Table of Contents

Introduction .................................................. 1
Quality requirements and indicators for excellent WLAN radio networks .......... 1
Use of IEEE 802.11 WLAN in industrial applications .................................. 2
WLAN basics and their effect on performance capacity ............................. 4
   Media access methods and coexistence ........................................ 4
   Use of frequencies and channels ......................................... 4
   Modulation schematics, MCS and rate adaptation .......................... 5
Selecting the right antennas .......... 6
New technologies to improve WLAN performance ...................................... 7
   Improved throughput by way of Adaptive Noise Immunity (ANI) ........... 7
   Adaptive RF Optimization .............................................. 7
   Band Steering and Client Steering ..................................... 8
   Airtime Fairness .................................................................. 8
   Use of parallel WLAN connections to increase reliability .................. 8
   Fast roaming ................................................................... 9
Summary ......................................................................... 10
References .......................................................... 11

Introduction

Today, IEEE 802.11 wireless networks are used in a variety of industrial applications. In particular, this technology is characterized by long range and high transmission speeds. The basis for a stable and powerful WLAN is, of course, a suitable network design with appropriate installations and configurations. Because of the many influential factors and configuration options, however, it is not always obvious how a WLAN can be optimized to meet the requirements of industrial applications. This article provides an overview of the factors that determine the quality of a WLAN and provides technical options for improving the quality of new and existing industrial wireless networks. It presents established techniques for optimization, as well as the latest technical options with the most modern equipment, addressing the requirements of industrial applications in particular.

Quality requirements and indicators for excellent WLAN radio networks

Wireless LANs offer many new options for addressing the growing demands of industrial applications. On the one hand, they are an installation-friendly option for providing network communication for facilities in fast-changing environments. On the other hand, the use of IEEE 802.11 networks allows previously unreachable or very expensive-to-reach devices or facility components to be connected without loss. Directed IEEE 802.11 wireless connections can link industrial plant components, even over long distances. Moreover, the use of mobile devices such as tablets and notebooks opens up new possibilities for maintaining, configuring and monitoring industrial applications. However, industrial applications place many demands on the quality of a wireless network, which go far beyond the requirements in offices and homes. Important quality indicators for an IEEE 802.11 network are:

a) packet loss rate - the percentage of sent messages (or packets/frames) that are not successfully received by the intended recipient

b) latency - the delay in transmission for the delivery of a message via a wireless connection
Generally, communication is possible with measured on a logarithmic scale in dB. In general, the signal-to-noise ratio is a representation of the SNR. Slowly and clearly. Figure 1 shows a graphical representation of how conversations at a party. If the signal-to-noise ratio is high, clear communication can be visualized by the example of how much louder the voice of the conversation partner is than the ambient noise and other conversations at a party. If the signal-to-noise (SNR) ratio is high, clear communication can take place at higher speeds. If the SNR is low, it is difficult to differentiate the signal from loud noises. In this case, the WLAN devices can communicate with each other only when they transmit their data very slowly and clearly. Figure 1 shows a graphical representation of the SNR.

In general, the signal-to-noise ratio is measured on a logarithmic scale in dB. Generally, communication is possible with the lowest data rate in a WLAN with an SNR of 6 dB (for example, at a noise level of -86 dBm a signal of -80 dBm is sufficient). High-quality WLAN devices allow the display of the current SNR via the web interface or via SNMP (Simple Network Management Protocol), so that this value can be taken into consideration when optimizing the WLAN.

Use of IEEE 802.11 WLAN in industrial applications

The following four industrial use cases serve to illustrate the influence of these quality characteristics in practice and demonstrate the broad applicability of WLAN in the industrial environment:

Coverage of facilities for monitoring and control of machines and components

Many plants today allow monitoring and control over the network. Whether using a notebook with special software or a tablet with an app, the use of mobile devices via WLAN connections makes it easier for users to operate and maintain machinery and equipment. Interactive services, in this case, require a high bandwidth, e.g. for the transmission of video data, 5 Mbit/s are required for each HD video stream and additional reserves are needed for the parallel use of the WLAN system by multiple users. Plus, moderate reaction times (e.g. < 100 ms) are required for efficient interactive service. Depending on the system, innovative applications such as augmented reality increase the requirements even more. High bandwidths (>10 Mbit/s per AR system – often in both directions) and short latencies (<50 ms) are important for sufficient quality in these cases. Likewise, good availability of the wireless network at all production points is necessary. Therefore, the core requirements for future-proof WLAN provision in a production facility are: high data throughput, low latency and good coverage.

Connection of plant components

Due to the rapid transmission of WLAN signals and the high range of directional WLAN connections, the WLAN transmission standard is ideally suited as a technology to connect individual plant components that are spatially distributed. WLAN directional radio paths can even connect networks that are several kilometers apart. Therefore, the range of a radio system is often of crucial importance. The latency and throughput of a connection are also important for ensuring a smooth operation. In addition, depending on the frequency band used in outdoor applications, aspects of radar detection must be taken into account. For applications that are sensitive to the loss of individual packets, redundancy techniques should be considered. Since many applications often share the point-to-point route, higher throughputs (> 100 Mbit/s) are usually required.

Coupling of trains and movable system components

Much like the connection of spatially distributed system components, IEEE 802.11 wireless networks can also bridge shorter distances. This especially makes sense if the use of cables is not possible due to adverse conditions. A good example of such an application is in the coupling of trains. Due to the mechanical stress on the connection between two cars, the digital interfaces between them must be very resilient (see Figure 2). In many cases this prevents broadband transmissions over fast but sensitive Ethernet cable. WLAN connections can help in this situation,
because transmission from car to car is possible even without physical contact. With the high data rates, broadband applications such as passenger Internet access or HD video monitoring can be transmitted beyond the confines of the cars (see Figure 3). Again, it is important to achieve the required quality in the latency and throughput. If a live image is to be transmitted, generally a latency of less than 100 ms is required. If multiple HD video streams are transmitted via the radio path, high throughputs of >50-100 Mbit/s are needed.

### Train-to-ground communication

WLANs are not only for use between the cars of the train, but also for communication between trains, streetcars, subways and the track-side infrastructure along the tracks. The network of a train—in passing—can be connected via special WLAN clients in the train with different access points along the route. The range of the access points and the WLAN client are particularly important for the reliability and efficiency of such a system, as is the duration of the interrupted connection if the WLAN client on the train switches the connection from the current access point to another access point along the route. To this end, mechanisms for fast roaming (switching between different access points) are needed. Interruptions of only a few milliseconds (<50ms) are generally necessary. If sufficiently fast roaming cannot be achieved, this often leads to interruptions when the train passes by the access points along the route. The roaming described is also used in a somewhat defused form in the connection of mobile system components, such as in forklifts, cranes, cable car gondolas, etc. Due to the lower speeds (compared to trains) of these mobile units, there are generally fewer
situations in which the access point needs to be switched. Nevertheless, a disconnection related to roaming also has a negative impact on these applications and their availability and reliability.

**WLAN basics and their effect on performance capacity**

The four application situations presented clearly show that there must always be a balance between the various performance characteristics of a network. Obviously, general availability and sufficient reliability are important. However, the transmission delay (latency) and the throughput of a WLAN communication link play a crucial role for the application. However, which technical aspects of an IEEE 802.11 wireless network influence these parameters? In the following, we will briefly discuss the technical basics of WLAN communication and how they determine the individual parameters. The security aspect will be discussed only in passing, as it hardly has any negative impact on the performance of the WLAN today. However, secure operation is an obvious fundamental requirement of a wireless network. We will address only the technical options of WLAN devices (mainly access points) and will not discuss the requirements and procedures for comprehensive coverage and basic WLAN planning. Sufficient coverage of the area, of course, is a basic requirement for the optimizations discussed in the following.

**Media access methods and coexistence**

In contrast to other radio technologies, IEEE 802.11 wireless networks use a CSMA/CA (Carrier Sense, Multiple Access/Collision Avoidance) access method. As the sequence of these letters already suggests, the selected channel is listened to first to determine if there is a competing transmission. If the radio medium is perceived as clear, a WLAN device, known as a station, can start to send. If the medium is occupied, there is a waiting period until the medium is clear. The receiver sends an acknowledgment after successful receipt so that the transmitter can identify packets (so-called frames) that have failed or been successfully received by the recipient. If no acknowledgment is received, the transmitter can deduce that the delivery of the packet failed (for example, from simultaneous transmission of a second station). In such case, the sending station retransmits the lost packet. If the retransmission fails several times successively, the transmitting station terminates the transmission and transmits the next packet. This original packet must then be considered lost or undeliverable. This basic pattern of behavior affects all WLAN enabled devices and provides the basis for wireless data transfer with WLAN connections.

The method described directly affects the expected parameters, such as transmission delay and packet loss. In largely interference-free situations, packet loss rates of WLAN connections in the range of 0.1% can be achieved easily, since most of the transmissions can be received without interference. In more disrupted (noisier) situations, typical error rates may reach ranges of several percent. Moreover, disrupted transmissions also have a direct impact on the transfer time, the so-called latency. Senders often need to send a packet multiple times before successful reception if the network is too noisy. Furthermore, in disrupted situations, the medium is often already occupied by other transmitting stations, so that there is a waiting period before a transmission can begin. Therefore, an important issue in the optimization of a wireless network is: how systematic disruption of transmissions (for example, through a congested channel) can be avoided from the outset or how a successful transmission can be made possible even in noisy situations. One option for achieving this is by using a different frequency range, for example.

**Use of frequencies and channels**

The first basic decision affecting network quality is the choice of which radio transmission frequency range to use. IEEE 802.11 wireless networks make it possible to use different frequency ranges. Thus, frequency bands in the range of 2.4 GHz and 5 GHz, for example, are available for wireless transfers. These frequency ranges are divided into channels. A channel represents a 20 MHz-wide section of the frequency spectrum. The choice of the frequency band has a significant impact on the range and frequency of interference caused by neighboring networks. Likewise, the choice of the frequency band determines the coexistence mechanisms that must be used for sharing with other users of the frequency range.

A vast number of different radio systems use the frequencies of the 2.4 GHz frequency band. On the one hand, this leads to a higher load on the radio channels, on the other hand it has resulted in strict regulatory requirements for compliance of coexistence mechanisms in Europe (see Figure 4). Since the enactment of the standard ETSI EN 300 328 V1.8.1, wireless systems must comply with even more stringent requirements when accessing the 2.4 GHz frequency band. One goal of the more stringent requirements is improved coexistence of the different wireless communication systems that are used in the 2.4 GHz band. For this reason, the receiver module of a device operating in the 2.4 GHz band must be able to adjust to the environment in order to identify other active transmission systems in the current channel. If the transmission of a coexisting system is detected, the sender must delay its own radio transmissions until the medium is free again. So that a transmitter doesn’t occupy a channel for too long, thereby gaining an advantage in the bandwidth it occupies, the following additional requirement is defined in the standard ETSI EN 300 328 V1.8.1. A maximum time for the transmission of radio signals must be adhered to, depending on the access mechanism used. Compared to other radio technologies, these requirements can be fulfilled relatively easily with WLAN connections. The CSMA-based access mechanism already provides for the testing on an occupied channel, so that the adaptation to the environment is reduced to a fine adjustment of the receiving level sensitivity. Due to the packet-based transmission, the maximum access time can also be maintained precisely. Therefore, due to the propagation characteristics, the 2.4
GHz band is suitable for use in industrial scenarios despite an often higher disruption frequency. In particular, radio waves in the 2.4 GHz frequency range penetrate walls and obstacles better than radio waves in higher frequencies.

The frequencies of the 5GHz band are often less burdened by competing networks, since other radio technologies such as Bluetooth, cordless phones and more favorable WLAN solutions are often limited to the 2.4 GHz band. However, using the 5GHz band also provides several challenges: First, the radio waves, because of their higher frequency, are significantly more affected by physical obstacles. Therefore, the range of 5GHz WLAN transmissions in buildings or industrial plants is usually slightly lower than that of a comparable transmission in the 2.4 GHz frequency range. On the other hand, depending on the frequency selection, coexistence mechanisms for frequency sharing with radar systems are needed in Europe. Channels 36, 40, 44 and 48 (5.15-5.25 GHz)\(^2\) are not affected by this, but these channels are only approved for use in buildings (indoor use). Other channels [5.25-5.35 GHz, 5.47-5.725 GHz], e.g. the channels from 52 to 64 and from 100 to 140, can also be used outside. Each country’s regulatory authority can release a part of the frequency band between 5.15-5.25 GHz and 5.875 GHz for WLAN use. In Germany, channels 155 to 171 (5.765-5.865 GHz)\(^2\) from this frequency band are reserved for permanent fixed WLAN installations that provide broadband Internet access to rural areas and therefore cannot be used by every operator.

When using outdoor channels in the 5 GHz range, the devices must detect radar systems and, if necessary, withdraw from the frequencies used by the radar system.\(^3\) The radar detection and possible change of the transmission frequency may have direct effects on the availability of the network. On the one hand, before a channel is used, it must be scanned for one minute for radar patterns. Additionally, the channel must be released immediately when radar patterns are detected during operation. This means that the entire WLAN must automatically switch to another channel in the 5 GHz range. This generally leads to a brief interruption of the entire communications network. The frequency bands also differ in their permissible transmission power. Generally, it can be said that the frequency bands in the 5 GHz range allow a higher transmission power than the 2.4 GHz frequencies. In any case, however, it is worth comparing the data sheets of WLAN products and the statutory requirements in order to fully exploit the potential of the regulatory framework.

The different characteristics and regulations in the various frequency bands offer potential for optimizing a WLAN. If the effects of radar detection are acceptable or if the WLAN is an indoor installation and the range is adequate, the 5 GHz band is preferable in most situations. Since many WLAN access points and clients support both 2.4 GHz and 5 GHz operation, an experimental change to the other frequency bands may improve WLAN performance and reliability. This improvement can be measured by comparing the signal-to-noise ratio or can be determined by observing the packet loss rates. However, it should be noted that some antennas are optimized to support either the 5 GHz or 2.4 GHz band. Therefore, checking the data sheets of the used access points and antennas before the test is worthwhile.

### Modulation schematics, MCS and rate adaptation

In WLAN systems, the signal quality (the SNR) between access points and clients can change frequently. The SNR is determined by many factors. For example, the following have a direct influence on the relationship between the useful signal and ambient noise: a) the distance between the access point and client, b) the interference from other radio systems, and c) the environment and spatial geometry (e.g., large metal machinery and metal supports). Since the signal-to-noise ratio cannot be accurately predicted at the outset, WLAN offers different adaptation mechanisms to achieve the highest transmission power for a given situation. Thus, the modulation mechanisms, i.e. the way in which data is transmitted as radio signals, is automatically selected depending on the signal quality. Generally speaking, a higher transmission rate also always requires a better signal-to-noise ratio. Lower transmission speeds are also associated with a poorer signal-to-noise ratio.

Since the introduction of IEEE 802.11n\(^4\), various techniques for increasing the transmission rate have been grouped...
in so called modulation and coding scheme (MCS) classes. MCS 0 stands for the slowest and most robust transmission rate while MCS 23 is the fastest IEEE 802.11n data rate that can be achieved with 3 antennas, and MCS 31 represents the fastest data rate that can be realized with four antennas. The resulting maximum data rates, with all other WLAN optimizations, amount to 15 Mbit/s at MCS0 and 600Mbit/s at MCS31. An important component of this data rate is the number of spatial streams. Simultaneously, with multiple antennas, the Multiple-Input-Multiple-Output (MiMo) technology allows for interference-free transmission of multiple signals on the same frequency. Thus, an access point with only one stream and one antenna at IEEE 802.11n, for example, can transmit a maximum of 150 Mbit/s, while an access point with two streams can transmit 300 Mbit/s. Three or four streams increase the throughput further to 450 Mbit/s with three streams and antennas and to 600Mbit/s with four streams and antennas.

In industrial plants, bandwidth requirements don’t often change. A dynamic adaptation of the transmission data rate towards the fastest data rate (and the one most prone to interference) may even have an adverse effect. An adaptation of the data rate to the best possible transmission rate can lead to the selection of a less robust transmission method and thus to higher packet loss.

In particular, when there is frequent change between different data rates, as can be observed in mobile scenarios, for example, this leads to a fluctuating rate of packet loss. Therefore, for high-quality WLAN access points, it is possible to fix the maximum transmission rate setting (that is, the highest MCS that a station may use). If data throughput of only a few Mbit/s is required, a maximum transmission rate of MCS 10 or MCS 17, for example, can be set. With these robust data rates, data throughputs up to 45 Mbit/s can be achieved in practice, while the required received signal quality is significantly lower than the signal quality of more complex modulation schemes. Such fixed maximum data rates make the behavior of a WLAN system, especially if it contains mobile clients, significantly more manageable. This has a positive effect on the packet loss rate and the variance in the transmission delay (jitter). The change between the modulation and the coding schematics thus allows the freedom to configure a WLAN system beyond traditional optimization in the office environment to the highest data rate possible.

Selecting the right antennas

The selection of the right antennas plays a decisive role in the performance of a WLAN installation. Depending on the emission characteristics, different antennas are appropriate for very different applications. Omnidirectional antennas transmit their signal in all directions and thus detect the counter signal from all directions. Directional antennas radiate primarily in one direction and amplify the counter signal coming from this direction significantly more than an omnidirectional antenna. For this reason, directional antennas are deaf in all other directions. Depending on the antenna, the signal can achieve varying amplifying performance (see Figure 5). While small rod antennas usually only amplify by 2–3 dB, higher quality directional antennas can achieve amplifying performance from 10–20 dB. Since the antennas are responsible for a significant proportion of the transmission signal amplification, they contribute significantly to the signal-to-noise ratio and thus to the range and speed of the WLAN connection.

In addition, the selection of the antenna is affected by the number of spatial streams that the antennas support. This problem arises particularly in panel antennas which can be connected to multiple antenna outputs of a WLAN access point. Thus, it is possible that a panel antenna can only be connected to one antenna output, while the other outputs must be disabled. In this case, the achievable data rate is reduced to the value achievable on one stream. Thus an access point, for example, which can reach 450 Mbit/s with three streams, may only reach 150 Mbit/s with the wrong antenna. If an antenna supports multiple streams (for example, by installing several emitters separated from one another by

![Figure 5: Various antenna characteristics. Omnidirectional antennas emit in all directions. Directional antennas amplify in a spatial direction. Antennas with multiple polarization axes transmit radio signals simultaneously in MiMo operation](image-url)
different polarizations), then the access point can reach its full potential in MIMO operation with the antenna as well.

The selection of the frequency band also affects the selection of the right antennas. Some antennas are suitable for both the 2.4 GHz band and the 5 GHz bands, while other antennas reach their full amplification in only one of the two frequency ranges. A look at the relevant data sheet provides clarity in these cases. Particular attention is required when converting the frequency band to be used, since otherwise the coverage and the quality of the WLAN may suffer in the case of unsuitable antennas.

The choice of antenna ultimately depends on the planned function of the network (see Figure 6). If two access points are to function as a WLAN bridge and communicate with one another, then directional antennas are best. Likewise, a directional antenna can be successfully used to cover an area in one direction. For mobile applications as well, in which a client moves on a specific route (e.g. in rail transport), directional antennas are well-suited to provide greater spatial coverage along the route. Omnidirectional antennas can be used in any situation where it is not clear where the signal is coming from. For this reason, a non-directional antenna is generally used for automated guided vehicles because it allows the vehicle to rotate freely in all directions without losing the connection. The use and optimal placement of suitable antennas enables significant improvement of the SNR and the overall performance of the wireless network. However, such an optimization step requires a higher level of expertise and greater planning efforts.

A reconsideration of the current antenna setting is worthwhile in any case since it may reveal future optimization potential.

**New technologies to improve WLAN performance**

In addition to the previously discussed basic optimization steps, various WLAN systems offer some further optimization possibilities. These require either special hardware or software and are, therefore, only available on certain WLAN products. The current industrial BAT WLAN devices from the Hirschmann access point family provide the greatest flexibility for using these technologies.

**Improved throughput by means of Adaptive Noise Immunity (ANI)**

In industrial environments, electromagnetic signals often occur in the frequency bands used by WLAN connections. Sources of these signals can be other wireless transmission systems, for example, Bluetooth, ZigBee or ISA100 used for networking sensors. Emissions from machines and devices installed in the plants are also a possibility. In these difficult environments, the performance of WLAN systems can be limited because the WLAN devices detect interfering signals as possible WLAN signals and try to receive and decode them. Consequently, subsequent transmissions can be missed by the receiver, since it is still erroneously attempting to decode the interference signal as a WLAN transmission. The receiving unit is then busy processing meaningless interference pulses and misses the actual WLAN transmissions. Furthermore, its own transmissions may be delayed, since the search for an open transmission time within the CSMA/CA media access method is erroneously perceived by the medium as occupied. This unnecessary waiting also results in reduced data throughput, although the transmission channel could provide more capacity.

With high-quality access points, enabling the Adaptive Noise Immunity (ANI) mechanism helps to hide such disruptive influences and thus improves the throughput possible. The interference is hidden by means of adaptive control of the reception sensitivity achieved by the WLAN radio module continuously providing measurements of interferences in the active channel. This reduces the likelihood of the receiver perceiving an otherwise interfering signal as a possible WLAN signal and processing it incorrectly in the receiver. As a consequence, the number of missed transmissions at the receiver, as well as the occurrence of transmissions with a delayed start, is reduced, thereby optimizing the utilization of the transmission medium.

**Adaptive RF Optimization**

For trouble-free operation of a WLAN system, external interference must be minimized. For this reason, it is recommended to adapt the choice of the radio channel at an access point to its environment. Interference can also, for example, represent neighboring access points whose radio ranges overlap on the same channel. In this case, the users in this area must share the entire available bandwidth (shared medium), increasing the likelihood of mutual transmission interference. Depending on the environment of the installed WLAN system, it is possible that external interferences can change dynamically and the configuration must be adapted accordingly. Modern access points provide an automatic mechanism that evaluates the interference in the current environment and switches to a higher-quality channel if necessary. This ensures the highest quality possible, even without manual administrative intervention. Even with long-term operation of wireless networks in a manufacturing plant, after
re-installation of another competing radio system, trouble-free operation of the wireless network can be achieved through automatic fallback to appropriate channels. However, this automation may be undesirable if the frequency for the different radio networks of a manufacturing plant is planned manually. In the case, the mechanism should not be used. This mechanism is supported from version 9.20 of the Hirschmann WLAN operating system HiLCOS.

**Band Steering and Client Steering**

Especially in scenarios with many access points and clients, it is useful to distribute these clients among the various usable frequency ranges in the WLAN system. An example of this could be an access point on the factory floor that supplies various tablets with network connections. When used in a train, an access point can provide passengers with access to the network. If this access point has several WLAN modules, it makes sense to steer clients that can communicate in the 5 GHz range onto this frequency band as well – even if they would normally prefer to connect to the WLAN module in 2.4 GHz. Such a shift reduces the load on the traditionally more heavily loaded 2.4 GHz band and enables systematic use of the 5 GHz band that often has a smaller load. Modern access points allow such an automatic shift by preferably responding to multi-band capable clients in the 5 GHz band to relieve the often overloaded 2.4 GHz band.

In controller-guided networks with many access points, client steering achieves a similar effect as band steering (see Figure 7). In this case, clients are not moved from a full frequency band into a less-loaded frequency band, but are shifted from overloaded access points to less loaded access points in the environment. This is accomplished by a selective response of the less-loaded access points to connection requests from the client. This results in an even distribution of the radio load in the wireless network and less disruption from interfering transmissions.

**Airtime Fairness**

Adjacent clients on a IEEE 802.11 wireless network often compete for the available bandwidth. A high density of clients not only creates a need for more bandwidth than is available, but also allows „slow clients“ to outmaneuver „faster clients“ with the transmission of their data. „Slow“ clients are those who can only send or receive signals with a low data rate, since these do not yet support the modern radio standard IEEE 802.11n or the SNR is not sufficient for a higher data rate. In comparison, the transmission of a packet encoded with a low data rate will accordingly occupy the channel for a longer time. The WLAN media access method, however, intends to give each participant an equal opportunity to access the channel. However, it does not account for how much time a user actually needs with his transmission process. Thus, the medium is occupied longer with transmissions to and from slower clients than with transmissions that can be completed very quickly using high data rates. The „airtime fairness“ method ensures a more efficient use of the available bandwidth for communication from the access point to the client. This method is realized by controlling the queue of packets to be transmitted at the access point. Slow clients are served with correspondingly fewer packets, so that almost equally long access times result in comparison to connections with fast clients. This way, clients can move more data in the downstream since they can use the channel for a longer time. Airtime fairness is available on all Hirschmann access points from version 9.20 of the HiLCOS WLAN operating system.

**Use of parallel WLAN connections to increase reliability**

For transmissions using radio technology, packet losses are always a major issue because the packets either arrive with insufficient quality or are disrupted by simultaneous transmissions from other users. However, the reliability of WLAN transmission can be drastically improved by using the Parallel Redundancy Protocol (PRP). With PRP, packets can be transmitted simultaneously over two independent radio links. In case of an interference in one radio link, PRP ensures secure delivery of the packet via the second link. With an interference-free transmission over both links, twice-received packets are sorted out before they are forwarded. Figure 8 illustrates this process. Despite interference in the transmission of packets 2, 4 and 6, there is no loss due to the double transmission. Actual packet loss only comes about when there is simultaneous interference in both transmissions of the packet. Only in this case is packet loss visible to the receiver. The power of this approach can be illustrated by an example calculation:

![Image of Band Steering](image-url)
Assuming that the loss rate without double transmission on both paths would be identical and would amount to 0.1%, the rate of the PRP overall system is only 0.0001% ((0.0001 x 0.0001) = 0.000001)—a 1000-fold better value. In practice, improvements can be achieved in the range of 500-fold (depending on the loss rates of the two individual paths).

PRP not only improves the reliability of WLAN connections but also reduces latency and jitter, since the faster of the two duplicates will be forwarded in each instance. If a WLAN path is not ready for transmission, the transmission can take place on the other path if necessary. Therefore, when using PRP, the resulting latency via WLAN is as good or better than the latency of the better of the two radio paths. The same applies to the jitter, the variance in the transmission delay. The jitter of the PRP transmission is also just as good or even better than the jitter of the better of the two paths.

PRP has to be specially supported by access points and clients and requires WLAN devices with two radio modules. The OpenBAT products from Hirschmann support this technology. Through the dramatic quality gains, the use of PRP in wireless networks opens up new applications of wireless transmission in the field of functional safety, e.g. as a significantly more reliable black channel (non-secure transmission path). Thus, it is worth including a redundant PRP WLAN path to make new radio paths more reliable or to upgrade existing radio paths.

Fast Roaming

Fast and reliable roaming is an important quality requirement for industrial WLAN systems, mainly in application scenarios with mobile clients, such as in trains (train-to-trackside communications), automated guided vehicles or other autonomous vehicles in the manufacturing industry. In these cases, a mobile client moves through the transmission ranges of several access points and the reliability of the communication and the available bandwidth must be guaranteed at all times (see Figure 9). Ideally, to optimize bandwidth, neighboring access points with overlapping radio coverage operate on different channels to minimize interference. A mobile client can then automatically connect to the access point with the best signal. Fast roaming between WLAN access points has been possible for a long time. Interruptions of less than 50 ms can be achieved in the 2.4 GHz band—but even faster roaming or roaming in the 5 GHz band requires some technical tricks.

Over time, continuous (necessary and important) security improvements have been added to the WLAN transmission standard. Today these improvements provide for very high security in IEEE 802.11 networks. But this security comes at a price: the connection setup and connection switching between access points is slower because the necessary security parameters must first be negotiated and exchanged. Here too, a certain level of technical trickery is needed to create both a secure and fast WLAN when roaming. In order to ensure both a fast and secure exchange, two problems must be solved: a) How can the mobile client switch as quickly as possible from access point to access point? and b) How can the time for the negotiation of security parameters be minimized? The answers to these two questions are discussed in the following.

Fast roaming through reduced scan times

When roaming between two access points, a client must first identify the target access point before switching the access point. This identification is a complex process. In order to avoid mutual interference between the neighboring access points, the target access point is typically operated on a different channel (i.e. a different frequency). However, a client can only receive the access points on the current channel. Therefore, when switching access points, the client must deactivate their current communication link in order to search other channels/frequencies for suitable access points. A mobile client must therefore periodically scan all eligible channels or frequencies to get an idea of the signal strengths of the other access points in the client’s environment. Only with this information can an access point decide whether there is a possible connection with a better
Quality than the present quality and then initiate the roaming process. Depending on the client’s mobility and the associated changes in the environment, the scanning processes must be performed repeatedly. Since the active connection cannot be used during these scans, it is not possible for the client to transfer the packets for industrial application during the scan. The network is not available during this time. For this reason, scan processes should be as short as possible. Therefore, it is important to use appropriate techniques to help reduce the scan times.

One way to keep the scanning time low is active scanning. In this method, the client issues a probe request on each channel to determine the possible access points. The client repeats this process for each channel. This way, in a short time the client identifies all potential roaming targets in his environment. If channels are used in which radar-detection is required (e.g. for outdoor operation in the 5 GHz band), this results in a problem. In these channels, active scanning with probe requests is prohibited because the proper operation of radar stations could be disrupted with the sending of the probe request. Therefore, first it must be determined whether there are primary users on the corresponding channel (for example, a radar station). Since this process must be performed again and again, and this determination requires a minute of passive eavesdropping, this is not an option for fast roaming outdoors. The client is therefore obliged to sequentially listen to all existing channels until the access points announce themselves. Each access point performs this announcement operation periodically, using so-called beacons. The scan duration for each channel depends on the period between of the beacon messages sent from the access point and the corresponding maximum waiting time of the client. Using the standard values, widely used in wireless LANs, quickly results in a scanning time of several seconds. This results in a disruption of the roaming of several seconds—a generally unacceptable value.

The faster the access points repeat their beacons, the faster the client can switch to the next channel without overlooking an access point. Therefore, for an operator, it is a great advantage to be able to configure, not only the period for sending beacon messages to the access point, but also to adapt the maximum waiting time of the client. With access points and clients specially optimized for fast roaming, the beacon and scan times can be fine-tuned. Thus, very fast roaming is facilitated by very fast beacons and very short scanning, even in outdoor operation in the less congested 5GHz band.

The current Hirschmann access points of the BAT and OpenBAT series support these settings that are specifically designed for the demanding requirements of rail traffic. In some countries, regulatory authorities permit targeted limitation of the channels to be scanned. In addition, multiple access points can be used for simultaneous roaming on the vehicle. The OpenBAT devices support roaming with multiple WLAN modules and simultaneous use of PRP that guarantees completely uninterrupted roaming (for fast scan times).

**Secure Fast Roaming**

If a client decides to switch its connection to an access point with better reception, it will initiate the procedure for the fast BSS (Basic Service Set) transition defined in the IEEE 802.11 standard, i.e. roaming. The security of a WLAN connection can only be guaranteed if a client properly authenticates at the access point when connecting and if a valid key for this connection is provided for encryption of the data packets. This takes time and must (insofar as no special techniques are used) be repeated with every roaming process. Fast roaming is therefore only possible using a fast authentication mechanism. Modern access points support an acceleration of roaming through proactive distribution of key information in the network. A coordination unit (the WLAN controller) distributes all necessary information for rapid authentication of the client among all WLAN access points in the network. This process is called opportunistic key caching. Thanks to this technology, each access point can identify every client on the network quickly, securely and uniquely using “WPA2 Enterprise.” Thus, fast roaming times of 50 ms can be achieved with full security features.

**Summary**

The fundamentals and techniques presented in this article show a portion of the scope involved in optimizing an IEEE 802.11 network in addition to planning for disruption-free coverage. On the one hand, fundamental decisions such as the choice of the frequency band and the antenna play a major role. On the other hand, techniques such as adaptive noise immunity and client or band steering significantly improve the performance of IEEE 802.11 wireless networks. The redundant layout of WLAN systems with PRP can also significantly improve the reliability and transmission latency. Finally, less delay in demanding mobile applications can be achieved by optimizing the roaming behavior. Many of these improvements can be achieved by selecting the right WLAN products and settings, so that significant improvement in WLAN performance may be achieved without great effort.
Belden Competence Center

As the complexity of communication and connectivity solutions has increased, so have the requirements for design, implementation and maintenance of these solutions. For users, acquiring and verifying the latest expert knowledge plays a decisive role in this. As a reliable partner for end-to-end solutions, Belden offers expert consulting, design, technical support, as well as technology and product training courses, from a single source: Belden Competence Center. In addition, we offer you the right qualification for every area of expertise through the world’s first certification program for industrial networks. Up-to-date manufacturer’s expertise, an international service network and access to external specialists guarantee you the best possible support for products from Belden, GarrettCom, Hirschmann, Lumberg Automation and Tofino Security. Irrespective of the technology you use, you can rely on our full support – from implementation to optimization of every aspect of daily operations.

About Belden

Belden Inc., a global leader in high quality, end-to-end signal transmission solutions, delivers a comprehensive product portfolio designed to meet the mission-critical network infrastructure needs of industrial, enterprise and broadcast markets. With innovative solutions targeted at reliable and secure transmission of rapidly growing amounts of data, audio and video needed for today’s applications, Belden is at the center of the global transformation to a connected world. Founded in 1902, the company is headquartered in St. Louis, USA, and has manufacturing capabilities in North and South America, Europe and Asia.

For more information, visit us at www.beldensolutions.com and follow us on Twitter @BeldenIND.