


Figure 5: TCP and UDP data rate vs. hour per day. Measured for 7 days from 25th of November 2006 to 1st of December 2006 (UDP) and from 10th of December 2006 to 16th of December 2006 (TCP). The input data rate of the UDP stream is 18 Mbit/s, the TCP window size is 64k. Confidence intervals are shown for a confidence level of 95%.

rate in this figure is 17.9 Mbit/s and the maximum confidence interval width is 92 Kbit/s. Although from this figure one might expect a correlation between the time of the day and the output data rate, this is disproved in Figure 5. This figure shows the mean values for the time of the day per hour for a measurement period of 7 days. It shows that all results for UDP are around 17 Mbit/s.

In addition to the UDP measurement we performed TCP measurements with TCP window size of 64k. These measurements started on December the 10th and lasted until December the 16th. The result is presented by the dotted line in Figure 5. The TCP algorithm determined the maximum input data rate. The range of the TCP output data rate is from 11.6 Mbit/s to 13.1 Mbit/s. The reason for the slight variation of the output data rate of the TCP stream is unknown and will be further studied in the scope of a bachelor thesis. A possible reason is the determination of the highest input data rate by the TCP algorithm. The reason for the lower output data rate of the TCP data stream compared to the UDP data stream are the parameters of the TCP connection (e.g. TCP window size) and the maximum transfer unit (MTU) size.

The metrics UDP output data rate, jitter, latency, and packet loss rate are measured depending on the input data rate. The results of this measurement are shown in Figures 6, 7 and 8. The input data rate increases from 1 Mbit/s in steps of 400 Kbit/s to a maximum input data rate of 23.4 Mbit/s. At this input data rate, the connection is saturated. The effective data rate begins to fall and the amount of dropped packets increases. Every value was measured 20 times before increasing. The measurements were done on November the 24th 2006 from 6:00am to 1:15pm.

In Figure 6 the solid lines show the mean values of the output data rates. In addition the dotted line shows the packet loss rate. The output data rate increases linearly to the input data rate to a maximum value of 21063 Kbit/s. Close to the maximum output data rate the

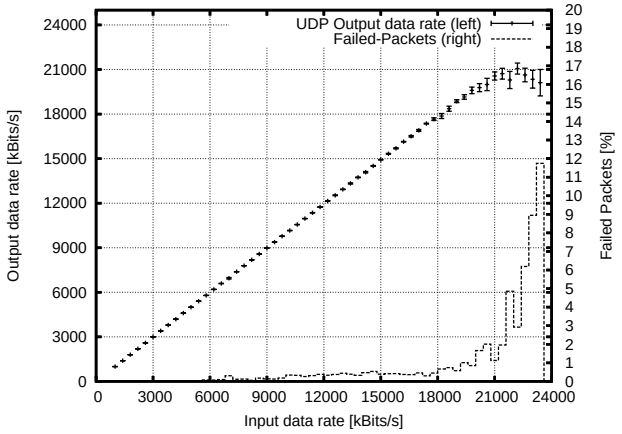


Figure 6: Output data rate and percentage of failed packets vs. input rate for an UDP stream. Confidence intervals are shown for a confidence level of 95%.

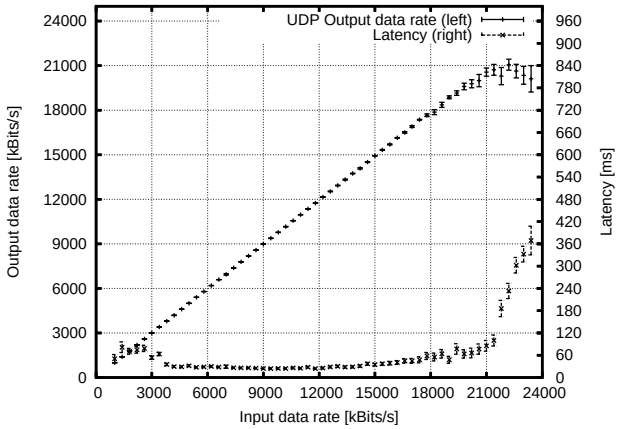


Figure 7: Mean packet latency and output data rate vs. input rate for an UDP stream. Confidence intervals are shown for a confidence level of 95%.

confidence intervals start to grow. This behavior depends on the failed packets ratio also shown in this figure. The packet loss rate escalates for input data rates over 21000 Kbit/s.

Figure 7 shows the corresponding latency of the ICMP data packets to the output data rate. The minimum latency of the ICMP packets is 23.95 ms and increase to 85.24 ms (input data rate = 21000 Kbit/s). Above this maximum output data rate the latency escalates similar to the packet fail rate. The reason for this behavior is the congestion of the transmit queues at the BSU. The latency values for input data rates smaller than 4000 Kbit/s are higher than the latency values between 4000 Kbit/s and 18000 Kbit/s.

The last metric of this measurement is the standard deviation of the UDP packet latency, called jitter. Figure 8 shows the results depending on the input data rate. The maximum mean value is 5.0 ms, the average of the mean values is 2.2 ms. The largest confidence interval width is 3.4 ms, hence, the maximum range is 8 ms. The jitter does not grow not above 21 Mbit/s since this value can only be measured for correctly transmitted packets. Thus, the

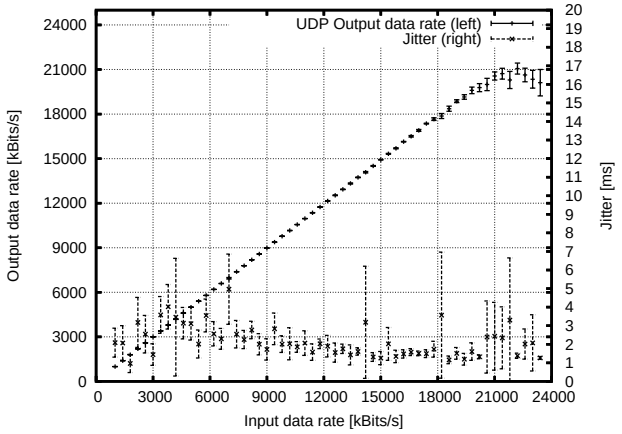


Figure 8: UDP packet jitter and output data rate vs. input rate for an UDP stream. Confidence intervals are shown for a confidence level of 95%.

measured jitter is quite equal for all UDP input data rates of the wireless link.

3.3 System failure measurements

Assume a system failure if the BSU is not able to send date to the SU. A failure is detected if the SNR value of the SU or the BSU is equal to zero, or if the number of registered subscriber units is zero. A failure is also detected if the respond time of a device grows larger than 5 seconds. If a device is not responding during this time, we assume that the device as well as the connection is down. The measurement for the failure times lasted for 28 days. It started on October the 8th and stopped on November the 4th. The histogram of the failure durations is shown in Figure 9. The histogram shows two peaks at 120 seconds and at 180 seconds. The reason for the 180 seconds peak is at the BSU. The BSU needs nearly 180 seconds to reboot the system to activate the wireless link. We do not know the reason for the 120 seconds peak, but since we can exclude BSU failures this may result from a failure at the subscriber unit. The mean value of the duration of a failure is 143 seconds.

A common system failure metric is shown in Figure 10. It shows the time between failures. The measurement period is the same as for Figure 9. During this period of measurement, the wireless connection was stable for a maximum time of 43.6 hours. The mean time between failures is approximately 8 hours. The availability of the connection is about 99.5 %.

The failures of the BSU and the SU may result from firmware or hardware problems or from automatic reset if a radar impulse is detected by the HF unit [13].

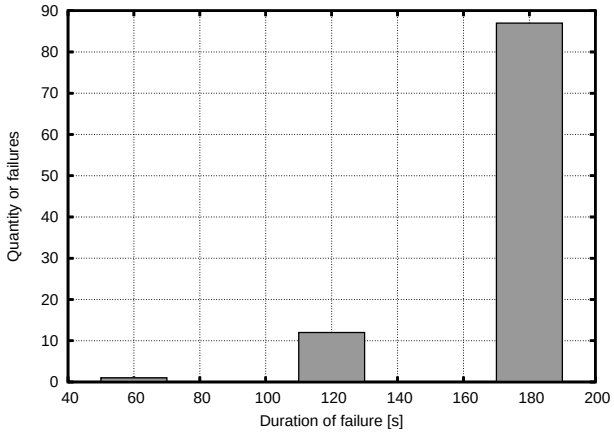


Figure 9: Duration of failure measured for a period of 28 days (8th October to 4th November 2006). The mean duration of a failure is 143 seconds.

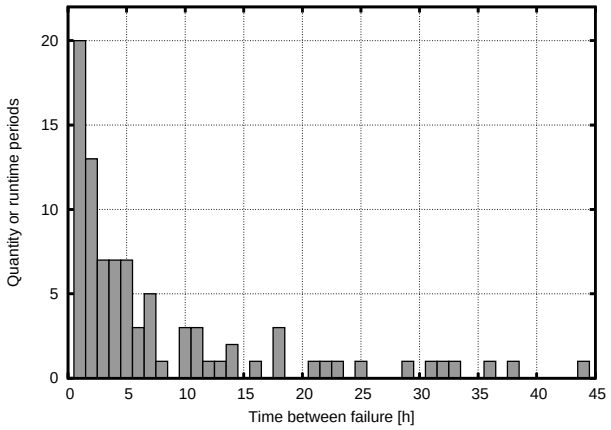


Figure 10: Time between failures measured for a period of 28 days (8th October to 4th November 2006). The mean time between failures (MTBF) is approximately 8 hours (28732 seconds).

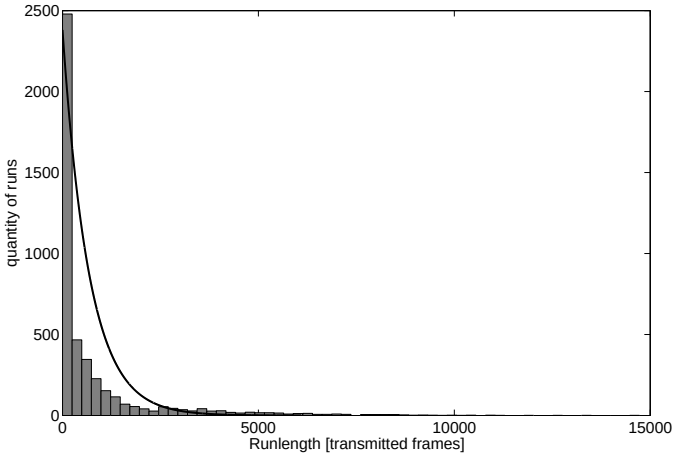


Figure 11: Histogram for the runlength of correctly received packets. The bars show the histogram of the runlength. The solid line represents an exponential distributed probability density function (PDF) parameterized with the mean of the measured runlength, i.e. 790 packets.

3.4 Runlength distribution

The runlength distribution gives an overview of the number of packets transmitted without a packet failure. Such a run represents the number of sequentially received packets without an error. To measure this, a UDP packet stream was sent over the connection with a fixed rate. Per second 500 packets with a size of 1024 byte were sent. Each packet contained a sequence number that was stored on the reflector.

Out of the data the number of packets that was transmitted sequentially without failures was calculated. The results of this measurement is shown in Figure 11 and 11. Figure 11 shows the histogram of the measured runlength. As can be seen, small runs of packets without failure occur much more often than long runs. The mean length of a run is about 790 transmitted packets without a failure. By observing the histogram shown in Figure 11 we assume the probability of the runlength to be exponentially distributed. For this reason an exponential probability density function parameterized with the mean of the measured data is also plotted in Figure 11. This probability density function resembles the the histogram of the measured values.

We further study this in Figure 12. Here, the solid line shows the empirical complementary cumulative distribution function (ECCDF) of the measured values and is compared to a exponential CCDF parameterized with the mean of the measured values. Since the measured data behaves similar to the shown exponential CCDF this leads to the assumption that the runlength is exponential distributed.

Comparing the observations of the measured values to the exponential distribution function confirms our assumption of an exponential probability distribution of for the runlength of the error free transmitted packets. Nevertheless more statistical tests are required to prove this assumption.

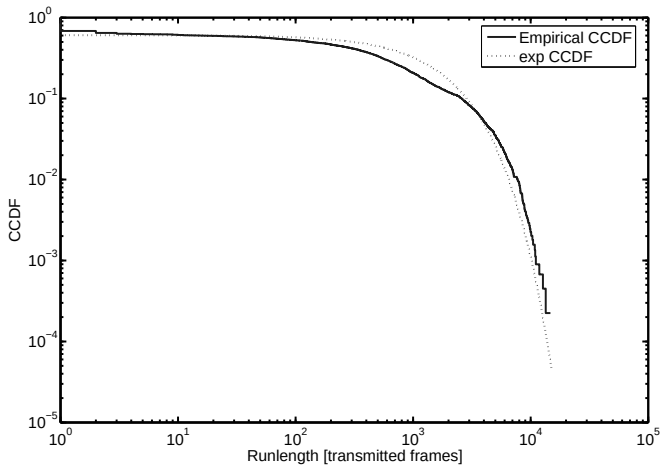


Figure 12: Empirical complementary cumulative distribution function (ECCDF) of the correctly received packet runlength compared to a standard exponential CCDF.

4 Conclusion

In this technical report we evaluated whether it is possible to exploit the benefits of WLAN technology, as typically used in indoor scenarios, even under medium range outdoor conditions. For this reason we analyzed the performance and stability of a peer-to-peer WLAN Line Of Sight (LOS) link by experiments within a measurement period of 4 months. Based on our measurement results we conclude as follows:

- **Channel conditions and physical layer performance:** The measurements on the physical layer showed that standard WLAN hardware is able to provide high on air data rates over medium range. The measured data rate mostly fluctuated between 36 and 48 Mbit/s. In the studied scenario an average on air-data rates of 36 Mbit/s can be expected without high variance. Only during a small period the signal to noise ratio showed a sudden decrease. This, naturally, had an impact on the on air data rate, but the impact was relatively small; during this period the on air data rate decreased to 24 to 36 Mbit/s. Thus, the physical layer measurements showed a high performance for this connection.

- **Application layer performance:** Measurements at the application layer lead to results similar to the physical layer study. High data rates were reached using the UDP and the TCP protocols with standard parameters. On the average application layer data rates of 17 Mbit/s with UDP and 12 Mbit/s with TCP were reached. For both protocols the results show only a small variance. The difference between the UDP and TCP results from the overhead due to the TCP acknowledgments and flow control functions. The media streaming relevant metrics packet latency and jitter also show high performance. The measurements show that the data rate of this medium range connection is comparable to a typical short range WLAN connection.

- **System stability:** An established connection between the devices is stable. As mentioned, it shows only a small variance in data rate and latency. This is the case for the Physical as well as for the Application layer. This availability of the connection satisfies the expectations for a typical WLAN link. Nevertheless, there were several *system stability* issues which lead to frequent device resets and, thus, disconnections of the stations for 143 seconds on the average. After this time the connection was available again. The mean time between these failures was measured to be approximately 8 hours. A possible cause of these disconnections are problems in Proxim's firmware Version 2.3 or resets due to (not logged) Radar beams recognized by the high frequency front end.

We conclude that it is possible to profit from cheap and easy to use and to deploy IEEE 802.11a-based WLAN technology in medium-range outdoor scenarios. Using the appropriate antennas, data rates and latencies comparable to indoor scenarios can be reached while staying within frequency and transmission power regulations. This high performance, if, e.g., compared to cellular approaches, is provided at acceptable variance and with almost no configuration and calibration overhead. However, while this significantly reduces deployment costs the required automatisms, e.g. frequency control, MAC, and radar recognition, may introduce unpredictable system behavior. Due to the system stability issues during the measurement period we conclude finally that high availability cannot be provided by the employed devices. This makes the studied scenario most suitable for non-critical applications, e.g. for providing backup links or public Wireless Metropolitan Area Networks (WMANs) with *soft* service level agreements.

References

[1] IEEE, *Standard for Information technology – Telecommunications and information exchange between systems – LAN/MAN Specific requirements – Part 11: Wireless LAN MAC and PHY Layer specifications*, Std 802.11 edition, 1999.

[2] IEEE, *Supplement to standard for telecommunications and information exchange between systems – LAN/MAN Specific requirements – Part 11: Wireless LAN MAC and PHY specifications: High speed physical layer in the 5-GHz band*, Std 802.11a edition, 1999.

[3] IEEE, *Standard for Information technology – Telecommunications and information exchange between systems – LAN/MAN Specific requirements – Part 11: Wireless LAN MAC and PHY Layer specifications: – Amendment 4: Further higher-speed physical layer extension in the 2.4 GHz band*, Std 802.11g, 1999 (reaff 2003) edition, 2003.

[4] B. O'Hara and A. Petrick, *IEEE 802.11 Handbook: A designers companion*, IEEE Press, 1999.

[5] Y. Xiao, "IEEE 802.11n: enhancements for higher throughput in wireless lans," *Wireless Communications, IEEE*, vol. 12, no. 6, pp. 82–91, Dec. 2005.

[6] M. K. A. Aziz, P. N. Fletcher, and A. R. Nix, "Performance analysis of IEEE 802.11n solutions combining MIMO architectures with iterative decoding and sub-optimal ML

detection via MMSE and zero forcing GIS solutions," in *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, 21-25 March 2004, vol. 3, pp. 1451–1456Vol.3.

[7] IEEE, *Standard for Local and metropolitan area networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems – Amendment 2: Medium Access Control Modifications and Additional Physical Layer Specifications for 2-11 GHz*, May 2003.

[8] IEEE, *Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, Nov. 2004.

[9] A. Ghosh, D.R. Wolter, J.G. Andrews, and R. Chen, "Broadband wireless access with WiMAX/802.16: current performance benchmarks and future potential," *IEEE Communications Magazine*, vol. 43, no. 2, pp. 129–136, Feb. 2005.

[10] "WiMAX forum," `http://www.wimaxforum.org/`.

[11] A. Köpke, A. Willig, and H. Karl, "Chaotic maps as parsimonious bit error models of wireless channels," in *Proc. IEEE INFOCOM*, San Francisco, CA, Mar. 2003.

[12] A. Willig, M. Kubisch, C. Hoene, and A. Wolisz, "Measurements of a wireless link in an industrial environment using an ieee 802.11-compliant physical layer," *IEEE Transactions on Industrial Electronics*, 2002.

[13] Proxim Wireless, *Tsunami MP.11 – Reference Manual*, 2.3 edition, 2004.

[14] Proxim Wireless, *Tsunami MP.11 model 2411 and model 5054 – Technical Specifications*, 2004.

[15] "17 dBi sector antenna specifications," Retrieved Jun. 16, 2006 from `http://www.proxim.com/products/bwa/accessories/5ghz/17dBi/`, 2005.

[16] "18 dBi panel antenna specifications," Retrieved Jun. 16, 2006 from `http://www.proxim.com/products/bwa/accessories/5ghz/18dBi/`, 2005.

[17] Bundesnetzagentur, *Allgemeinzuteilung von Frequenzen in den Bereichen 5150 MHz-5350 MHz und 5470 MHz-5725 MHz für Funkanwendungen zur breitbandigen Datenübertragung, WAS/WLAN (Wireless Access Systems including Wireless Local Area Networks) Vfg 8/2006*, 2006.

[18] "Weather observation station of the university of paderborn," `http://wetter.uni-paderborn.de/`, 2006.

[19] "Iperf - a network performance measurement tool," `http://dast.nlanr.net/Projects/Iperf/`, 2005.