Channel Access Rules for SRDs

November 2012

IMST GmbH

Carl-Friedrich-Gauß-Str. 2-4

47475 Kamp-Lintfort

Executive Summary

Short Range Devices (SRDs) are becoming increasingly popular as they benefit from the easy access to the radio spectrum in Europe and many other countries in the world using the license-exempt SRD bands. However, using license-exempt bands always means that there is a competition of different applications with different channel access schemes. This survey was charged by the Federal network Agency (BNetzA, Germany) to get an independent view to several aspects in the context of coexistence of different SRD applications working in the same band. Some key issues analysed in this report are:

- Characterisation of SRD applications
- Performance analysis of selected channel access scheme
- Reliability and latency of improved channel access schemes
- Coexistence of simple and improved access schemes
- Rewarding flexible systems with higher power or Duty Cycle? (e.g. CSMA, ACK, FH, AFA)

The analysis of potential SRD applications has shown that a large group of applications require small packet sizes and duty cycles below 1% for data transfer. Data rates in the order of ten to hundred kilobits per seconds are often used resulting in a typical bandwidth in the order of 100 kbps. Most applications have not very stringent latency requirements as even alarm systems can cope with a delay of few hundred milliseconds, but the requested link reliability might be high. A number of independent systems might be operated simultaneously within the same building, so that coexistence must be possible. As the majority of the SRDs will be battery operated, robust, simple, and energy efficient access schemes will be required.

Centralised **resource control** is known to provide a high resource utilisation, but a central control instance in one node will not be available in a scenario with simultaneously transmitting devices of different operators. Alternatively, resource allocation can be solved in a distributed manner defining a standardised common channel for resource control. Nevertheless, the overhead for neighbour node observation and resource allocation might be significant. Hence, this study focused on random access schemes.

Among the single carrier random access systems, **DC based random access** using unidirectional links for data transmission is the simplest one. This access scheme is used by applications requiring extremely low cost, small size "transmitter only" devices with low reliability requirements. The poor performance of uni-directional DC based random access justifies a strong limitation of the duty cycle on a single link, so that only a small portion of channel access time is used by this low efficient access scheme. A transmit duty cycle of 0.1% independent of the signal bandwidth might be reasonable for systems without LBT. A transmit power higher than 10 dBm shall be allowed at the cost of a lower duty cycle.

In order to maintain the same number of devices, the duty cycle of **non-adaptive FH** should not be higher than the duty cycle of a single carrier system. It is recommended to specify a minimum frequency separation of 100 kHz, corresponding to the typical bandwidth of SRD applications.

Using ALOHA like systems with an acknowledgement procedure significantly increases the number of devices operated within the same coverage area compared to DC based random access. Nevertheless, the performance of systems with packet loss detection considerably depends on the scheduling algorithm for packet retransmissions. The implementation of a load

dependent **backoff** procedure (e.g. binary exponential backoff) is strongly recommended to avoid a system collapse in higher traffic scenarios. ALOHA type systems shall have an application duty cycle of 0.1%, where ACK packet length and response time are added to the packet length of the transmitter for duty cycle calculations. ACK packets shall be allowed to be transmitted without LBT.

The system capacity can be more than doubled using CSMA-ACK instead of ALOHA. A listen-before-talk (LBT) procedure checks the channel state prior to each transmission and sends packets only if the channel is free. The performance of the LBT scheme significantly depends on the **LBT implementation parameters**, i.e. the minimum interferer measurement time and the dead time between the end of the channel measurement and the start of the packet transmission. Additionally, any harmful interferer which cannot be measured by the transmitter might significantly degrade the CSMA performance. The number of these hidden nodes needs to be minimised using a small **detection threshold** in the order of the typical receiver sensitivity level and independent on the transmit power. The duty cycle of LBT systems shall be 10 times higher than the duty cycle of non-LBT systems. While there is an easy trade-off between duty cycle and transmit power in non-LBT systems, the situation is more difficult in systems using LBT. Duty cycle restrictions for high power devices shall be more restrictive for LBT than for DC based random access systems. Alternatively, the SRD band needs to be separated into subbands with different power levels.

It is expected that a significant part of SRD applications will be single-carrier systems due to cost and complexity limitations. In general, the SRD band is not equally exploited using single carrier systems. Hence, the resource usage can be significantly improved by adding systems with a combination of listen before talk and frequency agility (**LBT & AFA**), as they will increase the traffic load on sparsely used frequency bands. As frequency agility helps to protect fixed frequency access systems, it shall be promoted by a higher duty cycle limit.

Operating high duty cycle **DSSS/ fast FH** in parallel to a LBT system is not recommended, as the threshold of the LBT should not be increased to cope with wideband signals. Hence, DSSS/ fast FH should be subject to transmit duty cycle limitations. Furthermore, SRD applications requiring low latency and high reliability (e.g. industrial automation) cannot be operated in parallel to random access schemes. For those applications, the SRD band can be only used in protected areas, where the access of SRDs is controlled by the premises owner. Otherwise, high data rate standards with guaranteed access for example in the 2.4 GHz band should be used.

The situation is slightly different for alarm systems like fire or intruder alarm, because the latency requirements are less stringent. Lost packets can be retransmitted based on acknowledgement procedures. If necessary, one could even think about different backoff procedures for safety-related applications to reduce the collision probability with a standard SRD application. Alarm systems themselves can implement redundancy, so that an alarm can be received by different devices with typically different interference situations. Most importantly, frequency agility can be used to select less congested channels for system operation. Hence, in general it should be possible to design highly reliable alarm systems without assigning a dedicated frequency band. Nevertheless, there is no guarantee in license-except bands, so there is always a certain channel load which will hamper a successful communication. Therefore, it might be reasonable to specify a small exclusive portion of the spectrum for very sensitive safety related applications like social alarms at the cost of a slightly lower spectral efficiency, which always results from splitting the SRD spectrum into different bands.

Contents

1. Referenced documents

[1] DIN EN 14604, Smoke alarm devices, 2005

[2] VdS 3515, VdS-Richtlinien mit Funk-Vernetzung, 2007-06, Germany

[3] ETSI TR 103 056, ERM, System Reference Document, SRD, Technical characteristics for SRD equipment for social alarm and alarm applications

[4] DIN EN54-25, Fire detection and fire alarm systems, Part 25: Components using radio links, 2009-02

[5] DIN EN 50131-5-3, Alarm systems. Intrusion systems. Part 5-3: Requirements for interconnections equipment using radio frequency techniques, 2009-06

[6] ETSI TR 102 649-2, ERM, Technical characteristics of SRD and RFID in the UHF Band, System Reference Document for RFID and SRD equipment, Part 2: Additional spectrum requirements for UHF RFID, non-specific SRDs and specific SRDs, 2010-06

[7] DIN EN 50134-5, Social alarms, Part 5: Alarm systems - Social alarm systems - Part 5: Interconnections and communications, 2005-08

[8] Directive 2006/32/EC of the European Parliament and of the Council on energy end-use efficiency and energy services and repealing Council Directive 93/76/EEC, 2006-04-05

[9] Directive 2006/72/EC of the European Parliament and of the Council on energy end-use efficiency and energy services and repealing Directive 2003/54/EC, 2009-07-13

[10] Directive 2006/73/EC of the European Parliament and of the Council concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC, 2009-07-13

[11] Standardization mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability, M/441, Final Report, Version 0.7, 2009-12-10

[12] EN 13757-4, Communication systems for meters and remote reading of meters - Part 4: Wireless meter readout (Radio meter reading for operation in SRD bands)

[13] ETSI TR 102 886, ERM, SM, SRD in the UHF band, System Reference Document, SRD, Spectrum Requirements for Smart Metering European access profile Protocol (PR-SMEP), 2011-07

[14] Netherlands Technical Agreement NTA 8130:2007; "Minimum set of functions for metering electricity, gas, thermal energy for domestic customers"

[15] ETSI EN 300 220, ERM, SRD, Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW, Part 1: Technical characteristics and test methods, 2012-01, Part 2: Supplementary parameters not intended for conformity purposes, 2000-09, Part 3: Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive, 2000-07

[16] ETSI EN 301 489, ERM, EMC, standard for radio equipment and services

[17] ERC Recommendation 70-03 relating to the use of short range devices (SRD), 2011-08-22

[18] ETSI TR 102 889-2, ERM, SRD, Part 2: Technical characteristics for SRD equipment for wireless industrial applications using technologies different from Ultra-Wide Band (UWB), 2011-08

[19] ZVEI Koexistenz von Funksystemen in der Automatisierungstechnik, 2008-11

[20] ETSI EN 301 839 ERM, SRD, Ultra Low Power Active Medical Implants (ULP-AMI) and Peripherals (ULP-AMP-P) operating in the frequency range 402 MHz to 405 MHz

[21] Ofcom, Spectrum Efficiency of wireless microphones, Final Report, 2010-06

[22] ETSI EN 300 422-1, ERM, Wireless microphones in the 25 MHz to 3 GHz frequency range, Part 1: Technical characteristics and methods of measurement, 2008-03

[23] ETSI EN 301 357, ERM, Cordless audio devices in the range 25 MHz to 2000 MHz, Part 1: Technical characteristics and test methods, 2006-05

[24] ETSI TR 102 449, TISPAN, Overview of Radio Frequency Identification (RFID) Tags in the telecommunications industry, 2006-01

[25] "Packet Switching in Radio Channels: Part I – Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics", Leonard Kleinrock, Fouad A. Tobagi, IEEE Transactions on Communications, Vol. 23, No. 12, December 1975

[26] "The Throughput of Packet Broadcasting Channels", Norman Abramson, IEEE Transactions on Communications, Vol. 25, No. 1, January 1977

[27] "Cascaded Clear Channel Assessment: Enhanced Carrier Sensing for Cognitive Radios", Soo Young Shin, I. Ramachandran, Sumit Roy, Wook Hyun Kwon, IEEE ICC, 2007

[28] ECC Report 37, Compatibility of planned SRD applications with currently existing radiocommunication applications in the frequency band 863-870 MHz, 2008-05

[29] Texas Instruments, White paper on Frequency Hopping Systems, AN017, K.K. Torvmark

[30] ETSI EN 300 328, ERM, Wideband transmission systems, Data transmission equipment operating in the 2,4 GHz ISM band and using wide band modulation techniques; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive, 2012-04

[31] ETSI EN 300 440, ERM, SRD, Radio equipment to be used in the 1 GHz to 40 GHz frequency range, Part 1, 2010-08

[32] Recommendation ITU-R P. 1238-7, Propagation data and prediction methods for the planning of indoor radio communication systems and radio local area networks in the frequency range 900 MHz to 100 GHz

[33] ECC Report 181, Improving spectrum efficiency in the SRD band, draft

2. Introduction

Short Range Devices (SRD) are becoming increasingly popular, not only for baby phones and door opener, but also for alarm applications, building automation, Smart Metering and others. These applications can be operated in license-exempt SRD bands (for example 433.05 - 434.79 MHz, 863 – 870 MHz, 2400.0 - 2483.5) and hence benefit from the easy access to the radio spectrum in Europe and many other countries in the world. Frequency harmonization supports economies of scale for equipment manufacturers reducing product costs. However, using license- exempt bands always means that there is a competition of different applications with different channel access schemes. Only for some safety related applications like alarms or social alarm there are exclusive bands available (e.g. 868.6 - 868.7 MHz, 869.200 - 869.400 MHz, 869.650 - 869.700 MHz).

Within the CEPT (European Conference of Postal and Telecommunications Administrations) there are ongoing activities to improve the regulation of the available spectrum for SRDs. The project team PT SE24 is responsible for compatibility studies in relation to SRDs and the Short Range Device Maintenance Group (SRD/MG) is responsible for the frequency regulation for SRDs (e.g. ERC Recommendation 70-03). Currently, there are a lot of activities within these groups to improve the spectrum use efficiency in SRD bands to account for the growing demand for low data rate SRDs (e.g. M2M, building automation, smart metering/smart grid).

This survey was charged by the Federal network Agency (BNetzA, Germany) to get an independent view to several aspects in the context of coexistence of different SRD applications working in the same band. The report is focused on low data rate applications which are mostly battery powered. Some key issues to be analysed in this report are:

- Performance analysis of channel access scheme
- Coexistence of simple and improved access schemes
- Coexistence of safety related systems with all others
- Are improved channel access schemes able to get a high reliability and low latency in all environments or are exclusive bands required for specific applications?
- Rewarding flexible and robust systems with higher power or Duty Cycle? (e.g. CSMA, ACK, FH, AFA)

The report is structured in the following way. Section 3 describes the main characteristics of SRD applications, which will be used to select suitable channel access schemes in section 4. The performance of the selected access schemes will be investigated in section 5 assuming that all devices within the neighbourhood are using the same access scheme with identical parameters settings. Section 6 analyses the coexistence of pairs of access schemes. Finally, the results of the performance analysis are translated into conclusions and recommendations in section 7.

This report will be publicly available in order to support the technical studies within CEPT.

3. SRD applications and their specifications

This section gives an overview on a selected set of SRD applications. These applications are either import from a social point of view like alarm systems including social alarms for elder people or safety relevant system like tire pressure monitoring or distance warning for automotives. Others are politically and economically driven like automatic metering systems promoting efficient use of energy resources with an expected significant increase of volume over the next decade. Further SRD applications with a growing market share are systems for home and building automation increasing comfort, safety, and energy consumption in residential and public buildings. Industrial automation will be another topic, although the focus of those applications will be on frequencies above 1.5 GHz. Furthermore, the high requirements towards reliability and latency will hamper an extensive use of the 870 MHz band, which will be the main focus of this study. Finally, the number of RFID systems especially in the 868 MHz band is expected to grow over the next years. The UHF band (300 MHz-3 GHz) provides an attractive transmission range of several meters and high data rates allowing simultaneous reading of a high number of tags.

These applications are described in more detail in the following chapters providing references to application standards where applicable. The main characteristics of the applications are summarised and translated to technical parameters like data volume, duty cycle, or latency requirements. Thereby, the following classifications are used:

Parameter	Value 1	Value 2	Value 3	Value 4
Packet size	small: < 300 bits	medium: <1kByte	large	
Data rate	small: < 50 kbps	medium: < 500 kbps	high	
Duty cycle	very low: < 0.1%	low <1%	medium<10%	high
Reliability	very high: virtually no message loss	high: message loss < 0.1%	medium: message loss < 1%	low
Link	unidirectional	bi-directional		
Latency	very small < 10ms	small < 100ms	medium < 1s	large
Installation	indoor	outdoor		
Power consumption	low: >10 years battery lifetime	medium: around 3 years battery lifetime	high: not battery powered	
Device size	very small: coins	small: match box	medium: pack of cigarettes	large

Table 1: Classification of parameters

3.1 Alarm systems

Alarm systems are designed to detect an event and to either distribute the alarm within the network or to pass the message to a central operation centre. There are numerous applications like smoke detection, fire alarm, intruder detection, or social alarms, which slightly differ with regards to their requirements. **Smoke detector** systems typically concentrate on the message spreading, so that if one sensor detects smoke, the alarms will sound on all the detectors in the network, improving the chances that occupants will be alerted. While wired smoke detectors are regulated by EN 14604 [1], there are only national standards for wireless smoke detector networks. For example, VdS 3515 [2] in Germany demands a battery lifetime of 10 years and a alarm forwarding delay of not more than 30 seconds on a single link. A typical smoke detector system consists of up to 20 sensors (see ETSI TR 103 056 [3]).

Parameter	Typical	Comment
Packet size	small	around 100 bits
Data rate	medium	100 kbps decreases power consumption, ETSI TR 102 649-2 [6]
Duty cycle	very low	alarm functionality, higher data traffic during alarm conditions
Reliability	high	
Link	bi-directional	
Latency	large	up to 30 seconds for a single link typically up to 120 seconds within a network
Installation	indoor	in buildings
Power consumption	low	>10 years battery life time
Device size	medium	

Table 2: Technical and implementation requirements for smoke detector systems

While smoke detector systems are typically installed in private residential buildings, **fire alarm** systems are widely deployed in commercial and industrial premises like shops, hotels or factories. The requirements for a fire alarm system as defined by EN 54-25 [4] are much more stringent, demanding regular network checks and high immunity to interference and site attenuation. A link failure needs to be detected within 300 s requiring bi-directional communication between all network nodes in even shorter time periods. Furthermore, simultaneous forwarding of different alarms within the same systems as well as parallel operation of two independent alarm systems of the same manufacturer shall be possible without messages losses and a maximum messages spreading time of 100 seconds. The battery lifetime is reduced to a minimum period of 36 months. A fire alarm network might include up to 500 devices, widely spread within a large building (see ETSI TR 103 056 [3]).

Parameter	Typical	Comment
Packet size	small	around 100 bits
Data rate	medium	100 kbps decreases power consumption, ETSI TR 102 649-2 [6]
Duty cycle	very low low	alarm functionality including regular network checks higher data traffic during alarm conditions
Reliability	very high	
Link	bi-directional	
Latency	medium to large	up to 100 seconds within a network
Installation	indoor (outdoor)	in and around buildings
Power consumption	medium	more than three years
Device size	medium	

Table 3: Technical and implementation requirements for fire alarm systems

For **intruder alarm** systems, the alert is typically transmitted to a central unit which for example sounds the siren outside the premises and optionally forwards the alert to a person or institution in charge (e.g. owner, surveillance centre, police). EN 50131 [5] specifies four different grades of security with increasing requirements on immunity to intentional and unintentional manipulation and interference, packet throughput and link failure detection. A link failure shall be detected and reported within 240 minutes for a grade 1 device, while only 10 seconds are allowed for grade 4 resulting in a relatively stringent requirement for periodic transmission. Typical residential alarm systems have less than 50 sensor devices (see ETSI TR 103 056 [3]).

Parameter	Typical	Comment
Packet size	small	around 100 bits
Data rate	medium	100 kbps decreases power consumption, ETSI TR 102 649-2 [6]
Duty cycle	very low low to medium	alarm functionality including regular network checks in between 240s (grade 1) down to 10s (grade 4) high data traffic during alarm conditions
Reliability	high to very high	message loss rate $< 10^{-3}$ (grade 1,2), $< 10^{-4}$ (grade 3,4)
Link	bi-directional	
Latency	large	several seconds, ETSI TR 103 056 [3]
Installation	indoor (outdoor)	in and around buildings
Power consumption	low	10 years for grade 1
Device size	small to medium	e.g. small sizes for door contacts

Table 4: Technical and implementation requirements for intruder alarm systems

There is an increasing trend for elder people to live independently in their own home despite of their physical handicaps. These systems for the so called Ambient Assisted Living (AAL) offering **social alarms** are only responsive in the case of emergency. A home ECG monitoring communicates exceeding limits only. A motion sensor could for example detect a collapse and initiate an automatic emergency call transmission. In an even simpler implementation the wearable transmitter just has an alarm button, which can be pressed in case of an emergency situation. EN 50134 [7] specifies the requirements for social alarms. The connection must be bi-directional allowing the health centre to confirm the alarm message and to communicate with the person in distress. Furthermore, alarm devices without controlled access to the frequency band shall use frequencies specifically dedicated to social alarm systems ([7], *page 7*). Social

alarms typically have a low duty cycle, but the requirements towards reliability during an alarm situation are high.

Parameter	Typical	Comment
Packet size	small	around 100 bits
Data rate	100 kbps	high data rate decreases power consumption, ETSI TR 102 649-2 [6]
Duty cycle	very low medium	alarm functionality high data traffic during alarm conditions due to communication function
Reliability	very high	
Link	bi-directional	
Latency	medium to large	several seconds, ETSI TR 103 056[3], ECC Report 181 [32]
Installation	indoor (outdoor)	in and around buildings
Power consumption	low	typically 10 years
Device size	small	

Table 5: Technical and implementation requirements for social alarm systems

An interesting additional functionality of all alarm systems is image transmission as a result of an alarm trigger. The image can be used by a monitoring centre to verify the alarm (see ETSI TR 103 056 [3] for more information). Although the required data volume is quite small, the image transmission might be shifted to another frequency band to keep the duty cycle for alarm transmissions as low as possible.

Especially devices for social alarms will have limited size so that they can be easily worn on body. Hence, alarm devices are not suited to frequencies below UHF. On the other side they should have a range of 20 m within buildings so that the higher frequencies above 1 GHz are not suitable due to the power limitations of a battery powered device. More information can be found in ETSI TR 102 649-2 [6].

3.2 Automatic Meter Reading (AMR)

To date remote metering (electricity, gas, water and heat) is used either by suppliers or by submetering service providers to determine the energy or water consumption in private houses from the outside without the need to enter the building. Meters can be simple transmitters connected to a central database for data collecting. Repeaters can be used to extend the range of the network, which might be either infrastructure devices or meter devices with repeater functionality. The latter requires the use of transceivers instead of simple transmitters, which increases the cost of the meter and its power consumption due to the forwarding functionality, but significantly reduces the infrastructure costs. Nevertheless, the use of transceivers in the meter devices offer additional features like reading data on demand, remote meter configuration and maintenance, or scheduled transmissions for collision avoidance.

Up to now remote metering has been done for billing purposes requiring a single measurement at the end of the year. The focus on energy efficiency (see Directive 2006/32/EC [8]) will dramatically change the attitude towards AMR requiring “intelligent” or smart metering with nearly real time data measurements. On the one hand it is expected that displaying the actual energy consumption allows the customer to make smarter decisions about his energy usage most likely resulting in energy savings, while on the other hand the management and control of

the power network will be supported by nearly real time information. Directive 2009/72/EC [9] for electricity and Directive 2009/73/EC [10] for gas extends the requirements towards intelligent metering systems assisting the active participation of consumers in the market. In March 2009, the European Commission issued a mandate M/441 [11] for the standardization of smart metering functionalities and communication for electricity, gas, heat, and water applications. Despite the fact that the smart metering requires significantly shorter measurement intervals, the final report of M/441 issued in December 2009 still considers battery powered devices: "Battery powered meters do have limited power supply resources as the communication process needs to be operated over many years without changing the power supply battery (typically at least 10 years and effective business cases may required longer periods). For this issue, specific communication procedures have been developed that are different from the electricity meters communications." Hence, most non-electricity meters are supposed to be battery powered and therefore limited with regards to their duty cycle. EN 13757-4 [12] specifies the requirements of parameters for the physical and the link layer for this kind of metering devices.

Metering devices should have a range of 20 m within building so that the higher frequencies above 1 GHz are not suitable due to the power limitations of a battery powered devices. ETSI TR 102 649-2 [6] recommends to use the same interface and frequency band for metering and alarm equipment, so that the same infrastructure can be used by both systems. For metering systems it might be further interesting to simplify the co-operation with home automation systems (see M/411 [11] for further information).

Smart meter working requirements can be found in ETSI TR 102 886 [13]. The reading intervals for gas and electricity are taken from Dutch Smart Meter specification and tender dossier NTA 8130 [14], which defines interval of 15 minutes for electricity and 60 minutes for gas meter. Other meters are transmitting with a significantly longer interval of eight hours. Typically, there is one electricity or gas meter per flat resulting in up to a hundred devices in a multi-storey building. The number of sub-metering devices like heat cost allocators and water meters might be by a factor of 10 higher.

Parameter	Typical	Comment
Packet size	small to medium	hundreds of bits
Data rate	medium	100 kbps decreases power consumption, ETSI TR 102 649-2 [6]
Duty cycle	low medium	non-electricity meters electricity meters, data collectors in networks, an overall duty cycle of 2.5% without peak limit is proposes in ETSI TR 102 886 [13]
Reliability	medium high	scheduled data transmission on demand
Link		in general no specific requirements, on demand functionality requires bi-directional link
Latency	large medium	scheduled data transmission, ETSI TR 102 886 [13] <1s on demand,
Installation	indoor	in buildings
Power consumption	low if battery powered	more than 10 years for non-electricity meters
Device size	small to medium	

Table 6: Technical and implementation requirements for metering systems

3.3 Automotive

In the automotive area several applications make use of SRD band frequencies, e.g. Keyless Entry systems, Remote Key, Car-2-Car, Vehicle Alarm, Personal Car Communication, or Tire Pressure Monitoring Systems. These applications have a broad range of requirements for the wireless link and are therefore treated separately within this document.

Common requirements for all automotive applications are the ECE Regulations (http://www.unece.org/trans/main/wp29/wp29regs.html). Some of the mentioned applications have dedicates ECE regulations, all have to be compliant to the generic regulations, e.g. ECE R10 "Approval of Vehicles with regard to electromagnetic stability". The ECE regulations themselves refer to other standards, like EN 300 220 [15], EN 301 489 [16] or ERC Recommendation 70-03 [17], which have to be observed by automotive equipment.

Remote Keyless Entry systems work typically at 433 or 868 MHz in Europe. The use case is to open the door lock as soon as the car driver approaches the car respectively close the door as soon as the driver leaves. Technically the car sends out a Low Frequency Signal (typically at 120 – 130 kHz) in order to wake up the key. After this an authentication handshake is performed between key and car at 433 or 868 MHz. It has to be detected very precisely if the key is inside or outside the car (location tracking). Therefore a communication between key and car is necessary as long as the key is nearby the car but the car is not driving with a certain speed. This leads to the following requirements:

Parameter	Typical	Comment
Packet size	small	around 250 bits
Data rate		no specific requirements
Duty cycle	very low medium	In case the key is far away from the car or the car is driving, no communication is performed. In case the key approaches the car or is nearby the car, the authentication handshake and location tracking of the key has to be performed
Reliability	high	
Latency	medium	
Installation	outdoor	
Power consumption	low	typically several years for the key
Device size	small medium	key receiver unit inside the car

Table 7:. Technical and implementation requirements for keyless entry systems

Remote Key is the feature for wireless door locking systems. A key with a transceiver communicates with the receiver unit in the car. The system is only active, if the button on the key is pressed.

Parameter	Typical	Comment
Packet size	small	around 100 bits
Data rate		no specific requirements
Duty cycle	very low	only active if the button on the key is pressed
Reliability	high	
Latency	medium	
Installation	outdoor	
Power consumption	low	typically several years for the key
Device size	small medium	key receiver unit inside the car

Table 8: Technical and implementation requirements for remote key systems

Personal Car Communication covers a broad range of applications, like safety, traffic management, driver assistance, pricing and payments, information services, multimedia streaming, synchronisation, and much more. Some of the applications use dedicated frequency bands, like Car-2-Car Communications, some use cellular mobile communications like UMTS or LTE, and some use ISM bands, often with technologies like WLAN.

Obviously this wide field of applications has versatile requirements, depending on the application. The following tables are exemplarily showing the application of synchronising an MP3 collection and billing in a car park

Parameter	Typical	Comment
Packet size	big	several kBytes
Data rate	high	several Mbps
Duty cycle	high	in case of transmission very high
Reliability	low	
Latency	medium	
Installation	outdoor	
Power consumption	high	due to high data rate
Device size	medium	

Table 9: Technical and implementation requirements for multimedia synchronisation

Parameter	Typical	Comment
Packet size	medium	several 100 bits
Data rate		no specific requirements
Duty cycle	very low	only during payment phase in a car park
Reliability	high	
Latency	medium	
Installation	outdoor	
Power consumption	low	
Device size	medium to big medium	car park unit receiver unit inside the car

Table 10: Technical and implementation requirements for car park billing systems

With **tire pressure monitoring systems** (TPMS) the tire pressure is continuously monitored. The tire pressure is important for safety and fuel consumption of the car. The system periodically sends the measured values from the wheel sensors to a receiver unit inside the car. The generic requirements for TPMS are written down in ECE R64. A TPMS is required to generate a warning message in case of a pressure loss within 10 minutes, if the car is moving. Therefore the transmission interval is at least around 10 minutes in case the car is driving. In TPMS system with wireless communication has also to fulfil ECE R10.

Parameter	Typical	Comment
Packet size	small	around 250 bits
Data rate		no specific requirements
Duty cycle	medium	transmission in intervals of around 10 minutes in case the car is driving
Reliability	high	
Latency	medium	
Installation	outdoor	
Power consumption	low to medium	typically several years for the wheel sensors
Device size	small medium	wheel sensor receiver unit inside the car

Table 11: Technical and implementation requirements for car TPMS systems

Electronic immobilizers of cars often make use of wireless communications. The systems are typically integrated with the remote key and keyless entry systems. The presence of a valid key deactivates the immobilizer. The requirements are summarised in Table 12.

Parameter	Typical	Comment
Packet size	small	around 250 bits
Data rate		no specific requirements
Duty cycle	very low	only in case the car is started
Reliability	high	
Latency	small	
Installation	outdoor	
Power consumption	low	typically several years for the key
Device size	small medium	key receiver unit inside the car

Table 12: Technical and implementation requirements for car immobilizer systems

Vehicle alarm systems often use wireless communication for arming and disarming the alarm system. Sometimes the alarm event itself is also transmitted wirelessly. Often the systems are integrated with keyless entry or remote key systems. The requirements for alarm systems are collected in ECE R97. In case an alarm system makes use of wireless communication, it has to fulfil also ECE R10.

Parameter	Typical	Comment
Packet size	small	around 250 bits
Data rate		no specific requirements
Duty cycle	very low	only in case alarm system as armed or disarmed, or an alarm occurs
Reliability	high	
Latency	medium	
Installation	outdoor	
Power consumption	low	typically several years for the key
Device size	small medium	key receiver unit inside the car

Table 13: Technical and implementation requirements for car alarm systems

Wireless **communications for truck and trailer** are used to transmit control signals or sensor data from door or temperature sensors. Some products are transmitting CAN bus signals.

Parameter	Typical	Comment
Packet size	medium	several 100 bits
Data rate	medium to high	high in case of can bus transmissions. Medium to low for sensor and control signals
Duty cycle	medium to high	high in case of can bus transmissions
Reliability	high	
Latency	small	low in case of can bus transmissions
Installation	outdoor	
Power consumption	medium to high	systems are powered from the car power supply
Device size	medium	

Table 14: Technical and implementation requirements for car truck and trailer communication

In case a car is brought to a garage, the technician connects a **diagnostic system** via CAN or OBD and reads error and status massages out of the electronic control units inside the car. Some automotive vendors plan to transmit this data wirelessly as soon as the car enters the garage area. This saves the time for connecting the wired equipment. Typically the diagnostic communication is integrated with other wireless communication systems available in the car.

Parameter	Typical	Comment
Packet size	medium to large	several 100 bits up to several kByte
Data rate	high	
Duty cycle	high	high in case the transmission takes place
Reliability	medium	
Latency	medium	
Installation	outdoor	
Power consumption	medium to high	systems are powered from the car power supply resp. from the garage
Device size	medium	

Table 15: Technical and implementation requirements for diagnostic systems

3.4 Home and building automation

Building automation or home automation when installed in private houses includes the remote control of a number of different applications like heating, air conditioning, lighting, shutter, television, garage doors, household appliances etc. In simple installations the lights are switched on when a person enters the room or the garage opens pressing a button on a separate device. Advanced systems will install a centralised control allowing to combine a number of different functionalities. For example, when a person enters the house, the garage door closes, the heating is turned up, the shutters are opened during the day or the light is switched on during the night, such providing improved convenience, comfort, and energy efficiency. Additionally, home automation might be combined with intruder or fire alarm systems or cooperate with smart metering systems. Devices should have a range of 20 m within buildings so that the higher frequencies above 1 GHz are not suitable due to the power limitations of a battery powered devices.

Parameter	Typical	Comment
Packet size	small to medium	hundreds of bits
Data rate	small	medium data rate is tens of kbps, ETSI TR 102 649-2 [6]
Duty cycle	low	
Reliability	medium to high	
Link	unidirectional bi-directional	simple, mostly old systems for advanced control functionality
Latency	small	
Installation	indoor (outdoor)	in and around buildings
Power consumption	low	5 to 10 years battery lifetime
Device size	small	

Table 16: Technical and implementation requirements for home and building automation

3.5 Industrial automation

Industrial automation generally requires high reliability and either very low latency or high data rate, which can be best fulfilled in frequency bands above 1.5 GHz (see ETSI TR 102 889 [18] and ZVEI [19]). Current developments are using primarily standardised wireless technologies in the 2.4 GHz band like IEEE 802.15.1 (Bluetooth), IEEE 802.15.4/4a or IEEE 802.11 (WLAN). Control and parameterisation tasks for example might use the Serial Port Profile (SPP) or Personal Area Networking Profile (PAN) of Bluetooth. In case reliability as well as low and predictable latency are required, the Bluetooth based WISA (Wireless Interface for Sensors and Actuators) technology can be used for short distance communication of a large number of devices with even wireless power supply. Large distances can be covered based on meshed network using for example the WirelessHART protocol, ZigBee or MeshScape, which are all based on the IEEE 802.15.4 standard, but differ with regards to reliability, latency and supported data rates.

Parameter	Typical	Comment
Packet size	typically small	
Data rate	medium high	lower than 250 kbps for IEEE 802.15.4 based standards up to tens of Mbps for WLAN
Duty cycle	low medium to high	single link in sensor systems sensor networks
Reliability	very high	
Link	bi-directional	
Latency	very small small to medium	a few ms for a single link, a few seconds in multi-hop networks in sensor networks for high data rate applications
Installation	indoor / outdoor	industrial environments, plants
Power consumption	low	battery powered (except WLAN), up to several years
Device size	small to medium	

Table 17: Technical and implementation requirements for home and building automation

3.6 Telehealth / telemedicine

In contrast to Ambient Assisted Living (AAL) systems (see social alarms in section 3.1) the clinical telehealth systems continuously monitor the vital signs like ECG, blood pressure, etc. and transmit data all the time to the clinical backend system. The backend generates alarms for nurses and doctors in case of irregularities. Nevertheless, telemedicine or telehealth is not bound to hospitals, but can also be used for people recovering at home. The recorded data can be used for analysis by the doctor, but also to quickly alert the medical staff in case of emergency. These systems have high duty cycle and high requirements towards reliability and latency as shown in Table 18. The connection must be bidirectional allowing the backend to acknowledge the successful transmission. Most applications are using standard technologies like WLAN, Bluetooth, ZigBee in the 2.4 GHz band.

Parameter	Typical	Comment
Packet size	small to large	depending on the application
Data rate	small to large	depending on the application
Duty cycle	high	up to 100%
Reliability	very high	
Link	bi-directional	
Latency	small	< 100 ms on a single link
Installation	indoor	
Power consumption	medium high	around some weeks battery lifetime not battery powered
Device size	small medium large	sensors data collector monitor

Table 18: Technical and implementation requirements for telemedicine / telehealth

Additionally, there is a specific frequency band for medical implant communication service (MICS) devices in the range 402 to 405 MHz specified in EN 301 839 [20]. The MICS devices include Medical Implant Telemetry System (MITS) and Medical Data Service (MEDS) devices,

which comprise medical implants and medical body-worn devices. Hence, there is little focus on the 868 MHz frequency band for medical applications.

3.7 Wireless audio

Wireless audio devices like microphones, assistive listening devices, speakers, and headphones significantly differ from the aforementioned applications due to their continuous data transmission requirement.

Radio **microphones** and **in-ear monitoring** for professional users have a typical bandwidth of 200 kHz for analog audio transmissions (Wireless Microphone study [21]), while the bandwidth might be smaller for digital audio. However, as digital processing like coding inevitably introduces delays, the bandwidth reduction is limited due the low latency requirements of less than a few ms for professionals. According to [21] professional users of wireless microphones are typically using a licensed, lower frequency band in order to avoid interference problems, while many wireless microphones purchased for consumer use do operate in the 863-865 MHz band. **Assistive listening** devices (ALD) are used by hearing impaired persons in addition or instead of a hearing aid. They consist of a microphone placed near the speaker and a loud speaker, headphone, or hearing aid on the receiver side, which amplifies the speaker's voice while suppressing the background noise. **Tour guide** systems are operating in a similar way, just having a number of persons receiving the same signal with a head-set. These applications are standardised by EN 300 422 [22].

Parameter	Typical	Comment
Packet size	n.a.	
Bandwidth	200 kHz high	medium data rate multichannel audio equipment
Duty cycle	continuous transmission	
Reliability	high	
Link	unidirectional	
Latency	very small	a few ms
Installation	indoor (outdoor)	in and around buildings
Power consumption	battery powered	
Device size	small to medium	

Table 19: Technical and implementation requirements for wireless audio

Wireless loudspeakers, headphones, in-vehicle audio devices, and consumer microphones are standardised by EN 301 357 [23]. Stereo equipment requires a bandwidth of 200 kHz or less, while multichannel audio equipment like surround sound systems are operating on a higher bandwidth, so that they are intended to be used in frequency bands above 1 GHz.

3.8 Radio frequency identification (RFID)

RFID systems allow reading data from tags attached to an object for the purposes of automatic identification and tracking. The majority of the tags are passive devices using the energy generated by the reader antenna for responding. LF and HF reader systems utilize inductive coupling (a magnetic field), while UHF reader systems utilize capacitive coupling (an electric field). In passive backscatter RFID systems, the reader continuously transmits at a constant radio frequency power level, while the tag answers by modifying the amount of reflected power. Alternatively, battery powered RFID can be used allowing to significantly increase the communication range at the expense of tag costs and size.

In case the tags are close to water surface or metal, the LF-band (< 135 kHz) is a good choice in order to avoid interference with radio waves. LF RFID applications are for example animal tracking (ISO 11784 and 11785), factory data collection, access control, or car immobiliser. While the distance between reader and tag is typically below 10 cm, a higher distance in the order of one meter can be achieved using the HF-band (13.56 MHz). The transponders are cheaper than the LF-variant and allow for a higher data rate and simultaneous multiple tag reading. Anti-collision procedures for example are standardised in ISO 14443 for proximity cards (distance < 1 m) and ISO 15693 for vicinity cards (distance 1-1.5 m). Typical application areas are ticketing, library sticker, access control, or transportation management.

A tremendous growth is expected for RFIDs using UHF frequencies due to an even larger communication range up to 3 m and higher bandwidth, which is required to either increase data volume or to read a higher number of tags within the same time. UHF RFIDs are used for example in asset tracking, waste management, parking lot access, or logistic and supply chains. It is expected that the density of tags in logistics will significantly increase in the future, so that simultaneous reading of up to 1500 tags might be required (ETSI TR 102 649-2 [6]), while the current regulation with a 200 kHz bandwidth limitation allows for only 200 tag readings per second.

Finally, RFID may also make use of the microwave frequencies (2.4 GHz), which provide very high data rates, but increase tag costs. Furthermore, microwave signals are attenuated and reflected by materials containing water or human tissue, which limits the range of use. Exemplary applications of microwave RFID systems are factory automation, access control and logistics.

One significant reason for the success of the LF and HF-band is the worldwide availability of the frequency bands, while there is no harmonised regulation for the UHF band. An international standard (ISO's 18000 series) exists defining the parameters for air interface communications for passive backscatter RFID systems. The standard encompasses all four different frequency bands. ISO18000-2 covers parameters for communications below 135 kHz (LF-band), while ISO18000-3, ISO18000-4, and ISO18000-6 apply to 13.56 MHz (HF-band), 2.4 GHz, and 860-960 MHz, respectively. More information and a summary of RFID standards can be found in ETSI TR 102 449 [24].

Table 20 focuses on requirements of RFIDs in the UHF band.

Parameter	Typical	Comment
Packet size	small	100-250 bits without encryption
Data rate (return link)	small medium	10 - 40 kbps, ISO18000-6 320 kbps, if 1500 tags need to be read, ETSI TR 102 649-2 [6]
Duty cycle	small medium up to 100%	tag reader with active tags reader with passive tags
Reliability	high	
Link	bi-directional	
Latency	small	
Installation	indoor / outdoor	commercial, industrial environments
Power consumption	low n.a.	active RFID tags passive RFID tags
Device size	small	

Table 20: Technical and implementation requirements for UHF - RFID

3.9 Wireless data transmission

Wireless data transmission serves as a cable replacement for a number of different applications. On the one side there are battery powered devices requiring data rates up to 1 Mbps over a short distance. Examples are a wireless connection between a PC and a mouse, keyboard, or printer, the link between the wireless controller and the game console, or a hands-free headset connected to the mobile phone via a radio link. The required range is typically below 10 m and the latency should be small. Applications are using primarily standardised wireless technologies in the 2.4 GHz band like IEEE 802.15.1 (Bluetooth) and IEEE 802.15.4. Although the latter can also be operated in the 868 MHz SRD band, the maximum data rate here is limited to 20 kbps, which is not sufficient for a number of applications.

Parameter	Typical	Comment
Packet size	small to medium	several hundred bits
Data rate	medium	higher data rate decreases power consumption, ETSI TR 102 649-2 [6]
Duty cycle	medium to high	dependent on application and number of devices
Reliability	high	
Link	bi-directional	
Latency	small	
Installation	indoor / outdoor	
Power consumption	medium	battery powered, in the order of weeks
Device size	small	

Table 21: Technical and implementation requirements for low power data transmission < 1Mbps

A significant higher bandwidth and transmission distance are required for wireless computer networks or the wireless connection of the computer to the internet via an access point. Over the last decade, Wireless Local Area Networks (WLAN) have gained strong popularity in a variety of different markets like health-care, manufacturing, retail, or warehousing. The doctor for example has an instant access to patient information during his ward round using a notebook with wireless network access to the hospital's data base. WLAN are defined by the IEEE 802.11 family of specifications, offering data rates in between 1 and 54 Mbps (up to 200 Mbps using

MIMO) and distances in the order of 30 m depending channel characteristics. These standards are operating in the 2.4 GHz ISM band or in the 5 GHz bands (5.15-5.35 GHz and 5.47-5.725 GHz), respectively.

Parameter	Typical	Comment
Packet size	medium - large	
Data rate	high	ten's of Mbps
Duty cycle	high	
Reliability	high	
Link	bi-directional	
Latency	small	
Installation	indoor / outdoor	
Power consumption	medium	battery powered, in the order of days
Device size	small	

Table 22: Technical and implementation requirements for high data transmissions

3.10 Summary

Comparing typical SRD applications with regards to their requirements for packet size, duty cycle (see Figure 1), latency, and reliability (Figure 2) it becomes obvious that there is no single set of specifications, which fits them all. Nevertheless, a high number of applications requires only small to medium packets sizes carrying a few hundred bits, while the duty cycle varies from very low to medium.

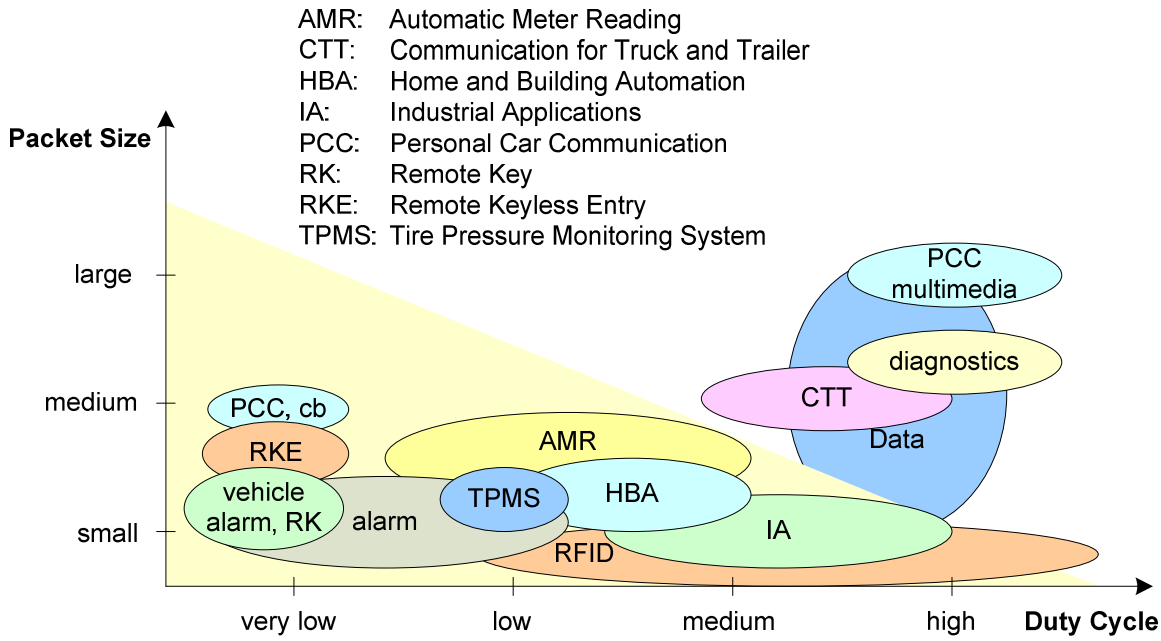


Figure 1: Comparison of SRD applications with regards to packet size and duty cycle

The applications located outside the yellow region like multimedia synchronising in personal car communication (PCC) or high data rate transmissions do not very well fit to the 868 MHz frequency band due to their high duty cycle and bandwidth requirements. They will be shifted to the 2.4 GHz band and are out to scope for this study.

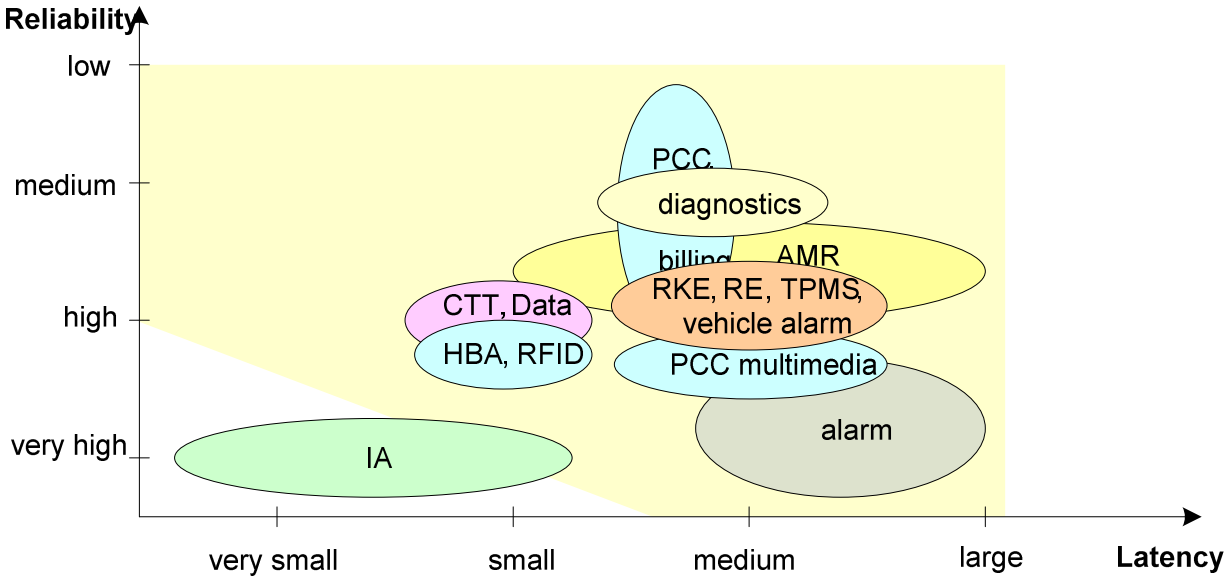


Figure 2: Comparison of SRD/ISM applications with regards to latency and reliability

Applications with high reliability requirements must be carefully examined if they shall be operated in an un-licensed band. Two examples have been described in more detail, the alarm systems and sensor/actor networks as well as machine-to-machine communication in industrial automation (IA). While the latency in alarm systems can be in the order of several seconds allowing for data retransmissions in case of packet losses, the latency requirements in IA are much more stringent. A response time in the order of milliseconds is often needed to avoid an interruption in the manufacturing process. Furthermore, industrial environments suffer from the predominant presence of electromagnetic disturbances, so that frequencies below 1.5 GHz should be avoided. Hence IA applications are not considered in this document.

Most of the SRD applications are operated within buildings, where a number of different systems might be installed within the same coverage area. Hence, coexistence of independent systems will be required. As the majority of the SRDs will be battery operated, the overhead for access coordination needs to be strictly minimised.

4. Channel access schemes

This section gives an overview on potential channel access schemes and compares their main characteristics to the typical requirements of SRD applications to assess their suitability as a common access scheme for SRDs.

4.1 FDMA and TDMA

FDMA and TDMA are channel access schemes assigning each user a dedicated resource for wireless data transmission. In FDMA schemes frequency dimension is subdivided into several frequency bands. The frequency bands are separated by guard bands in order to avoid overlapping of adjacent signals spectra. The number of users is limited by the number of frequency bands and the allocation of the frequency band to a specific user needs to be centrally controlled.

In TDMA systems users are transmitting in the same frequency band, where each user is allowed to transmit only within specified time slots. As the number of time slots can be adapted to the user requirements, TDMA provide a high amount of flexibility with regards to supported data rates and number of devices. The allocation of time slots is done by a central control node, whose primary function is to transmit a periodic beacon signal. The beacon signal indicates the position of the first slot within a frame and allows the network nodes to maintain their time synchronization. Additionally, it provides broadcast information like the slot usage information. Guard times are required in between successive time slots in order to cope with path delay variations and imperfect time synchronisation.

Both access schemes allow for channel usage close to hundred percent, but are not appropriate for access control of independently operating systems due to lack of central control instance. Although distributed resource allocation procedures are known for TDMA systems, the typically high number of SRDs transmitting short packets with a low duty cycle would results in an unacceptable control overhead for resource management, which makes TDMA systems unattractive as a common access scheme for all devices.

4.2 Duty Cycle based random access

A number of users can share the time axis without central control if the transmission time of each user is limited by a maximum allowed duty cycle. If the user transmits in regular intervals the duty cycle is defined by the ratio of transmit time T_{TX} and repetition interval T_{int}.

$$DC = \frac{T_{TX}}{T_{int}}$$

For sporadic transmissions it might be more reasonable to define a short term and a long term duty cycle. Due to the lack of a central control, the time of transmission within the repetition interval needs to be randomised in order to avoid continuous packet collisions. In case two users *m* and *n* are transmitting with random time offsets, the probability of a packet collision of user *n* depends on the two packet lengths $T_{Tx,m}$ and $T_{Tx,n}$ as well as the repetition interval $T_{int,m}$ of user *m*. If the user *m* starts its packet transmission within an interval of $T_{Tx,n}+T_{Tx,m}$, the packet will collide as shown in Figure 3. On the other side a packet start in the remaining time interval of $T_{int,m}$-$T_{Tx,n}$-$T_{Tx,m}$ allows for a collision-free transmission.

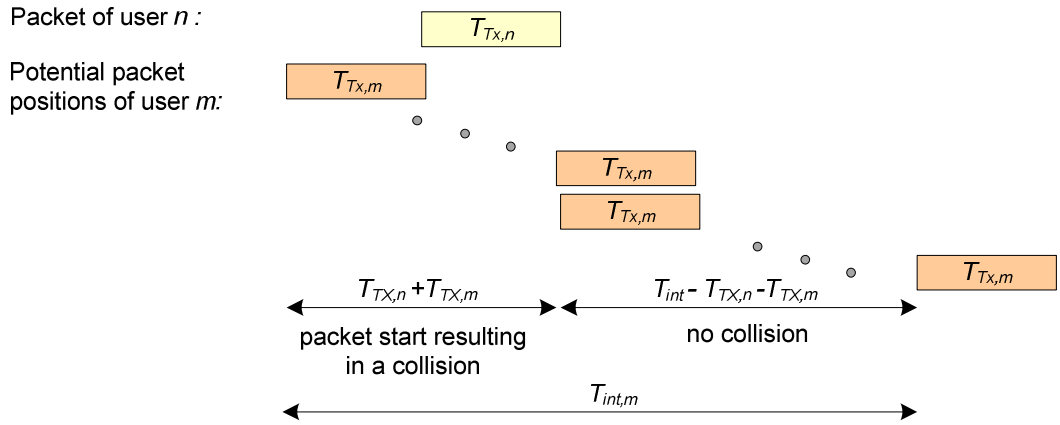
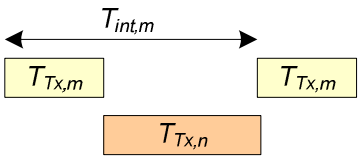


Figure 3: Packet start time resulting in a collision/successful transmission

Therefore, the probability of a successful transmission in a scenario with two devices can be calculated to

$$P_{success}(n) = \max\left(0{,}1 - \frac{T_{Tx,m} + T_{Tx,n}}{T_{int,m}}\right), \text{2 users}$$

The maximum operator avoids a negative success probability in case the interferer repetition interval is so small that the desired user packet does not fit in between the end of the previous interferer packet and the start of the next packet



$T_{int,m} \leq T_{Tx,m}+T_{Tx,n}$

Figure 4: Permanent collisions

In general, there are *N* users transmitting on the channel. The probability of a successful packet transmission of user *n* can be calculated to

$$P_{success}(n) = \prod_{\substack{m=1 \\ m \neq n}}^{N} \max\left(0{,}1 - \frac{T_{Tx,m} + T_{Tx,n}}{T_{int,m}}\right), \text{N users}$$

supposed that the packet transmission times are independent and exactly one packet is transmitted per repetition interval. Packet retransmissions in case of collisions are not considered.

In the ECC Report 181 [33] packet loss rates are calculated for a duty cycle limited scenario with *N* users assuming equal packet lengths and repetition intervals for all users. The packet loss rate P_{loss} is simply 1-$P_{success}$, so that the following equation applies:

$$T_{Tx,m} = T_{Tx,n} = T_{Tx}$$

$$T_{int,m} = T_{int,n} = T_{int}$$

$$P_{loss} = 1 - P_{success} = 1 - \left(1 - \frac{2T_{Tx}}{T_{int}}\right)^{N-1} = 1 - (1 - 2\,DC)^{N-1}, \text{N users}$$

Figure 5 shows the packet loss rate as a function of the number of users and the user duty cycle.

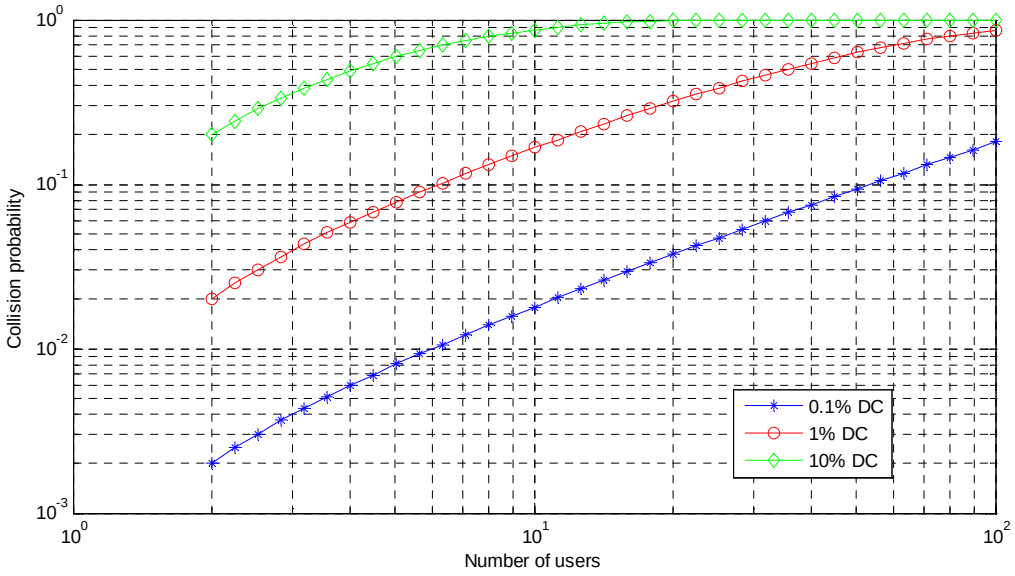


Figure 5: Collision probability as a function of the number of users (same packet length and DC)

However, the assumption of an equal packet length is generally not true, if the users belong to different systems. Nevertheless, the impact of different packet lengths on the packet loss rate might be significant. Figure 6 presents the packet loss rate in an exemplary situation, where 10 users are transmitting with the same DC of 1%. 9 users are sending packets of 10 ms length, while the packet length of the 10th user is iterated in between 1 ms and 100 ms. The blue curve (stars) indicates the packet loss rate of the 9 users, which slightly decreases when the packet length of the single user increases. There is significantly more impact on the packet loss of the single user. The red curve (circles) shows a small decrease of the packet loss probability for the small packet size, while large packets of 100 ms have a four times higher risk getting lost than packets of 10 ms duration.

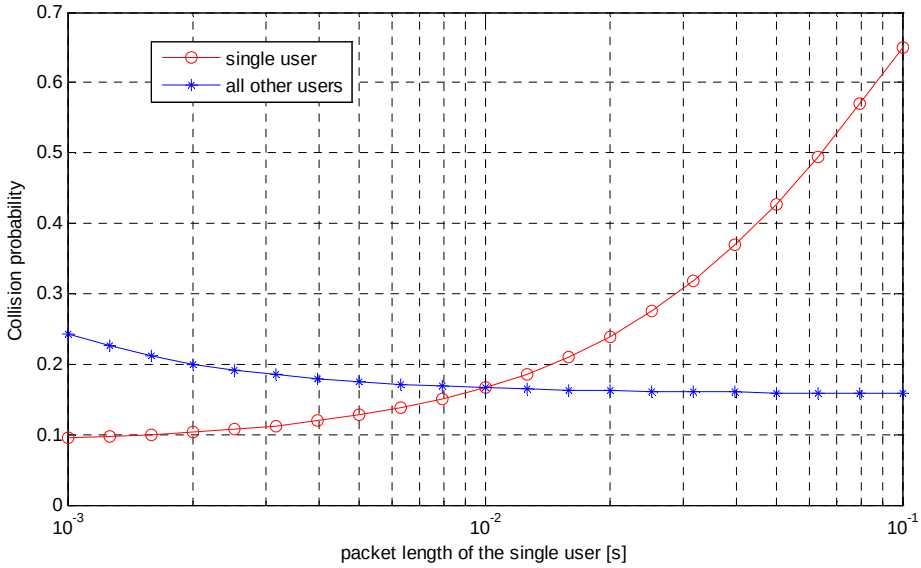


Figure 6: Collision probability in a scenario with 10 users with DC of 1%, packet length of 9 users is 10 ms, packet length of the 10th user varies from 1ms to 100ms

Figure 5 shows the collision probability for a duty cycle of 0.1% assuming equal packet lengths for all users. The calculations are repeated selecting a random packet length in between 1 ms and 100 ms for each user, while adapting the transmit interval such that the duty cycle remains at 0.1%. The resulting user specific packet loss rates are calculated for 10000 different random sets of packet lengths. The solid blue line in Figure 7 shows the packet loss rate when all packet lengths are identical. Each bar above and below this line corresponds to a calculated packet loss rate (PLR) for randomly selected packet lengths where the colour indicates the probability of occurrence. For example, a PLR in between 10% and 70% have been calculated if 100 users are transmitting in parallel. The probability of links with a PLR of 10% is indicated by a blue bar, which corresponds to a value below 5% but above 1%. More than 10% of the links have a PLR of 20% which is equal to the PLR in the equal length scenario. The majority of the links experience a PLR of 30%-40%.

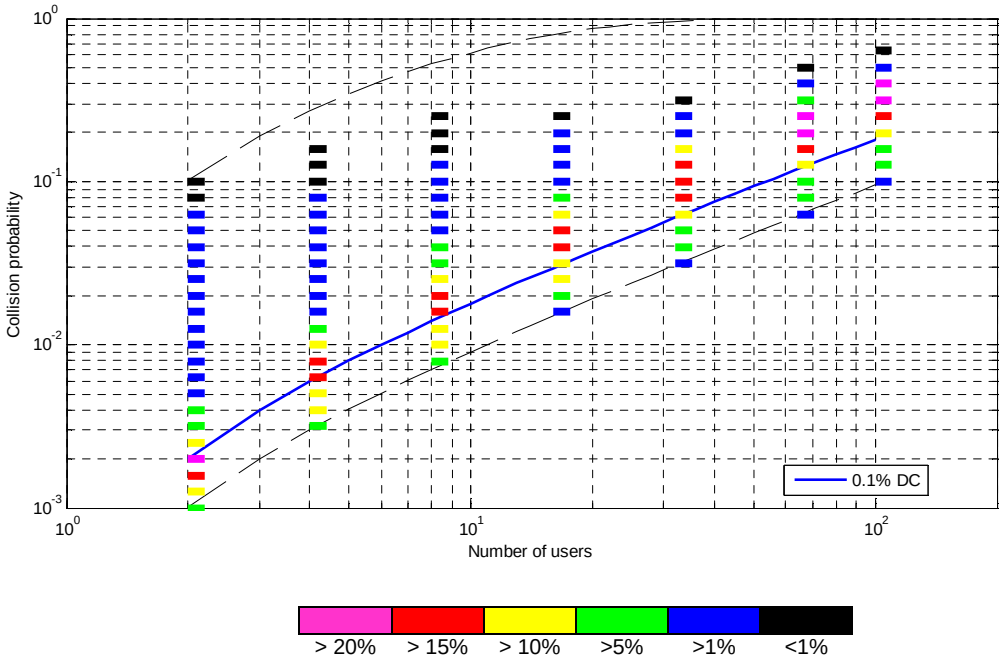


Figure 7: Collision probability as a function of the number of users, 0.1% DC, random packet length in between 1 ms and 100 ms

In general, the PLR can significantly vary. The black dotted line below the blue curve corresponds to the situation where the desired user transmits with the minimum packet length, while the other users are sending packets with the maximum packet length.

$$P_{coll,min} = 1 - \left(1 - \frac{T_{Tx,min} + T_{Tx,max}}{T_{int,max}}\right)^{N-1} = 1 - \left(1 - \frac{T_{Tx,min} + T_{Tx,max}}{T_{Tx,max}} \cdot DC\right)^{N-1}$$

Hence, a small PLR always corresponds to a small packet length on the considered link. The dotted black line above the blue line considers the opposite situation, where the desired user transmits with the maximum packet size, while the others are using the minimum packet size.

$$P_{coll,max} = 1 - \left(1 - \frac{T_{Tx,max} + T_{Tx,min}}{T_{int,min}}\right)^{N-1} = 1 - \left(1 - \frac{T_{Tx,max} + T_{Tx,min}}{T_{Tx,min}} \cdot DC\right)^{N-1}$$

The majority of the links will have a PLR which is close to the PLR in equal length scenarios for a single-digit number of nodes and around 1.5 to 2 times higher for large number of nodes. It

should be taken into account that these results are only valid for a system with uncoordinated users having constant, time invariant duty cycles and random, equally distributed packets starts. For any other scenario the calculations need to be revised.

4.3 ALOHA / Slotted ALOHA

4.3.1 ALOHA

The pure duty cycle access as discussed in the previous chapter does not consider retransmissions in case a packet is lost. This is typical for a system with unidirectional links, where the transmitter gets no feedback on a packet reception. Using bidirectional links allows the receiver to confirm a successful reception via an acknowledgement (ACK) packet, so that the transmitter can repeat the packet if no ACK packet has been received. The ACK-packet is typically very short, but certainly slightly increases the packet collision probability on the channel. The ACK-packet duration can be added to the transmitted packet duration in addition to the time interval between the two packets due to Rx/Tx switching time in the responding node. As shown in the previous chapter, the probability of a successful transmission depends on the channel load and can be written as

$$P_{success} = (1 - 2\,DC)^{N-1}$$

supposed that all *N* users are randomly transmitting packets of the same size and with the same duty cycle *DC*. The formula can be rewritten using its power series approximation:

$$P_{success} = 1 - (N-1)2DC + \frac{(N-1)(N-2)}{2!}(2DC)^2 - \frac{(N-1)(N-2)(N-3)}{3!}(2DC)^3 \pm \cdots$$

The product $N \cdot DC$ is denoted as channel load *G*. The same channel load can be caused by a small number of users with a high DC or by a high number of users with a small DC, respectively. If the number of users tends to infinity the power series approximation can be simplified to

$$P_{success,N\to\infty} = \left(1 - 2N \cdot DC + \frac{(2N \cdot DC)^2}{2!} - \frac{(2N \cdot DC)^3}{3!} \pm \cdots\right) = \exp(-2G)$$

The assumption of an infinite number of users is a worst case assumption (see Figure 8) as the success probability increases for a small number of users especially for low traffic loads.

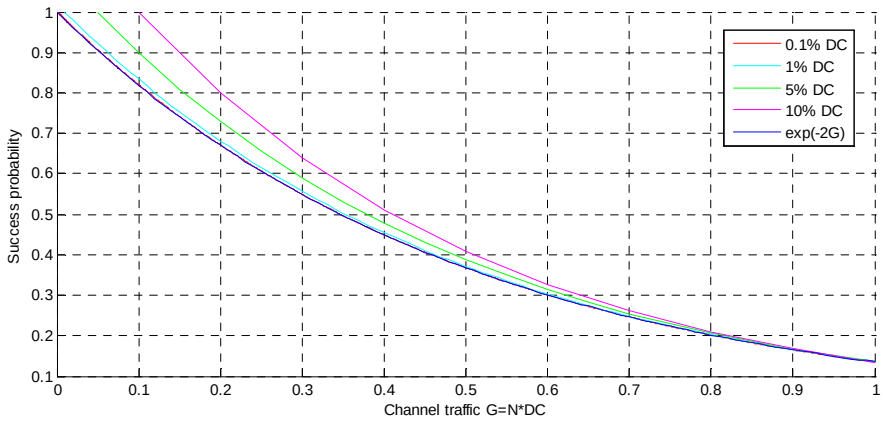


Figure 8: Packet transmission success probability as a function of the traffic load

The calculations above assume that each user transmits exactly one packet within the repetition interval T_{int}, so that there are N packet transmissions within T_{int}. The channel load G can be interpreted as the number of transmissions per packet duration T_{Tx}.

$$N \text{ packet transmissions within } T_{int}$$

$$G \text{ packet transmissions within } T_{Tx}$$

$$\Rightarrow \; G = N \cdot \frac{T_{Tx}}{T_{int}} = N \cdot DC$$

Channel access in a pure ALOHA system is identical to that of the DC system except the fact that a packet is retransmitted with a random time offset in case of a packet collision. Hence, the number of transmission G in a ALOHA system includes retransmissions in addition to the regular transmission attempts. Only a part of the packet transmissions are successful. The pure Aloha throughput S can be written as

$$S = P_{success} \cdot G = G \cdot \exp(-2G)$$

Figure 9 shows a maximum throughput of 18.4% at G=0.5.

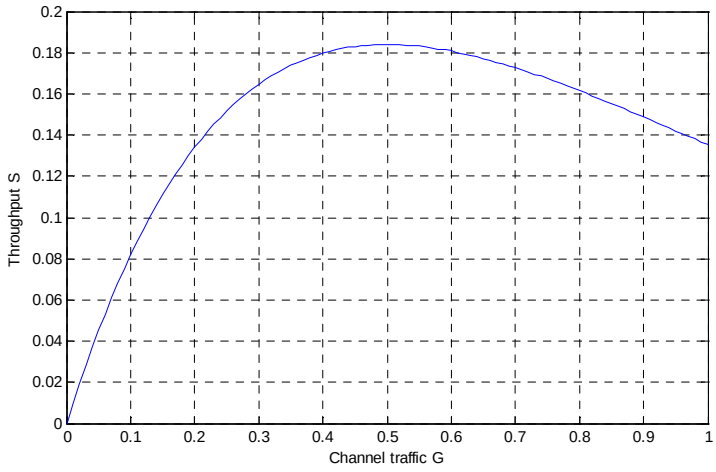


Figure 9: ALOHA throughput

The corresponding packet success rate of 0.184/0.5=36.8% (see also Figure 8) is quite low as nearly two of three packets are lost due to collisions and is even smaller if not all packets have the same packet length [26]. Furthermore, the throughput decreases if the channel traffic further increases. As the channel traffic includes repetitions, the system can easily collapse when operated close to the maximum throughput. Hence, the ALOHA system should be operated at lower channel access rates and the retransmissions need to be carefully scheduled to avoid local congestion as it will be shown later on in section 5.6.2. In order to allow coexistence of different systems the ALOHA protocol needs to be combined with duty cycle limitations, listen-before talk procedures or back off strategies (e.g. linear or exponential) in order to assure equity of channel access and sharing.

4.3.2 Slotted ALOHA

While the ALOHA protocol is a fully decentralised mechanism, the slotted ALOHA needs a form of coordination allowing transmissions only within timeslots. By synchronising the packet transmissions, the collision probability can be significantly reduced. If all users are transmitting

with the same packet length, the time slot duration can be optimised to contain exactly one packet and its acknowledgement packet. In this case the throughput doubles with regards the basic ALOHA protocol. The theoretical maximum of 36.8% is achieved for G equal to 1.

$$S = P_{success} \cdot G = G \cdot \exp(-G)$$

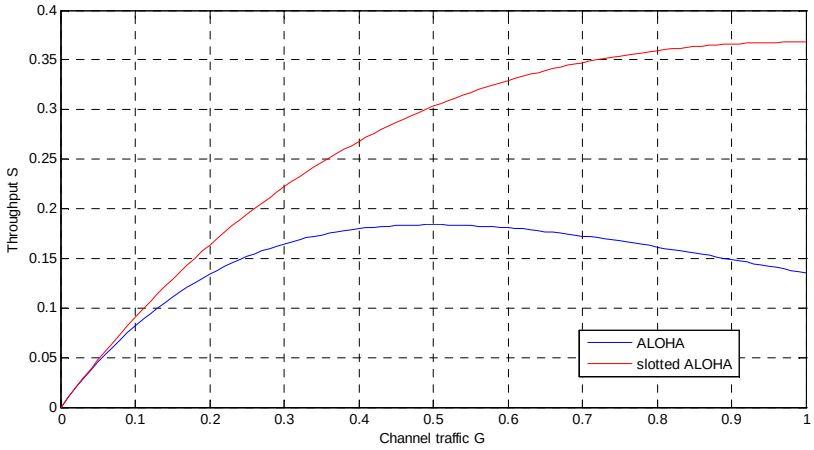


Figure 10: Throughput comparison of ALOHA and slotted ALOHA

Nevertheless, the achievable throughput is reduced by the overhead required for synchronisation. Furthermore, packet durations are not always identical even within a single system. The time slot duration might be either too small so that long packets need to be split and transmitted in different time slots or too large so that time slots are only partly used. This is even more problematic if different independent systems are operated in parallel. However, the main reason for not implementing slotted ALOHA in a multi-system environment is the requirement for a common time synchronisation.

4.4 Listen Before Talk (LBT)

While the ALOHA protocol blindly transmits the packet and afterwards gets information on a collision based on a missing ACK-packet, a device using listen before talk (LBT) first checks whether the channel is free using the clear-channel assessment (CCA) of the physical layer. Standard CCA methods are energy detection (ED) and preamble detection (PD) [27]. PD requires a constantly running detector to catch the preamble of all incoming packets resulting in high power consumption. Furthermore, only users of the same systems can be detected unless the preamble signal format is standardised, so PD cannot be easily used in multi-system environments. ED is a robust mechanism that can be deployed without requiring any knowledge of the type of underlying modulation scheme. The received signal strength indicator (RSSI) can be checked just prior to an intended transmission. However, ED is inherently less reliable at low signal-to-noise ratios.

CCA performance is characterized by two different probabilities, the missed alarm probability P_{MA} and the false alarm probability P_{FA}. P_{FA} denotes the probability that the CCA indicates a busy channel (i.e. RSSI > LBT threshold), while in effect the channel is free. An alarm has been missed if the RSSI value is below the LBT threshold while an interferer is active. The two probabilities depend on the actual signal-to-noise ratio (SNR) and the LBT threshold setting. If the threshold is high, the missed alarm probability increases, while the false alarm probability becomes small. While the latter just prevents the user from transmitting his packet, the missed

alarm probability affects the system performance due to collisions and hence needs to be fairly small.

The performance of the LBT method is not only influenced by the reliability of the CCA signal, but also by the dead time T_D, the listening time T_L (both Figure 11) and the minimum interference detection interval T_R (Figure 12). The dead time is the time between the end of the listening time and the start of the transmission. The listening interval T_L is the time that the node listens for a received signal at or above the LBT threshold level. The signal must be present for at least T_R seconds in order to be measured.

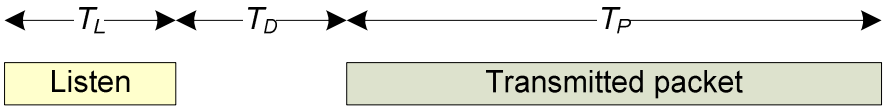


Figure 11: LBT Timing parameters

Any signal received during the dead time is not detected, so that the packet is transmitted although a signal is present. Figure 12 shows the transmitter *A* measuring the channel prior to transmission and different positions of the packet *B*, which are resulting in a collision although both nodes are using LBT. The collision interval duration can be calculated to $T_{Coll} = 2 \cdot (T_R + T_D)$.

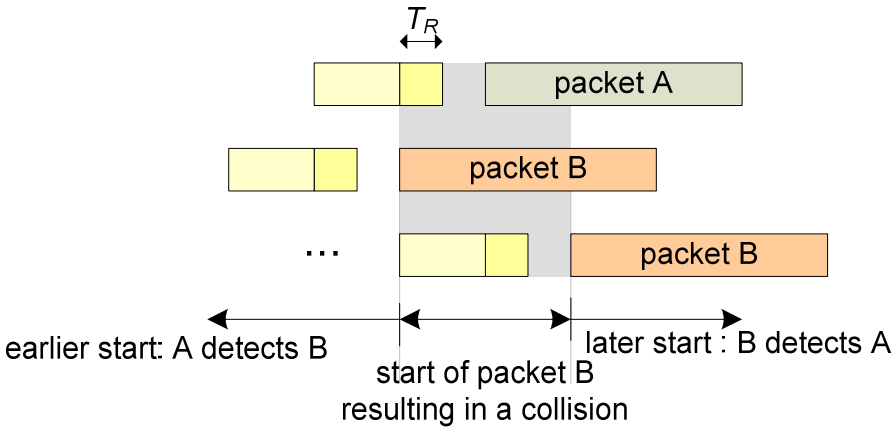


Figure 12: Collision in a LBT based system due to the dead time

It is a drawback of LBT systems that even with perfect signal detection (T_D+T_R=0) the LBT scheme cannot exactly determine, whether another link will be disturbed by the own transmission. This requires information on the victim receiver which is not available. As a consequence LBT suffers from hidden node and exposed node problems shown in Figure 13.

A hidden node is a device which generates harmful interference at the receiver position, but cannot be measured by the transmitter. Hence, the transmitter cannot detect an ongoing transmission of the hidden node, so that the own packet is transmitted simultaneously inevitably resulting in a collision at the receiver position. While the hidden node problem affects the system performance and need to be carefully considered (see section 5.6.3), the exposed node problem only slightly decreases the maximum system throughput. An exposed node denotes a device inside the detection range of dedicated transmitter, which generates no harmful interferer at the position of the receiver. Hence, the transmitter refrains from transmitting its packet in case the exposed node is already active, although the packet would have been successfully received by the dedicated receiver. Nevertheless, it still might be reasonable to delay the own transmission because the two packet might collide at the position of the exposed node receiver.

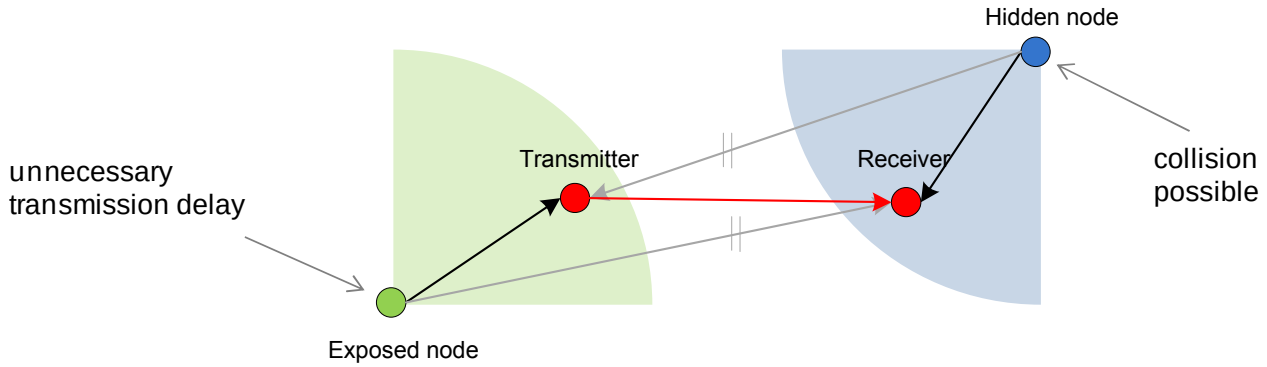


Figure 13: Hidden and exposed node scenario

This chapter just describes LBT as a method to refrain from a transmission when the CCA signal of the physical layer indicates a busy channel. In case the application can cope with packet losses, the transmitter can simply skip the packet. Otherwise, a retransmission needs to be scheduled. Different timing methods of the retransmission are described in the next chapter on Carrier Sense Multiple Access (CSMA) systems with collision avoidance based on LBT. The majority of the CSMA systems additionally perform packet loss detection expecting an immediate acknowledgment from the receiver. For systems with acknowledgements it should be taken into account that the interference situation might be different in forward and return link.

4.5 CSMA

Carrier Sense Multiple Access (CSMA) systems are using LBT to decide if the packet can be transmitted. In case the channel is busy, there are different protocols for scheduling the retrials.

The **1-persistent** method assumes that the node continuously senses the channel and transmits the packet as soon as the channel becomes idle. In case that more than one node is waiting for a transmission, their packets will collide. The ***P*-persistent** protocol is a variant, where the node transmits its packet with a probability of *P* as soon as the channel becomes idle. Hence, the node refrains from an immediate transmission with probability (1-*P*) and sends the packet after a fixed time offset with probability *P*. The persistent parameter *P* significantly influence system throughput and the optimum value depends on the number of contending nodes. The probability value should be small in case of a high traffic load in order to reduce the collision probability, while a large value is required for optimum bandwidth utilization if the channel is idle. Hence, the probability *P* cannot be optimised for an unknown or time varying number of contending nodes. Furthermore, the time offset until the next retrial is typically depended on the packet length. In a scenario with different independent systems operating in parallel an optimisation of the time offset is not possible.

In contrast to persistent CSMA **non-persistent** CSMA does not continuously observe the channel once a busy channel has been detected. The transmission trial is simply delayed by a random back off interval. Prior to the next transmit interval the node performs a new channel measurements and directly transmits the packet in case the channel is free.

Both, persistent and non-persistent CSMA can be used in unslotted and slotted systems. Similar to slotted ALOHA, a slotted CSMA requires system wide time synchronization which is not applicable for scenarios with independently operating systems. Hence, slotted CSMA is not considered in this report. Supposed that there are an infinite number of users, which are all in

range of each other and transmitting packets of the same length, the throughput per packet time can be calculated as a function of the offered channel traffic [25]:

1-persistent CSMA: $$S = \frac{G\cdot(1+G+\alpha G(1+G+\alpha G/2))\cdot e^{-G(1+2\alpha)}}{G\cdot(1+2\alpha)-(1-e^{-\alpha G})+(1+\alpha\cdot G)e^{-G(1+\alpha)}}$$

Non-persistent CSMA: $$S = \frac{Ge^{-\alpha G}}{G(1+2\alpha)+e^{-\alpha G}}$$

Thereby, perfect LBT has been assumed. The required measurement interval and the time offset in between the measurement and the start of the transmission are zero. The parameter α is the propagation delay divided by the packet length and hence a very small value. G represents the offered traffic including transmission trials which are skipped due a busy medium. Hence the actual number of transmissions per packet length is significantly smaller than G especially for high values of G. In case an acknowledgement based retransmission procedure is implemented, the offered traffic not only includes new packets but also previously collided packets which are retransmitted. In general, the start times of packets are no longer independent and exponential distributed if retransmissions are considered. Nevertheless, the assumption is still a good approximation as soon as the retransmission intervals are large compared to the packet length.

A comparison of non-persistent and 1-persitent CSMA is shown in Figure 14 for different channel delay values of 0%, 1% and 10% of the packet length. The latter is extremely high if only path delay is considered. However, there will be additional delays in between the measurement time and the arrival of the packet at the receiver in a realistic LBT scheme. The 1-persistent CSMA reaches its maximum throughput slightly above G=1 for α=0, and slightly below G=1 for α=0.1. Similar to ALOHA the throughput significantly decreases for higher traffic loads resulting in a system collapse. The performance of the non persistent CSMA is slightly worse for low traffic loads, but outperforms the 1 persistent CSMA at high traffic loads, so that non-persistent CSMA is strongly favoured for SRD applications as the amount of interference in the SRD band cannot be controlled and robust access schemes are required. Nevertheless, a significant impact of the delay α can be observed.

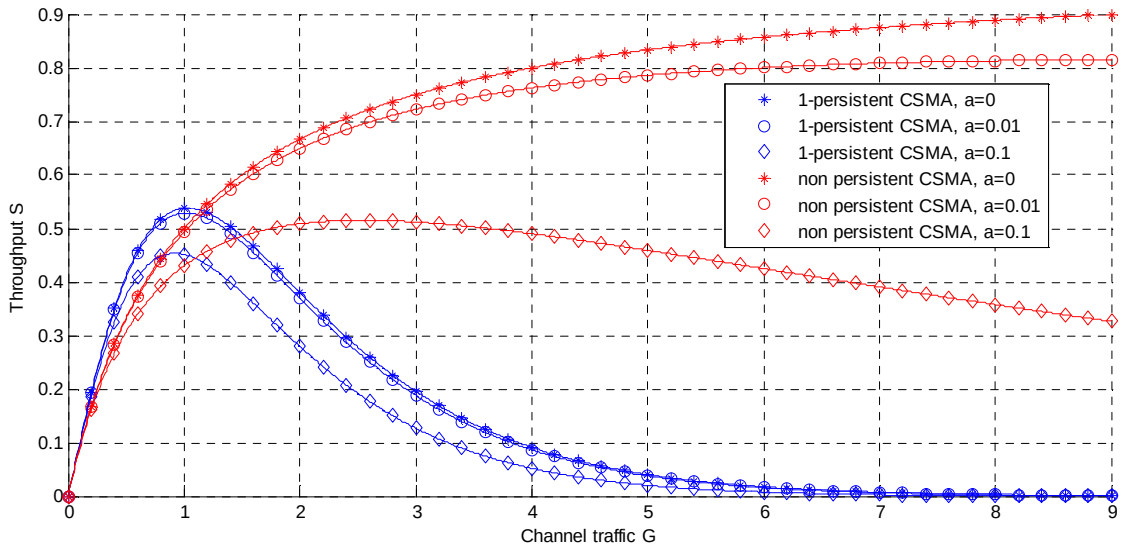


Figure 14: Throughput comparison of non-persistent and 1 persistent CSMA

In Figure 15 the throughput results are compared to ALOHA for lower traffic situations. Whether the offered traffic is below 10% the ALOHA protocol is only slightly worse than CSMA. The difference increases as the load on the channel becomes higher. While the ALOHA protocol reaches its maximum at *G* equal to 0.5, the throughput of the CSMA systems is still increasing.

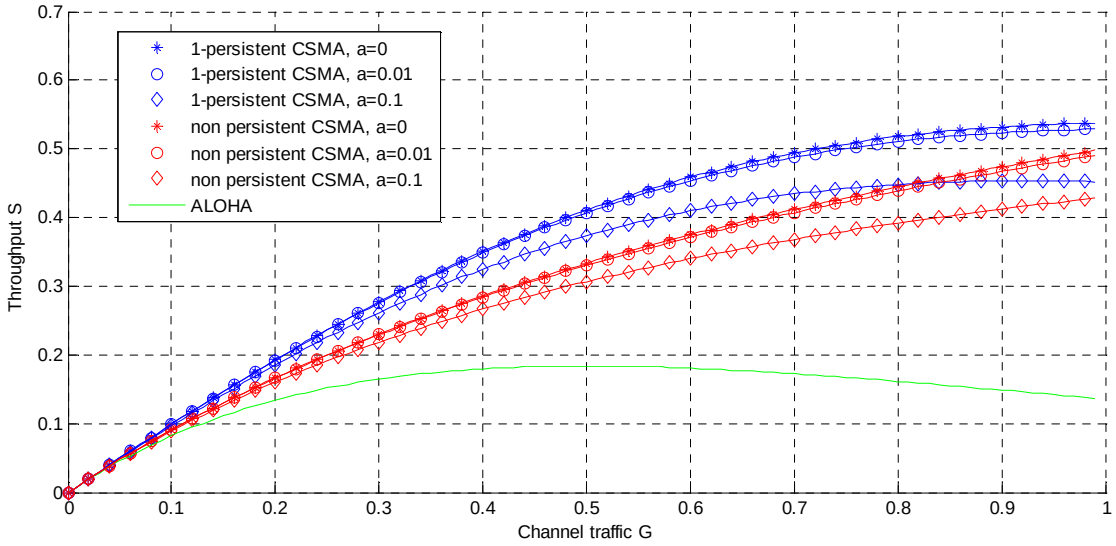


Figure 15: Throughput comparison of non-persistent, 1 persistent CSMA and Aloha

However, it has to be taken into account that the CSMA as well as the Aloha calculations are based on certain assumptions, like an infinite number of users, which are all in radio range of each other, high retransmission delays resulting in a large transmission latency in case of packet losses, the same packet length for all users, and a channel in equilibrium. Hence, neither a dynamic behaviour nor the impact of imperfect LBT is considered. The performance in more realistic scenarios will be investigated in section 5.6.3 and section 5.6.4 for CSMA system without and with acknowledgement procedure, respectively.

4.6 DSSS, DS-CDMA

Originally, direct sequence spread spectrum modulation has been developed for military applications due to its robustness against narrowband interference (e.g. jamming) and the low spectral density on the air interface making the signal hard to detect. Thereby, a narrow band signal is multiplied with a pseudo random spreading code with much higher chip rate compared to the data rate, resulting in large transmit bandwidth. The relationship between the chip rate and data rate is called the processing gain. The receiver correlates the incoming signal with the same pseudo random code, thereby reconstructing the original narrowband data signal and widening the bandwidth of the interferer. A low pass filter after the correlator allows to improve the signal-to-interference ratio.

DSSS can also be used as a multiple access technique, where simultaneously operating links are using different pseudo random codes as it is done in CDMA systems. As the processing gain is large, there is no need for time synchronization between users, so that DS-CDMA systems can be operated without a central control. The wideband DSSS signal resembles white noise, allowing to operate DS-CDMA in parallel to narrowband systems. However, the high processing gain requires correlators operating at a very high chip rate resulting in complex receivers with high power consumption. Furthermore, a large continuous spectrum is required for transmission,

which is not available in the 868 MHz band, so that large processing gains cannot be achieved. Without a large processing gain the performance of DSSS seriously suffers from the near-by-problem, as the processing gain is not sufficient to suppress narrow interferers within a short distance to the receiver. Hence, DSSS is not considered as a suitable multiple access technique for simple, low-cost ISM band transceivers.

4.7 Frequency Hopping (FH), FH-CDMA

An alternative spread spectrum modulation is based on frequency hopping. Like in a FDMA system the bandwidth is divided in non-overlapping frequency bands. In a frequency hopping system there is no fixed allocation of a frequency band to a user, but the transmitter successively hops between all frequencies bands according to a pseudo random code. The receiver operates in synchronisation with the transmitter and remains tuned to the same centre frequency. In general, the pseudo random code is designed such that the all hop channels are visited once within a fixed period of time, the FH cycle. In this case, the duty cycle on each hop frequency is the duty cycle of the link divided by the number of hop frequencies. The time spent on each channel for data transmission is called the dwell time, which is slightly shorter than the hop duration as the PLL requires some time for settling after a frequency change.

Similar to DSSS, FH exploits the advantage of frequency diversity. Even if one or more carriers are corrupted due to narrowband interference or multipath effects, data are still properly transmitted on the remaining hop frequencies. In combination with forward error correction (FEC), lost data can be reconstructed in the receiver. In contrast to DSSS, the spectrum does not need to be continuous.

There are two different kinds of FH systems, **fast (FFH)** and **slow (SFH)** frequency hopping. In the former the dwell time is equal or even shorter than the data symbol duration, so that one data symbol is divided over multiple hops. The resulting FFH signal looks like noise similar to DSSS. Nevertheless, the required implementation complexity of fast FFH is high, so that this access scheme is quite unattractive for SRDs and will not be considered in this study. In SFH the dwell time is larger than the data symbol duration and a short burst of data is transmitted before the frequency is changed. Most FH systems are using SFH for bandwidth spreading (see Annex H of [28]). In a low-data rate system, SFH has a hopping rate in the order of 50 to several hundred hops per seconds [29]. The typical lock time or settling time of the PLL after a frequency change is in the order of 100 µs to 200 µs depending on the loop filter bandwidth. Additionally, some time is needed for reprogramming of the registers. In [29] a value of 50-60 µs is given assuming a 1 MHz clock. The time on a carrier without data transmission is sometimes called the blanking interval and slightly reduces the maximum achievable duty cycle (see Figure 16).

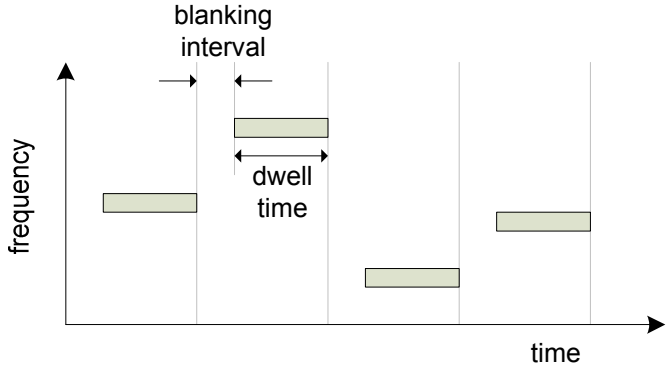


Figure 16: Frequency hopping

Like DSSS, FH can be used as a medium access scheme where each device uses a different pseudo random hop sequence. Within a single FH-CDMA system the users can be synchronised in time, so that it is possible to avoid collisions using orthogonal codes. In case independent FH systems are operated in parallel, a large number of carriers allows for unsynchronised user transmissions, as the probability to use the same frequency at the same time is quite small.

The probability that more than one user selects the same hop frequency can be calculated supposed that *N* users are continuously transmitting using random hop sequences based on the same set of *M* hop frequencies and the same hopping interval duration.

Synchronous hop intervals: $$P_{Coll,sync} = 1 - \left(1 - \frac{1}{M}\right)^{N-1}$$

Asynchronous hop intervals: $$P_{Coll,async} = 1 - \left(1 - \frac{2}{M}\right)^{N-1}$$

The first formula assumes time synchronised frequency changes, which can only be guaranteed within a single systems. For independently operating systems, the collision probability increases as the concurrent devices most likely will change their frequency within the dwell time of the desired user transmission. The results are shown in Figure 17 for 5, 10 and 20 users and a varying number of hop frequencies. The number of frequencies needs to be significantly larger than the number of users for a collision probability of 10%. However, the users are typically not transmitting with a duty cycle of 100%, so that the resulting collision probability might significantly deviate from the calculated values.

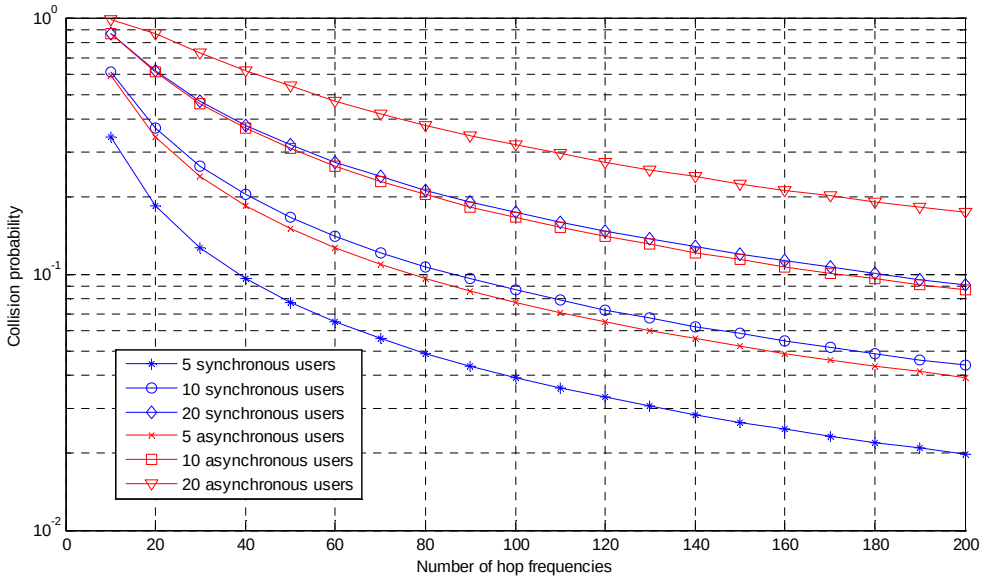


Figure 17: Collision probability of FH systems

SFH can be easily combined with **detect and avoid** (DAA) mechanisms. One prominent example is to perform LBT prior to each transmission on a hop frequency. This scheme is also known as **Adaptive Frequency Hopping** (AFH). In case the channel is occupied, the own transmission is either skipped or delayed until the channel is free or the end of the dwell time is reached (see [30]). LBT allows for a passive evaluation of each channel, but might fail to accurately forecast a collision at the receiver as explained in chapter 4.4 due to different interference situations at transmitter and receiver. In case contention is detected on the same frequency during successive

visits, the carrier can be removed from the frequency hopping list. However, this removal needs to be communicated to the receiver to maintain synchronisation.

Alternatively, the packet is transmitted without LBT and a link quality measurement is fed back on a duplex link. A bad link quality indicator causes the transmitter to skip this frequency in the next few cycles. Short dwell times are required to guarantee that the same frequency is revisited within short time periods. After a few cycles, the hopping frequency is considered again as free. Both DAA schemes slightly reduce the overall duty cycle due to either the LBT measurement time or the overhead for the return link.

4.8 LBT and AFA

Adaptive Frequency Agility (AFA) can be used in combination with LBT to dynamically change the carrier frequency (see EN 300 220-1 [15], EN 300 440 [31]). The exact preconditions for a frequency change are not specified.

In Annex J of ECC Report 37, AFA is defined as procedure, where the transmitter remains on the same frequency unless contention is discovered. If the CCA indicates a busy channel, the transmitter actively searches for a free carrier to continue transmission. As the packet can be directly transmitted on the new channel, this procedure minimises the transmission latency. This implementation might be used in RFID systems, where the receiver requires no knowledge on the carrier frequency, because it simply backscatters the received signal. In other systems, it is very difficult for a remote receiver to maintain synchronisation. The transmitter cannot inform the receiver on the frequency change, as data transmission on the actual, but busy frequency is not allowed. Although the receiver might know in advance to which frequency the transmitter will switch, it then needs to observe more than one channel while waiting for packets. This method requires a complex receiver and implementation is absolutely not straight forward.

One alternative is to consider only slow frequency changes on the basis of a long term channel observation. If the CCA signals in the past often indicated a busy channel and/or the packet loss rate in systems with acknowledgment procedure is above a given threshold, the transmitter can decide to change to another frequency in the near future. It communicates the new frequency value in the next data communication on the actual frequency and changes the frequency only if the receiver has confirmed the reception on the frequency change notification. In this case the latency of a single packet transmission is not reduced as the frequency is only changed after a successful communication on the actual frequency. Nevertheless, this scheme avoids crowded frequencies, which are used by a high number of fixed carrier systems, and helps to equally distribute the channel load on the available frequency bands. In order to reduce the communication overhead, frequency changes should only be initiated if necessary. As long as the channel is only sparsely occupied the link frequency is not modified.

Another alternative is the use of AFH as described chapter 4.7. In this case the frequency is changed in fixed time intervals according to a hop sequence, which allows the receiver to follow the transmitter even if no data is transmitted in case a busy channel is discovered. In principle black lists can be established to avoid a certain hop frequency in case of consecutive disturbances, but this procedure is only reasonable for fixed frequency interferers having a high duty cycle. The exclusion of hop frequencies requires a highly reliable communication with the receiver in order to avoid synchronisation loss. The adaptive maintenance of black lists is sometimes called dynamic frequency selection (DFS).

5. Assessment of individual access schemes

In the previous section some channel access schemes have been excluded because they are not attractive for SRD applications. This section will focus on the remaining random based access schemes requiring no control overhead. The performance of these access schemes will be investigated assuming that all devices within the coverage area are using the same access scheme. Performance will be measured by the number of devices and their duty cycle, which can be operated in parallel without significant packet losses. As most SRD applications are operated in buildings an indoor scenario will be used for analysis. In case systems are using a packet retransmission procedure calculations of system performance becomes very difficult, as the duty cycle becomes time variant and dependent on retransmission schedule. Hence, the performance analysis will be mainly based on simulations, which are supplemented by packet loss calculations for systems without retransmission procedure.

5.1 Indoor channel path loss model

The ITU Indoor Propagation Model defined in Recommendation ITU-R P. 1238-7 [32], also known as ITU Model for Indoor Attenuation, is a radio propagation model that estimates the path loss inside a room or a closed area inside a building delimited by walls of any form. This model approximates the total path loss of an indoor link and is applicable to indoor environments like multi-store office buildings or one story commercial areas. The ITU indoor path loss model is formally expressed as:

$$PL = 20 \cdot \log\left(\frac{f}{MHz}\right) dB + a \cdot 10 \cdot \log\left(\frac{d}{m}\right) dB + L_f(s) - 28\ dB$$

where *PL* is the path loss in decibel, *f* the carrier frequency in megahertz, *d* the distance in meter, *a* the path loss exponent, *s* the number of floor between transmitter and receiver and L_f(s) the corresponding floor loss penetration factor as specified in Table 23.

Parameter		Office Area
Path loss exponent a		3.3
Floor loss penetration factor $L_f(s)$	1 floor	9 dB
	2 floors	19 dB
	3 floors	24 dB

Table 23: Channel parameters from ITU-R P. 1238-7 at 900 MHz

5.1.1 Interference

In a multi-user environment the quality of the communication link is determined by the amount of interference caused by simultaneous transmissions in the same frequency band in addition to noise. The link quality can be measured by the Signal to Interference plus Noise Ratio (SINR). For large distances between concurrent devices or during idle intervals the link quality is dominated by noise, where receiver noise figure (*NF*) adds to the thermal noise (N_0). For high user densities the system is typically interference limited, which means that the received interferer signal power is significantly above the noise floor and the noise becomes approximately negligible. In general, the SINR can be calculated as follows supposed that all values are given in linear scale:

Received power of the desired user: $P_{rx,0} = P_{tx,0}/PL_{lin,0}$

Received power of the *k*-th interferer: $I_{rx,k} = P_{tx,k}/PL_{lin,k}$

Signal to interference-plus-noise ratio: $SINR_{lin} = \frac{P_{rx,0}}{\sum_k I_{rx,k} + N_0 + NF}$

5.2 Simulated scenarios

In section 4 the performance of some random time based access schemes like ALOHA and CSMA has been calculated based on the assumption that all users are in radio range and the overlapping of two packets always results in a loss of both packets. In this section the performance of the multi-user access schemes will be investigated in a more generalised indoor environment, where the receiver power levels are dependent on the distance between transmitter and receiver resulting in hidden and exposed node situations.

5.2.1 Reference scenario (scenario 1)

The reference scenario has been the basis for the analytical performance calculations presented in section 4 and is defined by the following characteristics:

- All *N* users are in radio range
- Any overlap of the two packets causes the loss of both packets

This scenario will be used as a reference to verify the simulation results.

5.2.2 Office area (scenario 2)

The office area scenario considers a four storey building with *N* devices randomly distributed within the building. A path loss exponent of 3.3 will be assumed with an additional power loss dependent on the number of floors in between transmitter and receiver as defined in section 5.1. The building has a surface area of 80 m times 40 m with a height of 20 m. The transmit power is programmable to change the average number of neighbours in radio range and to emulate the coexistence of different SRD systems within the same building.

Each node transmits and receives data packets to one dedicated receiver. The links are randomly selected among all neighbours with an SNR above the receiver sensitivity level. It is assumed that all devices are transmitting with the same signal bandwidth of 200 kHz according to the SEAMCAT simulations in annex 2 of ECC Report 181 [33]. The noise floor is calculated from the formula $N = kTB$ by adding 10 dB for the receiver noise figure and 5 dB for man made noise.

Parameter	Value
Bandwidth BW	200 kHz
Thermal noise	-121 dBm
Noise floor	-106 dBm (F=15 dB)
Receiver sensitivity (Prx,min)	-96 dBm
$SNR_{min} = C/(N+I)$	10 dB

Figure 18: Fixed simulation parameters

The office area is characterized by the following items:

- The SNR on a link between two dedicated link partners is above the sensitivity value plus an optional link margin.
- Packets are received if the SINR is above the minimum value SNR_{min}.
- Only peer-to-peer links are considered in the simulation. The data transmissions of the two link partners are not synchronised. Nevertheless, if a node has just received a data packet from its dedicated transmitter, which needs to be acknowledged, the ACK packet is transmitted with highest priority. A potential own data packet is delayed until the end of the ACK packet.

5.3 Application

Each device is running the same application, which generates equidistant data packets of length T_{Tx}. The packets length as well as the repetition interval T_{int} can be individually defined. The signal bandwidth is assumed to be identical for all applications. In systems using packet retransmissions, the retransmissions need to be scheduled prior to the next new packet generation. If all retransmissions have not been successful, the old packet will be dropped as soon as a new packet is available for transmission. Hence, there is no buffer in the data link layer.

5.4 Simulator

The simulator consists of two parts, a Matlab script and the C^{++} event driven simulator. The Matlab program is responsible for the scenario description and the specification of the device functionality. In summary, the script performs the following functions:

- Random selection of device positions within the building.
- Calculation of received power level for each transmitter at the position of all other devices.
- Selection of network links such that $SNR \geq SNR_{min}$
- Selection of packet sizes and repetition intervals for each transmitter
- Specification of device functionality (LBT=0/1, ACK=0/1)
- Generation of the device and channel description file as input for the C^{++} simulator

The C^{++} simulator emulates the packet transmissions and receptions of N independent nodes within a given simulation time interval. It is assumed that links are operated either with a sufficiently high link margin or are protected by a forward error control (FEC) scheme, so that packet losses due to thermal or receiver noise can be neglected. Hence, packets are only lost due to collisions on the channel. A collision results in a burst error, which typically cannot be corrected by the FEC unless it is a very powerful one. As the collisions should be a rare event, packet retransmissions are much more effective than a powerful FEC with a small code rate.

The functionality of each device is defined by the device description file containing the packet length, the repetition interval, the dedicated receiver ID and two bits, the LBT and ACK setting. If the **ACK bit** is one, the transmitter sets a timeout timer as soon as a data packet has been transmitted, which indicates the arrival time of the expected ACK packet. In case no ACK has been received, the packet is rescheduled after a random offset selected from the interval $[0,2T_{TimeOutRep}]$. It is assumed that the transmitter can only buffer a single data packet. Hence, the arrival of a new packet from the application layer will cancel the retransmission of the old packet, which is then simply dropped. On receiving a packet targeted to the own address a device returns an ACK packet supposed that an ACK is requested by the transmitter. ACK packets are always transmitted $T_{Response}$ ms after the end of the corresponding data packet, where the time offset considers data processing and switching time between receive and transmit mode. In case an own data packet transmission is scheduled while an ACK needs to be transmitted, the own data packet will be delayed until the end of the ACK packet transmission.

Setting the **LBT bit** to one causes the device to perform a channel measurement prior to each transmission. If the channel is busy, the next trial is performed after a random time offset in the interval $[0,2T_{Rep}]$. If T_{Rep} is equal to minus 1, the transmission is simply skipped and no packet is transmitted within the actual repetition interval. Otherwise, the device schedules new transmissions trials until the channel is free. In case the LBT bit is zero, the device directly sends its data packet without listening.

The flowchart of a device implementation in the C^{++} simulator is shown Figure 19, highlighting the OSI layers by different colours. The yellow application layer schedules the data packets sending exactly one packet at the beginning of each repetition interval. The start of the first repetition interval is randomly selected within $[0,T_{int}]$. The orange data link layer (DLL) might add a random offset to the packet transmission time in order to avoid continuous packet collisions of two neighboured nodes. Additionally, the DLL layer is responsible for packet retransmissions supposed that the ACK bit is set to 1. The grey Medium Access Control (MAC) optionally performs LBT prior to the packet transmission. The blue physical layer (PHY) sends the packets to the channel (green), which forwards the packet to all users in the system. Each copy of the packet is complemented by received power information depending on the distance between transmitter and the actual receiver. On receiving a packet the PHY calculates the SINR and compares the result to the required minimum value. Only packets with a higher SINR are forwarded to the MAC, the others are simply discarded because they have been lost due to a collision. The MAC deletes the packets with a target address differing from the own address, while own packets are forwarded to the DLL layer. The DLL schedules the ACK packet if required, which is transmitted by the PHY after $T_{Response}$ seconds. The time offset $T_{Response}$ considers the time for switching from receive to transmit mode in the PHY and the assembly of the ACK packet. In case a received packet is an expected ACK packet, the DLL layer deletes the timeout for retransmissions and waits for the next data packet from the application layer.

Figure 19: Simulator flowchart

The simulation parameter are summarised in Table 24. It should be taken into account that the table does not define retry limits for LBT trials or packet retransmissions in ACK procedures as the number of retries in inherently limited by the fact that the packet is skipped as soon as the new data packet is generated in the application layer. The minimum time available for retries is specified by $T_{int} - T_{Random}$, where T_{Random} denotes a random offset interval for the first trial or first packet transmission in case of a non-LBT system. The offset guarantees that the data packets are quasi randomly transmitted on the channel although they are periodically generated in the application layer. Furthermore, the start time for the data generation in the application layer is a random variable within $[0, T_{int}]$ and therefore different for all devices. In general, the following simulator parameters are configurable:

Symbol	Parameter	Unit
N	Number of devices in the building	
NF	Receiver noise figure plus man made noise	dB
$P_{rx,min}$	Receiver sensitivity level	dB
$SINR_{min}$	Minimum SINR for packet demodulation	dB
$T_{int,k}$	Repetition interval of the k-th user (device description file)	ms
$T_{Tx,k}$	Packet duration of the k-th user (device description file)	ms
T_{Random}	Random offset for data packet transmissions in the DLL	ms
P_{det}	LBT: Minimum received power for interferer detection	dB
T_L	LBT: measurement time for interference detection	ms
T_R	LBT: minimum interferer packet time within T_L for detection	ms
T_D	LBT: dead time	ms
T_{Rep}	LBT: if the channel is busy, a new transmission trial is scheduled after a random time offset uniformly distributed in $[0, 2T_{Rep}]$. If T_{Rep}=-1, the actual packet is simply dropped.	ms
T_{Ack}	ACK: Acknowledgement packet duration	ms
$T_{Response}$	ACK: Time offset in between the end of the data packet and the start of the ACK-packet	ms
$T_{TimeOutRep}$	ACK: After timeout the transmission of the packet is repeated with a random time offset uniformly distributed in $[0, 2T_{TimeOutRep}]$.	ms

Table 24: Simulation parameter

As the offset to the next trial in a LBT based system is a random variable, the maximum number of trials might slightly change from interval to interval. Nevertheless, in the average the number of trials is defined by T_{int}/T_{Rep}. Similar calculations can be done for the channel access scheme with ACK. The average maximum number of retransmissions is given by $T_{int}/T_{TimeOutRep}$. A CSMA with ACK procedure has typically a smaller limit for packet retransmissions, as some time is needed to transmit the packet in case of high traffic loads. One example is shown in Figure 20, where all random time offsets T are denoted by their interval $[0, T_x]$ with $0 \leq T < T_x$. The figure is not to scale, but shows the principle of packet scheduling.

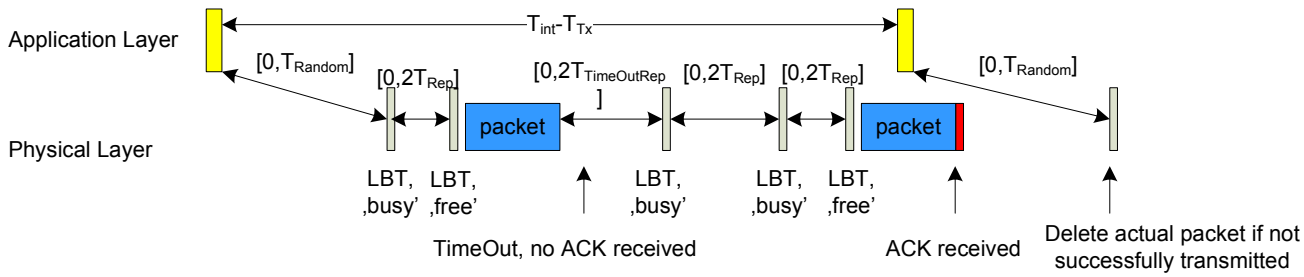


Figure 20: Example for packet scheduling in a CSMA system with LBT

5.5 Simulation results for the reference scenario

The reference scenario is used to compare simulation results with calculated packet loss rates to verify the simulator operation and to analyse the impact of implementation and timing parameters on the performance of access schemes.

5.5.1 Duty cycle based random access

The collision probability for DC based random access schemes has been calculated in chapter 4.2 and the results are shown in Figure 5 for three different DC values of 0.1%, 1% and 10% and the same packet length for all users. The packet duration has no impact on the performance results as long as the repetition interval is adapted accordingly to maintain the same duty cycle. The reference scenario is used for simulator verification. The simulated number of users is set to 2, 4, 6, 10, 20, 40, 60 and 100. As the application generates equidistant packets and all users are transmitting with the same repetition interval, the transmit time should be randomised in order to avoid a continuous loss of packets due to a similar start time selection. The random offset interval is maximised using

$$T_{Random} = T_{int} - T_{Tx}$$

The simulation results in Figure 21 show an exact match of calculated and simulated packet loss probabilities.

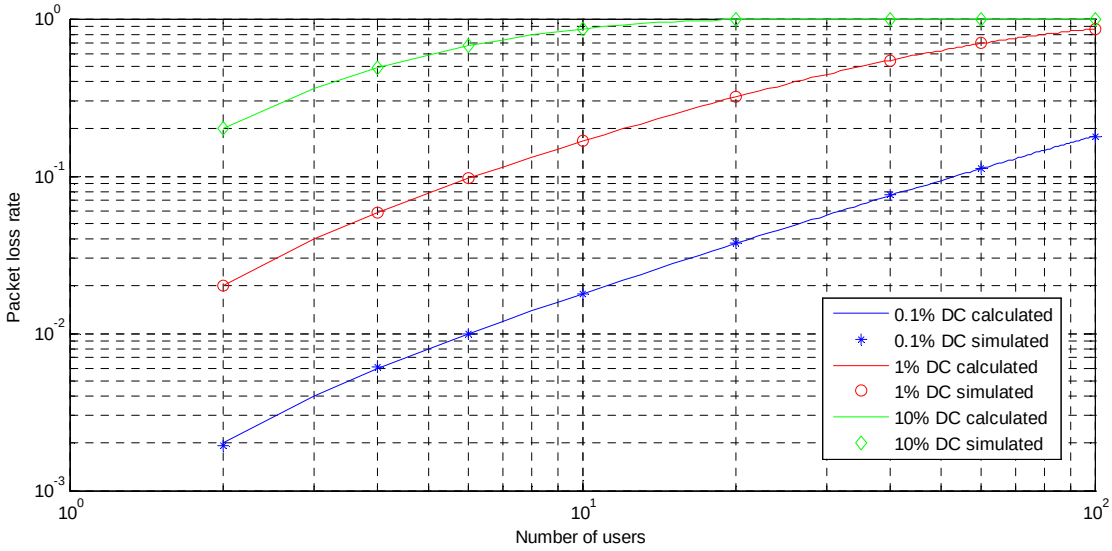


Figure 21: Comparison of calculated and simulated PLR as a function of the number of users (same packet length and DC)

The offered load and the measured channel load on the air interface are shown in Figure 22. The offered load can be simply calculated by $N \cdot DC$, where N is the number of users and DC the duty cycle on each link. The measured channel load is always equal or smaller than the offered load due to packet collisions. The deviation is an indicator for the number of collisions.

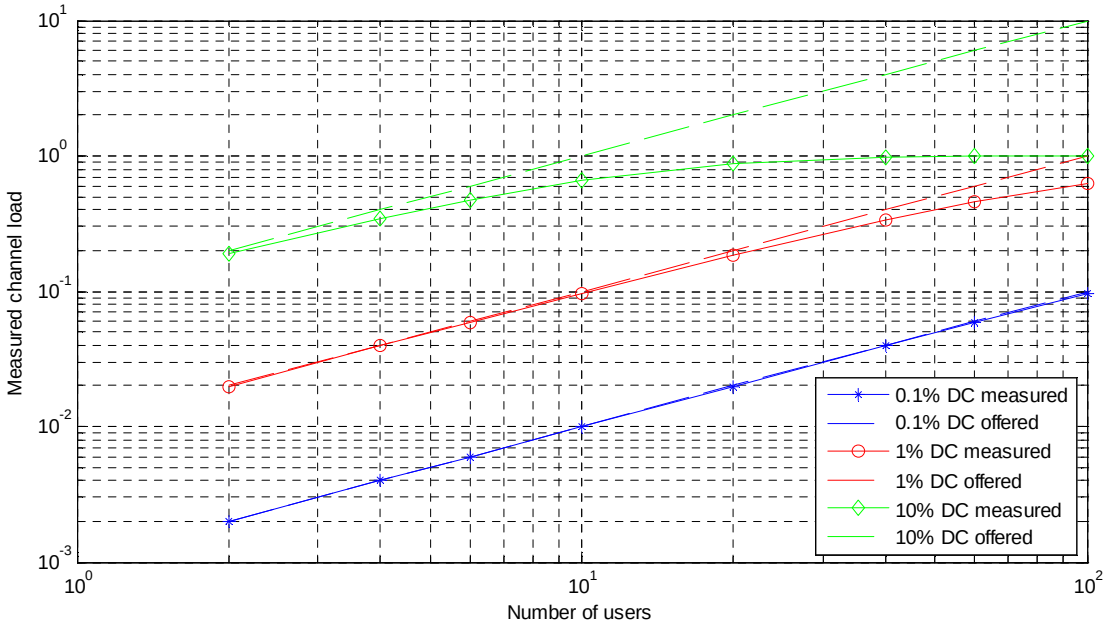


Figure 22: Comparison of offered load and the measured channel occupation as a function of the number of users (same packet length and DC)

The previous simulation assumed equal packet length for all users. Supposed that two different systems are operated in parallel, they will typically use different packet lengths even if their duty cycles are identical. In case each system consists of $N/2$ devices and the packet length of the first system is R times higher than the packet length of the second system, the packet loss rates in both systems can be calculated according to

$$R = \frac{T_{Tx,long}}{T_{Tx,short}} = \frac{T_{int,long}}{T_{int,short}}$$

$$PLR_{short} = 1 - (1 - 2 \cdot DC)^{\frac{N}{2}-1} \cdot \left(1 - DC - \frac{DC}{R}\right)^{N/2}$$

$$PLR_{long} = 1 - (1 - 2 \cdot DC)^{\frac{N}{2}-1} \cdot (1 - DC - R \cdot DC)^{N/2}$$

as described in section 4.2. Two simulations have been performed for different packet length assumptions and a constant duty cycle of 1% on each link. In the first simulation $N/2$ devices are transmitting packets of 2 ms, while the packet length of the remaining $N/2$ is 20 ms, so that R is equal to 10. In the second simulation the parameter R is increased to 20, resulting in a packet length of 40 ms for the system with the long packets.

Figure 23 compares the simulated and calculated packet loss rates for $R = 10$ on the left and $R = 20$ on the right side. The red curve indicates the loss rate for a user transmitting short packets, while the green curve belongs to the user with long packets. The blue curve is added as a reference, showing the PLR in a scenario with equal packet lengths. The simulation results are consistent with the calculated results. The PLR is significantly higher for the devices transmitting long packets.

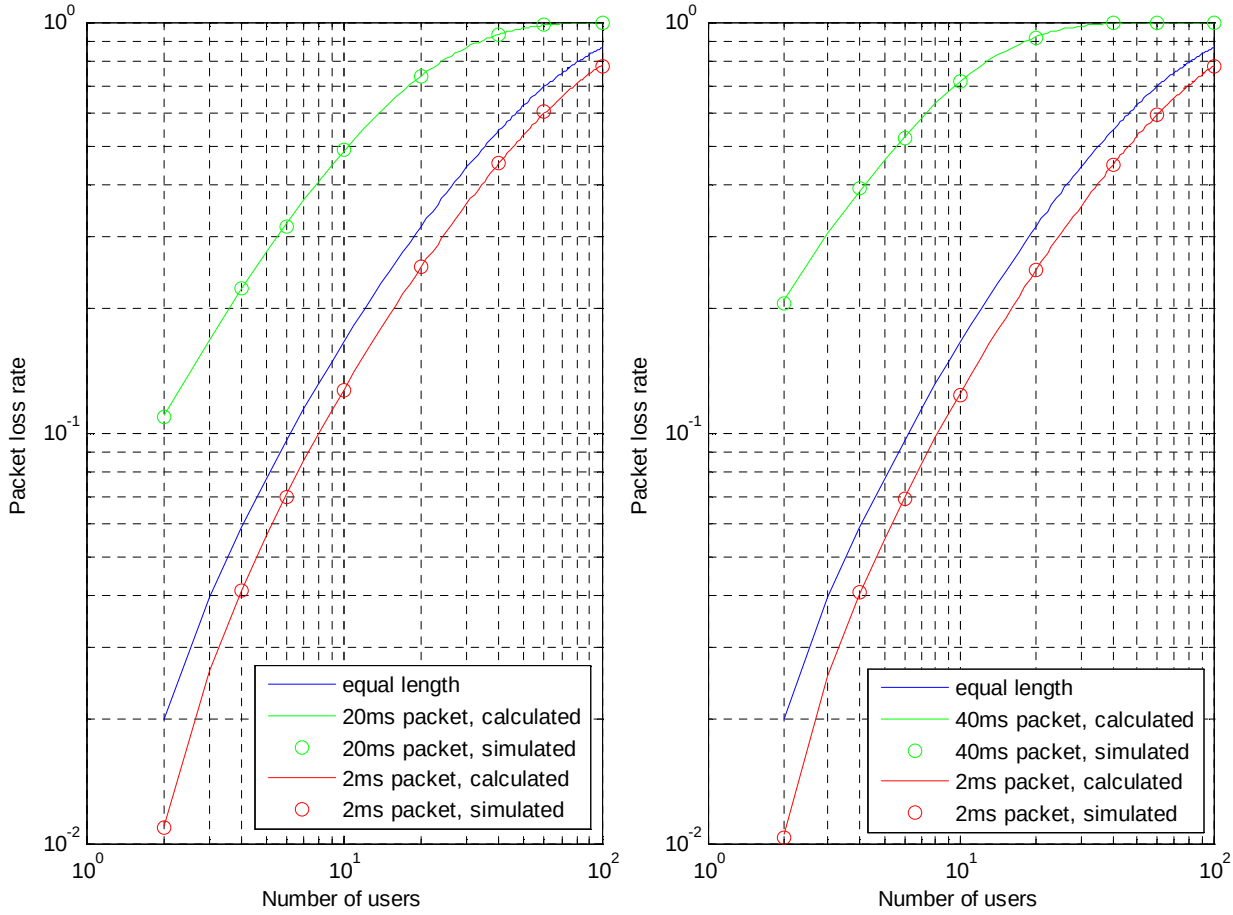


Figure 23: Comparison of calculated and simulated PLR in two systems with different packet lengths

5.5.2 Aloha

Each user transmits the periodically generated data packets with a small random time jitter to avoid constant overlapping of the first transmission trials on the one hand, but to maintain sufficient time for retransmissions in case of collisions. The simulations are repeated for 1000 different sets of randomly selected start times.

The first simulation assumes that all users are transmitting with an application DC of 1% and a packet length of 2 ms. The length of the ACK packet (T_{Ack}) as well as its distance to the data packet ($T_{Response}$) is set to 0, resulting in an ACK packet loss rate of zero.

Parameter	Value	Comment
DC_{APP}	1%	Duty cycle in the application layer
T_{Tx}	2 ms	Packet length
T_{Random}	40 ms	Random offset after packet generation
$T_{TimeOutRep}$	10, 25, 50 ms	ACK: Mean retransmission interval
$T_{Response}$	0	ACK: Distance between the end of the data packet and the start of the ACK-packet (ideal)
T_{ACK}	0	ACK: Length of the ACK packet (ideal)

Table 25: ALOHA simulation parameters in the reference scenario

In case no ACK packet has been received the data packet is retransmitted after a randomly selected time offset in between $[0,2 \cdot T_{TimeOutRep}]$. The time offset needs to be large enough to minimize the probability that the retransmitted packets are once more colliding. On the other side, a large time offset reduces the number of retransmission possibilities within the repetition interval, as the retransmission is aborted as soon as a new packet is generated in the application layer. Three different values, 10, 25 and 50 ms, have been simulated to analyze the impact of the retransmission interval on the system performance.

Figure 24 shows the offered load and the measured channel load on the air interface as a function of the mean retransmission offset. The simulator counts the total number of packets generated in the application layer (N_{new}) and packet retransmissions (N_{rep}) initialised by the DLL layer during the simulation time. Hence, the offered load on the channel can be calculated as follows:

$$G = \frac{(N_{new} + N_{rep})T_{Tx}}{T_{simulation}}$$

where T_{Tx} is the data packet duration and $T_{simulation}$ denotes the simulation time. The black line in Figure 22 represents the offered data traffic excluding retransmissions and can be simply calculated to $\frac{N_{new} \cdot T_{Tx}}{T_{simulation}}$, which is always equal to $N \cdot DC_{APP}$ where N denotes the number of users.

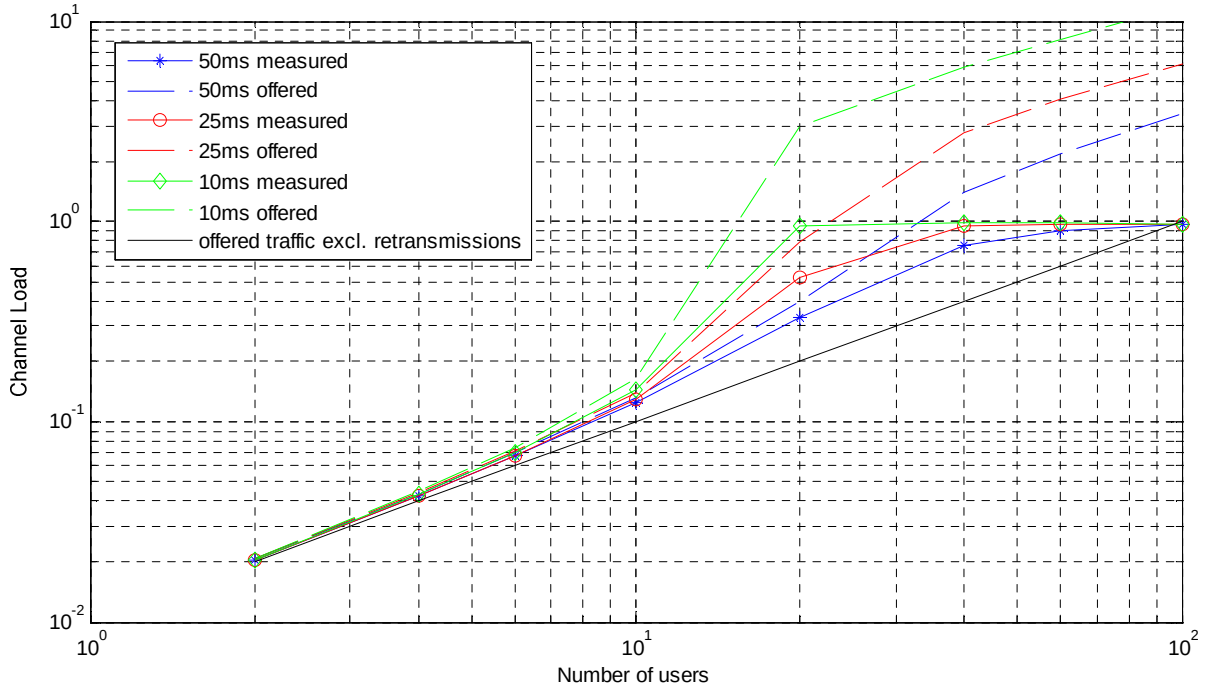


Figure 24: Measured channel load on the air interface as a function of the mean retransmission offset

The offered and measured traffic in the simulation is close to the black line in low traffic scenarios with two or four devices. There are only a few collisions, so that the number of packet retransmissions is still significantly smaller than the number of data packets generated in the application layer. In a scenario with ten users or more the impact of collisions is no longer negligible. Supposed that 20 devices are transmitting in parallel, the offered traffic excluding

retransmissions is 0.2 (black line). If retransmissions are considered, then the offered traffic significantly depends of the selected mean retransmission interval. For a mean interval of 50 ms the offered traffic is equal to 0.4 (blue dashed line) so that each data packet is transmitted twice in the average. Lowering the retransmission interval to 25 ms, the offered traffic increases to 0.8 which is 2 times higher. The measured channel load is always equal or lower than the offered traffic due to packet overlapping und upper limited by 1.0 corresponding to a channel load of 100%. The distance between the offered traffic and the measured channel load is an indicator for packet collisions.

Based on the offered traffic load determined in the simulation, the expected number of successfully received packets can be calculated to $S = G\exp(-2G)$. Figure 25 compares the calculated packet success rate (blue line) to the number of received data packets divided by the number of transmitted data packets (incl. retransmissions) counted in the simulator for the a retransmission interval of 50ms. The two curves are almost overlapping.

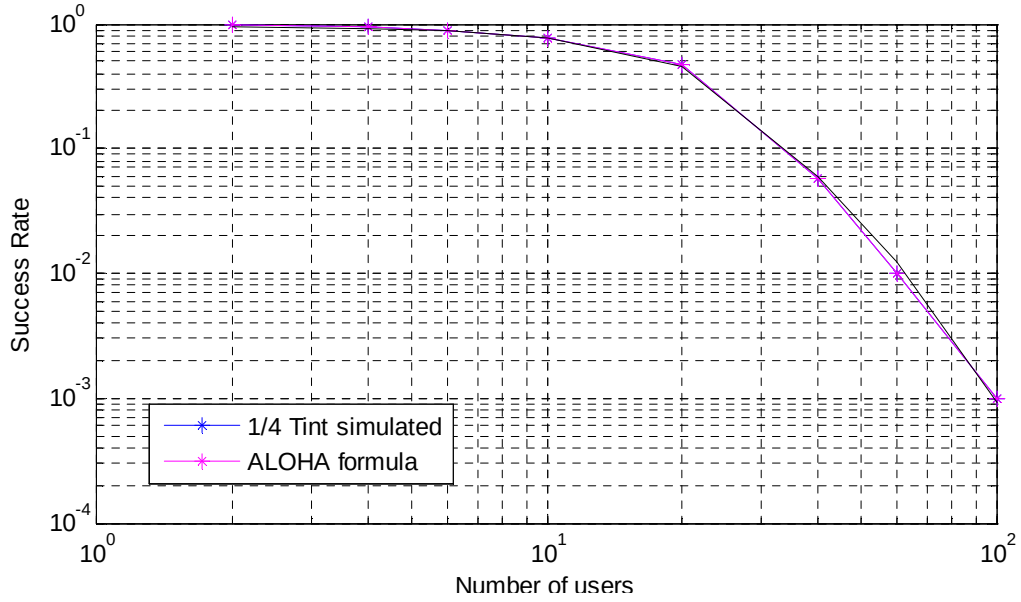


Figure 25: Comparison of calculated and simulated success rate as a function of the number of nodes (DC=1%, $T_{TimeOutRep}$= 50ms)

The ALOHA formula calculates the transmission success rate on the channel, while only the packet loss rate in the application layer is relevant for the analysis of system performance. Packets transmitted on the channel might get lost if at least one copy of each data packet is successfully transmitted. The number of retransmissions is limited, as packets are skipped in the transmitter as soon as a new data packet is generated in the application layer. Hence, the packet loss rate in the application layer for a system with packet retransmissions just depends on the number of skipped packets in the transmitter and the results are presented in Figure 26 as a function of the number of users and the mean retransmission interval. Comparing the packet loss rate in a system with packet repetitions to a DC based system with a single transmission trial per data packet (black line), the packet loss rate in the ALOHA system is significantly smaller if the number of users is small. Furthermore, a short retrial time significantly reduces the packet loss probability as the number of possible retransmissions becomes higher. Nevertheless, the performance significantly degrades if the channel load increases. Especially for short retransmission times, the probability that the retransmitted packets are again colliding becomes very high for more than 10 users operating in parallel. Hence, a retransmission interval of

25 ms, which is slightly more than 10 times the packet length, seems to be a good compromise if the load on the channel is unknown

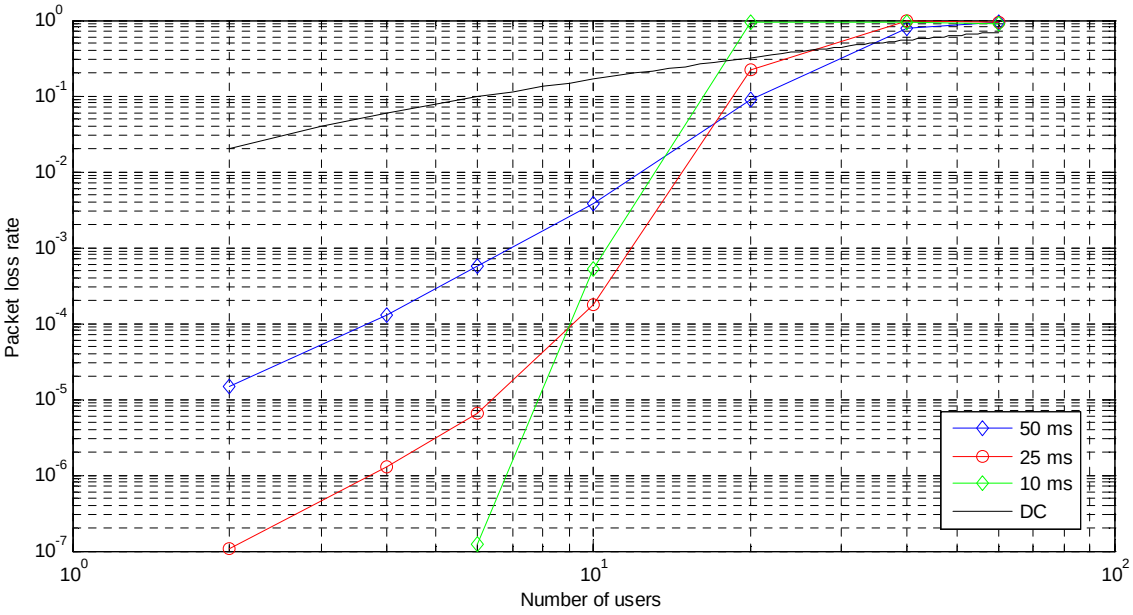


Figure 26: Packet loss rate as a function of the number of nodes (DC=1%) with different retransmission intervals compared to a DC based random access

Considering a non-zero ACK packet length and a delay between the received data packet and the transmitted ACK packet slightly worsens the system performance. Figure 27 shows the simulated packet loss rates for the zero ACK packet duration (blue), for an ACK packet duration of 0.5 ms and zero response time (red) and finally an ACK packet duration of 0.5 ms and a response time of 0.5 ms, while the packet duration itself is 2 ms. Both, ACK packet duration and response time, obviously increase the effective packet duration and hence need to be considered in the duty cycle calculations.

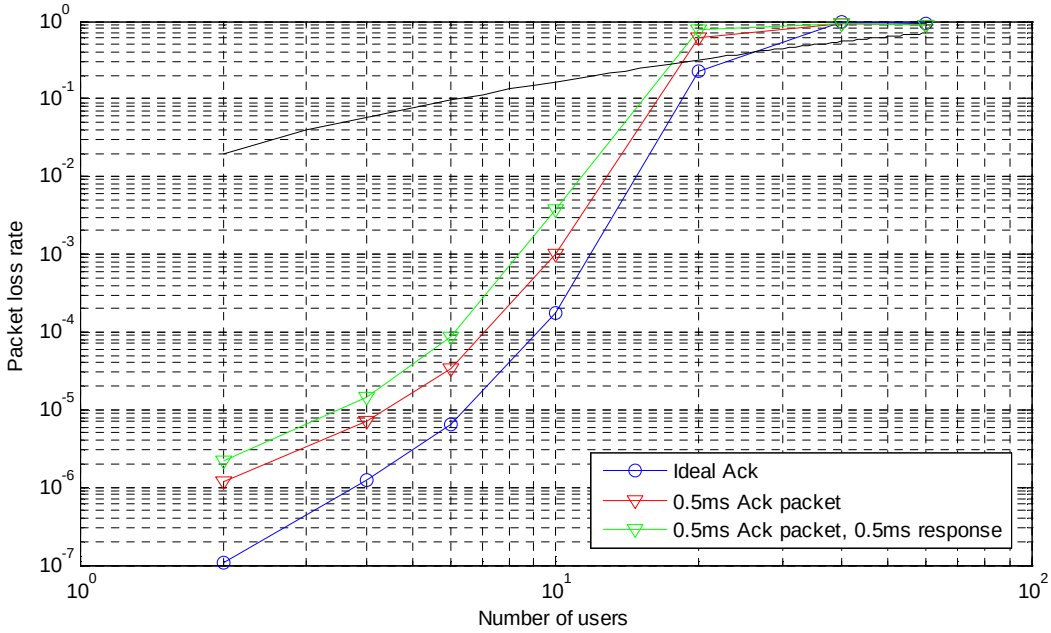


Figure 27: Packet loss rate as a function of the number of nodes (DC=1%) for a non-zero ACK length and response time, a retransmission interval of 25 ms and a packet length of 2 ms

5.5.3 LBT

Instead of retransmitting a packet in case of a collision, the probability of a collision can be reduced using LBT. In a first step, the LBT procedure is implemented in the simulator based on energy detection to check if the channel is available for transmission. An interferer needs to be present for at least T_R seconds within the measurement interval T_L in order to be detected. After the channel measurement the transceiver switches from receive to transmit mode to send the data packet in case the channel is free. The dead time T_D in between the end of the measurement and the start of the packet is a simulation parameter

In the simplest LBT system the packet is simply skipped if the channel measurement indicates a busy channel, so that there is no further transmission trial. It is expected that for perfect channel measurements, the packet loss rate is approximately halved. While a collision of two packets in the DC systems results in a loss of both packets, the LBT system only looses the skipped packet, while the other packet can be successfully transmitted.

In detail, the packet loss probability can be calculated as follows supposed that only two devices are transmitting. The number of packet losses depends on the time offset between the measurement intervals of the two nodes. In the first case device A detects the packet of device B and skips its own packet transmission. Case 2 describes the LBT failure as described in section 4.4, where the two devices get a "channel free" signal and the transmitted packets will collide. The third situation is similar to the first. This time, device B detects the packet transmission of device A and skips its own transmission.

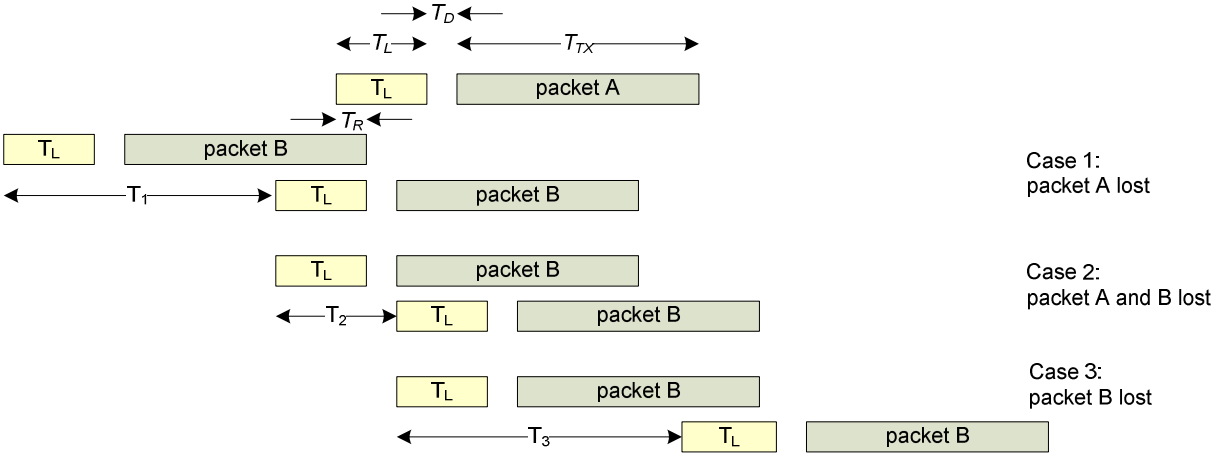


Figure 28: Simple LBT scheme with two devices

Calculating the time offsets T_1, T_2 and T_3 as shown in Figure 28,

$$T_1 = T_{Tx} + T_L - 2T_R$$
$$T_2 = 2T_D + 2T_R$$
$$T_3 = T_{Tx} + T_L - 2T_R = T_1$$

the packet loss rate can be calculated to

$$PLR = \frac{T_1 + T_3 + 2T_2}{2\,T_{int}} = \frac{T_1 + T_2}{T_{int}} = \frac{T_{TX} + T_L + 2T_D}{T_{int}}$$

The PLR of a DC based random access is equal to

$$PLR_{DC} = \frac{2T_{TX}}{T_{int}}$$

Hence, the LBT is expected to outperform the DC based system as long as the measurement interval and the dead time are small compared to the packet length. Figure 29 compares the simulated packet loss rate of the LBT system for different dead times T_D in between the channel measurement and the packet transmission. The packet length is 2 ms with a duty cycle of 1% on each link. The simulation has been repeated for the following time settings:

T_{Tx}	2 ms			
T_{int}	200 ms			
T_L	1 ms			
T_D	0 ms	0.25 ms	0.75 ms	1.75 ms
T_R	0 ms	0.25 ms	0.25 ms	0.25 ms

Table 26: LBT simulation parameters

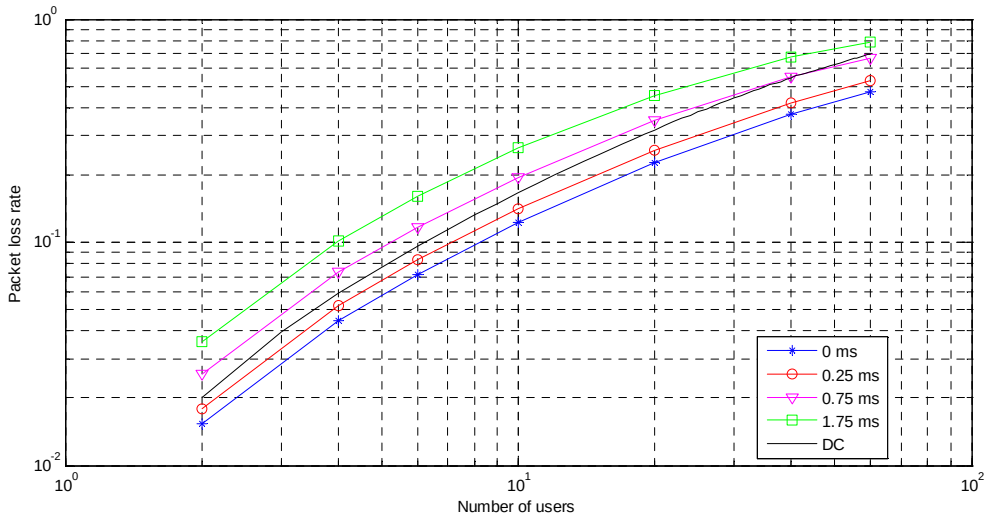


Figure 29: Packet loss rate for LBT system without retrials, DC=1%, 2ms packets as a function of T_D

The blue curve belongs to an ideal LBT system with a PLR, which is smaller than the PLR of the duty cycle based random access scheme. Nevertheless, the PLR is not halved as the measurement interval of 1 ms is already large compared to the packet length. From the calculations above the expected PLR rate is 3/200=0.015, which is close to the simulated result for two devices. Increasing the dead time decreases the performance gain, so that the LBT system might be even worse than the DC system. The table below compares the calculated and measured packet loss rate as a function of the dead time for a system with only two devices.

T_D	0 ms	0.25 ms	0.75 ms	1.75 ms
PLR_{Calc}	0.015	0.0175	0.0225	0.0325
PLR_{Sim}	0.0153	0.0179	0.0255	0.0357

Table 27: Comparison of calculated and simulated PLR for two devices

Nevertheless, the impact of the parameters T_L and T_D reduces if the packet becomes larger. Figure 30 presents the results for a packet length of 20 ms maintaining a duty cycle of 1% on each link. In this case, LBT always outperforms the DC based random access.

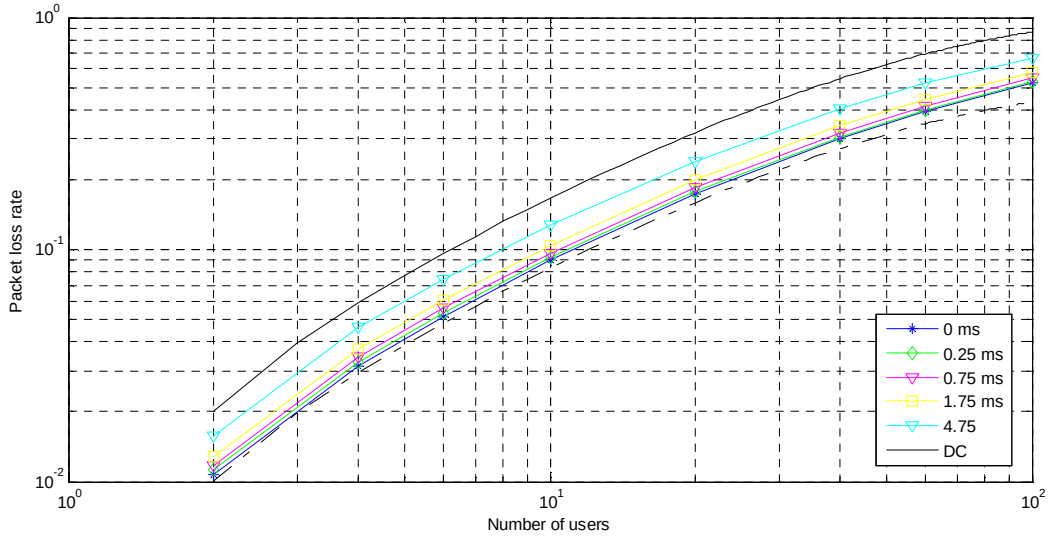


Figure 30: Packet loss rate for LBT system without retrials, DC=1%, 20ms packets as a function of T_D

T_L	1 ms				
T_R	0 ms	0.25 ms	0.25 ms	0.25 ms	0.25 ms
T_D	0 ms	0.25 ms	0.75 ms	1.75 ms	4.75 ms
PLR_{Calc}	0.0105	0.0108	0.0113	0.0123	0.0153
PLR_{Sim}	0.0107	0.0112	0.0117	0.0128	0.0159

The comparison of simulated and calculated packet loss rate has shown that the LBT procedure in the simulator properly works. Nevertheless, the benefit of this simple approach is so small, that it is not considered as a access scheme variant for the more realistic office scenario simulations. LBT should always be combined with retrials in case of a channel busy indication. The resulting CSMA scheme is discussed in the following section.

5.5.4 Non-persistent CSMA

The CSMA simulation uses LBT prior for each packet transmission. In case the channel is busy, a new trial is initialized after a randomly selected time offset in between $[0, 2 \cdot T_{Rep}]$ as shown in the figure below.

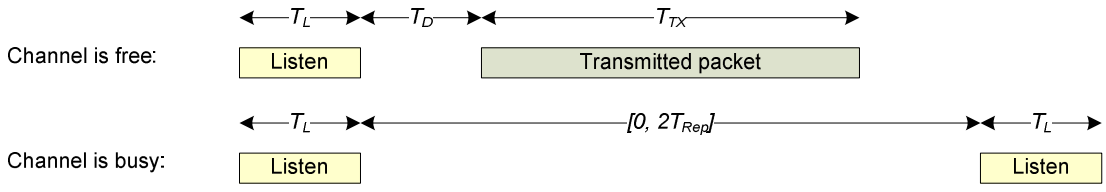


Figure 31: LBT timing parameters

Note, that the measurement interval as well as the dead time reduces the maximum possible channel load as spaces in between packet transmissions cannot be avoided. In principle, the minimum distance in between two successful packets is obtained, if the new device starts its listening interval less than T_R seconds prior to the end of the last packet transmission as shown in Figure 32.

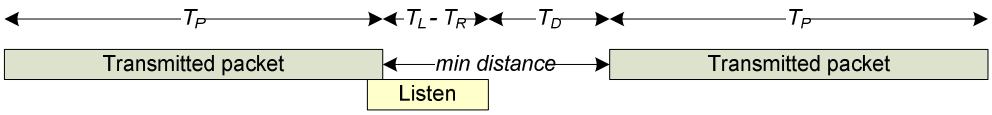


Figure 32: Minimum time offset between packets using LBT

The listening time T_L will again be fixed to 1 ms. Furthermore, it is assumed that a signal needs to be present for at least $T_R = 0.25$ ms in order to be measured. The time for a new trial should be randomly distributed. Supposed that two devices simultaneously detect a busy channel, the next trial time offsets are selected from the interval $[0,2 \cdot T_{Rep}]$. A small value of T_{Rep} increases the probability that the forthcoming measurement intervals will coincide resulting in a packet loss if the channel is free and both users are transmitting. On the other side, a large value decreases the number of transmission trials within a data repetition interval. Hence, a value of 10 times the packet length seems to be a good compromise, which allows for random distribution, but also enables several transmission trials prior to the next data packet generation. The simulation parameters are summarised in Table 28.

Parameter	Value	Comment
DC	1%	Duty cycle on each link
T_{Tx}	2 ms, 20 ms	Packet length
T_L	1 ms	LBT: RSSI measurement interval
T_D	0,0.25,0.75,1.75,4.75 ms	LBT: Dead time
T_R	0,0.25 ms	LBT: RSSI detection interval
T_{Rep}	$10 \cdot T_{Tx}$	CSMA: Mean transmission retrial interval

Table 28: CSMA-ACK simulation parameters in the reference scenario

There are two reasons for packet losses. On the one side, measurement intervals are overlapping so that two devices cannot detect each other. The probability increases for larger dead times. On the other side, successive transmissions trials may fail due to a high traffic load on the channel. In this case a new data packet might be generated in the application layer before the last one has been transmitted. In the simulation the buffer can only memorize a single packet and the old packet is skipped as soon as the new one arrives. The number of cancelled packet transmissions is counted, so that the two effects can be separated in the forthcoming analysis.

The probability of a packet loss as a function of the dead time and the number of users is shown in Figure 33. All devices are generating one data packet of 2 ms within a 200 ms interval. The number of users is shown on the x-axis while the parameter in the legend represents the term $T_R + T_D$. The packet loss rate includes packet losses due to buffer overflow as well as collisions on the channel.

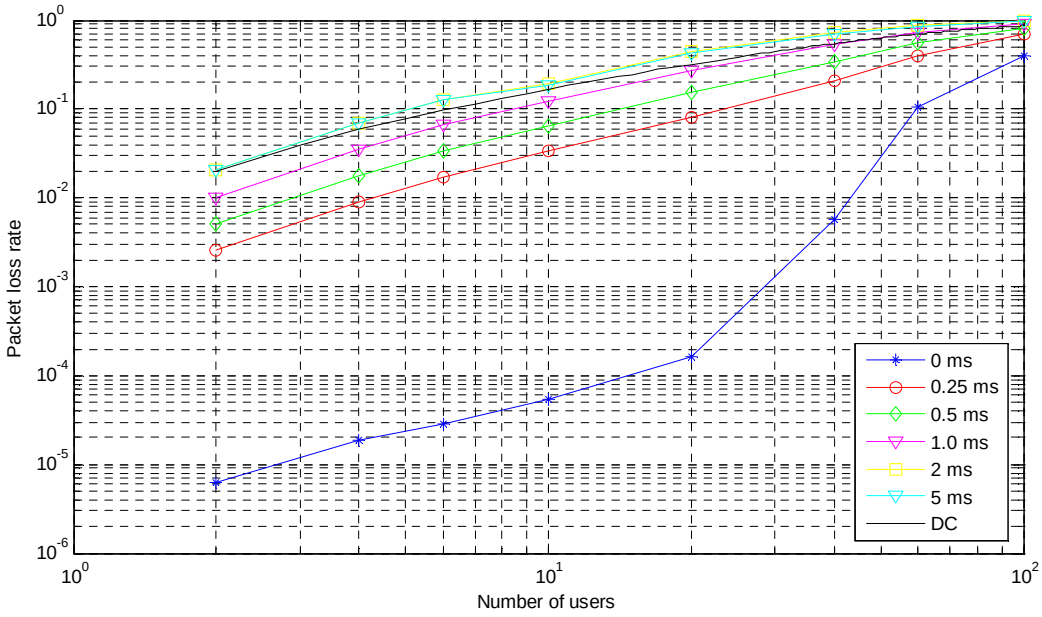


Figure 33: Total packet loss rate in a CSMA system as a function of $T_R + T_D$, 2ms packets, DC=1%

Figure 34 separates the packet loss caused by buffer overflow. As long as no more than 10 devices are operating in parallel, packet overflows do not exist. Hence, the packet losses shown in Figure 33 are solely caused by the overlapping of measurement intervals. If the term $T_R + T_D$ is zero, the chance that the measurement intervals of two devices starts at exactly the same time should be close to zero. Nevertheless, time offsets in the simulator are calculated based the rand() function resulting in just 32767 different time offsets. If two devices are operating in parallel, the chance that they both select the same offset is equal to $3 \cdot 10^{-5}$. Hence, the probability is not as close to zero as expected. The first buffer overflows have been detected operating 20 users in parallel, although the resulting number of packet losses is still smaller than the number of collisions caused by the limited time resolution.

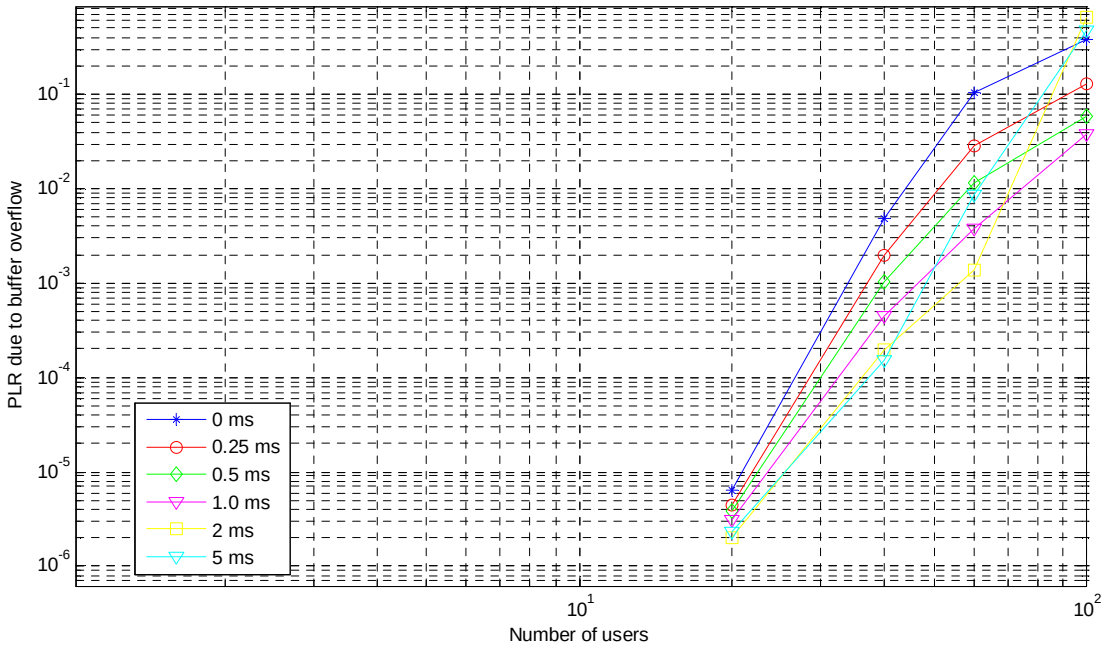


Figure 34: Packet loss rate due to buffer overflow in a CSMA system as a function of $T_R + T_D$

This is no longer true for high traffic loads, where the packet loss due to buffer overflow becomes the dominant effect. The MAC layers fails to find a free channel for transmission before the next packet is generated in the application layer. A large dead time reduces the probability of an overflow, because the LBT often fails to detect the neighbour signal. Hence, the channel seems to be free and the packet is transmitted. Nevertheless, the packet will be lost due to a collision on the channel, so that the total PLR in Figure 33 is higher.

In practice, the neighbour signal needs to be present within the measurement interval for a certain amount of time to be detected. Furthermore, the packet cannot be transmitted directly at the end of the measurement interval. At least switching from receive to transmit mode requires some time, so that the sum of the two terms will certainly greater than zero. Setting the sum to 0.25 ms significantly increases the packet loss rate as shown in Figure 33. Even if only two users are transmitting in parallel a packet loss rate of 0.26 % is measured although no packet has been lost due to a buffer overflow as shown in Figure 34.

The packet loss rate for two devices using LBT can be calculated as described in section 4.4. The time offset of the two channel measurement start times needs to be larger than $2(T_R + T_D)$ in order to detect the neighbour transmission (see Figure 12). As the start times are randomly selected from the interval [0, T_{int}] the probability of a packet loss is equal to

$$PLR = \frac{2(T_D + T_R)}{T_{int}} \text{, if } T_D + T_R < T_{Tx}$$

$$PLR \approx \frac{2T_{Tx}}{T_{int}} \text{, if } T_D + T_R > T_{Tx}$$

If the term $T_R + T_D$ is larger than the packet duration, LBT is no longer of any use and the systems performs slightly worse than a DC based system, as the maximum channel load is reduced. The following results are obtained as a function of T_R and T_D and compared to the simulation results.

T_D	0	0.25 ms	0.75 ms	1.75 ms	4.75 ms
T_R	0.25 ms	0.25 ms	0.25 ms	0.25 ms	0.25 ms
$T_D + T_R$	0.25 ms	0.5 ms	1.0 ms	2.0 ms	5 ms
PLR (calculated)	$2.5\ 10^{-3}$	$5.0\ 10^{-3}$	$1.0\ 10^{-2}$	$2.0\ 10^{-2}$	$2.0\ 10^{-2}$
PLR (simulated)	$2.57\ 10^{-3}$	$5.11\ 10^{-3}$	$1.02\ 10^{-2}$	$2.04\ 10^{-2}$	$2.04\ 10^{-2}$

Table 29: Expected packet loss rate for 2 users with CSMA (LBT) as a function of the dead time

The calculated PLR are quite similar confirming the simulator results. The degradation is large for a system transmitting with small repetition intervals as the PLR depends on the ratio of the implementation parameter divided by the repetition interval. Repeating the simulation with the same duty cycle on each link, but a larger packet duration of 20 ms proofs the usefulness of CSMA compared to a simple DC based random access system.

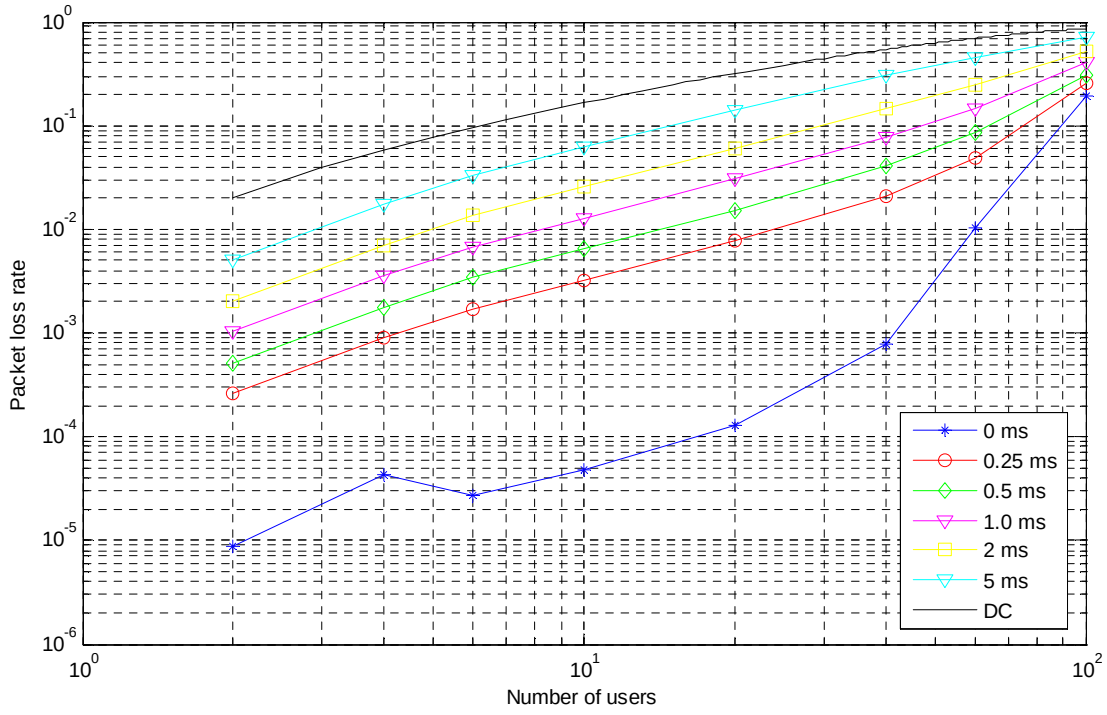


Figure 35: Total packet loss rate in a CSMA system as a function of $T_R + T_D$, 20ms packets, DC=1%

In case two CSMA systems are operating in parallel using the same implementation parameters T_R and T_D, a duty cycle of 1% and a retrial interval T_{Rep} of 10 times the packet length, but different packet lengths, the results in Figure 36 are obtained. The average packet loss rate of the *N*/2 devices transmitting 2 ms packets is nearly identical to the packet loss rate of the remaining *N*/2 devices transmitting 20 ms packets as soon as there are more than 6 devices in the system. The reason is that the interference situation of each device becomes comparable if the number of devices in the system increases.

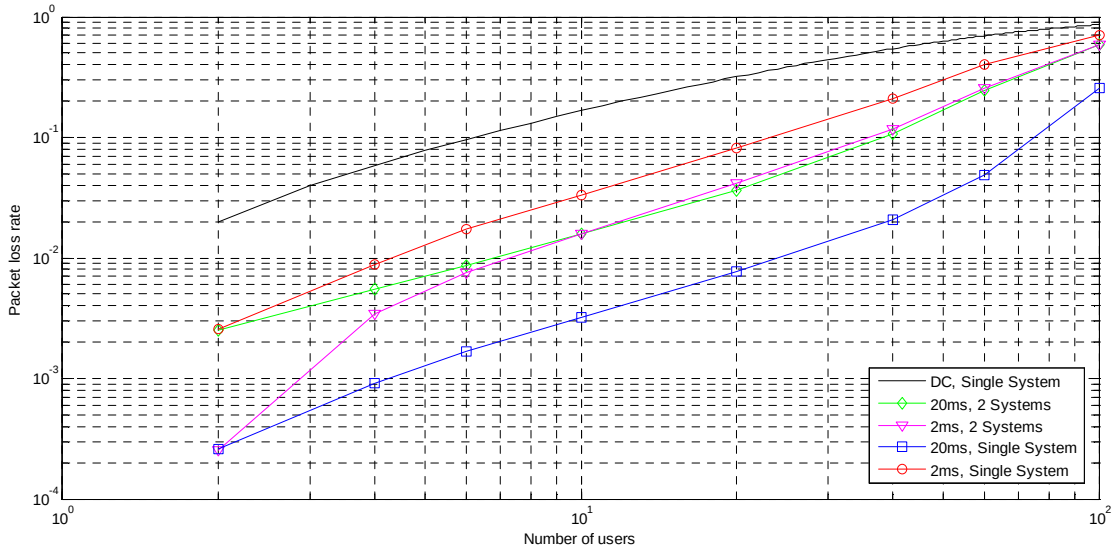


Figure 36: Total packet loss rate in a CSMA system, 2 different systems with 2/20ms packets, DC=1%, $T_R + T_D = 250\mu s$

The PLR of a CSMA system can be significantly lowered if the packets are retransmitted in case of a packet collision. The performance of CSMA with collision detection (CD) is discussed in the following section.

5.5.5 CSMA with ACK

The non-persistent CSMA system analysed in the previous section is extended by an ACK procedure, allowing the transmitting node to retransmits a packet if the expected ACK packet is missing. The duty cycle in the application layer is 1% and the retrial interval T_{Rep} after a channel busy indication corresponds to 10 times the packet duration T_{Tx} .The retransmission interval after an ACK loss $T_{TimeOutRep}$ is set to $20 \cdot T_{Tx}$ and a small time offset of 250 µs has been assumed for the sum of the minimum RSSI measurement time T_R and the dead time T_D for the LBT procedure. The simulation parameters are summarised in Table 30.

Parameter	Value	Comment
DC_{APP}	1%	Duty cycle on each link
T_{Tx}	2 ms, 20 ms	Packet length
T_L	1 ms	LBT: RSSI measurement interval
T_D	0.15 ms	LBT: Dead time
T_R	0.1 ms	LBT: RSSI detection interval
T_{Rep}	$10\% \cdot T_{Int} = 10 \cdot T_{Tx}$	CSMA: Mean transmission retrial interval
$T_{TimeOutRep}$	$20\% \cdot T_{Int} = 20 \cdot T_{Tx}$	ACK: Mean retransmission interval
$T_{Response}$	0	ACK: Distance between the end of the data packet and the start of the ACK-packet (ideal)
T_{ACK}	0	ACK: Length of the ACK packet (ideal)

Table 30: CSMA-ACK simulation parameters in the reference scenario

The packet loss rate of three different systems has been analyzed. In the first two systems all devices are transmitting with either 2 ms or 20 ms packets. The third system assumes two independently operating systems where half of the devices are transmitting long packets of 20 ms, while the rest uses short packets of 2 ms. The resulting packet loss rates are shown in Figure 37. The best performance is obtained sending long packets, where up to 90 devices might be operated in parallel with a packet loss rate of 10%. The number of users reduces to 40 users when short packets are transmitted due to the LBT detection problem and the resulting higher number of packet retransmission. The PLR for the devices in the third scenario can be found in between the two single system loss rates.

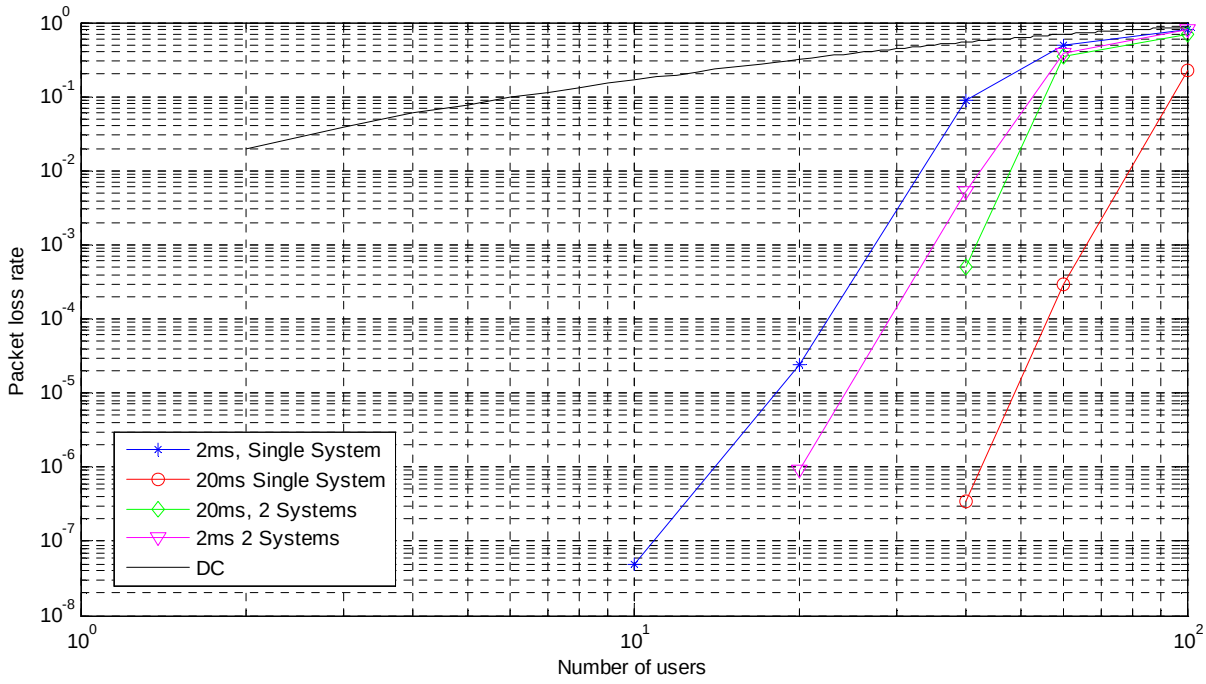


Figure 37: Packet loss rate in a CSMA-ACK system with ideal ACK, DC=1%, $T_R + T_D = 250\mu s$ as a function of the number of users and the packet lengths

The advantage of CSMA-ACK compared to ALOHA is the limitation of packet retransmissions in high traffic scenarios due to the fact that the channel is simply not free. Hence, the measured channel load is close to the offered data traffic on the application layer (see Figure 38 below compared to Figure 24 for ALOHA).

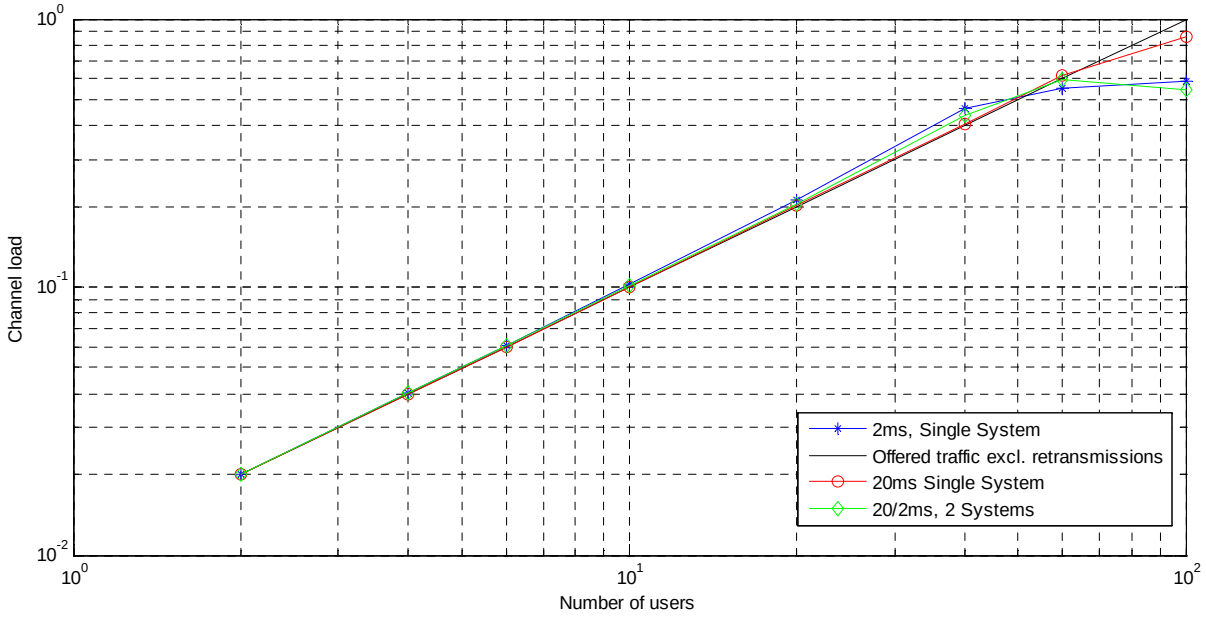


Figure 38: Measured channel load of a CSMA-ACK system with ideal ACK, DC=1%, $T_R + T_D = 250\mu s$ as a function of the number of users and the packet lengths

5.6 Simulation results for the office area

As described in section 5.2.2 *N* devices are placed within the office building. The positions of the first *N*/2 devices are randomly selected, while the positions of the communication partners are influenced by the actual transmit power level. Each partner is randomly placed in the vicinity of its communication partner such that

- the received power is higher than the sensitivity level plus an optional minimum link margin
- the position is within the building
- the distance to the partner is larger than one meter

The resulting possible partner positions are indicated by the light green area in Figure 39.

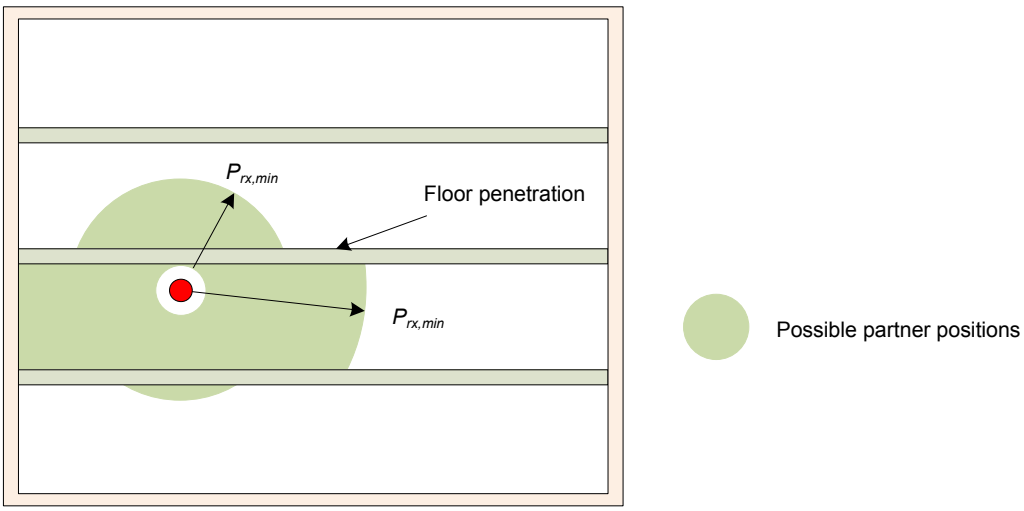


Figure 39: Positioning of the communication partner in the office scenario

To simplify the comparison of different access scheme, the same device positions are used for DC, ALOHA, and CSMA simulations. The duty cycle on the application layer will be 0.1% and the packet duration will be fixed to 20 ms. The packet loss rate not only depends on the device positions, but also on the start times of the periodic packet generation in the application layer. The packet loss rate on each link will be averaged over up to 1000 different sets of randomly generated start times for each device position set.

The transmit power is varied in between -30 dBm, -10dBm and 10 dBm as specified in first row of Table 31. The corresponding radio range can be calculated based on the ITU indoor path loss model, which has been described in section 5.1. For the small transmit power the range within the same storey is limited to 11.4 m. Most devices located in the storey above or below cannot be received due to the additional attenuation of the floor plate. The maximum distance in the vertical direction reduces to 6.1 m. Increasing the transmit power by 20 dB leads to a more typical situation, where the radio range covers a large part of the own storey and a few devices can even be received with two floor plates in between. Finally, simulations have been repeated with a high transmit power which allows to receive signals from all devices in the same storey and in the storey below and above, a large number of devices separated by two floors, and some devices separated by three floors. Hence, a modification of the power level results in three different coverage scenarios.

P_{tx} [dBm]		-30	-10	10
Range [m]	Same floor	11.4	46.1	>80m
	Next floor	6.1	24.6	>80m
	Separated by 2 floors	-	12.3	49.5
	Separated by 3 floors	-	-	34.9

Table 31: Transmission range as a function of the transmit power

It is well known that the attenuation within the building significantly depends on the building materials and the room furniture. The radio range might be significantly smaller than calculated by the ITU path loss model. In this case a similar system behaviour is obtained increasing the transmit power or, alternatively, increasing the devices density, because the performance of the radio link only depends on the characteristics of interference within the vicinity of the communicating devices. Nevertheless, links with a large link margin can be operated in the presence of weak interferer. Hence, the more relevant number is the number of harmful interferers, whose packet transmission will lead to a loss of the own packet in case of a collision.

- A **harmful interferer** results in a packet loss when colliding with the packet transmitted by the communication partner at the position of the receiver, because the received power levels are such that the SINR is below the minimum value.

Note, that devices with a lower receive power level might disturb as well if more than one interferer packet arrives simultaneously. Nevertheless, the probability is quite small, so that their influence is significantly smaller. Finally, the LBT performance will depend on the number of hidden nodes.

- A **hidden node** is a node which generates harmful interference to the receiver, but cannot be detected by the transmitter (relevant for LBT systems only)

The number of hidden nodes depends on the detection threshold and the link margin. Table 32 summarises the devices without hidden nodes and the maximum number of hidden nodes within each scenario. While a large radio range results in the highest number of harmful interferers, the number of hidden nodes is relatively small, because a significant part of the devices within the building can be detected. The most difficult hidden node scenario is obtained for the average transmit power level, where approximately half of the building is covered. Devices at the building edges communicating with a partner in the centre of the building will have a quite high number of hidden nodes.

P_{tx} [dBm]		-30	-10	10
Number of harmful interferers (N_{HI})	Average	5.8	20.7	43.2
	Minimum	1	1	1
	Maximum	23	88	99
Number of devices without hidden nodes	Pdet = -96 dBm	59	56	63
	Pdet = -86 dBm	52	42	51
Maximum number of hidden nodes	Pdet = -96 dBm	18	65	27
	Pdet = -86 dBm	20	75	51

Table 32: Scenario characteristics as a function of the transmit power

5.6.1 DC based random access

Although the application layer generates data packets in periodic intervals, a randomly selected transmit offset from the interval $[0, T_{Random}]$ is added at the transmitter prior to transmission to equally distribute the packet start time within the repetition interval T_{int}. As the offset is changed from data packet to data packet, the transmitted packets are not equidistant. The simulation parameters for the DC based random access performance are shown in Table 33.

Parameter	Value	Comment
N	100	Number of devices within the building
DC	0.1%	Transmit duty cycle on each link
T_{Tx}	20 ms	Packet length
T_{int}	20 s	Repetition interval
T_{Random}	$0.8 \cdot T_{int}$	Maximum offset between packet generation in the APP layer and the transmission in the MAC

Table 33: DC simulation parameters in the office scenario

The simulator outputs the PLR of the 100 different links for each of the three coverage scenarios. Each link can be characterised by the number of harmful interferers at the position of the receiver. Figure 40 plots the PLR of all 100 links and the three coverage scenarios as a function of the number of harmful interferes.

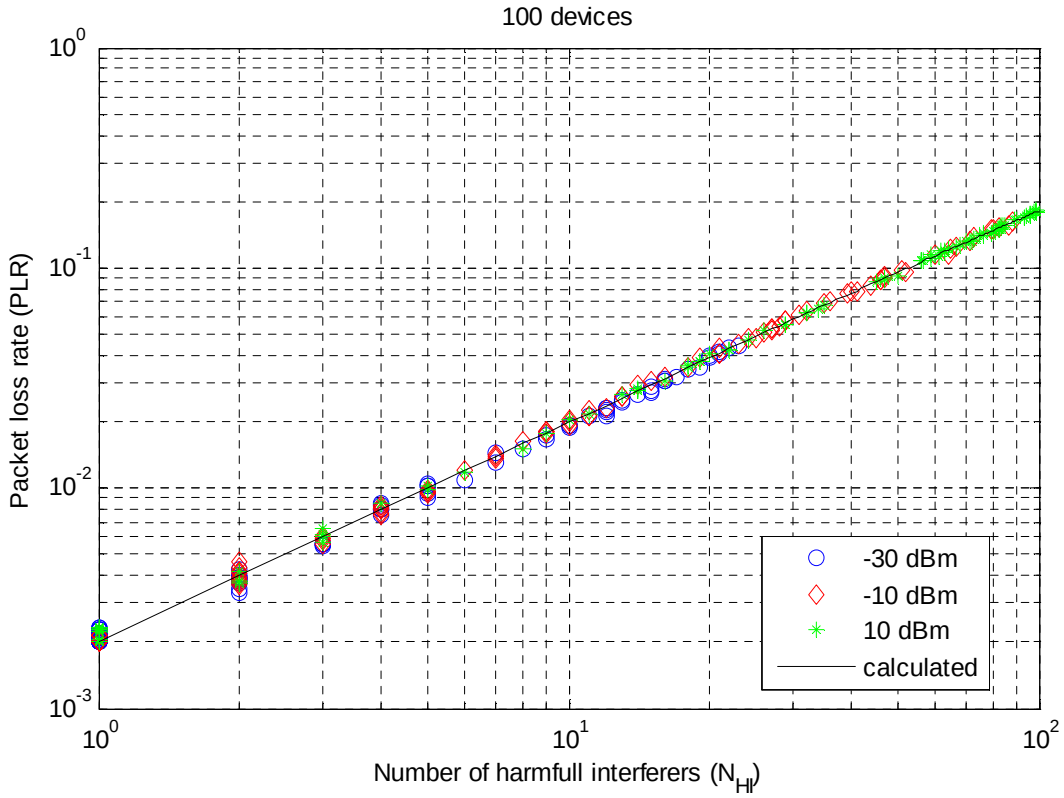


Figure 40: PLR for DC based random access in the office scenario as a function of the transmit power and the number of harmful interferers, 100 devices, duty cycle = 0.1%

The results are all positioned on a straight line. Hence, the PLR rate just depends on the number of interferers (N_{HI}) in the vicinity of the receiver. The minimum PLR of around 0.002 corresponds to the situation where the received power level of the link partner is significantly larger than the

power level of the surrounding interferers. As the link partner itself transmit data packets, which are not synchronised with the own transmissions, packets are only lost, if both devices are transmitting simultaneously. The corresponding PLR can be calculated to

$$PLR = 1 - (1 - 2 \cdot DC) = 2 \cdot DC = 0.002$$

The maximum *PLR* is measured on weak links in the middle of the building, where up to 99 interferers might collide with the own packet transmissions. The corresponding PLR is equal to 0.18. The black line in Figure 40 indicates the calculated PLR values as a function of the number of harmful interferers according to:

$$PLR(N_{HI}) = 1 - (1 - 2 \cdot DC)^{N_{HI}} = 1 - 0.998^{N_{HI}}$$

As the average number of harmful interferers depends of the transmit power, the three scenarios have a different distribution of PLRs rate as shown in Table 34. A higher transmit power increases the number of harmful interferers, so that the average PLR in the scenario increases.

P_{tx} [dBm]	PLR<10^{-2}	10^{-2}<PLR<10^{-1}	PLR≥10^{-1}	mean(PLR)
-30	64	36	0	0.011
-10	40	49	11	0.040
+10	24	31	45	0.081

Table 34: Distribution of PLRs for the DC based random access, 100 devices

The packet loss rate in Table 34 specifies the loss probability supposed that each data packet generated in the application layer is transmitted exactly once. In general, the DC based access scheme is used if the devices are simply transmitters, so that they are not aware of a packet loss. In order to increase the reliability of the data transmission N_{Rep} copies of the same packet can be transmitted hoping that at least one packet can be successfully received by the link partner. Consequently, the duty cycle in the physical layer is N_{Rep} times higher than the duty cycle of the application:

$$DC = N_{Rep} \cdot DC_{App}$$

Supposed that the collision probabilities of successive packets are uncorrelated, the probability of losing all N_{Rep} repetitions is equal to

$$PLR_{App} = PLR^{N_{Rep}} = \left(1 - \left(1 - 2 \cdot N_{Rep} \cdot DC_{App}\right)^{N_{HI}}\right)^{N_{Rep}}$$

The formula above can be used to calculate the PLR in the application layer as a function of the number of packet copies on the air interface. The scenario with 100 devices transmitting with a power of -10 dBm is used as an example in Figure 41. The blue stars correspond to the simulated results where only one copy of each application packet has been transmitted. Forty links in the scenario have a sufficiently small number of harmful interferers to achieve a packet loss rate below 10^{-2} (see Table 34). Transmitting three copies of the packet can significantly improve the packet loss rate on the application layer. Although the packet loss rate on the channel increases due to the higher transmit duty cycle on each link, the probability to properly receive at least one copy increases as well. Now there are already 81 links with a PLR lower than 10^{-2} in the application layer. The optimum value seems to be in the order of 5 to 7 copies with 87 links below the 10^{-2} target PLR. A further increase only slightly improves the situation for links with already small PLR while links with a relatively high PLR start to degrade.

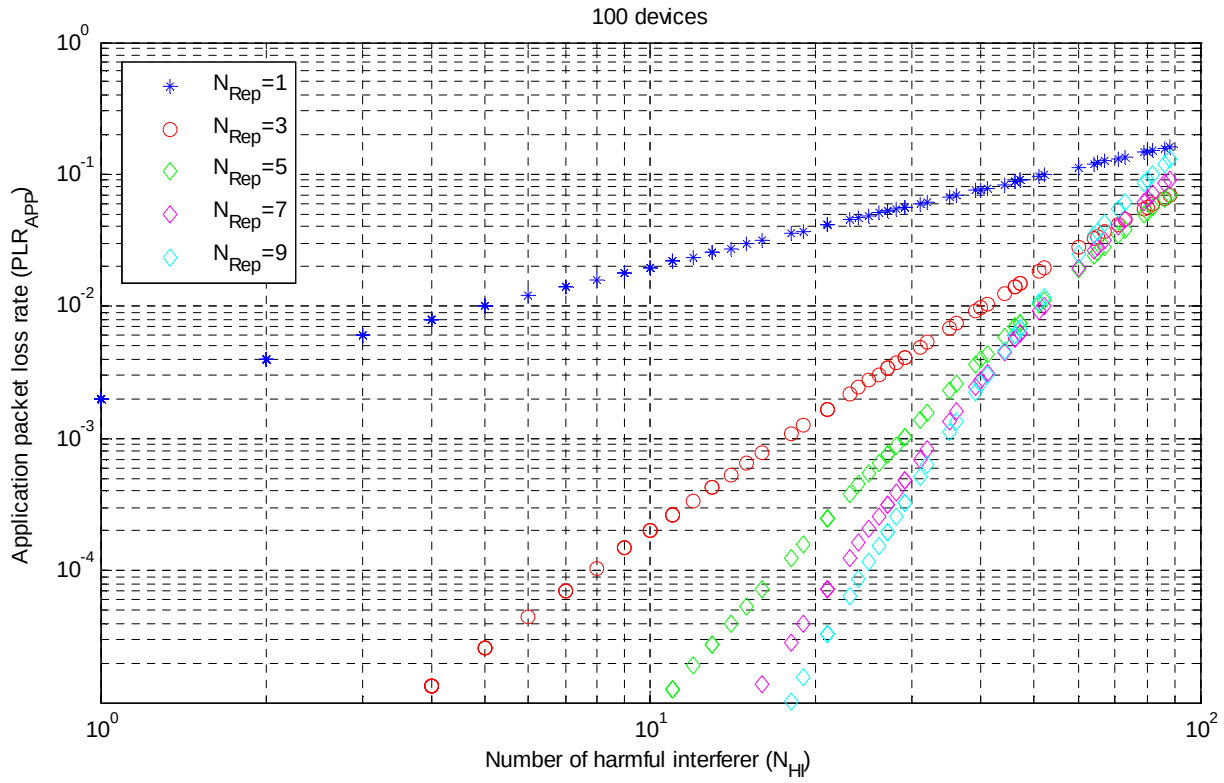


Figure 41: Packet loss rate as a function of the packet repetitions, duty cycle of the application is 0.1%, transmit duty cycle is $N_{Rep} \cdot 0.1\%$, P_{tx}=-10 dBm

The packet repetition rate is fixed to 6 copies, which seems to be a good compromise in all situations. The corresponding calculated packet loss rate as a function of the number of interferers is shown in Figure 42.

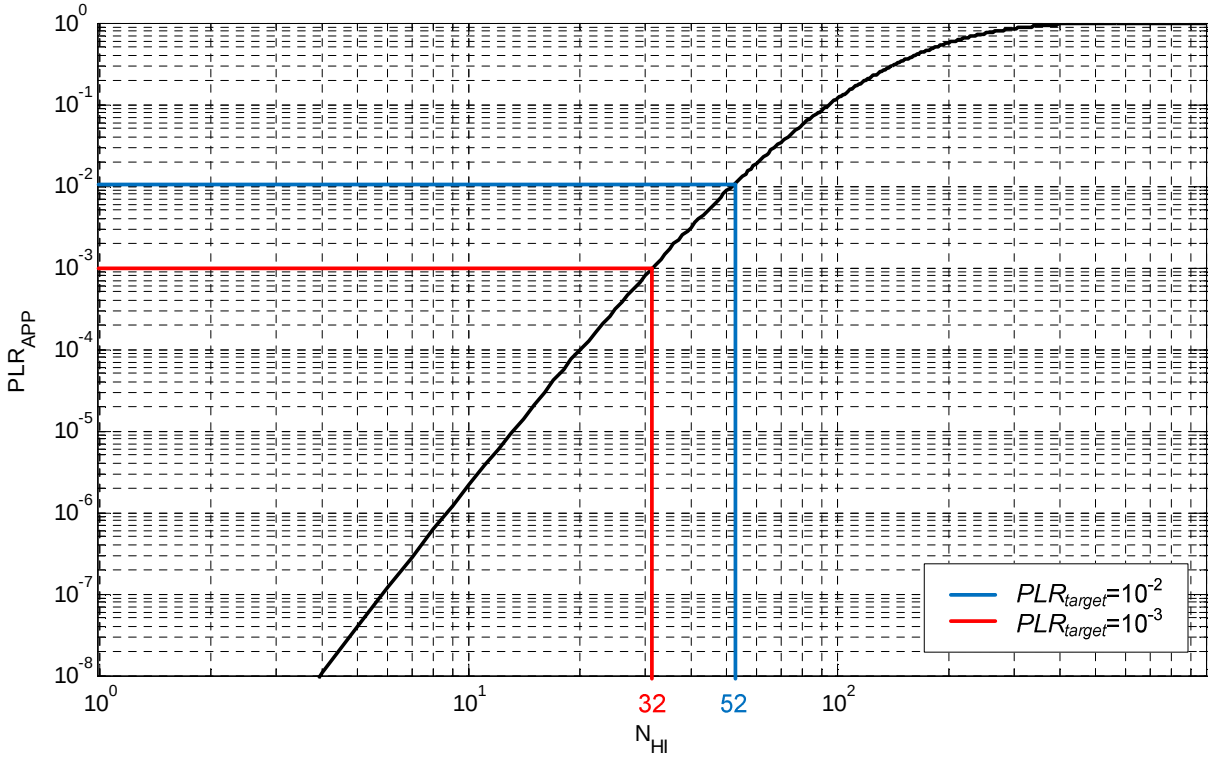


Figure 42: Packet loss rate for 6 packet copies, duty cycle of the application is 0.1%, transmit duty cycle is 0.6%

The relative number of links with a small packet loss rate decreases for higher user densities, as the number of harmful interferers increases. As shown in Figure 42 a target packet loss rate of 10^{-3} corresponds to a link with less than 32 harmful interferers, while up to 52 harmful interferers can be tolerated for a target packet loss rate of 10^{-2}. Only some links at the border of the building have a sufficiently small number of interferers. Hence, duty cycle based random access are only suited for small node densities.

5.6.2 ALOHA

Achieving link reliability by blindly sending a predefined number of packet copies only makes sense if the link is unidirectional using simple transmitters for extremely simple, low cost applications. The majority of SRDs will use transceivers which allow the receiver to inform the transmitting device on the reception success. Packets only need to be retransmitted in case of a packet loss, which significantly lowers the channel load. Nevertheless, the channel load is no longer time invariant like in the simulated DC based system. As described in section 4.3.1 retransmissions need to be carefully scheduled to avoid a system collapse. Two different retransmission schemes will be tested in the office scenario, a constant backoff scheme and a load dependent backoff scheme with a linearly increasing repetition interval. The constant backoff selects the offset to the next retransmissions randomly from a fixed interval $[0,\ 2 \cdot T_{TimeOutRep}]$. The simulation parameters of the constant backoff are summarised in Table 35.

Parameter	Value	Comment
N	100 - 400	Number of devices within the building
DC_{APP}	0.1%	Duty cycle on each link in the application layer
T_{Tx}	20 ms	Packet length
T_{int}	20 s	Repetition interval
T_{Random}	$0.6 \cdot T_{int}$	Random offset between packet generation in the APP layer and first transmission trial in the MAC
$T_{TimeOutRep}$	$20 \cdot T_{Tx}$	ACK: Mean retransmission interval
$T_{Response}$	0	ACK: Distance between the end of the data packet and the start of the ACK-packet (ideal)
T_{ACK}	0	ACK: Length of the ACK packet (ideal)

Table 35: ALOHA (constant backoff) simulation parameters in the office scenario

Although the packet generation in the application layer is periodic with repetition interval T_{int}, the first transmission trial of each packet is randomised due to a offset selected from the interval $[0, T_{Random}]$, which is added in the DLL layer to the packet generation time in the application layer. The mean retransmission interval in case of a packet loss is set to 20 times the packet length. The maximum number of packet retransmissions is limited by the fact that the transmission retrials of the actual packet are aborted as soon as a new packet is forwarded to the DLL layer. The minimum and average number of retransmissions can be calculated as follows:

$$N_{trials,min} = \frac{T_{int} - T_{Random}}{T_{TimeOutRep}}, \quad N_{trials,mean} = \frac{T_{int}}{T_{TimeOutRep}}$$

Inserting the simulation parameters values gives a minimum of 20 possible repetitions, while in the average 50 retransmissions can be scheduled before the packet needs to be skipped. The acknowledge procedure is ideal with a zero ACK packet length and a zero time offset in between the end of the data packet and the ACK packet. Nevertheless, the SINR is calculated at the position of the data as wells as the ACK packet receiver based on the signal power level and the actual interference situation. Hence, an ACK packet might be lost although the data has been successfully received on the reverse link due to a different interference situation.

The same scenarios are simulated which has been used for the performance of the DC based access scheme. In case that there are 100 devices within the building all application data packets are successfully transmitted as shown in Figure 43. The number of devices can be even doubled, while maintaining a zero packet loss rate.

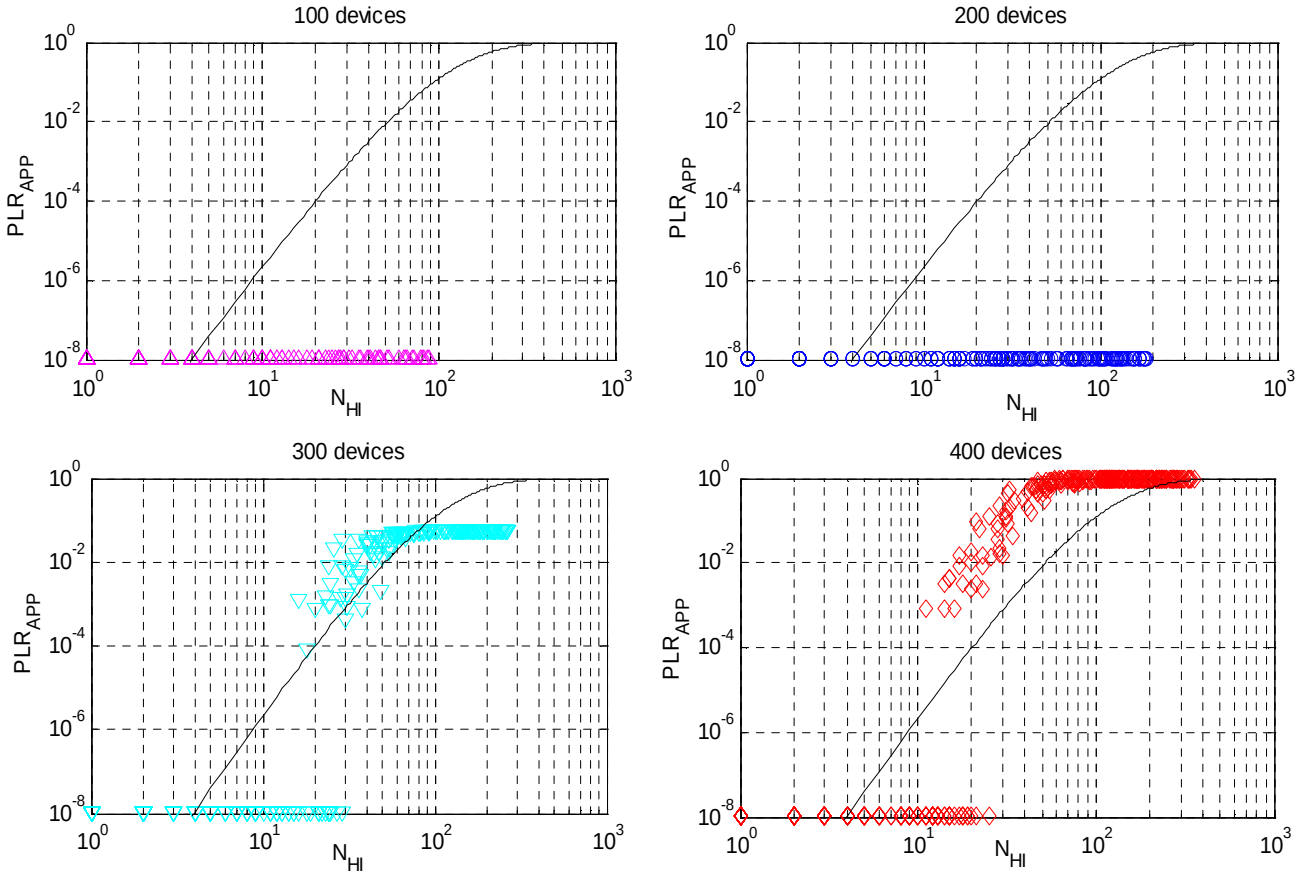


Figure 43: Application PLR in an ALOHA system with constant backoff as a function of the number of devices, duty cycle of the application is 0.1%, $P_{tx} = -10dBm$

A further increase of devices significantly worsens the situation for a high number of links. The black line indicates the performance of a DC based random access scheme with six packet copies. For some links the ALOHA approach leads to a even higher PLR on the application layer as all neighbours are simultaneously retransmitting their packets leading to a higher channel load than in the DC based system. Placing 400 devices within the building leads to a packet loss rate of 1 for more than 50% of the links, meaning that the system collapses. The number of links with an application packet loss rate within a certain range are summarised in Table 36.

Number of devices	PLR<10^{-4}	10^{-4}<PLR<10^{-3}	10^{-3}<PLR<10^{-2}	10^{-2}<PLR<10^{-1}	10^{-1}<PLR
100	100 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	0 (0 %)
200	200 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	0 (0 %)
300	126 (42 %)	6 (2 %)	16 (5.3 %)	152 (50.7 %)	0 (0 %)
400	158 (39.5 %)	3 (0.75 %)	9 (2.25 %)	15 (3.75 %)	215 (53.75 %)

Table 36: Distribution of PLR results for 100 to 400 devices within the building for ALOHA with constant repetition windows, constant backoff, $P_{tx} = -10dBm$

The performance of the ALOHA approach can be improved using a retransmission offset, which depends on the actual channel load. In general, a high channel load leads to a high number of retransmissions due to recent packet losses. One simple solution implements a repetition counter in the DLL layer and multiplies the randomly selected time offset to the next packet retransmission by the actual counter value. Hence, the time offsets doubles for the second repetition of a packet, while a factor of three is used for the third retransmission, etc. as shown in Figure 44.

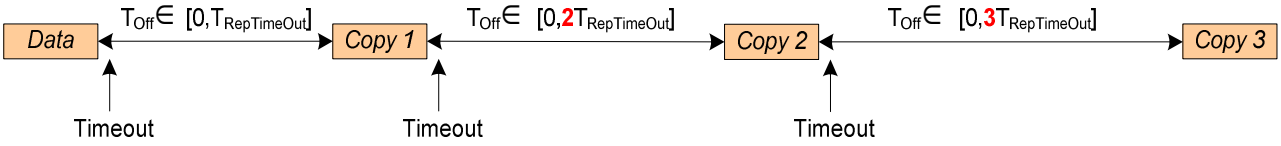


Figure 44: ALOHA with linearly increasing backoff

In order to get a rough idea on the performance gain, the simulations are repeated using a linearly increasing backoff. In principle, the same simulation parameters have been used except that the window for random offset selection has been halved.

Parameter	Value	Comment
N	100 - 600	Number of devices within the building
DC_{APP}	0.1%	Duty cycle on each link in the application layer
T_{int}	20 s	Repetition interval
T_{Random}	$0.6 \cdot T_{int}$	Random offset between packet generation in the APP layer and first transmission trial in the MAC
T_{Tx}	20 ms	Packet length
$T_{TimeOutRep}$	$10 \cdot T_{Tx}$	ACK: Mean retransmission interval
$T_{Response}$	0	ACK: Distance between the end of the data packet and the start of the ACK-packet (ideal)
T_{ACK}	0	ACK: Length of the ACK packet (ideal)

Table 37: ALOHA (linearly increasing backoff) simulation parameters in the office scenario

The resulting packet loss rates are simulated for the scenarios with 100, 200, 300, 400, 500 and 600 devices and presented in Figure 45 for those scenarios with non-zero packet losses.

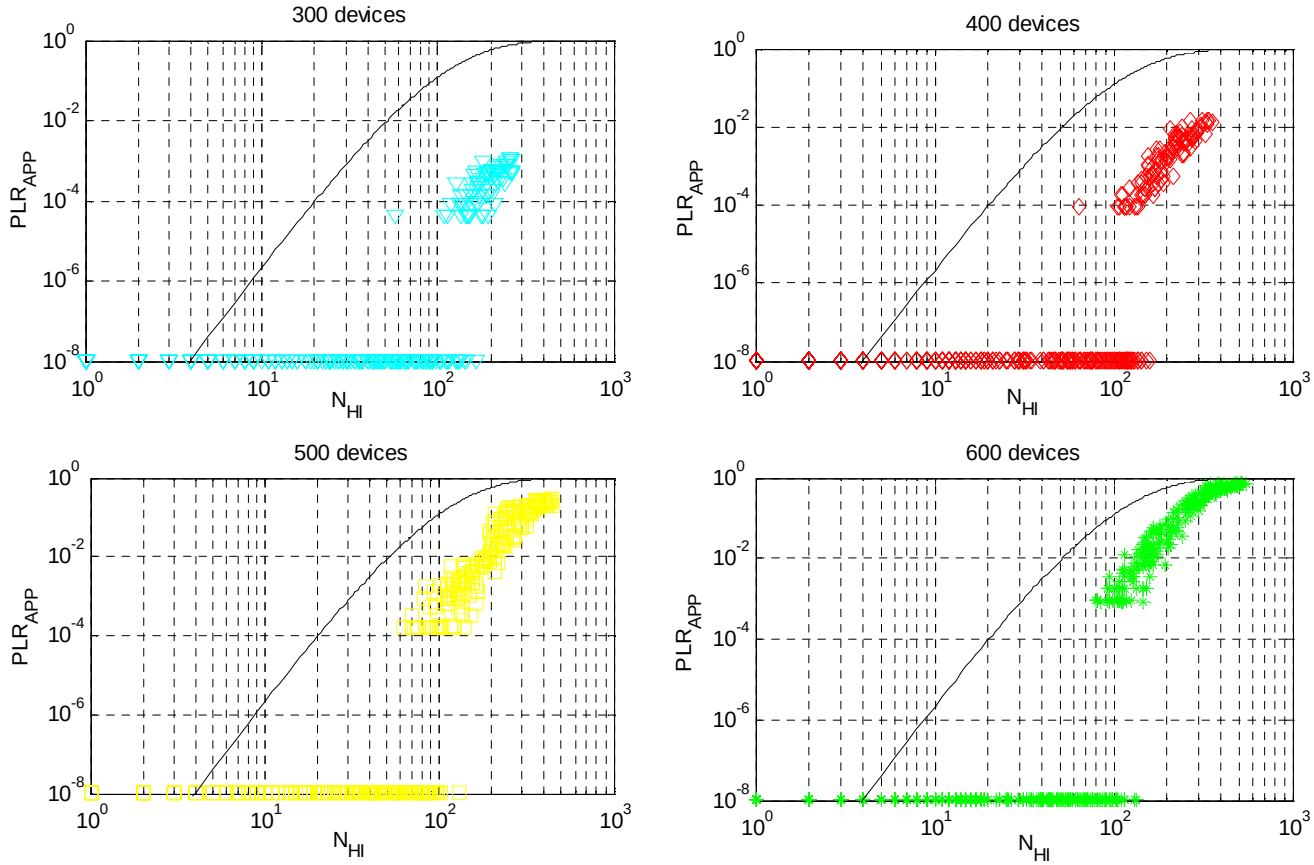


Figure 45: Application PLR in an ALOHA system with linearly increasing backoff as a function of the number of devices, duty cycle of the application is 0.1%, $P_{tx} = -10dBm$

The first packet losses on the application layer are again measured in an office scenario with 300 devices. Comparing the results in Figure 43 and Figure 45, the linearly increasing backoff significantly outperforms the constant backoff system. The packet loss rate is significantly lower and more harmful interferers can be tolerated. The results for the linearly increasing backoff as a function of the number of devices within the building are summarised in Table 38.

Number of devices	PLR<10^{-4}	10^{-4}<PLR<10^{-3}	10^{-3}<PLR<10^{-2}	10^{-2}<PLR<10^{-1}	10^{-1}<PLR
100	100 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	0 (0 %)
200	200 (100 %)	0 (0 %)	0 (0 %)	0 (0 %)	0 (0 %)
300	250 (83.3 %)	47 (15.7 %)	3 (1.0 %)	0 (0 %)	0 (0 %)
400	303 (75.8 %)	33 (8.3 %)	56 (14.0 %)	8 (2.0 %)	0 (0 %)
500	315 (63.0 %)	34 (6.8 %)	55 (11.0 %)	42 (8.4 %)	54 (10.8 %)
600	370 (61.7 %)	22 (3.7 %)	38 (6.3 %)	54 (9.0 %)	116 (19.3 %)

Table 38: Distribution of PLR results for 100 to 400 devices within the building for ALOHA with constant repetition windows, linearly increasing backoff

In general, it can be observed that the PLR is not solely a function of the number of harmful interferers of the own link like in a DC based system. A link with 200 harmful interferers has a maximum PLR of 10^{-3} in the scenario with 300 devices, while the same number of harmful interferers might result in a PLR of 10^{-1} in the scenario with 600 devices. The reason is that the PLR additionally depends of the number of harmful interferers of the neighboured links. As higher the number of nodes within the building as higher is the probability that the neighbours

will require more packet retransmissions because their number of harmful interferers increases. Hence, the channel load increases although the number of harmful interferers on the own link is identical.

Independent of the node density the ALOHA system with the linearly increasing backoff outperforms the DC based random access system for all links. The increasingly high distance between retransmissions artificially limits the channel load. Analysing the mean number of packet retransmissions on each link within the scenario shows that with a constant backoff strategy some links needs to send up to 18 copies of the same data packet, if there are 400 or more devices within the building.

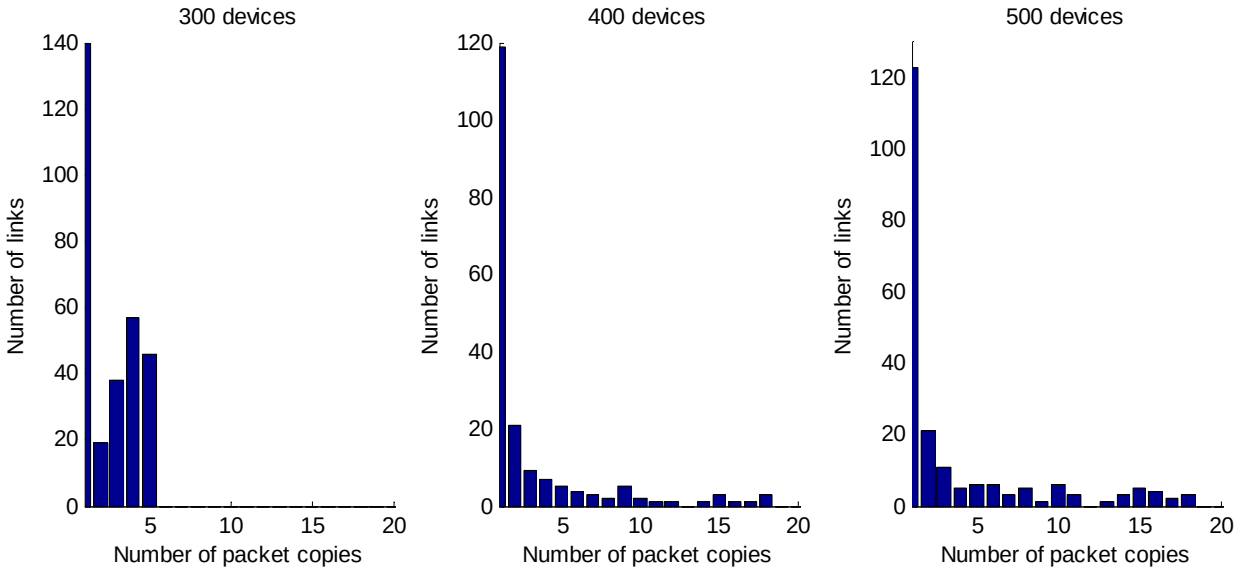


Figure 46: Number of transmitted packet copies for the constant backoff

The mean number of retransmissions is much lower using the linearly increasing backoff strategy. A maximum of six packet copies has been measured in the scenario with 500 devices on a small number of links (see Figure 47). Hence, the channel load is still smaller than the channel load in the DC based random access systems, where 6 packet copies are transmitted on each link.

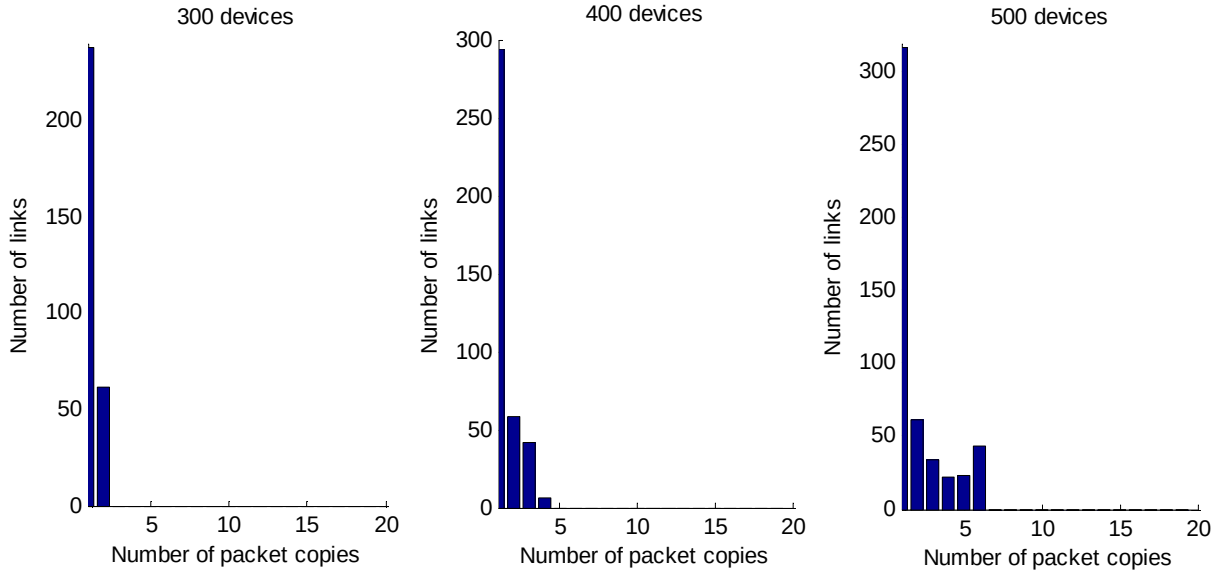


Figure 47: Number of transmitted packet copies for the linearly increasing backoff

The simulated ALOHA access with linearly increasing backoff works quite well for the office scenario with up to 400 devices. However, 500 devices within the building result in a PLR larger than 10^{-2} for 20% of the links. Nevertheless, it should be taken into account that the parameter settings in Table 37 have not been optimised. Furthermore, the simulation always resets the backoff window to its minimum value as soon as an ACK has been received thus forgetting the knowledge of the current congestion level on the link. It might be reasonable to maintain a larger backoff as long as the packet loss probability is quite high. Additionally, slightly different results might be achieved with other backoff strategies such that an exponential binary backoff so the potential of ALOHA is not fully tapped in this study.

Another interesting alternative is the use of LBT prior to transmissions, because the distance between retransmissions automatically increases in high load scenario, because it might take a longer time to find a free channel. The performance of a CSMA system with acknowledgement packets will be analysed in 5.6.4.

5.6.3 Non-persistent CSMA

Prior to the performance investigation of CSMA system with packet loss detection, non-persistent CSMA without retransmissions will be analysed. It will be shown that system performance can be approximated by a simple formula which allows to study the impact of hidden nodes and LBT implementation parameters. The non-persistent CSMA uses LBT based on energy detection and repeats a transmission trial after a random time offset in case the channel has been busy. Although the packet generation in the application layer is periodic with repetition interval T_{int}, the first transmission trial of each packet is randomised due to a offset selected from the interval $[0, T_{Random}]$, which is added in the DLL layer to the packet generation time in the application layer. The mean retrial time T_{Rep} is set to 10 times the packet length as shown in Table 39. In case no free channel has been found for transmission in the MAC layer until a new packet is available for transmission, the actual packet is skipped. The minimum number of trials can be calculated to $N_{trials,min} = (T_{int} - T_{Random})/T_{Rep} = 40$.

Two different transmission detection thresholds have been used. In the first iteration the detection threshold has been equal to the sensitivity level of -96 dBm, while a 10 dB higher value of -86 dBm has been used in the second iteration.

Parameter	Value	Comment
N	100	Number of devices within the building
DC	0.1%	Transmit duty cycle on each link
T_{Tx}	2 ms, 20 ms	Packet length
T_{int}	T_{Tx}/DC	Repetition interval
T_{Random}	$0.6 \cdot T_{int}$	Random offset between packet generation in the APP layer and first transmission trial in the MAC
T_L	1 ms	LBT: RSSI measurement interval
T_D	0.15 ms	LBT: Dead time
T_R	0.1 ms	LBT: RSSI detection interval
P_{det}	-96 dBm, -86 dBm,	LBT: Interference detection threshold
T_{Rep}	$10 \cdot T_{Tx}$	CSMA: Mean transmission retrial interval

Table 39: CSMA simulation parameters in the office scenario

The PLR in the CSMA system transmitting packets of 20 ms is shown in Figure 48 for a detection threshold of -96 dBm. As stated in section 5.5.4, the minimum PLR depends on the LBT implementation parameters and can be calculated for a two user environment to

$$PLR = \frac{2(T_D + T_R)}{T_{int}} = \frac{2 \cdot 0.25\ ms}{20s} = 2.5\ 10^{-5}$$

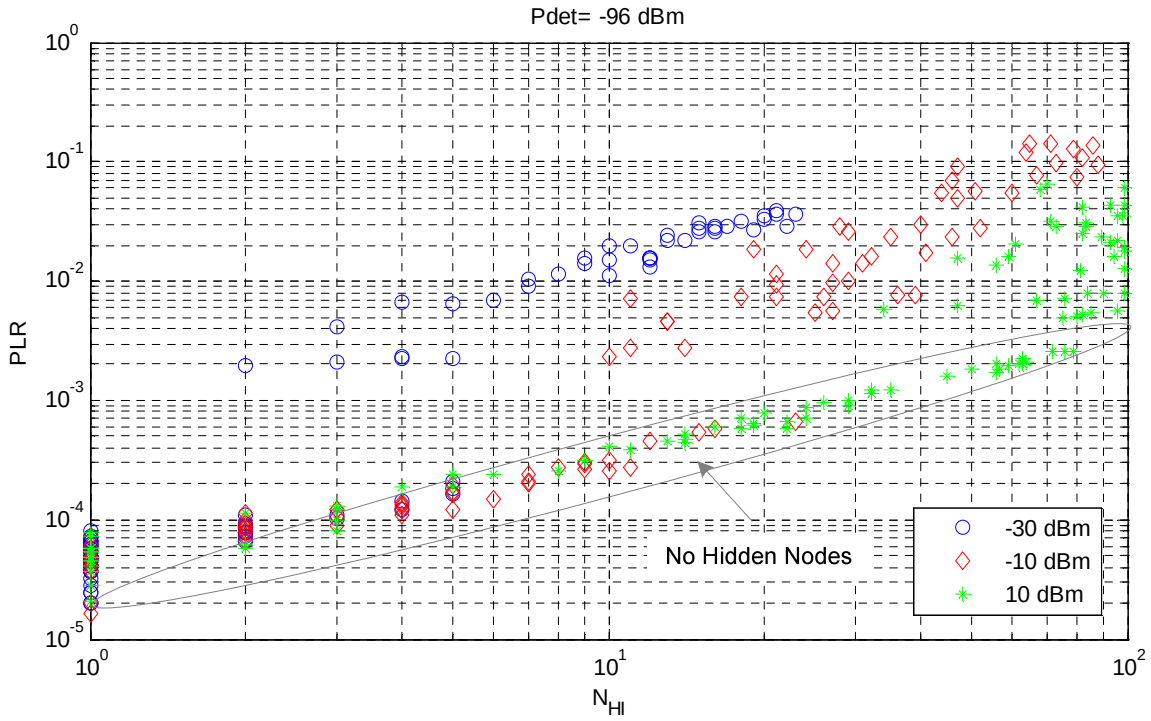


*Figure 48: **Simulated** PLR for CSMA in the office scenario as a function of the number of harmful interferers, 100 devices, transmit duty cycle = 0.1%, P_{det}=**-96 dBm**, 20ms packets*

Two different effects can be clearly separated. The PLR of all devices without hidden nodes are positioned on a straight line starting from the minimum PLR of $2.5 \cdot 10^{-5}$ and ending at a PLR of 0.003 for nodes with 99 harmful interferers. The PLR of the remaining nodes can be significantly higher due to collisions with hidden nodes. The collision probability with a hidden node is equal to 0.002 (see DC calculations in section 5.6.1), which is 80 times higher than the collision probability with a detectable interferer. None of the packets has been lost due to buffer overflows due to the small duty cycle on a single link allowing a high number of transmission trials. There is always sufficient time to transmit the packet until the next packet is generated in the application layer. In this case, the following formula seems to be a good approximation

$$PLR(N_{HI}, N_{HN}) \approx 1 - \left(1 - 2\frac{T_D + T_R}{T_{int}}\right)^{(N_{HI} - N_{HN})} \left(1 - 2\frac{T_{TX}}{T_{int}}\right)^{N_{HN}}$$

where N_{HI} denotes the number of harmful interferers and N_{HN} equals the number of hidden nodes for this specific link. The number N_{HI} and N_{HN} can be calculated based on the device positions and the transmit power level. It should be taken into account that this formula is only valid if all devices are using the same detection threshold. The calculated PLR on the basis of these data is shown in Figure 49. The simulated and calculated results are quite similar so that the formula can be used as an approximation.

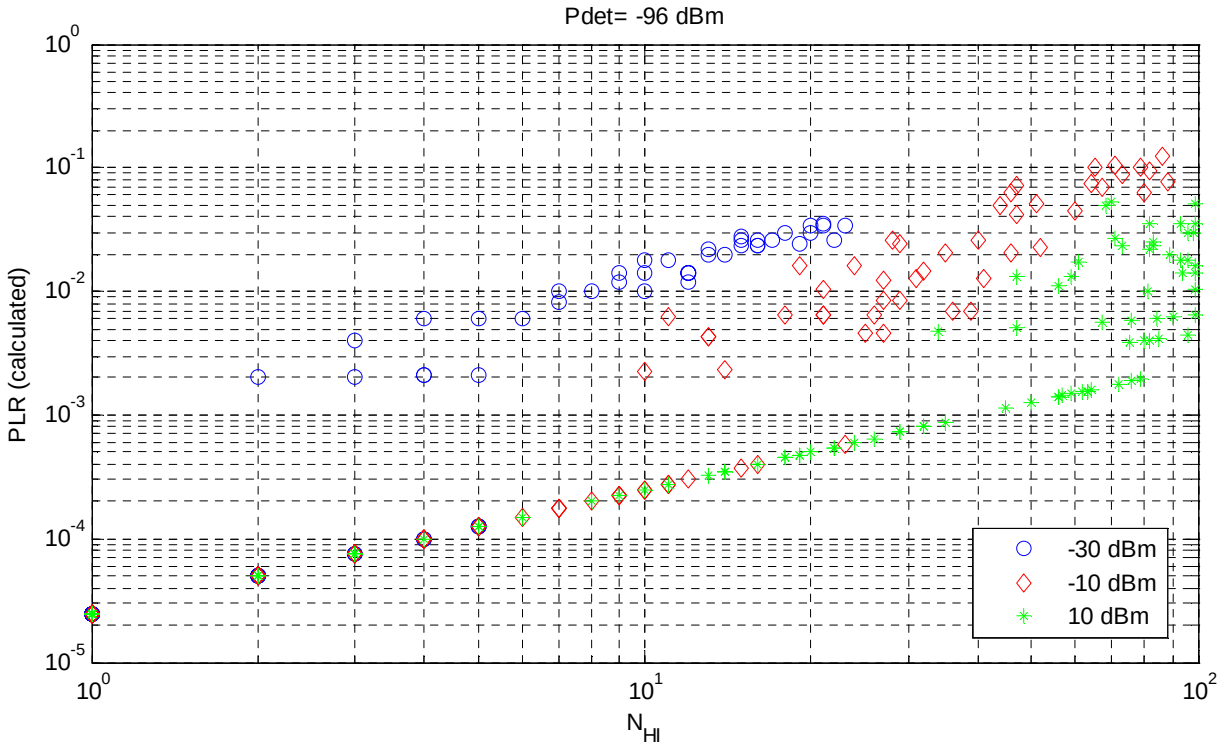


*Figure 49: **Calculated** PLR for CSMA in the office scenario as a function of the number of harmful interferers, 100 devices, transmit duty cycle = 0.1%, P_{det}=**-96 dBm**, 20ms packets*

Using a higher threshold increases the number of hidden nodes, so that the formula above forecasts a higher PLR. A comparison of the simulated PLR for the two different detection thresholds in the second coverage scenario proofs that the PLR is indeed higher especially for nodes with a moderate number of harmful interferers.

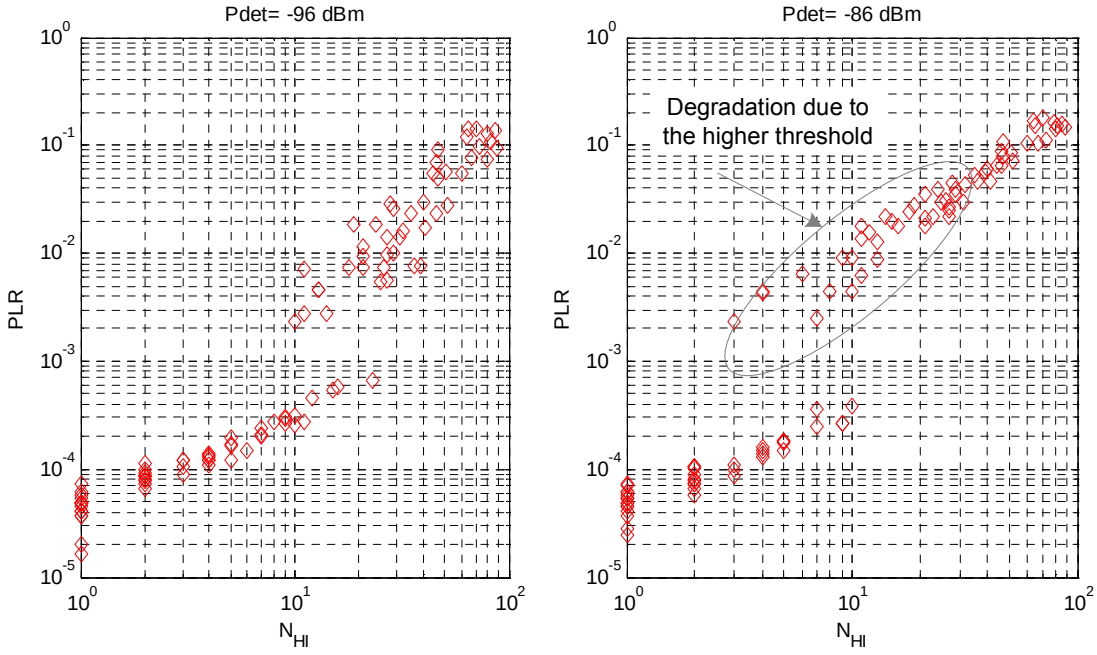


Figure 50: Comparison of the PLR as a function of the detection threshold

Table 40 compares the number of links with a PLR within a given interval for the two different threshold settings.

Ptx [dBm]	Pdet [dBm]	PLR<10^{-4}	10^{-4}≤PLR<10^{-3}	10^{-3}≤PLR<10^{-2}	10^{-2}≤PLR<10^{-1}	PLR>10^{-1}	Mean(PLR)
-30	-96	51	8	10	31	0	0.0077
	-86	51	1	14	34	0	0.0103
-10	-96	26	29	16	23	6	0.0188
	-86	25	17	11	35	12	0.0310
+ 10	-96	19	28	28	25	0	0.0086
	-86	19	27	6	43	5	0.0285

Table 40: Influence of the detection threshold, 20 ms packets

Looking at the mean PLR of the 100 links shown in the last column of the table, the total system performance always worsens selecting a higher detection threshold.

In order to analyse the impact of hidden nodes, the PLR is now analysed as a function of the ratio of hidden nodes among the harmful interferers. The plot on the left side of Figure 51 compares the calculated PLR for a CSMA system as a function of the number of harmful interferers and the ratio of hidden nodes for a packet length of 20 ms. On the right side, the same analysis is done for the simulation results. Hence, the right figure includes the PLR loss rates in the office scenario for all different transmit power levels and the two different interferer detection thresholds. The colour of the PLR results indicates the specific ratio N_{HN}/N_{HI} for the corresponding link.

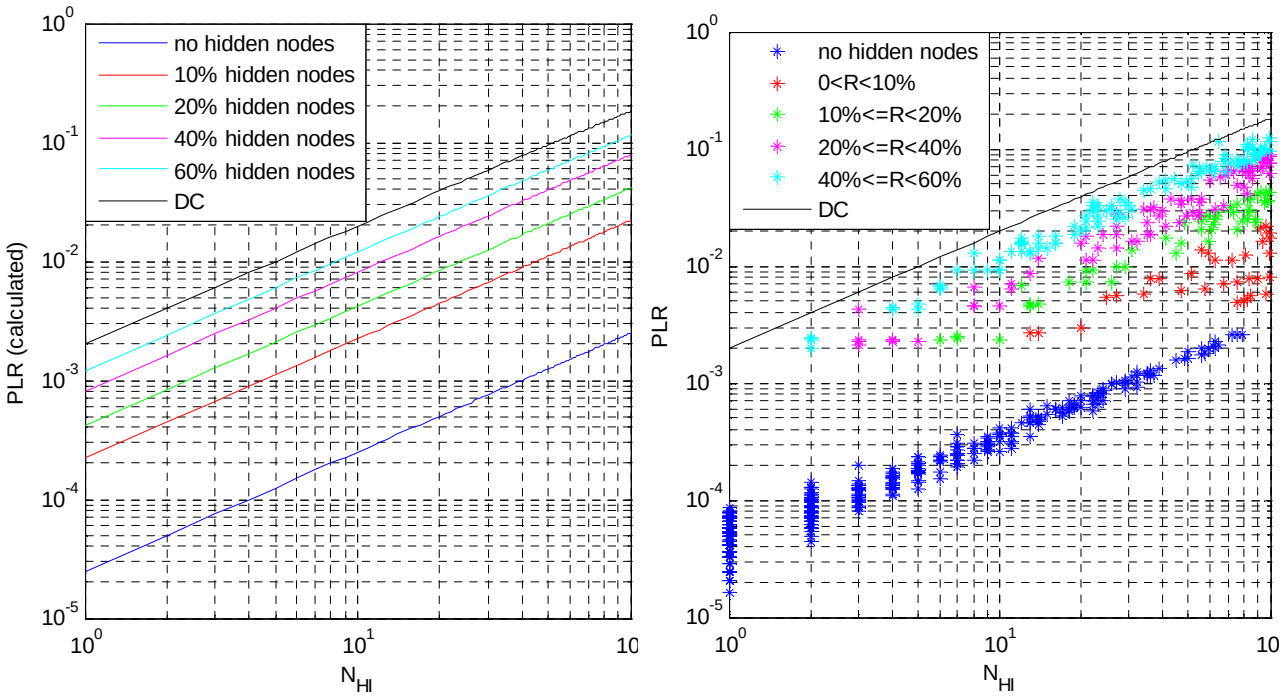


Figure 51: Calculated and simulated PLR for CSMA as a function the number of harmful interferers and the ratio of hidden nodes for CSMA and DC based random access, transmit duty cycle = 0.1%, 20ms packets, $P_{Tx} = -30, -10, 10\ dBm, P_{det} = -86, -96\ dBm$

For links without hidden nodes, the PLR can be reduced by a factor of 80 using CSMA instead of DC. Nevertheless, the gain is reduced to a factor of 10 if 10% of the harmful interferers are hidden nodes. For a higher ratio the performance approaches the performance of a DC based random access (see black line).

As a consequence, the hidden node ratio should be as small as possible. It directly depends on the interferer threshold level as shown in Figure 52. The left plot presents the hidden node ratio of all nodes in the simulated office scenario using a threshold of -96 dBm. Links with a short distance and a resulting link margin of more than 20 dB have a maximum ratio of 20%, while the same margin corresponds to a hidden node ratio of up to 80% with the threshold of -86 dBm (see right plot). Hence, the low LBT threshold and a high link margin can be used to minimise the hidden node ratio in CSMA.

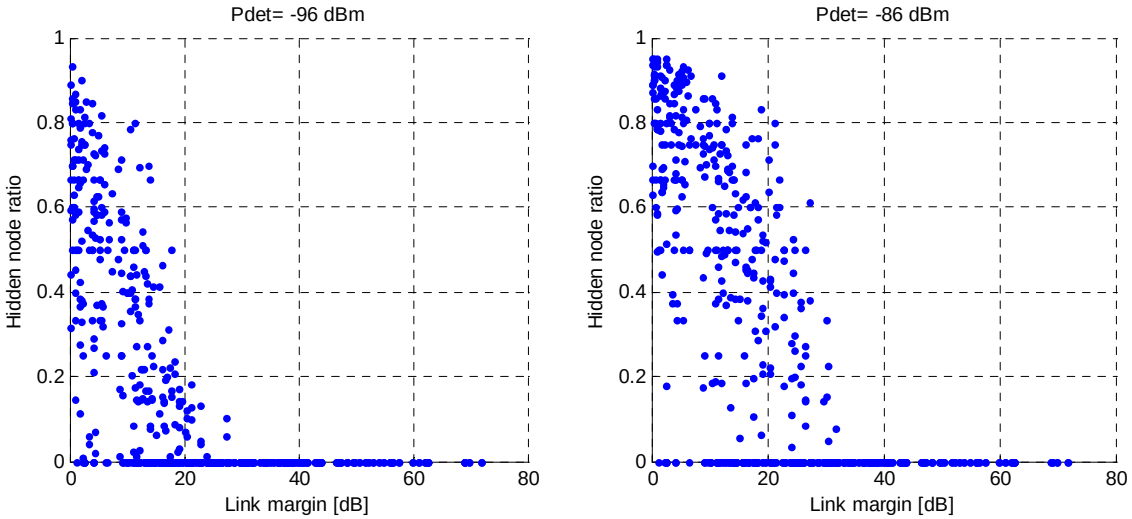


Figure 52: Hidden node ratio as a function of the link margin and the detection threshold in the office scenario

In principle, CSMA can be combined with packet repetition in order to reduce the PLR on all links similar as it has been done for the DC based random access scheme. Nevertheless, the LBT procedure already requires transceivers instead of simple transmitters in order to perform the channel measurements. Hence, it is straight forward to implement an ACK procedure, which allows to restrict packet retransmissions to situations where a packet has been lost.

5.6.4 CSMA-ACK

Finally, an acknowledgement procedure is added for packet loss detection. An ideal ACK procedure is assumed with a zero ACK packet length and a zero time offset in between the end of the data packet and the ACK packet. Nevertheless, the SINR is calculated at the position of the data as wells as the ACK packet receiver based on the packet power level and the actual interference situation. Hence, the transmission success rate of ACK packets might be smaller than 1, as it might happen that an interferer starts is packet transmission shortly after the start of the data packet due to an overlapping of RSSI measurement intervals (see left side of Figure 53). In case the interferer generates no harmful interference at the position of the link partner, the packet can be successfully received. However, the ACK packet reception might fail because the interferer is still active and generates harmful interference at the position of the data packet transmitter. A non-zero response time would lead to a similar situation as shown on the right side of Figure 53. An interferer might start its packet transmission with a minimum offset of T_D

after the end of the data packet. As the ACK packet is typically transmitted without LBT, it collides with the interferer transmission and might be lost.

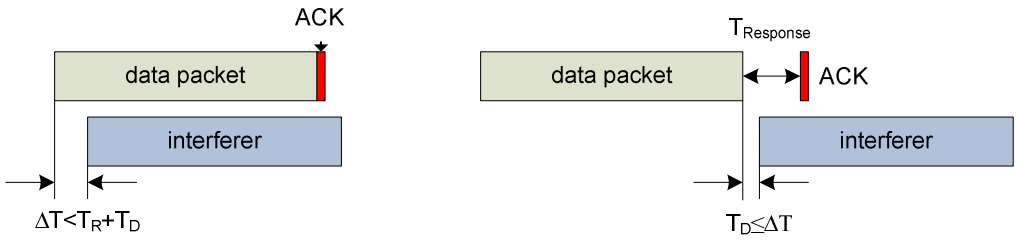


Figure 53: Simulation (left) and a similar situation for a non-zero response time (right)

In case of an missing ACK packet, a new transmission trial is scheduled after a random offset equally distributed within the interval [0, $2 \cdot T_{TimeOutRep}$]. The simulation parameters are shown in Table 41. The maximum number of packet retransmissions is limited by the fact that the transmission retrials of the actual packet are aborted as soon as a new packet is forwarded to the DLL layer. The minimum number of retransmissions depends on the number of times the channel has been busy before the packet has been transmitted. If N_{LBT_Trials} denotes the number of channel measurement prior to one packet transmission, the minimum number of packet retransmissions can be written as

$$N_{trials,min} = \frac{T_{int} - T_{Random}}{N_{LBT\_Trials} \cdot T_{Rep} + T_{TimeOutRep}}$$

In case there are typically six channel measurements prior to a packet transmission, the minimum number of packet retransmissions is equal to five based on the simulation parameters summarized in Table 41. In the average there are even 10 retransmissions before the packet is skipped in the transmitter.

Parameter	Value	Comment
DC_{APP}	0.1%	Application duty cycle
T_{Tx}	20 ms	Packet length
T_{int}	T_{Tx}/DC_{APP}	Repetition interval
T_{Random}	$0.6 \cdot T_{int}$	Random offset between packet generation in the APP layer and first transmission trial in the MAC
T_L	1 ms	LBT: RSSI measurement interval
T_D	0.15 ms	LBT: Dead time
T_R	0.1 ms	LBT: RSSI detection interval
P_{det}	-96 dBm, -86 dBm,	LBT: Interference detection threshold
T_{Rep}	$10 \cdot T_{Tx}$	CSMA: Mean transmission retrial interval
$T_{TimeOutRep}$	$20 \cdot T_{Tx}$	ACK: Mean retransmission interval
$T_{Response}$	0	ACK: Distance between the end of the data packet and the start of the ACK-packet (ideal)
T_{ACK}	0	ACK: Length of the ACK packet (ideal)

Table 41: CSMA-ACK simulation parameters in the office scenario

Figure 54 shows the simulated packet loss rate in the application layer, where a zero PLR has been replaced by 10^{-8} to allow plotting in a logarithm scale. For both threshold settings, the packet loss rates have been zero for all links. Due to the low duty cycle, there is sufficient time to retransmit lost packets before the next new data packet is generated in the application layer.

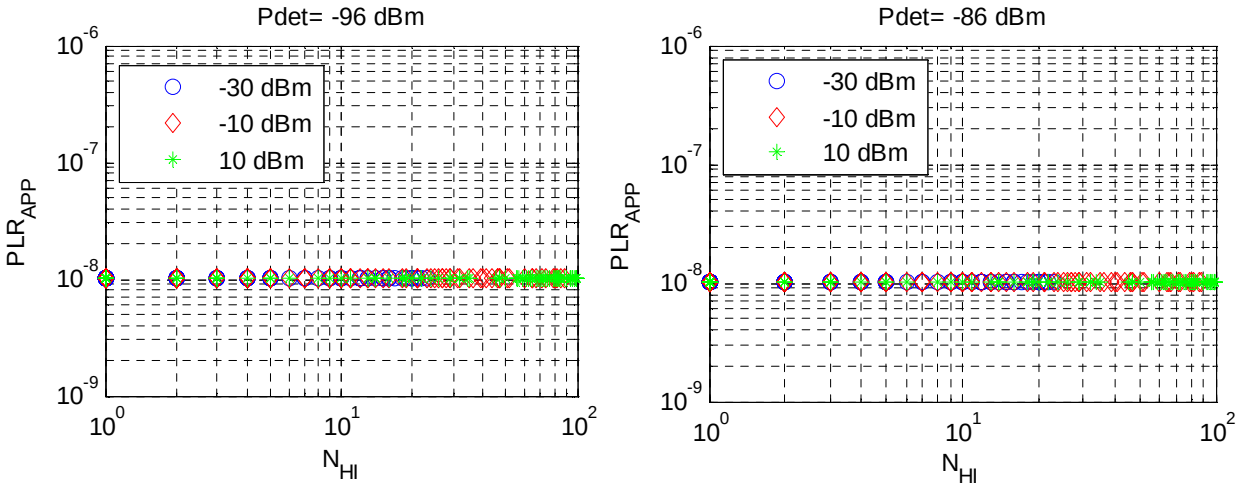


*Figure 54: PLR for CSMA-ACK in the office scenario as a function of the transmit power, 100 devices, application duty cycle = **0.1%**, P_{det}=-96/86 dBm, **20ms** packets*

In order to analyse the performance limits of CDMA-ACK, the number of devices within the building is continuously increased. As a result the number of harmful interferers linearly increases as shown in Table 42. The highest number of harmful interferes (N_{HI}) is always around 90% of the total number of devices, while in the average 20% of the nodes disturb the own communication. The ratio of hidden nodes for those links with a very small link margin remains in the order of 85%, while in the average 20% of the harmful interferers are hidden nodes.

Number of devices	max(NHI)	mean(NHI)	max(NHN/NHI)	mean(NHN/NHI)
200	183	46.2	87 %	20.4 %
300	265	70.33	84 %	21.2 %
400	365	80.2	89 %	20.0 %
500	445	96.4	88 %	18.7 %
600	549	117.0	83 %	18.6 %
700	634	144.0	83%	24.5 %

Table 42: Scenario characteristics for increased node densities, minimum link margin = 0 dB, $P_{tx} = -10\ dBm$, 20ms packets, $P_{det} = -96\ dBm$

The simulation results shown in Figure 55 are based on a packet length of 20 ms, an interferer detection threshold of -96 dBm and a transmit power level of -10 dBm. The minimum link margin in the device positioning algorithm is 0 dB, so that some links cannot cope with any interference. The number of devices can be increased to 400 without any packet loss in the application layer. Although the packet loss rate on the channel constantly increases, the number of retransmissions is sufficient to properly transfer the data packet within the given time frame. Hence, the CSMA-ACK system (Figure 55) significantly outperforms the simulated ALOHA system with a linearly increasing backoff (see Figure 45).

The first non-zero packet loss rates have been found in the scenario with 500 devices. Some links with more than 200 harmful interferers in the vicinity of the receiver and a high hidden node ratio of more than 40% show a packet loss rate in the order of 10^{-4} to 10^{-3}. The PLR is still so small that most applications can cope with this. Adding additional 100 devices significantly worsens the system performance. There are numerous links with a high number of interferers and high hidden node ratios with a packet loss rate of 1. It is interesting to note that the PLR of links with the same number of harmful interferers and a similar ratio of hidden nodes might significantly differ. The PLR additionally depends on the number of neighbours above the interferer detection threshold and their duty cycle on the channel. For a high number of neighbours the probability to detect a free channel becomes smaller and the time until the next packet appears in the DLL layer might not be sufficient to allow a successful transmission on the channel. The same happens for a smaller number of neighbours with small link margin, because packets often need to be retransmitted.

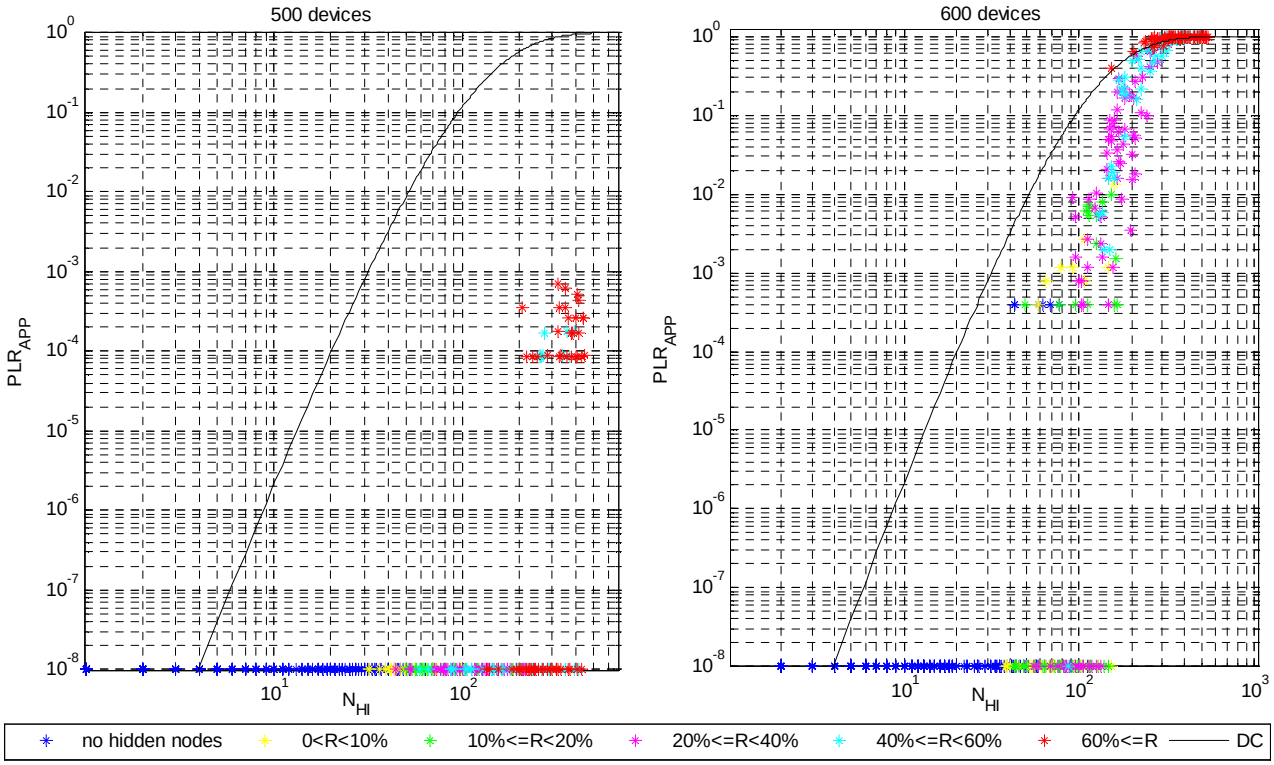


Figure 55: Application PLR in a CSMA-ACK system for 500 (left) and 600 (right) devices as a function of the number of harmful interferers (N_{HI}) and the hidden node ratio, 0.1% duty cycle in the application, minimal 0dB link margin, $P_{tx} = -10\ dBm, P_{det} = -96\ dBm$

The average number of packet retransmission is shown in Figure 56. A comparison with the results of the ALOHA system with linearly increasing backoff shows a significantly smaller number of packet copies for up to 500 devices in the building. Hence, the CSMA-ACK approach achieves a smaller PLR with even a smaller number of repetitions, so that the energy consumption for LBT measurements can be easily compensated.

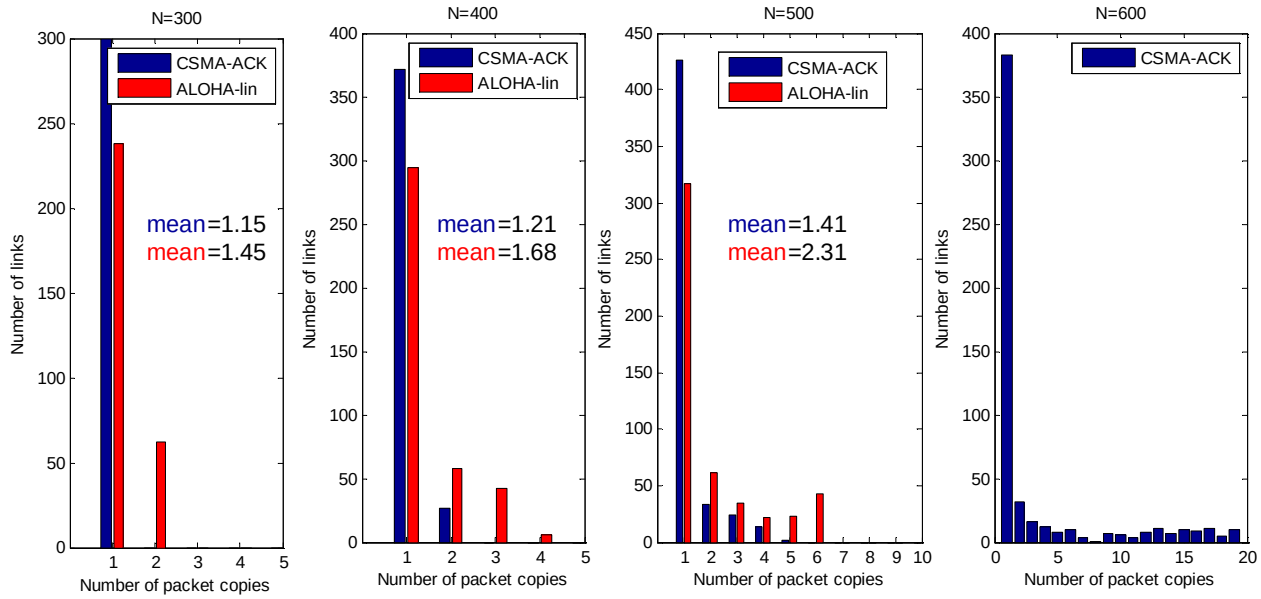


Figure 56: Average number of transmitted packet copies for CSMA-ACK and ALOHA

Placing 600 devices within the building significantly worsens the system due to the higher number of nodes with a large hidden node ratio. The maximum number of mean packet copies on a single link increases by a factor of 4. Hence, the CSMA-ACK channel access scheme might collapse in high load scenarios due to the hidden nodes problematic, so it seems to be reasonable to limit the number of retransmissions by defining an upper limit for the transmit duty cycle or to implement a load dependent backoff procedure as proposed for the ALOHA scheme.

Many applications like alarm or metering systems are based on networks with fixed device positions. This allows to position the devices such that a minimum link margin is maintained on the majority of the links. A higher link margin reduces the number of harmful interferers and the hidden node ratio as shown in Table 43 for a minimum link margin of 10 dB. It is expected that the scenario with 500 devices and a minimum link margin of 0 dB is worse than a scenario of 1000 devices with a minimum link margin of 10 dB. They both have an average number of 96.5 harmful interferers, but the hidden node ratio in the second scenario is more than halved. A mean hidden node ratio of approximately 8 % is obtained for almost all simulated node densities as shown in Table 43.

Number of devices	max(NHI)	mean(NHI)	max(NHN/NHI)	mean(NHN/NHI)
600	318	55.7	67 %	7.8 %
700	373	65.6	65 %	7.8 %
800	366	74.5	62 %	8.2 %
900	474	88.7	60 %	9.0 %
1000	492	96.6	62%	8.5%
1100	529	95.8	58%	7.7%
1200	658	106.5	72%	8.0%
1300	676	119.3	69%	8.0%
1400	712	129.8	64%	8.0%
1500	745	138.1	71%	8.2%

Table 43: Scenario characteristics for increased node densities, minimum link margin = 10 dB, $P_{tx} = -10\ dBm, P_{det} = -96\ dBm$

In fact the simulated PLR has been zero for simulations with 200 to 1100 devices within the building. Higher nodes densities are presented in Figure 57. All links with less than 300 harmful interferers had successfully transmitted their data packets for up to 1400 devices in the building. Only some of the links with a hidden node ratio of more than 20% have experienced packet losses in the order of 10^{-3} to 10^{-2}.

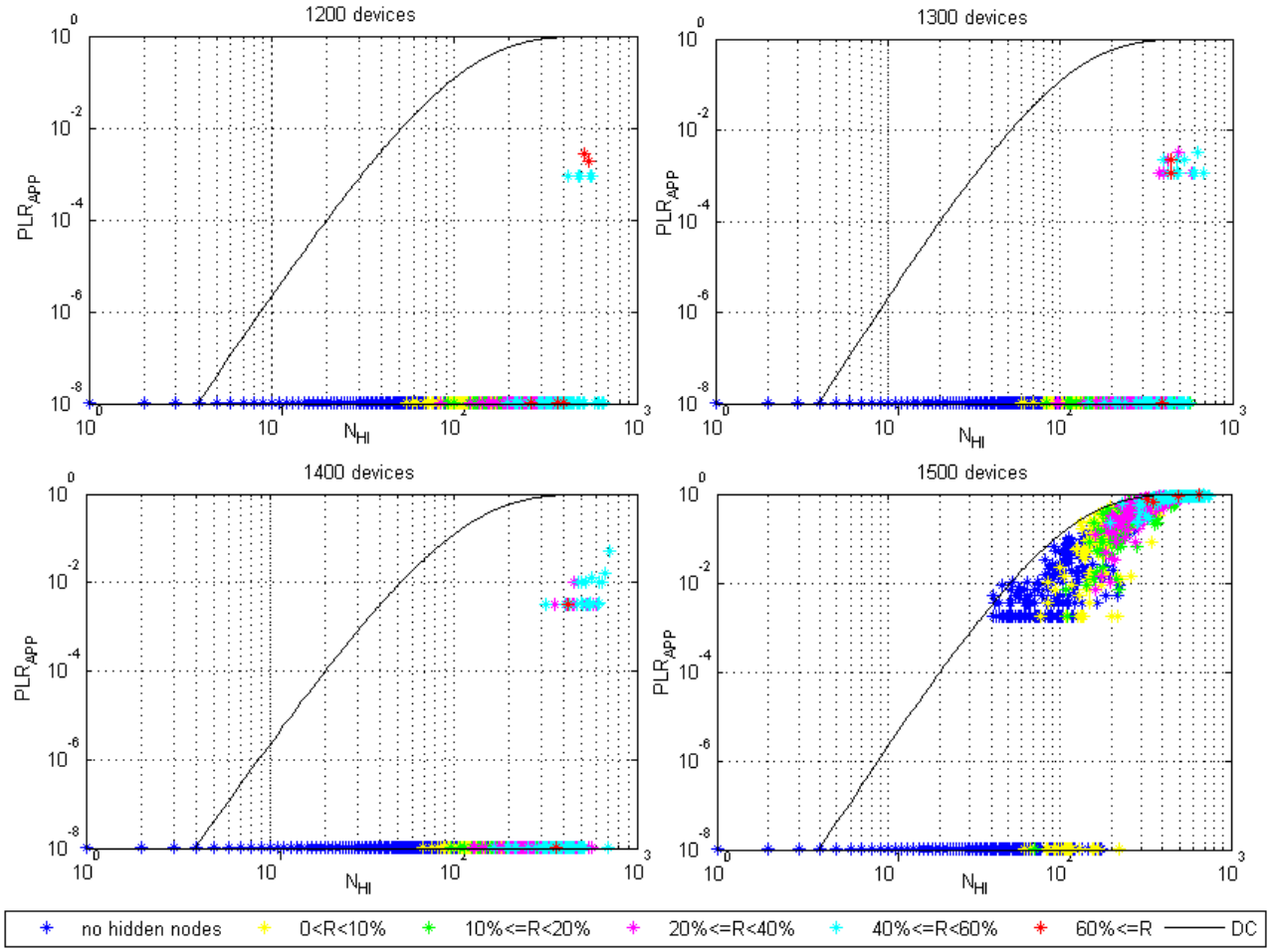


Figure 57: Application PLR in a CSMA-ACK system for 1200 to 1500 devices as a function of the number of harmful interferers (N_{HI}) and the hidden node ratio for 0.1% duty cycle in the application and minimal 10dB link margin

As expected, the results in Figure 57 outperform the results in Figure 55 with the generally higher hidden node ratio, where the maximum number of harmful interferers has been 200 in order to guarantee a zero packet loss rate.

In any case, the performance of a CSMA-ACK system is always higher than the performance of a DC based random access scheme with packet repetition and the simulated ALOHA access with linearly increasing backoff. For very high load scenarios some links have a packet loss rate close to the DC performance, but the majority of the links are significantly better. In moderate traffic scenarios apparently no application data packet is lost on the majority of the links and those links with a non-zero PLR can be improved reducing the hidden node ratio by using a higher link margin or lowering the detection threshold.

5.7 Comparison of simulation results

Table 44 summarises the simulation results in the office scenario for the selected single-carrier random access schemes. The number of harmful interferes in a DC based random access with an application duty cycle of 0.1% and 6 packet copies has to be lower than 31 in order to achieve a reliable system with a packet loss rate of lower than 0.1%. The number of tolerated harmful interferers can be increased by a factor of 8.5 using ALOHA based channel access supposed that a load dependent backoff procedure (e.g. linearly increasing backoff) is used to avoid the problem of local channel congestion. Using an acknowledgement procedure instead of a blind transmission of packet copies significantly reduces the packet loss rate on the majority of the links with an even considerably lower number of required packet copy transmissions. Hence, ALOHA outperforms the DC based random access scheme with regards to reliability and latency. Furthermore, even power consumption will be lower as the additional power required for acknowledgement packet reception will be more than compensated by the lower number of packet copy transmissions.

Channel access	max(NHI) for PLR_{APP} $<10^{-3}$	max(NHI) for PLR_{APP} close to 0	Time averaged number of packet copies	
			max	Averaged over all links
DC based random access with 6 copies	31	9 ($<10^{-6}$)	6	6
ALOHA with linearly increasing backoff	265	100	≤ 2.8	1.45
CSMA-ACK with 0dB link margin	445	200	≤ 5.1	1.41
CSMA-ACK with 10dB link margin	650	400	≤ 6.2	1.25

Table 44: Comparison of channel access schemes for a application duty cycle of 0.1% on each link

Adding an LBT procedure prior to a scheduled packet transmission converts the ALOHA access scheme into CSMA-ACK. The number of acceptable harmful interferers in a CSMA-ACK system almost doubles with respect to the ALOHA system if a minimum link margin of 0 dB is used in the device positioning procedure. The mean number of packet copies in the CSMA-ACK system is almost the same than in the ALOHA system although the channel load is significantly higher. A comparison of the number of retransmissions in a ALOHA system with linearly increasing backoff and a CSMA-ACK system for the same number of harmful interferers has shown that the CSMA-ACK always gets along with a smaller number of retransmissions, as a number of collisions can be avoided. Hence, the expected latency as well as the power consumption will be smaller in a CSMA-ACK system than in an ALOHA system. Setting the minimum link margin to 10 dB increases the number of tolerated harmful interferers in a CSMA-ACK system again by a factor of 1.5 to 2 dependent on the target packet loss rate in the application layer. The reason is that the higher link margin reduces the hidden node ratio, so that the collision probability is lowered and a smaller number of packet copies is required on each link. Nevertheless, the collision probability will be always greater than zero due to imperfections in the LBT implementation and a load dependent backoff procedures as in ALOHA is recommended in order to increase robustness of CSMA-ACK in high traffic load scenarios.

6. Coexistence of selected access schemes

In the previous section the performance of single-carrier random access schemes has been investigated assuming that all devices in the coverage area are using the same access scheme. This section analyzes the performance of access schemes provided that two independent systems are operated in parallel which either are using different access schemes or the same access scheme with different power levels.

6.1 Coexistence of two DC based random access systems with different power levels

The performance on the DC based random access links simply depends on the number of harmful interferers seen by the receiver. If all devices are using the same transmit duty cycle and the same packet length, the packet loss rate can be calculated analytically by

$$PLR_{equal} = 1 - (1 - 2 \cdot DC)^{N_{HI}}$$

Now, the power of each p-th interferers within the system is increased by a factor of R_P. Supposed that the devices with the high transmit power are randomly selected, is can be expected that the number of harmful interferers with the original transmit power reduces by a factor of (1-1/p). On the other side the number of harmful interferers with a high transmit power significantly increases due the higher transmission range. The increase of the transmission range R_d depends on the power increase and the path loss exponent of the channel model (a).

$$R_d = \sqrt[a]{R_P}$$

If all devices are placed in a two dimensional space, the area with potential interferers increases by a factor of R_A.

$$R_A = \left(\sqrt[a]{R_p}\right)^2$$

Supposed that the number of harmful interferers has been N_{HI} in the equal power scenario, half of the devices remain low power devices in the mixed power scenario. Hence, the number of weak interferers in the mixed power scenario becomes

$$N_{HI_{weak}} = \left(1 - \frac{1}{p}\right) N_{HI}, \text{ with } 0 < p < 1$$

while the number of harmful interferers with high transmit power increases to

$$N_{HI_{strong}} = \frac{1}{p} N_{HI} R_A$$

The resulting packet loss rate in the mixed power system can be calculated to

$$PLR_{mixed} = 1 - (1 - 2 \cdot DC)^{N_{HI_{weak}}} \cdot (1 - 2 \cdot DC_x)^{N_{HI_{strong}}}$$

where DC_x considers the transmit duty cycle of the high power devices. The packet loss rate of the equal power and the mixed power systems shall be identical:

$$PLR_{mixed} = PLR_{equal}$$

$$\Leftrightarrow 1-(1-2\cdot DC)^{N_{HI_{weak}}}\cdot(1-2\cdot DC_x)^{N_{HI_{strong}}}=1-(1-2\cdot DC)^{N_{HI}}$$

$$\Leftrightarrow (1-2\cdot DC)^{\left(1-\frac{1}{p}\right)N_{HI}}\cdot(1-2\cdot DC_x)^{\frac{1}{p}N_{HI}R_A}=(1-2\cdot DC)^{N_{HI}}$$

$$\Leftrightarrow (1-2\cdot DC_x)^{\frac{1}{p}R_A}=(1-2\cdot DC)^{\frac{1}{p}}$$

$$\Leftrightarrow DC_x=0.5\left(1-(1-2\cdot DC)^{\frac{1}{RA}}\right)$$

Hence, the duty cycle on the high power links in no function of the number of high power devices. This formula can be quite accurately approximated by

$$DC_{x,app}=\frac{1}{R_A}\cdot DC$$

as shown in Table 45 for some exemplary calculations. The reduction factor for the transmit duty cycle in the high power system only slightly depends on the absolute value of the low power system duty cycle. Increasing the transmit power of half the devices by a factor of 10 for example requires a reduction of the transmit duty cycle by a factor of 4 on these links to obtain the same packet loss rate than in the equal power system. Thereby, a path loss exponent of 3.3 has been assumed. The reduction factor increases for a lower path loss exponent as the number of high power interferers increases.

Duty cycle in the low power system	Ratio of high to low transmit power R_P			
	4	10	25	100
DC=5%	2.249	3.882	6.727	15.528
DC=1%	2.303	4.006	6.974	16.144
DC=0.1%	2.315	4.034	7.028	16.282
Approximated	2.317	4.037	7.035	16.297

Table 45: Ratio of the transmit DC in the low and high power system (DC/DC_X) as a function of the transmit power ratio R_p and the duty cycle in the low power system for a path loss exponent of 3.3

It should be taken into account that the formula above is independent of the part of links which are using high transmit power. Although it has been assumed that half of the interferers are using a high transmit power, the same result is obtained if only one or even all devices are transmitting with a high power. In ETSI TR 102 649-2 [6] a transmit power dependent transmit duty cycle is proposed for DC limited systems in the 873 MHz to 876 MHz band.

Power	DC
≤ 1 mW	≤ 5%
≤ 25 mW	≤ 1%
≤ 100 mW	≤ 0.1%

Table 46: Transmit power and transmit duty cycle limits for the 873 to 876 MHz band as proposed in [6]

Power	DC
≤ 1 mW	≤ 7%
≤ 25 mW	≤ 1%
≤ 100 mW	≤ 0.43%

Table 47: Calculated transmit power and transmit duty cycle limits

The duty cycle limits for the 1 mW and 100 mW transmit power links are similar but slightly lower in the proposed regulation than in the calculations. It should be taken into account that the duty cycle values in Table 47 are just presented for comparison and are higher than the values proposed in section 7.

6.2 Coexistence of CSMA systems with different power levels

In case two CSMA systems with different power levels are operated in parallel, the analysis is slightly more difficult, as the packet loss rate not only depends on the number of harmful interferers, but also on the hidden node ratio (HNR). As shown in section 5.6.3 the packet loss rate in a CSMA system without acknowledgements can be approximated by

$$PLR = 1 - \left(\left(1 - 2\frac{T_R + T_D}{T_{int}} \right)^{1-HNR} \left(1 - 2 \cdot \frac{T_{Tx}}{T_{int}} \right)^{HNR} \right)^{N_{HI}}$$

$$\text{with} \quad HNR = N_{HN}/N_{HI}$$

The formula assumes that each device uses the same transmit power. Now, the power of half of the devices is increased by a factor of R_p as described in the previous section. If all devices are placed in a two dimensional space, the area with potential high power interferers increases by a factor of R_A

$$R_A = \left(\sqrt[a]{R_p} \right)^2$$

where a represents the path loss exponent of the channel. The number of low power and high power interferers can again be calculated to

$$N_{HI_{weak}} = \frac{N_{HI}}{2}$$

$$N_{HI_{strong}} = \frac{N_{HI}}{2} R_A$$

where N_{HI} is the number of harmful interferers in a scenario with just low power devices. Supposed that the links with a high and a low power transmitter have the same link margin, their number of harmful interferers will be identical assuming a random distribution of high and low power interferers. Nevertheless, it is expected that the hidden node ratio will be different for links with a small and high transmit power. The hidden node ratio for equal and mixed power scenarios is determined by a MATLAB simulation. The desired link with a link margin of 10 dB is surrounded by randomly placed high power and low power interferers having the same device density. For each random set of device positions the number of harmful interferers at the desired receiver position is determined, which should be equal to

$$N_{HI,mixed} = \frac{1}{2}(1 + R_A)\, N_{HI}$$

Each harmful interferer belongs to one of the following three groups:

- Group 1: The desired transmitter detects the harmful interferer and the harmful interferer detects the desired transmitter
- Group 2: The desired transmitter detects the harmful interferer, but the interferer cannot detect the desired transmitter or the desired transmitter cannot detect the harmful interferer, but the interferer detects the desired transmitter
- Group 3: Neither the desired transmitter detects the interferer nor the interferer detects the desired transmitter.

The collision probability with a harmful interferer in the first group is equal to

$$P_{Coll,Group\,1} = 2 \cdot \frac{T_R + T_D}{T_{int}}$$

while the collision probability is higher for harmful interferers in the second group. If device *A* can detect device *B*, a collision can be avoided supposed that the signal *B* is already present if *A* checks the channel. In case device *A* transmits first and devices B cannot detect device *A*, any packet start of *B* during the whole packet duration of *A* will result in a packet loss on the desired link. Hence, the collision probability can be calculated to

$$P_{Coll,Group\,2} = \frac{T_R + T_D + T_{Tx}}{T_{int}}$$

Finally, any harmful interferer in the third group is a hidden node, so that the corresponding collision probability is equal to

$$P_{Coll,Group\,3} = 2 \cdot \frac{T_{Tx}}{T_{int}}$$

In case R_i denotes the part of the harmful interferers within in *i*-th group, the resulting packet loss rate can be calculated to

$$PLR = 1 - \left(\left(1 - 2 \cdot \frac{T_R + T_D}{T_{int}}\right)^{R_1} \cdot \left(1 - \frac{T_R + T_D + T_{Tx}}{T_{int}}\right)^{R_2} \cdot \left(1 - 2 \cdot \frac{T_{Tx}}{T_{int}}\right)^{R_3} \right)^{N_{HI,mixed}}$$

$$\text{with} \quad R_i = \frac{N_{Group\,i}}{N_{HI}}, \qquad i = 1,2,3$$

Now, the number of harmful interferers within each group is determined in the Matlab simulation for 1000 different sets of random interferer positions. Table 48 shows the results in the equal power scenario and a link margin of 10 dB. A large part (i.e. 68%) of the harmful interferers can be detected by the desired transmitter, while the hidden node ratio is equal to 32%. As the transmit powers are all equal, device *B* always detects device *A*, if *A* detects *B*. Hence, there are no harmful interferers in the second group.

R_p	R_A	$\frac{N_{HI,mixed}}{N_{HI,equal}}_{calc}$	$\frac{N_{HI,mixed}}{N_{HI,equal}}_{sim}$	R_1	R_2	R_3	Exposed node ratio
1	1	1.0	1.0	68 %	0	32 %	30 %

Table 48: Harmful interferer grouping in the equal power scenario, 10 dB link margin, P_{det}=-96 dBm

It is interesting to note that the exposed node ratio is only 30%. In case the desired packet transmitter detects an interferer prior to an own packet transmission, there is a high probability of 70% that the signal would in fact harmfully interfere with the own packet transmission at the position of the dedicated receiver and a collision can be successively avoided. Even if the interferer is an exposed node with regards to the own link, LBT might still avoid a collision of the own packet with the interferer packet at the position of the interfering link receiver. Hence, the LBT measurements unnecessarily delays the own transmission only if the desired node is an exposed node for the interferer link.

Now, the transmit power of half of the interferers is increased by a factor of R_p. Supposed that the desired link itself is a low power link, the results are shown in Table 49.

R_p	$R_A = {R_p}^{2/3.3}$	$\frac{N_{HI,mixed}}{N_{HI,equal}}_{calc}$	$\frac{N_{HI,mixed}}{N_{HI,equal}}_{sim}$	R_1	R_2	R_3	Exposed node ratio
4	2.32	1.658	1.66	49.8 %	25.4 %	24.8 %	23 %
10	4.04	2.519	2.52	32.7 %	47.5 %	19.8 %	28 %
25	7.03	4.017	4.02	20.5 %	64.0 %	15.5 %	13 %
100	16.3	8.649	8.65	9.6 %	80.0 %	10.4 %	8 %

*Table 49: Harmful interferer grouping in a mixed power scenario, desired link has a **low** transmit power*

The simulated number of harmful interferers in the fourth column increases as expected and perfectly fits to the calculated result in the third column. Thereby, the number of harmful interferers with a low transmit power is constant, while only the number of harmful, high power interferes increases due to the higher radio range of those devices. As the desired transmitter is a low power transmitter, all low power interferers behave as in an equal power system. Hence, 68% of the low power devices can be found in the first group and the remaining 32% belong to the third group, while there are no low power interferers in the second group. On the other side, most of the high power interferers can be detected by the desired transmitter, while this is often not true for the reverse direction. Hence, a large part of the harmful interferers with a high transmit power can be found in the second group. As the number of high power interferers increases by a factor of R_A, their influence becomes dominant if R_p increases. Consequently, the part of harmful interferers in the second group increases, while the part of harmful interferers in the two others groups decreases. The exposed node ratio is the rightmost column improves. A large part of the harmful interferers with a high power can be detected by the dedicated transmitter, due to the short distance of link partners on a low power link.

In case the desired link has a high power transmitter, the results are quite different as shown in Table 52. Now, the harmful interferers with a high transmit power have the same power than the desired transmitter. Hence, 68% of the high power interferers can be found in the first group, while the remaining 32% are hidden nodes and therefore located in group 3. On the other side, a large part of the harmful interferers with a low transmit power can detect the desired transmitter, while they are themselves typically hidden nodes. Hence, most of the low power

interferers can be found in the second group. As the high power interferers gain influence increasing R_p, the part of harmful interferers in the first and third group increases, while the part in the second group decreases.

R_p	R_A	$\frac{N_{HI,mixed}}{N_{HI,equal\ calc}}$	$\frac{N_{HI,mixed}}{N_{HI,equal\ sim}}$	R_1	R_2	R_3	Exposed node ratio
4	2.32	1.658	1.66	0.632	0.112	0.256	35 %
10	4.04	2.519	2.52	0.621	0.122	0.257	34 %
25	7.03	4.017	4.02	0.623	0.097	0.280	35 %
100	16.3	8.649	8.65	0.640	0.058	0.302	35 %

*Table 50: Harmful interferer grouping in a mixed power scenario, desired link has a **high** transmit power*

The exposed node ratio on a high power link in a mixed power scenario is slightly higher than in an equal power system, because most of the low power interferers in the neighbourhood of the transmitter are exposed nodes. They typically generate no harmful interference at the receiver position due to the large distance between the high power transmitter and its dedicated receiver.

The number of interferers within each group can be used to calculate the packet loss rate on high power and low power links in a CSMA system without packet retransmissions. Although the number of harmful interferers at the position of the high power and low power link receivers are identical, the resulting packet loss rate is slightly different as shown in Figure 58. While the packet loss rate on the high power links is almost identical to the packet loss rate in an equal power system with the same number of harmful interferers, the performance on the low power links slightly degrades, if the power ratio increases.

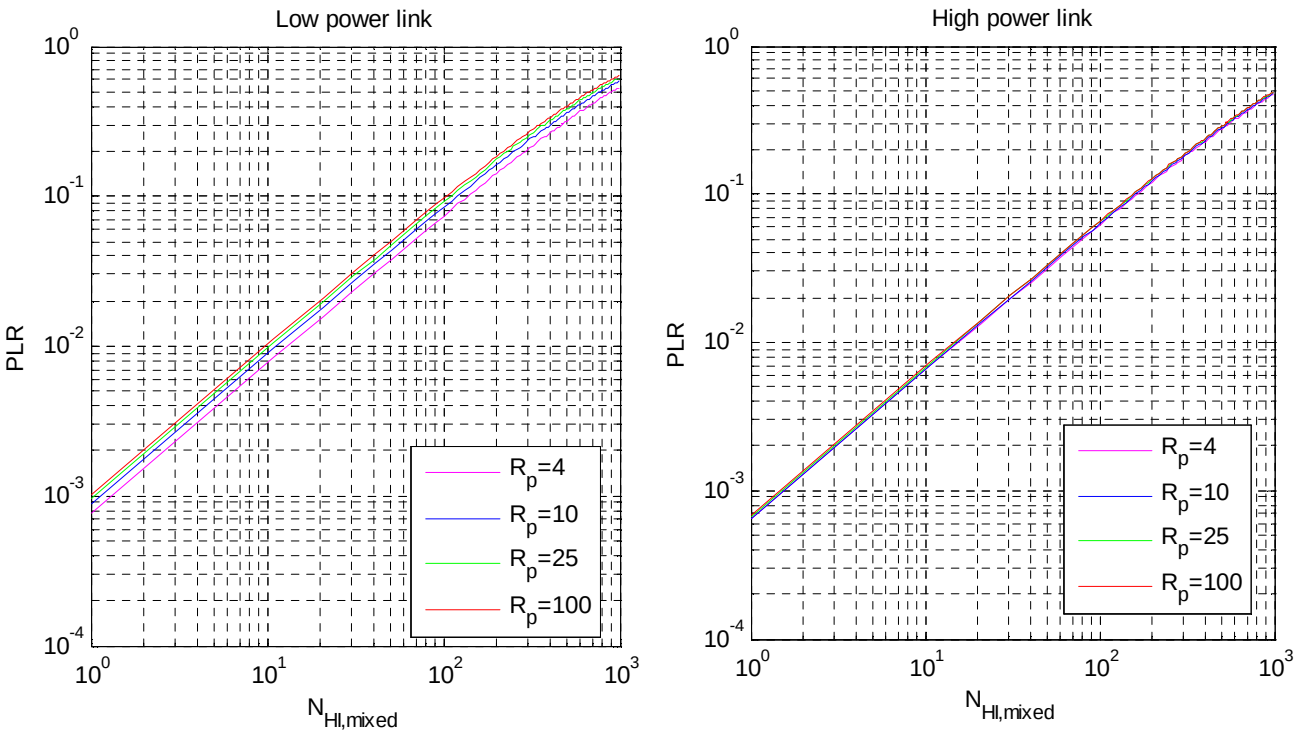


Figure 58: PLR on low (left) and high (right) power links in a mixed power scenario as a function of the number of harmful interferers and the power ratio R_p, T_R+T_D=0.25 ms, T_{Tx}=20ms, T_{int}=20s, P_{det}=-96dBm, 10 dB link margin

The PLR rate is by a factor of 1.5 higher for a power ratio of 100. The degradation on the low power links becomes larger if the CSMA-ACK link is either operated with a higher link margin or uses a lower detection threshold. In both cases the number of hidden nodes decreases. The performance for a link margin of 14 dB is shown in Figure 59. The PLR rate is by a factor of 4.5 higher on low power links than on high power links for a power ratio of 100.

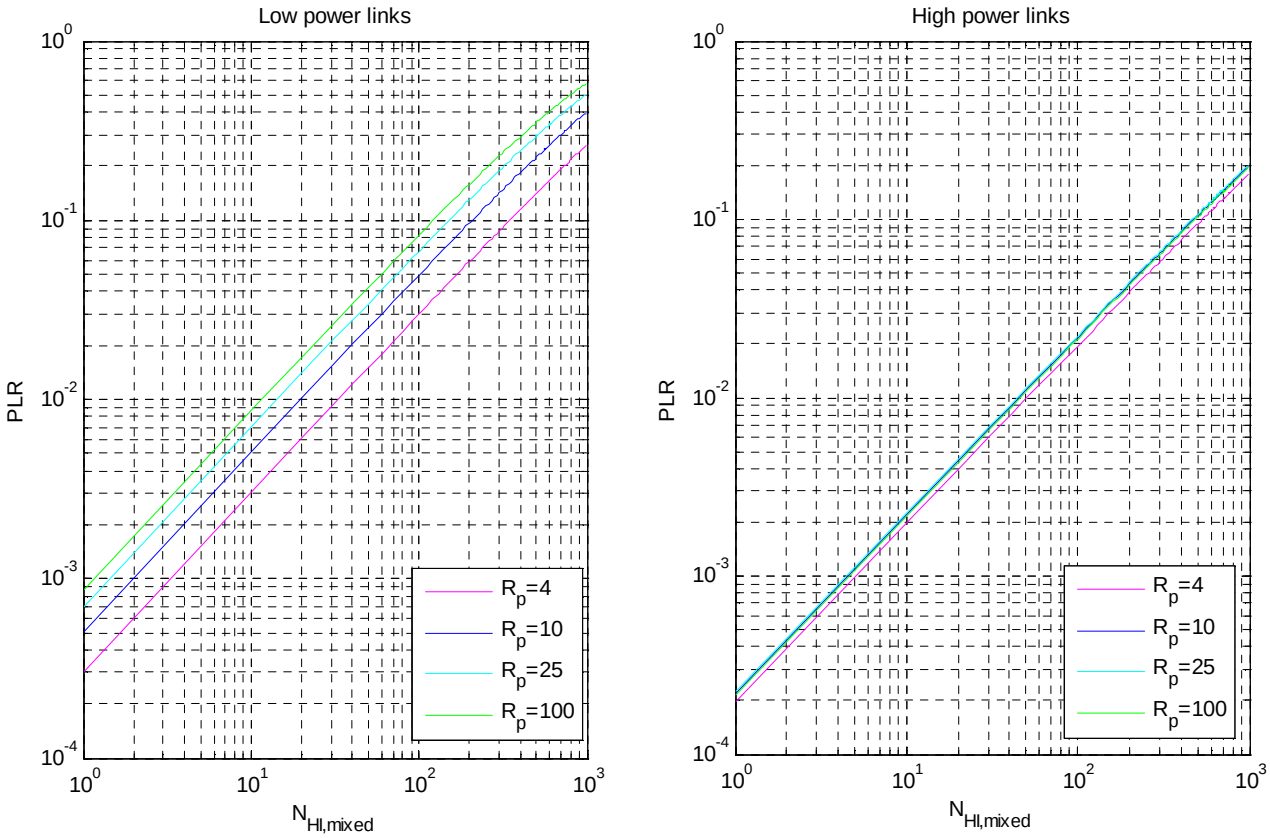


Figure 59: PLR on low (left) and high (right) power links in a mixed power scenario as a function of the number of harmful interferers and the power ratio R_p, T_R+T_D=0.25 ms, T_{Tx}=20ms, T_{int}=20s, P_{det}=-96dBm, 14 dB link margin

Supposed that the duty cycle of the high power links is reduced to compensate for a higher transmit power, the duty cycle reduction not only has to compensate for the higher number of interferers, but also for the higher packet loss rate on low power links due to the fact that a large part of the high power interferers cannot detect the small power transmitters. The relationship of power und duty cycle therefore strongly depends on the performance of the CSMA systems, which is determined by the implementation parameters and the scenario assumptions. The DC limit on high power links definitely needs to be smaller than the value proposed for DC based random access schemes. Alternatively, different bands can be considered for different power levels.

6.3 Coexistence of DC based random access and CSMA-ACK

In case DC based random access and CSMA-ACK systems are operated in parallel, the impact of the DC based random access links on the performance of the CSMA-ACK links as well as the impact of the CSMA-ACK links on the performance of the DC based random access links need to be analysed.

6.3.1 Impact on the CSMA-ACK links

The performance of a system where all links are using CSMA-ACK has been analysed in section 5.6.4. Supposed that a minimum link margin of 10 dB has been realised on all links, the indoor simulation has shown that 1100 devices with an application duty cycle of 0.1 % can be operated in parallel without any packet loss in the application layer during the simulation time. Now 550 randomly selected links are replaced by DC based random access links. The transmit duty cycle of the DC links is iteratively increased from 0.05%, 0.1% to 0.2% and the resulting packet loss rate in the application layer of the CSMA-ACK links is shown in Figure 60.

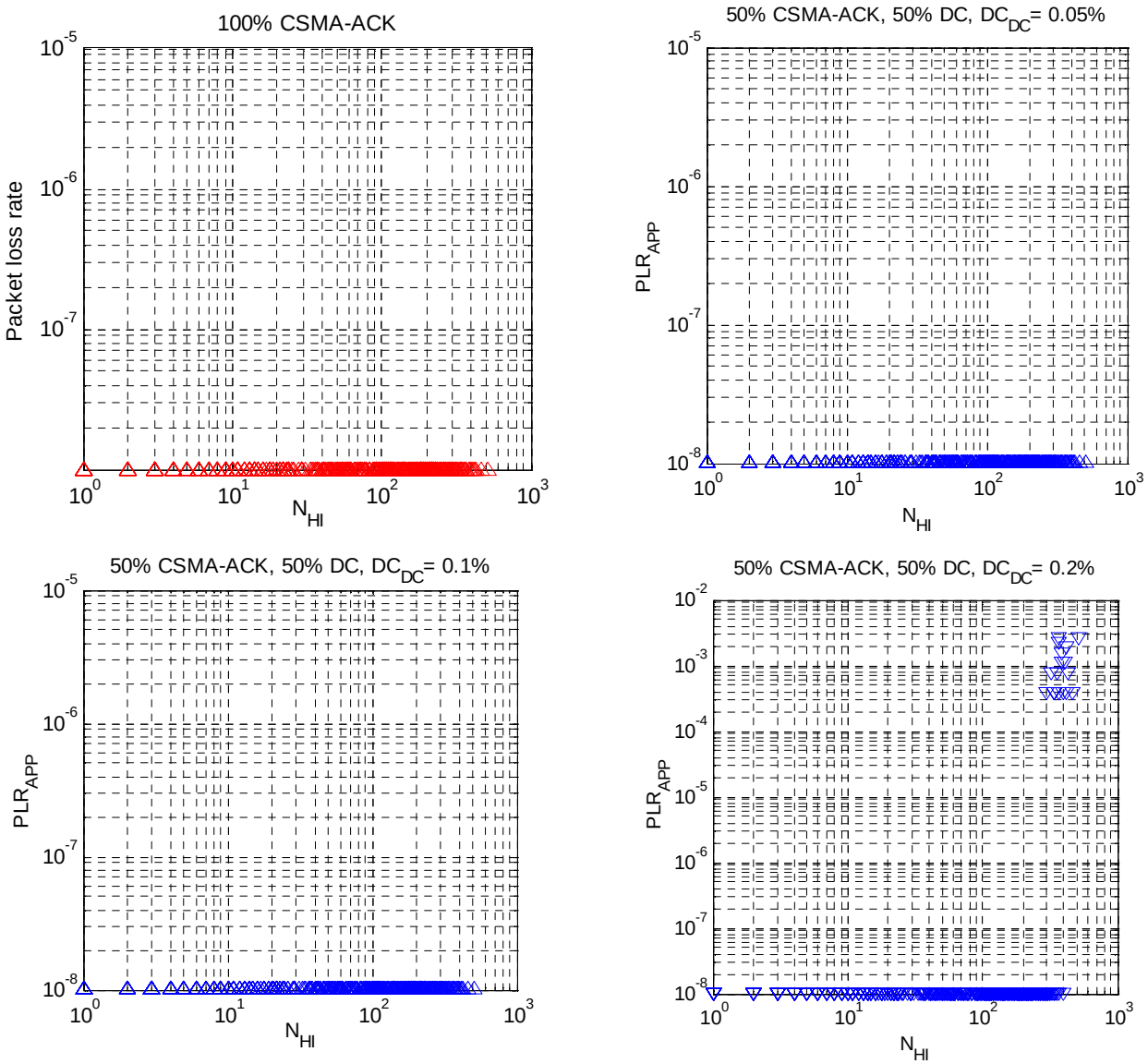


Figure 60: PLR in the application layer of the 550 CSMA-ACK links with DC_{APP} =0.1% as a function on the transmit duty cycle of the DC based random access links, packet length=20 ms, $P_{tx} = -10\ dBm,\ P_{det} = -96\ dBm$

The first non-zero packet loss rates are measured using a transmit duty cycle of 0.2% on the DC based random access links. Hence, the maximum acceptable transmit duty cycle seems to be in the order of 0.1% in order to maintain the high reliability on the remaining CSMA-ACK links. A transmit duty cycle of 0.1% on the DC based random access links is still smaller than the transmit duty cycle on the former CSMA-ACK links. Especially those CSMA-ACK links with high numbers of harmful interferers required a number of retransmissions, so that the duty cycle of 0.1% in the application layer results in a significantly higher duty cycle on the air interface. Hence, replacing these links by DC based random access links lowers the overall transmit duty cycle. Nevertheless, this advantage is compensated by a higher collision probability without the LBT procedure.

While the duty cycle on the DC based random access links has been selected such that the performance on links with high number of interferers is almost the same, it is expected that links with a small number of interferers slightly suffer. Their transmit duty cycle has been already close to 0.1% using CSMA-ACK and is not much lowered using DC based random access. Hence, the collision probability will increase resulting in a higher number of packet retransmission for those links. This can be confirmed comparing the average number of transmitted packet copies in the original CSMA-ACK simulation with the results in the mixed scenario.

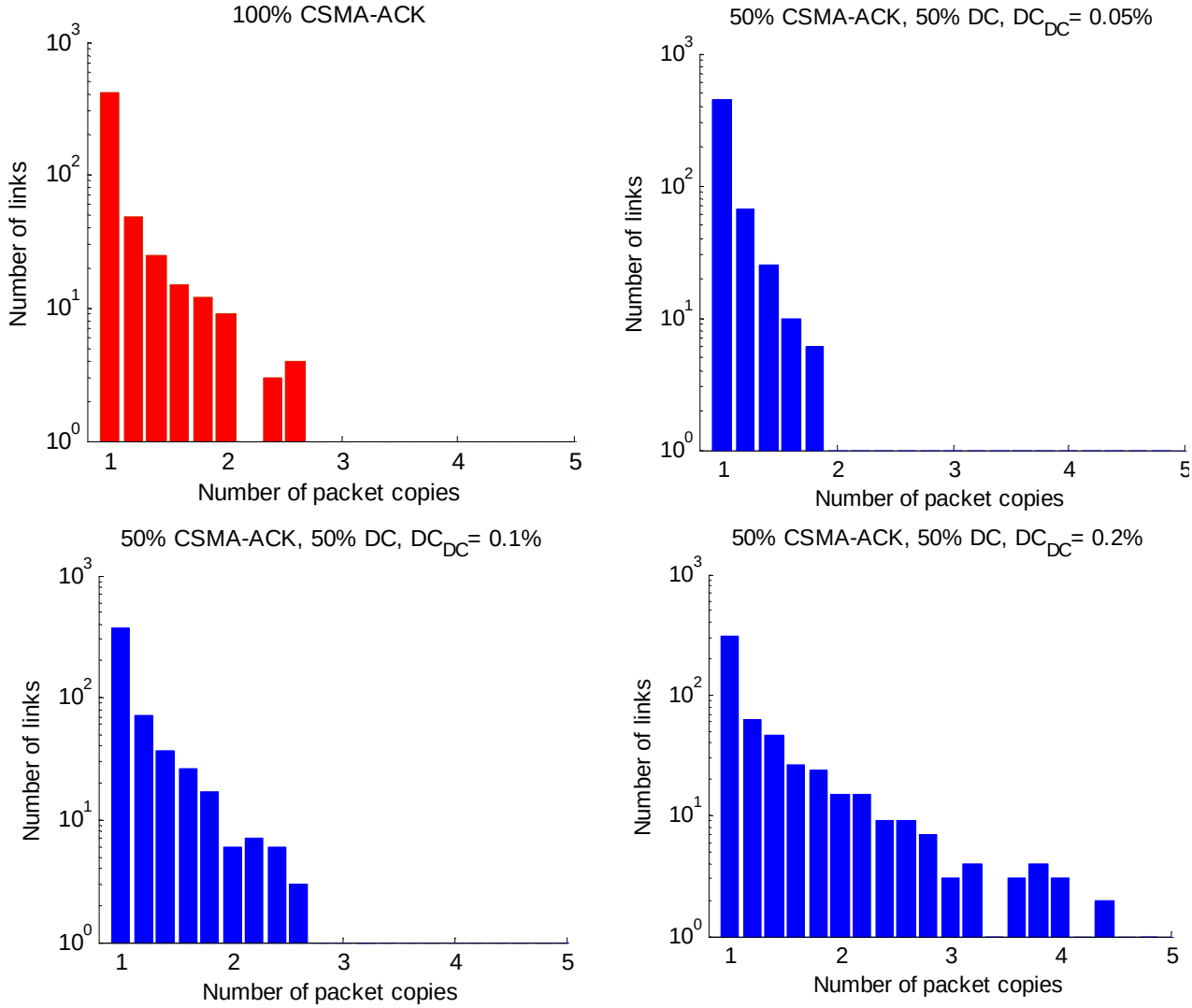


Figure 61: Number of mean packet copies on the 550 CSMA-ACK links with DC_{APP} =0.1% as a function on the transmit duty cycle of the DC based random access links, packet length=20 ms, $P_{tx} = -10\ dBm,\ P_{det} = -96\ dBm,$

In the original CSMA-ACK simulation shown in the left upper plot of Figure 61, the links with the highest number of retransmissions require on the average 2.6 packets per data packet. The mean value for 550 CSMA-ACK links is 1.11. The three remaining plots in Figure 61 shows the mean number of packet copies on the CSMA-ACK links in a mixed scenario for a transmit duty cycle of 0.05%, 0.1%, and 0.2% on the CD based random access links. Using a transmit duty cycle of 0.05% reduces the average packet copies on the CSMA-ACK links, so that the performance even improves. Using a transmit duty cycle of 0.1% on the DC based random access links results in the histogram on the lower left position. The maximum number of packet copies equals the results in original CSMA-ACK simulation, so that the performance of those links with the high number of harmful interferers seems to be comparable. Nevertheless the mean value averaged over all 550 CSMA-ACK links increases from 1.11 to 1.21, so that the number of repetitions changes from 0.11 to 0.21 as the first copy is always the original data packet. Hence, in the average the number of repetitions doubles when using DC based random access instead of CSMA-ACK on half of the links.

The same observation can be done comparing the channel packet loss rates of 550 selected CSMA links in a pure CSMA-ACK system to the simulation results in the mixed scenario with a transmit duty cycle of 0.1% on the DC based random access links. The red diamonds in Figure 62 are the sorted channel PLR values belonging to the original CSMA-ACK simulation, while the blue cycles represent the results in the mixed scenario. In both simulations, the highest channel PLRs are almost identical, so that the performance on links with a high number of harmful interferers is almost identical. Nevertheless, more reliable links with a formerly low channel PLR significantly worsen if half of the links apply DC based random access. This explains the higher number of retransmissions in order to achieve an almost zero PLR on the application layer.

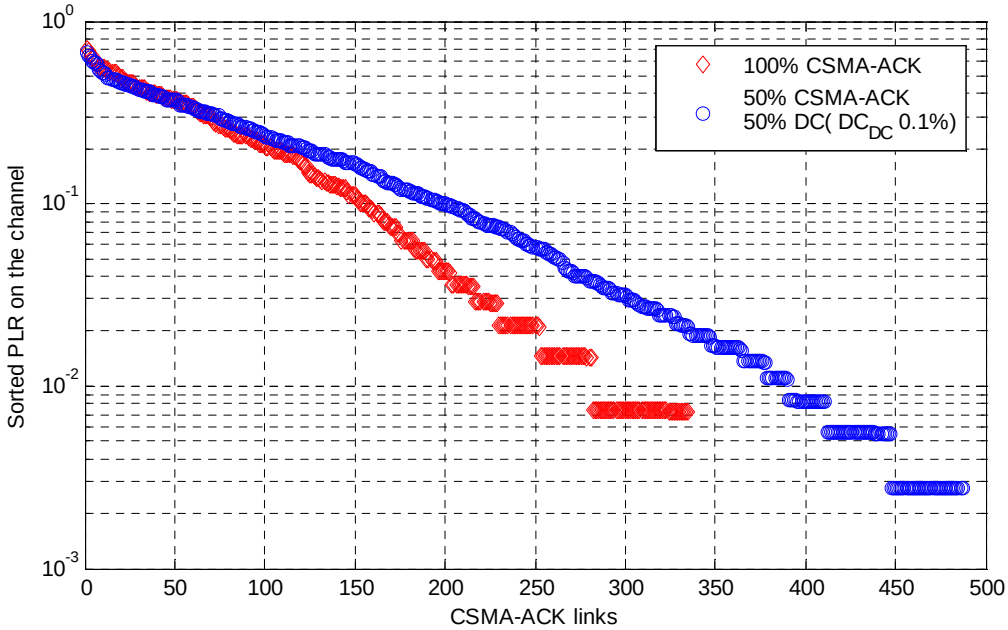


Figure 62: Sorted PLR on the channel for the 550 CSMA-ACK links, the other 550 links are CSMA-ACK links (red), DC limited links with DC=0.1% (blue)

Hence, DC based random access links can be operated in parallel to CSMA-ACK links, but in the transmit duty cycle needs to be smaller in order to compensate for the higher collision probability. In the simulation scenario the maximum transmit duty cycle on the DC limited links should be no larger than 0.1%. While the PLR is zero on the CSMA-ACK links, it is significantly above zero for a large number of DC based random access links as shown on the left side of

Figure 63. The right plot of Figure 63 shows the resulting PLR in the application layer using 6 copies. The application PLR is below 10^{-3} for 80% of the links, while 10% of the links have an application PLR higher than 10^{-2}. If necessary, the reliability of the latter can be increased lowering the distance of the corresponding link partners.

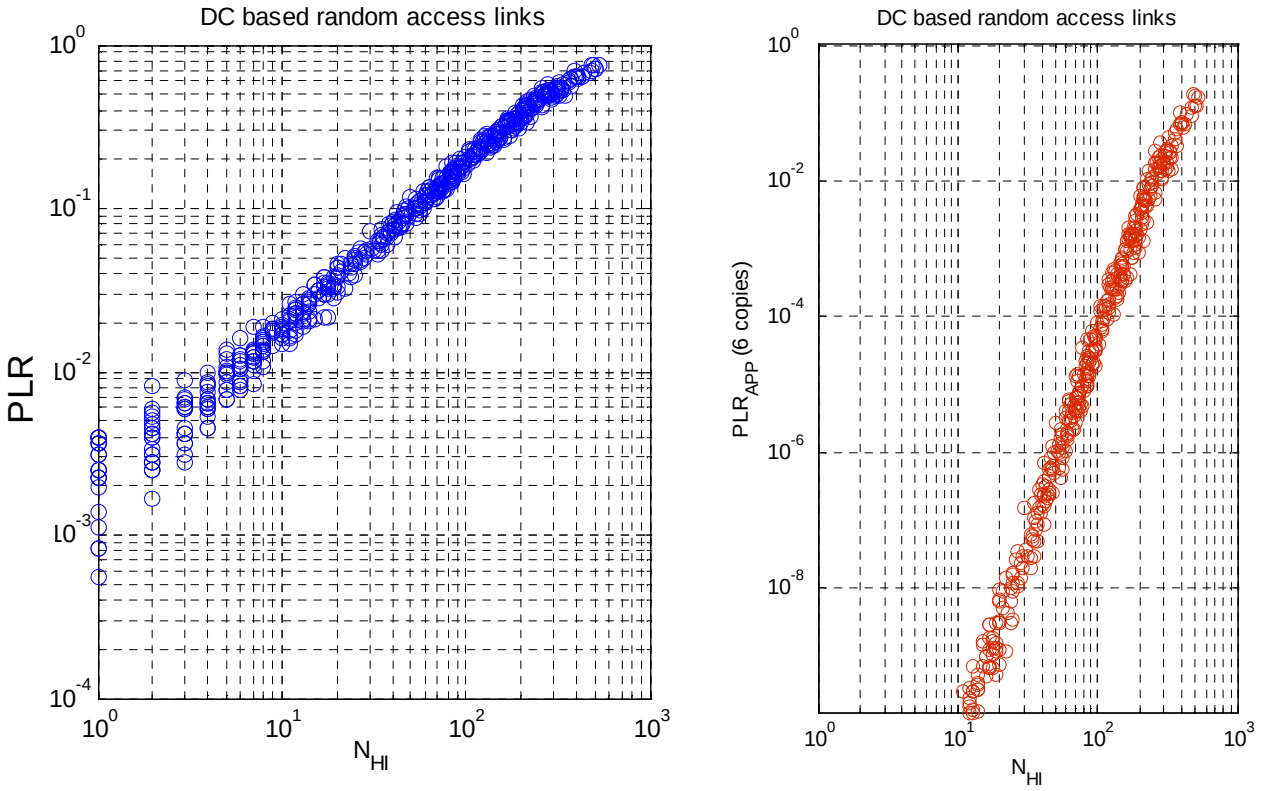


Figure 63: PLR on the channel (left) and in the application layer (left, 6 copies) for the DC based random access links

As a conclusion, the application duty cycle on the DC limited links will be by factor of around 6 smaller than the duty cycle of the original CSMA-ACK links, while at the same time a lower reliability needs to be accepted on the DC based random access links.

6.3.2 Impact on the DC based random access links

Similarly, the impact of CSMA-ACK links on the packet loss rate of DC based random access links can be analysed and compared to the performance of pure DC based random access system. The DC based random access simulations described in section 5.6.1 have shown that the maximum number of harmful interferers needs to be below 52 in order to achieve an application packet loss rate below 10^{-2} for a duty cycle of 0.1% in the application layer and six packet copies per data packet. This can be achieved with 100 devices within the building and a minimum link margin of 10 dB.

Now, 50 randomly selected links are replaced by CSMA-ACK links. It is expected that the system performance significantly increases, if the same duty cycle is maintained in the application layer. On the one hand the number of packet retransmission will be much smaller on the CSMA-ACK links and on the other hand a number of collisions can be avoided due to the LBT procedure.

Next, the duty cycle on the CSMA-ACK links is successively increased until almost the same PLR is obtained than in the pure DC based random system. Figure 64 shows the measured application PLR in three different iterations, where the application duty cycle of the CSMA-ACK

links varies from 0.2% in the left plot to 1.0% in the right plot. The black line always indicates the application PLR in the pure DC limited system.

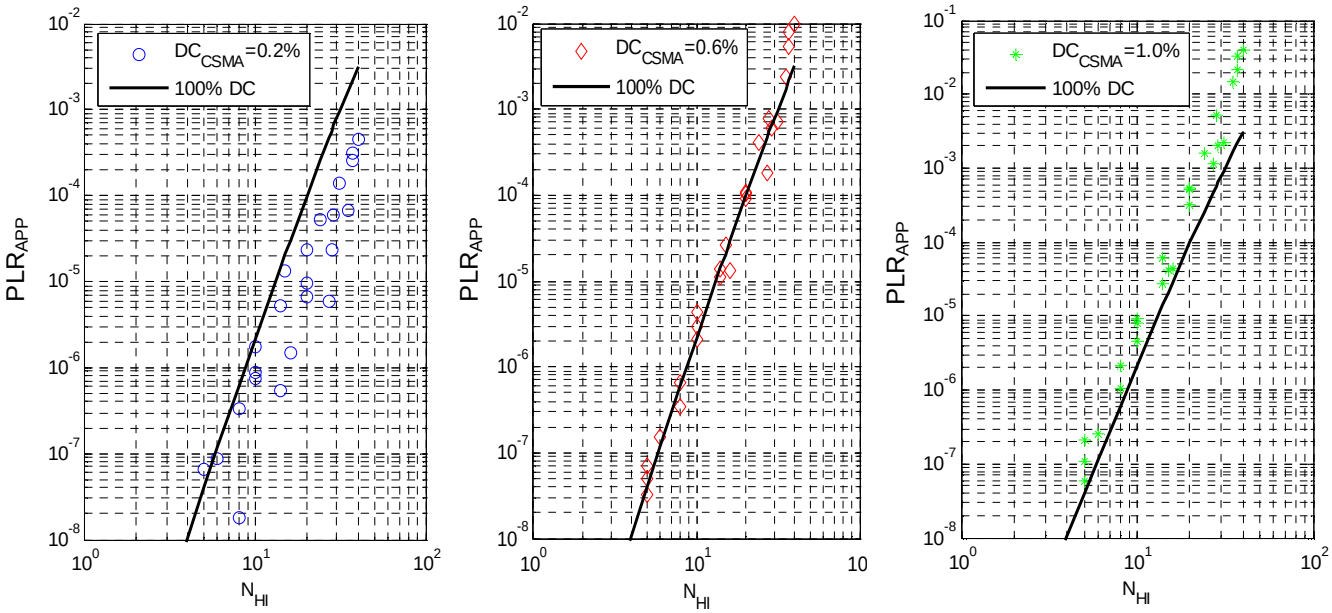


Figure 64: PLR in the application layer of the 550 DC links with DC_{APP} =0.1% as a function on the application duty cycle of the CSMA-ACK links, packet length=20 ms, $P_{tx} = -10\,dBm$, $P_{det} = -96\,dBm$

The PLR seems to be almost identical using an application duty cycle of 0.6% on the CSMA-ACK links. Due to some repetitions the transmit duty cycle on the CSMA-ACK links is therefore larger than it has been in the pure DC based random access system. Nevertheless, the higher channel load does not result in a higher PLR on the channel as a part of the collisions can be avoided using LBT.

As a conclusion, a CSMA-ACK system can be operated in parallel to a DC based random access scheme. Once again, the application duty cycle on the CSMA-ACK links is by a factor of 6 higher than it has been using DC based random access. Furthermore, the application PLR on the CSMA-ACK links has been zero in the simulation, so that the reliability can be significantly improved. Hence, the overall system performance increases with each link using CSMA-ACK instead of DC based random access.

6.4 Coexistence of two CSMA-ACK with different power levels

So far, the performance of a CSMA-ACK system has been analysed in a scenario where all devices are transmitting with the same power (see section 5.6.4). Hence, a transmitter detecting an interferer signal can assume that its own signal will be received with the same power at the position of the interferer. If the two devices are using different power levels, this is no longer true. A high power device can be detected by a small power device, while this might not be true in the opposite direction as described in 6.2. This section investigates the impact on the system performance of two simultaneously operating CSMA-ACK systems with different power level.

In section 5.6.4 the first packet losses in the application layer have been measured with 1200 devices within the building using an equal transmit power level of -10 dBm, an application duty cycle of 0.1% and a minimum link margin of 10 dB. Now, the power on half of the links is increased by 10 dB. In general, the greater radio range of the high power transmitters will

increase the number of harmful interferers at all receiver positions, so that the absolute number of devices within the building needs to be reduced to maintain reliable connections. Table 51 compares the number of critical links with a high number of harmful interferers (N_{HI}) in the equal power scenario with 1200 devices to the number of critical links in a mixed power scenario with 700, 800, 836, 840 and 900 devices.

	Number links with N_{HI}>300	Number links with N_{HI}>400
1200 (equal power)	114	48
700 (power mix)	47	11
800 (power mix)	80	21
836 (power mix)	107	41
840 (power mix)	122	56
900 (power mix)	163	73

Table 51: Comparison of scenario parameters

From Table 51 it is expected that the system performance of the equal power scenario with 1200 is slightly worse than the performance of the mixed power scenario with 836 devices, but better than a scenario with 840 devices. It is interesting to note that the number of devices in the mixed power system is larger than expected from calculations in section 6.2. The reason is that even if the coverage area of devices with a 10 dB higher transmit power increases by a factor of 4 for a path loss exponent of 3.3, the increase of harmful interferers with a high power level is significantly smaller in the simulation. The resulting coverage area of high power devices is larger than the building and there are no devices outside the building.

The simulations have been repeated for 700, 800, 836, 840 and 900 devices with the same parameter settings, except that the power on half of the randomly selected links has been increased to 0 dBm, while the power on the remaining links is -10 dBm. The results are shown in Figure 65.

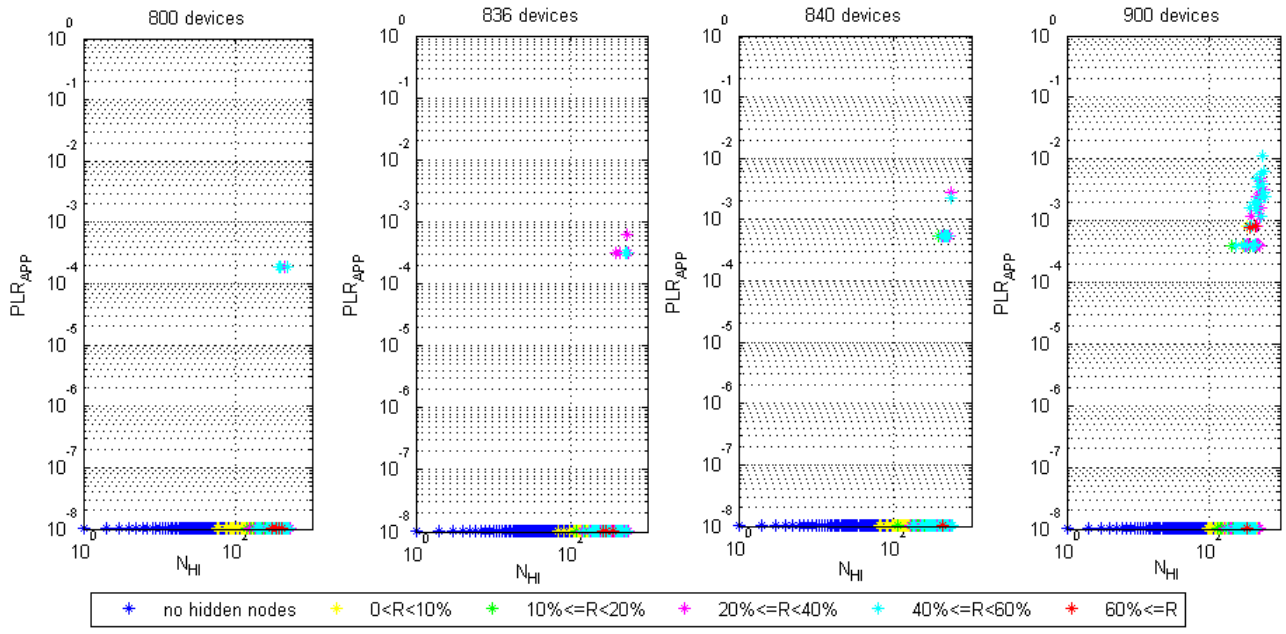


Figure 65: Application PLR for a mixed power scenario with 800 to 900 devices, 10 dB link margin, Pdet=-96 dBm, DC_{APP}=0.1%. P_{tx}=0/-10dBm

The first packet losses are measured on 4 links in a scenario with 800 devices. Nevertheless, the PLR is still below 10^{-3} so that reliable communication is possible on all links. The results are better than the PLR in the equal power scenario with 1200 devices, where 7 links have a non-zero PLR below 10^{-3}, while 2 links have a slightly higher PLR below 10^{-2} as shown in Table 52. As expected, the performance of the equal power scenario is well in between the performances of the mixed power scenario with 836 and 840 devices.

Number of devices	10^{-4}<PLR<10^{-3}	10^{-3}<PLR<10^{-2}	PLR>10^{-2}
1200 (equal power)	7	2	0
700 (power mix)	0	0	0
800 (power mix)	4	0	0
836 (power mix)	6	0	0
840 (power mix)	10	2	0
900 (power mix)	39	27	1

Table 52: PLR results of the mixed power scenarios as a function of the number of devices

So far, the overall system performance has been investigated. In a next step, the individual performance of the two systems in the mixed power scenario with 840 devices is analysed separately. The link performance of the high and low transmit power devices depends on the number of harmful interferers and the hidden node ratio.

The number of harmful interferers is presented in Figure 66 as a function of the link margin for the high power devices on the left side and the low power devices on the right side. The number of harmful interferers is almost identical for high power and low power links, as it is only a function of the desired link margin and the number of high power and low power interferers in the neighbourhood. As the high power and low power links are randomly distributed the interference situation is comparable for links with the same link margin independent of the transmit power as confirmed by Figure 66.

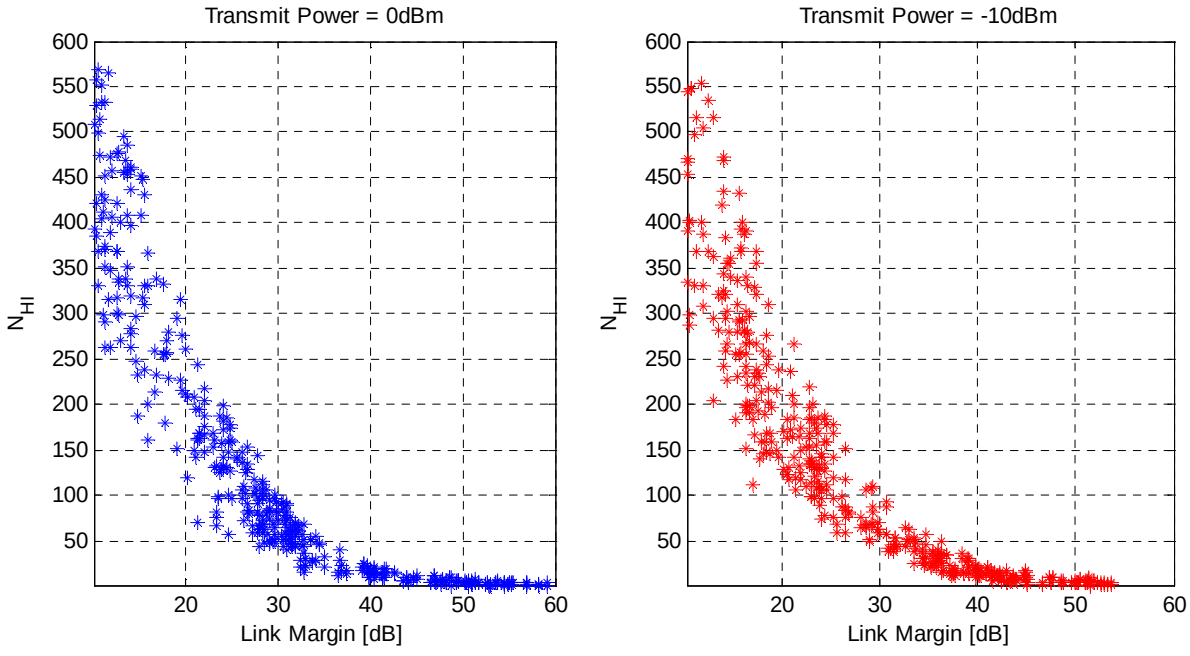


Figure 66: Number of harmful interferers for devices with a high transmit power (left) and devices with a small transmit power (right)

The PLR in the application layer is analysed separately for high power (P_{tx}=0dBm) and low power (P_{tx}=-10dBm) devices. The results are shown in Figure 67 for the high power devices on the left und the low power devices on the right.

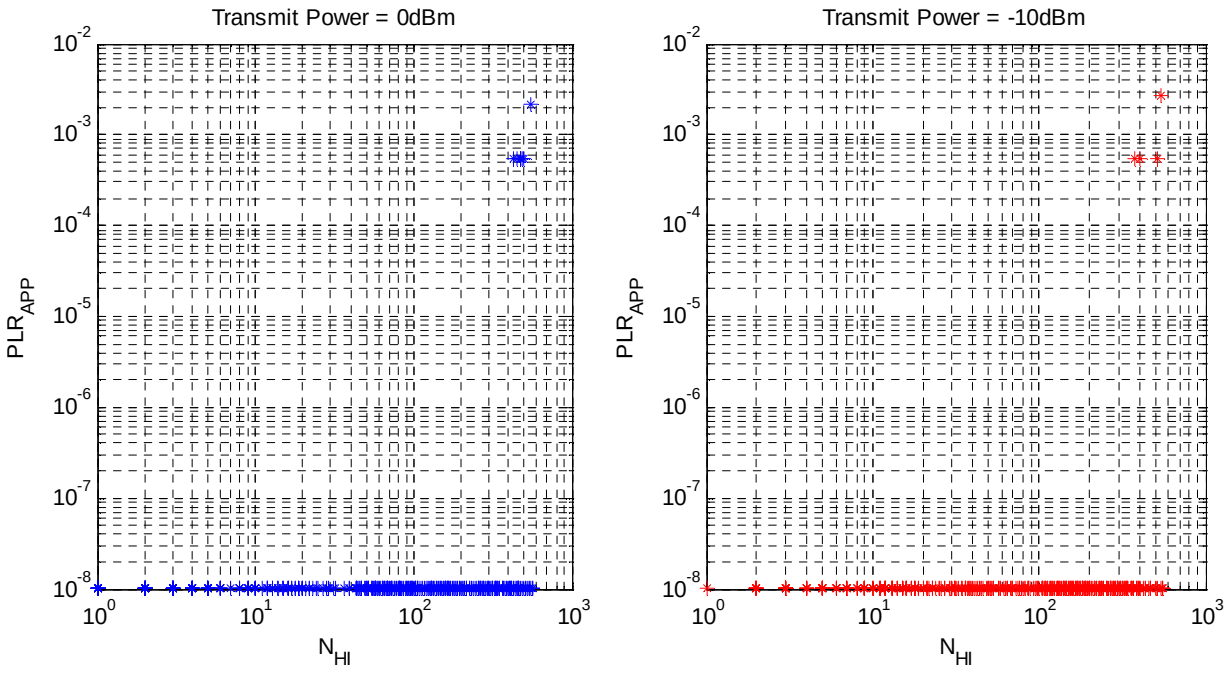


Figure 67: Application PLR for a mixed power scenario with 840 devices, 10 dB link margin, Pdet=-96 dBm, DC_{APP}=0.1% (high transmit power (left) and small transmit power (middle)) compared the same scenario with low transmit power for all devices

The application PLR rates on te high power and low power links are almost identical. There are 7 high power links with a still relatively small PLR of $5 \cdot 10^{-4}$ and one high power link with a packet loss of $2 \cdot 10^{-3}$, while the remaining high power links have been simulated without packet losses. The PLRs of the small power links are shown in the right plot. Four links have a PLR greater than zero with values similar to the high power links.

Figure 68 shows the mean number of packet transmissions per data packet on the links with the high transmit power on the left and with the low transmit power on the right side.

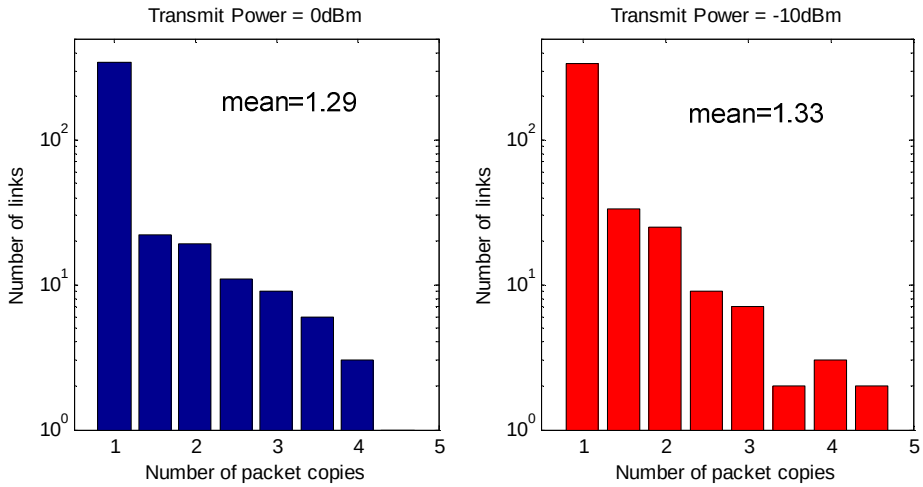


Figure 68: Mean number of packet copies for a mixed power scenario with 840 devices, 10 dB link margin, Pdet=-96 dBm, DC_{APP}=0.1% (high transmit power (left), small transmit power (right))

They both require typically up to 4 packet transmissions per data packet. There is only one low power link requiring 4.5 packets. The mean number of packet copies is slightly lower on the high power links, so that the packet loss rate on the channel is slightly higher on low power links.

Hence, the performance of the high power and low power system seems to be almost comparable in the simulated scenario with a slightly higher number of packet losses on the low power links. Nevertheless, it has to be taken into account that the number of harmful interferers with a high transmit power is artificially limited by the building size, because there are no devices outside the building. Hence, the performance difference of low and high power links is smaller than expected from section 6.2 for CSMA systems. Again, the impact of high power transmitters on low power links significantly depends on the CSMA system performance given by the implementation parameters and the scenario assumptions.

Adaption of the detection threshold:

EN 300 328 proposes a detection threshold proportional to the transmit power of the transmitter for LBT based DAA. The argument is that devices with a small transmit power might use a higher detection threshold because their range is so small that a large part of the detectable interferers are exposed nodes. The same simulations with 700, 800 and 900 devices within the building has been repeated using a detection threshold of -96 dBm for the high power devices (P_{tx}=0dBm) and a threshold of -86 dBm for the devices with a 10 dB lower transmit power. The results are shown in Figure 69 for exactly the same device densities and positions.

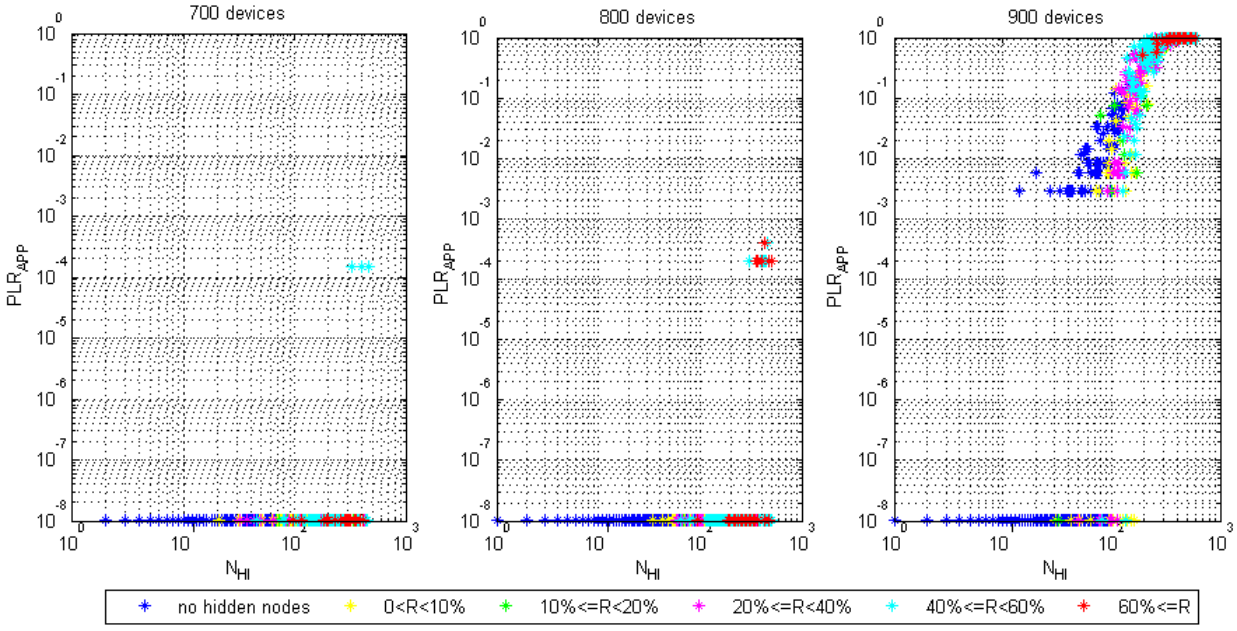


Figure 69: Application PLR for a mixed power scenario with 700 to 900 devices, 10 dB link margin, Pdet=-96 dBm, DC_{APP}=0.1%

The system performance significantly degrades using the higher detection threshold for the low power devices. There are already some non zero PLR links in the scenario with 700 devices and a very high number of links have an unacceptable high PLR in the scenario with 900 devices. Table 53 compares the average packet loss rate in the high and low power systems with 800 devices for an equal, low detection threshold of -96 dBm for all devices and a threshold of -96/-86 dBm depending on the transmit power.

	P_{Det} = -96 dBm	P_{Det} = -96/-86 dBm
High power system	$1.42\ 10^{-6}$	$4.04\ 10^{-6}$
Low power system	$4.85\ 10^{-7}$	$3.52\ 10^{-6}$

Table 53: Mean PLR in mixed power scenario with 800 devices as a function of the detection threshold

The PLR of both systems increases using a higher detection threshold for the low power links. This is especially true for the low power devices, which cannot profit from the lower number of exposed nodes. Using a higher detection threshold for the low power devices generally increases the hidden node ratio for the own link as shown in Figure 70.

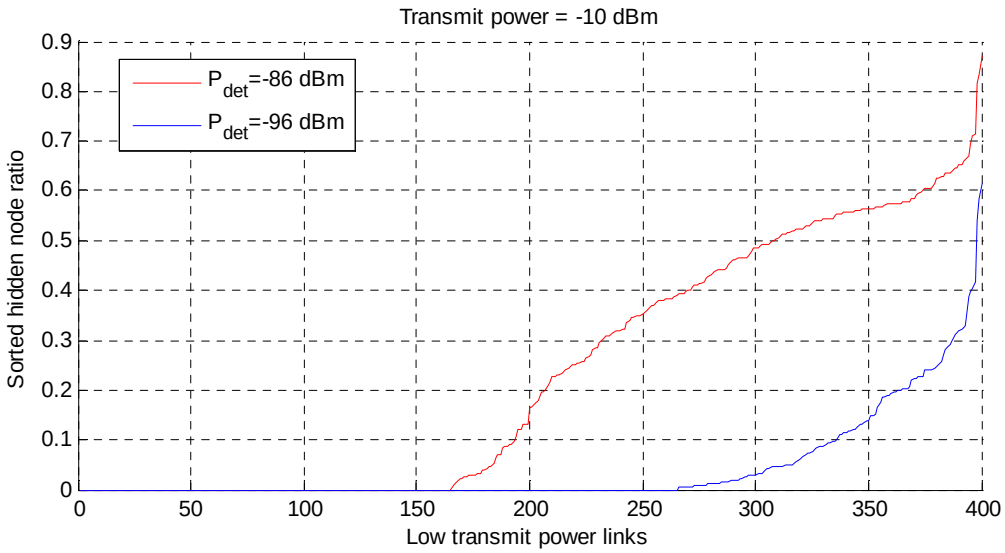


Figure 70: Hidden node ratio for a mixed power scenario with 800 devices and the same detection threshold of -96 dBm for all devices (blue line) and a 10 dB higher detection threshold for low power devices (red line)

Any additional hidden node significantly degrades the link performance, while exposed nodes typically only lead to an additional transmission delay. As most SRD applications have less stringent latency requirements, a higher threshold is not recommended.

6.5 Coexistence with multi-carrier systems

6.5.1 Slow FH systems

In slow frequency hopping systems the transmitter changes the carrier frequency according to a FH pattern known to transmitter and receiver. Typically, the *N* hop frequencies are occupied with equal probability. In this case the transmit duty cycle on each frequency corresponds to the duty cycle of the transmitter divided by the number of hop frequencies. At any point in time the multiband interferer looks like a single-carrier duty cycle random access interferer with a small duty cycle. Hence, a single-band CSMA or DC based random access schemes can coexist with slow FH links.

Using single carrier access schemes results in unequal distribution of traffic load on the available frequency bands. Non adaptive FH helps to randomize the frequency access, but cannot omit

crowded frequencies with a high number of single carrier devices. Hence, only frequency agility allows to achieve a nearly equal band usage.

6.5.2 Coexistence with systems using LBT with frequency agility

Systems with frequency agility always need to solve the problem to maintain frequency synchronisation between transmitter and receiver. Most of the SRD applications listed in section 0 require small, simple, battery power devices, so it is unlikely that the receiver can simultaneously listen on different frequency bands. Section 4.8 outlines two possible solutions to that problem.

Adaptive frequency hopping (AFH):

In a frequency hopping system the new frequency and switch time is a priori known by the receiver. A slow frequency hopping system can be combined with a LBT procedure, which performs a channel measurement prior to each transmission on a new hop frequency. In case the CCA has indicated a busy channel, the transmitter simply remains silent for the rest of the dwell time supposed that the dwell time is not significantly longer than the packet duration including on optional acknowledgement packet. A new trial is then performed on the next hop frequency with a typically different interference situation.

The collision probability of the first packet transmission is equal to the collision probability in single carrier CSMA-ACK system. Nevertheless, if at least one colliding device uses frequency hopping, the retransmissions are typically sent on different frequencies. Hence, the congestion problem can be reduced using adaptive frequency hopping and the performance will be even better due to an improved traffic randomisation.

CSMA & AFA:

Alternatively, the transmitter remains on a selected frequency and checks the channel occupation prior to each transmission. In case the number of trials and/or packet retransmissions in the past has been above a certain threshold, transmitter and receiver may agree on a frequency change in the next communication cycle. In this case, frequency changes are much slower and frequency synchronisation is obtained by communication. As packet retransmissions are always performed on the same frequency, the collision probabilities for the data packet as well as the packet retransmissions are the same for single frequency CSMA and CSMA & AFA systems. Nevertheless, CSMA & AFA always search for frequency bands with a low traffic load so that in general crowded frequencies used by fixed frequency systems are completely avoided.

7. Conclusions and recommendations

The analysis of potential SRD applications in section 3 has shown that a large group of applications require only small packet sizes of a few hundred bits and low to medium duty cycles below 1% for data transfer. Furthermore, they typically have not very stringent latency requirements as even alarm systems can cope with a delay of few hundred milliseconds, but the requested link reliability might be high. Many applications are operated indoor and a number of independent systems might be simultaneously operated within the same building, so that coexistence must be possible. However, it sometimes will be the case that the same party is operating the different systems, so that adjustments in deployment may be possible in challenging scenarios. As the majority of the SRDs will be battery operated, robust, simple, and energy efficient access schemes will be required.

Centralised resource control is known to provide a high resource utilisation, but a central control instance in one node will not be available in a scenario with simultaneously transmitting networks of different operators. Alternatively, resource allocation can be solved in a distributed manner defining a common control channel, which would be then used for neighbour detection and resource reservation. The air interface format and the protocols of the common channel need to be standardised, so that information can be exchanged between devices belonging to different networks. Nevertheless, it has to be taken into account that the number of devices might be quite large, while the duty cycle on a single link is typically small. Hence, listening to the resource allocation of the neighbour nodes and making own reservations prior to a short packet transmission might require much more energy than the transmission of the data packet itself. As the majority of the SRDs will be battery operated, the overhead required for resource control in general cannot be spent. Hence, this study focused on random access schemes.

Among the single carrier random access systems, **DC based random access** using unidirectional links for data transmission is the simplest one. This access scheme is used by applications requiring extremely low cost, small size "transmitter only" devices with low reliability requirements. Calculations as well as simulations in section 5.6.1 have shown that the maximum achievable accumulated DC in the application layer is approximately 3% for a packet loss rate of 0.1% transmitting six packet copies for each data packet to increase reliability. Thereby, the accumulated DC is the product of the number of harmful interferers and the application duty cycle on the links. For example, 30 devices with an application duty cycle of 0.1% or, alternatively, 3 devices with an application duty cycle of 1% can transmit in parallel supposed that the band is exclusively dedicated to DC based random access users. The latency will be similar to the latency in ALOHA systems with a constant repetition interval. In both systems the time interval between packet copies should be randomly selected and large enough to avoid that the new packet copy will again collide if the previous has been already lost due to a collision. The poor performance of uni-directional DC based random access justifies a strong limitation of the duty cycle on a single link, so that only a small portion of channel access time is used by this low efficient access scheme. A transmit duty cycle of 0.1% at a transmit power level of 10 dBm is proposed and even smaller transmit duty cycles are recommended for higher transmit power levels. Section 6.1 provides a formula for the relationship of transmit duty cycles and transmit power as a function of the path loss exponent.

Using a bi-directional protocol with an acknowledgement procedure can significantly increase the system performance. The device costs are slightly higher as a transceiver is required to establish the bi-directional link. Simulations presented in section 5.6.2 have shown that **ALOHA** achieves an up to 9 times higher accumulated application duty cycle than DC based random

access systems for the same target packet loss rate and the same device constellation. Additionally, the number of transmitted copies per data packet is significantly smaller if packets are only retransmitted if being lost. Hence, the power consumption for implementing the acknowledge procedure is more than compensated by the smaller number of packet transmissions, so that ALOHA outperforms DC based random access with regards to reliability and power consumption. Nevertheless, the ALOHA performance significantly depends on the scheduling algorithm for the retransmissions. The time offset in between packets should be always randomly selected, but if the mean offset is too short, the system can easily collapse. The implementation of a load dependent **backoff** procedure (e.g. binary exponential backoff) is strongly recommended.

The system capacity can be further increased using the receiver which is anyway required for the acknowledgment procedure of ALOHA systems to check the channel state prior to transmission. The assess scheme is then denoted as **CSMA-ACK**, which uses the listen-before-talk (LBT) procedure to send packets only if the channel is free. This feature can be implemented with no additional hardware costs. Simulations presented in section 5.6.4 have shown that the number of harmful interferers which can be tolerated in the vicinity of the receiver can be increased by a factor of 2-3 compared to ALOHA with linearly increasing backoff for the considered parameter settings and simulation environment. Hence, CSMA-ACK increases the accumulated application duty cycle by a factor of 2-3 compared to ALOHA, while the packet loss rate in the application layer remains almost zero. Furthermore, the number of packet retransmissions is significantly smaller in CSMA-ACK systems than in ALOHA (see Figure 56) so that the additional power consumption for the CCA measurement of the LBT procedure is more than compensated. Nevertheless, the performance of the LBT scheme significantly depends on the **LBT implementation parameters**, i.e. the minimum interferer measurement time and the dead time between the end of the channel measurement and the start of the packet transmission in case the channel has been detect as to be free. Even if the transmitter can detect all harmful interferers, a non-zero collision probability is observed as explained in section 5.6.3. Additionally, any harmful interferer which cannot be measured by the desired transmitter significantly degrades the CSMA performance, as collisions with a packet of a so called **hidden node** cannot the actively avoided. The number of hidden nodes depends on the interferer detection method and the **detection threshold setting**. Hence, LBT implementation parameters as well as the interference detection threshold need to be properly upper limited in order to guarantee that LBT significantly lowers the packet collision rate on the channel compared to a non-LBT access scheme. Anyway, the effective channel packet loss rate in a realistic implementation will always be greater than zero so that CSMA-ACK experiences a performance limiting congestion similar to the ALOHA system although the corresponding traffic load is significantly higher. Hence, a load dependent **back-off** procedure is recommended to achieve a graceful degradation instead of a system collapse.

While there is an easy trade-off between duty cycle and transmit power in non-LBT systems, the situation is more difficult in systems using LBT. In case transmitter and interferer are using the same transmit power, signal detection works equally in both directions. If the transmitter can detect the interferer, the interferer can detect the transmitter as well as the physical channel itself is reversible. This is no longer true using different transmit power levels. A low power transmitter will detect a large number of harmful interferers with a high transmit power, but only a few of them will be able to measure the signal of the low power transmitter. Hence, LBT successfully avoids a collision only if the interferer packet transmission starts prior to the scheduled transmission on the desired link, while any later start during the desired packet transmission will inevitably result in a packet collision. The performance degradation of LBT systems due to

different power levels depends on the performance of the LBT itself. Hence, a common agreement on the LBT parameters and the scenario assumptions is required prior to a decision on the duty cycle limitation for high power links. Alternatively, the spectrum may be subdivided into different bands allowing LBT with specific transmit power levels within each band.

In general, the needed transmit bandwidth of an SRD is significantly smaller than the available bandwidth in the SRD band. Section 3 has shown that many SRD applications are using data rates in the order of ten to hundred kilobits per seconds, which often is a good compromise between transmission range and energy consumption for packet transmission. Hence, a typical bandwidth is in the order of 100 kbps. Using single-carrier access schemes has the disadvantage that the spectrum is not equally exploited. Some of the 100 kHz sub bands might be much more crowded than others. Hence, the use of systems with frequency agility shall be encouraged to obtain equal spectrum exploitation. Potential implementations of LBT&AFA have been described in section 4.8.

In order to enable a high number of simultaneously operating devices, the duty cycle on a single link needs to be limited. For systems using single carrier, **DC based random access on uni-directional links** the duty cycle limit should be very low:

- Transmit DC of 0.1% might be reasonable for systems without LBT
- Duty cycle is independent of the signal bandwidth
- Allow higher transmit power at the cost of a lower duty cycle
- Define maximum Ton and minimum Toff time

In order to maintain the same number of devices, the duty cycle of **non-adaptive FH** should not be higher than the duty cycle of a single carrier system. In this case, the duty cycle on a hop frequency is equal to 0.1%/*N*, supposed that *N* is the number of hop frequencies and all frequencies are equally used. As FH helps to randomize the channel load over the frequency band, a higher duty cycle limit might be applied to promote FH systems and thus drive the resulting capacity increase. It is recommended to specify a minimum frequency separation in the order of the typical signal bandwidth of single carrier systems.

- Transmit DC of 0.1%, maybe higher to promote FH
- Minimum frequency separation of 100 kHz recommended

For systems using bi-directional links with **acknowledgement procedure** the following rules are proposed:

- ACK packets shall be allowed to be transmitted without LBT
- ACK packet length and response time shall be added to the packet length of the transmitter for DC calculations
- Application duty cycle shall be 0.1% including ACK
- Number of retransmissions shall be limited by duty cycle restriction or load dependent backoff procedures for packet retransmissions need to be defined
- Define maximum communication time and minimum T_{off} time

Systems should be encouraged to use **LBT** to increase the efficiency of resource usage. As the performance of the LBT procedure significantly depends on the interferer detection reliability and the implementation parameters, these parameters shall be specified.

- Energy detection is recommended as interferer detection method
- Detection threshold shall be in the order of the typical receiver sensitivity level
- Detection threshold shall be no function of the transmit power
- It is recommended that the minimum required interference measurement time and the dead time are specified
- The duty cycle of LBT systems shall be 10 times higher than the duty cycle of non-LBT systems
- Different power levels lower the LBT performance. Duty cycle restrictions for high power devices shall be carefully selected and shall be more restrictive for LBT than for DC based random access systems. Alternatively, the SRD band needs to be separated into subbands with different power levels.

It is expected that a significant part of SRD applications will be single-carrier systems due to cost and complexity limitations. In general, the SRD band is not equally exploited using single carrier systems. Hence, the resource usage can be significantly improved by adding systems with a combination of listen before talk and frequency agility (**LBT & AFA**), as they will increase the traffic load on sparsely used frequency bands. As frequency agility helps to protect fixed frequency access systems, it shall be promoted by a higher duty cycle limit.

- The duty cycle limit of LBT&AFA systems shall be higher than the duty cycle limit of LBT systems.

In general, it is recommended that a maximum communication time (T_{ON}) followed by a quiet time period (T_{OFF}) time is defined to make sure that other users can intervene and start their own transmission during the quiet time period. The maximum T_{ON} time should consider the latency requirements of SRD applications.

- T_{ON} shall be smaller than 50 ms.

Operation of high duty cycle **DSSS/ fast FH** in parallel to a LBT system is not recommended, as the threshold of the LBT should not be increased to cope with wideband signals. This would significantly degrade coexistence with other LBT devices.

- DSSS/ fast FH should be subject to transmit duty cycle limitations.

Some applications cannot be operated in parallel to low duty cycle, random access schemes. For example, a separate band shall be foreseen for audio systems with 100% duty cycle transmissions. In order to exploit the frequency band in the absence of audio applications, LBT & AFA shall be allowed even in this special band.

Furthermore, SRD applications requiring low latency and high reliability (e.g. industrial automation) cannot be operated in parallel to random access schemes. Hence, the SRD band can be only used in protected areas, where the access of SRDs is controlled by the premises owner. Otherwise, high data rate standards with guaranteed access for example in the 2.4 GHz band should be used.

The situation is slightly different for alarm systems like fire or intruder alarm, because the latency requirements are less stringent. Lost packets can be retransmitted based on acknowledgement procedures. If necessary, one could even think about different backoff procedures for safety-related applications to reduce the collision probability with a standard SRD application. Alarm systems themselves can implement redundancy, so that an alarm can be received by different devices with typically different interference situations. Most importantly, frequency agility can be used to select less congested channels for system operation. Hence, in general it should be possible to design highly reliable alarm systems without assigning a dedicated frequency band. Nevertheless, there is no guarantee in license-except bands, so there is always a certain channel load which will hamper a successful communication. Therefore, it might be reasonable to specify a small exclusive portion of the spectrum for very sensitive safety related applications like social alarms at the cost of a slightly lower spectral efficiency, which always results from splitting the SRD spectrum into different bands.

List of abbreviations

AAL	Ambient Assisted Living
ACK	Acknowledgement
ALD	Assistive Listening Devices
AFA	Adaptive Frequency Agility
AFH	Adaptive Frequency Hopping
ALD	Assistive Listening Device
AMR	Automatic Meter Reading
CCA	Clear Channel Assessment
CD	Collision Detection
CDMA	Code Division Multiple Access
CSMA	Carrier Sense Multiple Access
DAA	Detect And Avoid
DC	(Transmit) Duty Cycle
DC_{APP}	Application Duty Cycle
DFS	Dynamic Frequency Selection
DLL	Data Link Layer
DSSS	Direct Sequence Spread Spectrum
ECC	Electronic Communications Committee
ECG	Electrocardiography
ED	Energy Detection
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FFH	Fast Frequency Hopping
FH	Frequency Hopping
HF	High Frequency
IA	Industrial Automation
ISM	Industrial, Scientific, Medical
ITU	International Telecommunication Union
LBT	Listen Before Talk
LF	Low Frequency
MAC	Medium Access Control
NF	Noise Figure
OSI	Open System Interconnections
PC	Personal Computer
PCC	Personal Car Communication
PD	Preamble Detection
PHY	Physical Layer
PLL	Phase Locked Loop
PLR	Packet Loss Rate
RFID	Radio Frequency IDentification
RSSI	Received Signal Strength Indication

SFH	Slow Frequency Hopping
SINR	Signal to Interference plus Noise Ratio
SNR	Signal to Noise Ratio
SRD	Short Range Device
TDMA	Time Division Multiple Access
TPMS	Tire Pressure Monitoring System
UHF	Ultra High Frequency
UWB	Ultra Wide Band
WLAN	Wireless Local Area Network