IEEE 802.11 - Technologies for Fast Roaming

Fast roaming – a particular challenge for industrial WiFi

Nowadays, IEEE 802.11 WiFi wireless networks are used in a wide variety of applications. This technology is well known for its long range and high transmission speeds. However, a particular challenge for the quality characteristics of WiFi networks in industrial environments is fast roaming. Fast roaming is especially important when the reliability and security of communication in a mobile application scenario needs to be unaffected. However, due to the complexity of this application, optimising a wireless network for operation is far from straightforward. This article provides an overview of the influencing factors that determine the quality of a WiFi network; it also provides technical options for improving the quality of new and existing wireless networks in this environment. It presents already established approaches for optimisation, as well as recently developed technical options on the latest devices, addressing the specific requirements for reliability and security of these mobile industrial applications in particular.

Quality standards for Train-to-Ground Communication and Automated Guided Vehicles (AGVs)

Wireless networks can offer many new options for the implementation of industrial applications. On the one hand, they offer an easy-to-install option to provide facilities in changing environments with network communications. On the other hand, the use of wireless networks minimises the cost of applications in which wear and tear would damage or destroy cable connections quickly. In addition, the use of wireless communication systems becomes mandatory whenever communication between mobile clients' needs to be implemented. Due to their long range and high data rates, wireless IEEE 802.11 networks are suitable for the sophisticated application scenarios of Train-to-Ground Communication and Automated Guided Vehicles (AGVs) in which the participants can be moving at high speeds.

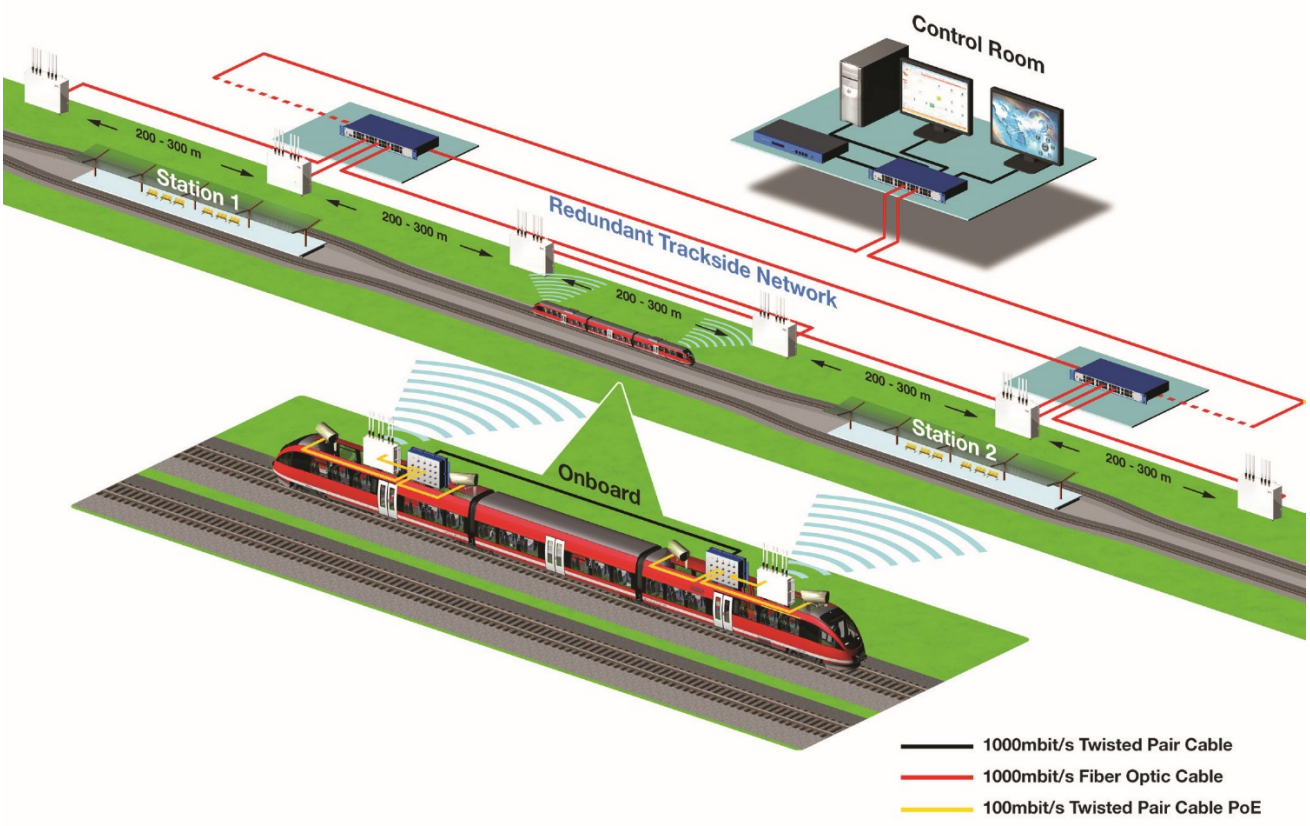

Image 1: Application example of Train-to-Trackside Communication

The objective of train-to-ground communication is to establish fast and reliable signal transmission between trains and the subway and track-side infrastructure. The network on a train can connect WLAN clients on the train via specialised WiFi with different access points along the route. The communication range of the trackside access points and the wireless network on-train clients are particularly important for the reliability and efficiency of such a system since every switchover (roaming) of a client between two different access points along the route causes an interruption of the train-to-ground connection. Hence, frequent roaming degrades the connection, especially when the interruption is long.

The network requirements for the AGV application are very similar in terms of coverage and interruptions. In this case, vehicles are moving autonomously through a manufacturing site to independently fulfil various tasks. The vehicles communicate with the infrastructure about sensitive and time-critical information necessary for autonomous operation, such as receiving control commands. Thus any longer interruption on the communication network might cause the stop of an AGV which could lead to disruptions in the manufacturing process.

For the precise characterisation of the extent to which WiFi can meet the requirements of both applications, the most important quality indicators of a wireless network are specified below:

- **packet loss rate** – the percentage of sent messages (or packets/frames) that are not successfully received by the intended recipient
- **latency** – the delay in transmission for the delivery of a message via a wireless connection
- **data throughput** of the wireless connection – the ability to transmit a certain amount of data within a specified time
- **interruption** – a break in transmission that takes place when a client roams from one access point to another
- **communication range** – the area covered by an access point or the seamlessness in the coverage of a facility that determines whether the WiFi connections are strong enough to reach all necessary locations

Generally speaking, the importance of each parameter varies according to the application. When it comes to **train-to-ground communication** and **AGVs**, reliable communication has top priority. The wireless network must deliver a certain data throughput with minimal packet loss at every point of the area. A standard requirement of a train-to-ground installation is 20 to 80 Mbit/s data throughput with less than 1% packet loss. Especially the requirement on high reliability is similar for AGV scenarios, since any interruption in communication might cause the AGV to stop its operation.

To ensure this reliability can be achieved, the installation must have sufficient network coverage; in addition, the interruptions of a mobile client during the switch from one access point to another should be as short as possible (typically < 50 ms). Insufficient coverage results in a stark reduction of the data throughput, and interruptions that are too long lead to extreme packet loss.

For these reasons, an optimal mechanism for changing the connection from the client to the access points factors into both aspects. Roaming needs to occur as quickly as possible and must be initiated precisely when the client leaves the range of the current access point and the next access point offers a stronger signal transmission which leads to a more reliable data throughput.

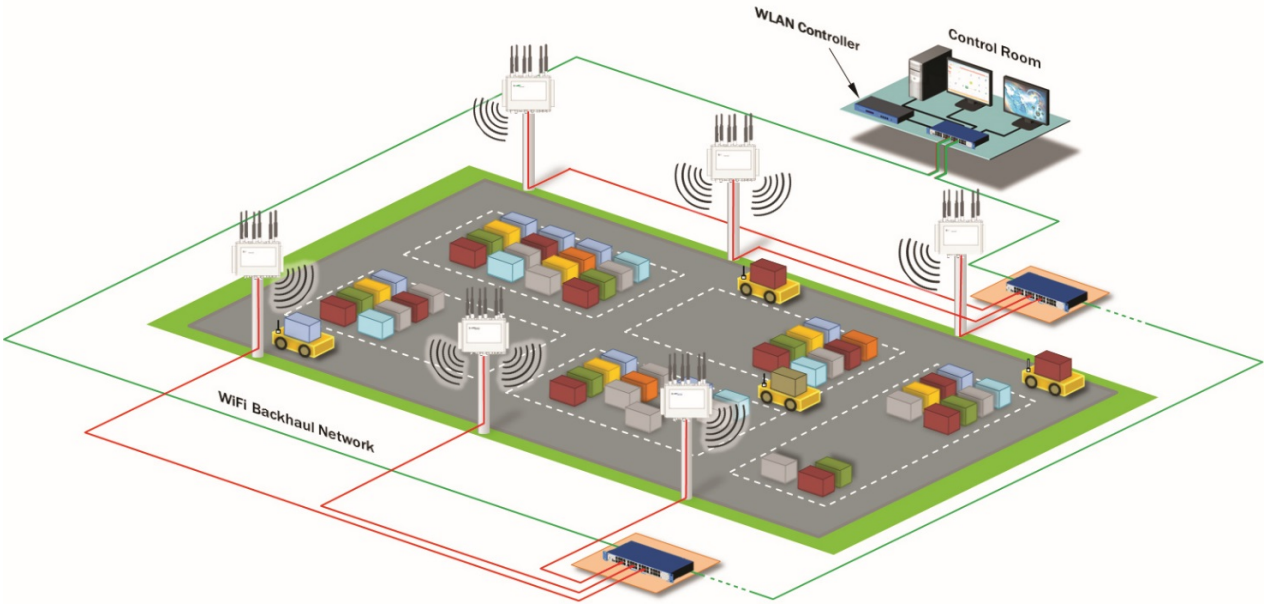

Image 2: Application example of an AGV Communication

Technologies for „fast roaming" with WiFi

In the following sections, we discuss the various technological capabilities of a wireless network that enable client devices to rapidly change between access points. Since the security of the wireless network should be ensured at all times, including in scenarios with high mobility, there should be no compromises of the implemented security technology in favour of faster roaming times. Therefore, technologies for faster roaming are always to be viewed in the context of the underlying security mechanisms. These roaming enhancements are often specific to special hardware or software features and therefore are only available on certain wireless network products. For example, the current BAT devices of the Hirschmann access point series support the following technologies:

- Fast Roaming
- Fast Roaming Through Reduced Scan Times
- Secure Fast Roaming

Fast Roaming

Although a mobile client moves through the transmission range of several different access points, the reliability of the communication and the available bandwidth must be guaranteed at all times. Ideally, to optimise bandwidth, neighbouring access points with overlapping radio coverage should operate on different channels to minimise interference. A mobile client can connect automatically to the access point with the best signal. Fast roaming between wireless network access points has been possible for a long time. Interruptions of less than 50 ms can be achieved; however, even faster roaming requires further technical tricks and achieving such fast roaming times with proper security is even more challenging.
Over time, more and more (necessary and important) security mechanisms have been added to wireless networks, so that wireless networks today are very secure. 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 secure and fast WiFi when roaming. In order to ensure both a fast and secure exchange, two problems must be solved:

- how can the mobile client switch as quickly as possible between access points?
- how can the time for the negotiation of security parameters be minimised?

We discuss the answers to these two questions in the following.

Fast Roaming Through Reduced Scan Times

When roaming between two access points, an on-train client must first identify the next target access point. This is not as simple as it may sound, because in order to avoid interference between the neighbouring access points, these access points typically operate on different channels, meaning different frequencies. However, a client can only communicate with access points on one channel at a time. Therefore, when searching for candidate target access points, the client must deactivate its current communication connection in order to search other channels/frequencies for suitable access points.

A mobile client must therefore periodically interrupt its established connection to scan all eligible channels/frequencies to obtain an overview of signal strengths of the other access points in its environment. Only with this information can a client decide whether there is a possible connection with a better quality than the present quality, and then initiate the roaming process. Depending on the train's speed and the associated changes in the environment of the WLAN client, 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 the application during the scan – the network is not available whenever the client scans. 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. The client visits a channel and probes for access points with a short probe request, "Who is there?". The available access points quickly reply: "Me." The client repeats this process for each channel. This way, the client quickly learns which potential roaming target points are in its surroundings.

However, if there are also channels used in which radar detection is required (i.e. in outdoor operation within 5 GHz band), this poses a further challenge: for those channels, clients are not allowed to actively search for access points (by sending probe requests, for example), but must determine first if the channel has a primary user, meaning a radar station. Since this determination must be repeated and requires one minute of passive listening, this is not an option for fast roaming outdoors.

Therefore, the client is obliged to sequentially listen to all existing channels until the access points make themselves known. The access points do this periodically through so-called beacons. Typically, these beacons are not sent with high urgency. Hence, typical beacon times are in the order of 50 ms to 100 ms. This determines the scan time for these channels from the period of beacon messages sent from the access point and the corresponding maximum wait period of the client (how long will the client spend on each scanning channel to wait for further beacons?). Using the standard values widely used in wireless networks, this quickly results in a scanning time of several seconds. Consequentially, this means an interruption of several seconds while roaming – which is unacceptable in most cases. Moreover, when the scanning process completes after several seconds, the results may already be obsolete because of the fast movement of the train.

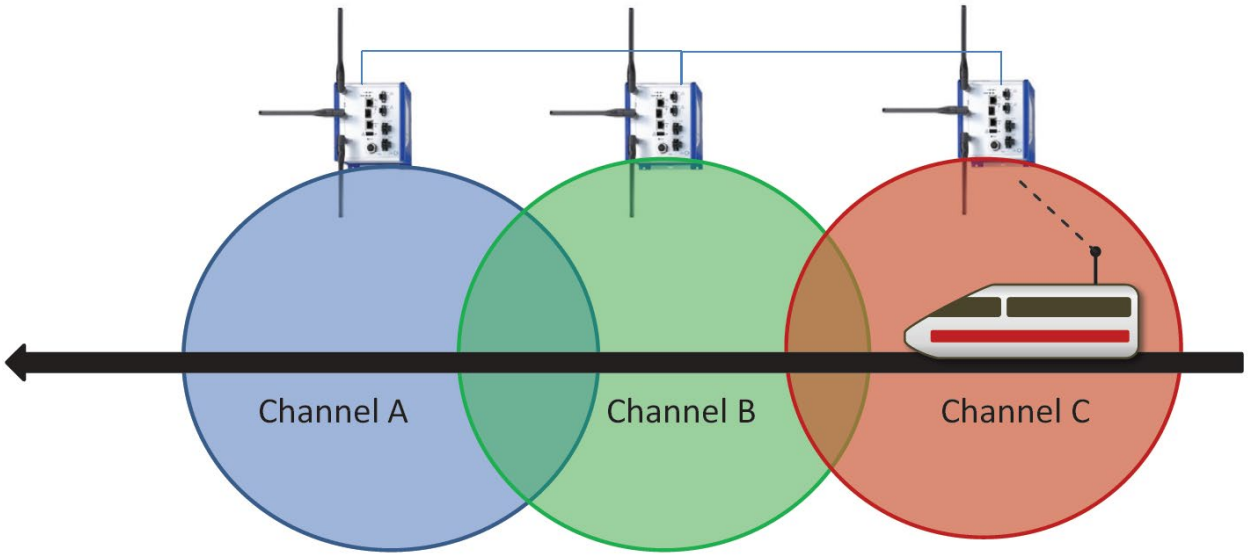

Image 3: A mobile client on a train or AGV moves through the wireless networks of different access points

The faster the access points repeat their beacons, the faster the client can jump to the next channel without overlooking an access point. For an operator therefore, it is a great advantage to be able to configure not only the period for sending beacon messages by the access point, but also to adapt the maximum waiting time of the client. With access points specially optimised 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, especially in outdoor operation in the less congested 5 GHz band. The current Hirschmann access points of the BAT and OpenBAT series support full configuration of these settings, which are specifically designed for the demanding requirements of rail traffic.

Likewise, a restriction of the number of channels to be scanned is possible with accuracy. Of course, when there are fewer channels to scan, the scan time is also reduced. In addition, multiple access points can be used for simultaneous roaming on the train. The OpenBAT devices support roaming with multiple wireless network modules and simultaneous use of Parallel Redundancy Protocols (PRP), which even guarantees completely uninterrupted roaming by always staying connected with one WLAN module while the other module roams. Uninterrupted roaming with most likely no packet loss while roaming leads to a highly reliable data communication. Therefore, uninterrupted roaming enables the possibility to perform AGV real time control or monitoring using WiFi.

Secure Fast Roaming

Whenever a client decides to switch its connection to a different access point, it will initiate the procedure for the fast BSS (Basic Service Set) transition defined in the IEEE 802.11 standard, meaning the actual roaming to the better access point. In consideration of the highest WiFi security, fast roaming is usually labelled as Fast BSS Transition. The security of a WiFi connection can only be guaranteed if a client properly authenticates at the target 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 faster authentication mechanism.

Based on these aspects, it is appropriate to take a closer look at the available authentication

methods of the WPA2 (WiFi Protected Access 2) standards. WPA2 provides two modes: Personal and Enterprise. Using WPA Personal, there is a common password for all WiFi devices (Pre-Shared Key). In larger facilities, the use of a single password by everyone is quite insecure; however, the simplicity of this approach makes roaming very fast, since all access points and clients already know the passwords and keys used. The establishment of a connection for roaming uses the standard key negotiation (four-way Handshake). Normally, this could presumably be done in less than 50 ms. The interruption period while roaming is therefore short. Due to the widespread knowledge of the keys, however, this authentication is only useful for very small networks: otherwise, the key is stored in too many places and too many people can gain knowledge of the keys, giving a hacker numerous possibilities to obtain the keys.

For larger networks, it is therefore recommended to use the WPA 2 Enterprise mode and to authenticate the clients with unique keys per client, which are managed in a central authentication database (for example, a RADIUS server). The access point of each wireless network device can be separately authenticated when establishing a connection as per the authentication standard IEEE standard 802.1X. However, the request to the authentication database results in a new delay of roaming. Therefore, this method is not suitable without optimisation for fast roaming. Secret cryptographic key information from the client must not be stored in the access point. Therefore, the client must perform a complete IEEE 802.1X authentication. Under certain circumstances – e.g. when access points are far away from the authentication server, as is typical in train-to-ground networks – the authentication could take a very long time.

The following optimisations lead to a significantly faster roaming while continuing to maintain good security:

PMK (Pre Master Key) Caching

The PMK Caching method also uses a full authentication via IEEE 802.1X. However, the client and access points store/cache the negotiated keys and can reuse them for quick access to their next connection. Nevertheless, this method for fast roaming can only be used to a limited extent, since a client would have to log in to all access points in the system in order for the roaming processes to use the stored key information for a fast connection later on.

Pre-Authentication

The Pre-Authentication method enables the client to authenticate via IEEE 802.1X to the next access point via the wired backhaul network, independent from the actual roaming procedure. This way, the client does not communicate directly with the access point via WiFi but uses its currently active connection with the wired LAN in order to connect to the next access point. During this early authentication process, the Master Key is already negotiated between the client and the access point, which means that, when roaming at a later point, the connection to this access point is made without authentication.

Although this method makes fast roaming possible, there are still some disadvantages: as a requirement for Pre-Authentication, a client must be able to predict with which access point it will connect as early as possible. This information may not be available in certain circumstances, since a client would have to scan the WiFi channels in its surroundings for access points often and continuously. This in turn leads to loss of performance and interruptions. Alternatively, of course, a client can authenticate itself with as many access points as possible, regardless of whether it will connect with them later on. However, since a full IEEE 802.1X process is required for every authentication, this approach generates a significant load on the authentication server. Therefore, this Pre-Authentication method for fast roaming has limited applicability.

Opportunistic Key Caching

The utilisation of Opportunistic Key Caching (OKC) can provide fast roaming without generating a heavy load on the IEEE 802.1X authentication server. The central approach of this method is the managing of key information for all access points by a WiFi controller. The WiFi controller can distribute the authentication information to all WiFi access points under its control. Therefore, a client must no longer negotiate its own Pre-Master Key for every access point but is able to use the same Pre-Master Key for all access points managed by the single WiFi controller. The Pre-Master Key will be negotiated during the first IEEE 802.1X authentication. Thus, a client must only complete a single IEEE 802.1X authentication to any access point in order to connect to all access points of the network. For this reason, fast roaming times of 50 ms are possible through the use of OKC, despite the use of the full security of IEEE 802.1X.

IEEE 802.11r

A conceptually very similar procedure to the Opportunistic Key Caching, 802.11r is specified in the IEEE standard. A significant difference between this specification and OKC is the use of a defined key hierarchy at the WiFi controller and the connecting clients. Based on this hierarchy, the access point and the client are able to gain access to a part of the necessary information for key negotiation.

The HiLCOS software used for Hirschmann access points, clients and WiFi controllers offers solutions for both core challenges of fast roaming. On the one hand, HiLCOS offers comprehensive configuration options for the scanning behaviour of a client in order to facilitate efficient, optimal roaming decisions. On the other hand, the mechanisms for fast roaming in combination with IEEE 802.1X authentication, such as Pre-Authentication, Opportunistic Key Caching, and IEEE 802.11r (WiFi Controller and Access Point) are supported under HiLCOS.[1)]

Summary

This article illustrates, using the examples of train-to-ground communication and AGV application scenarios, which technologies are required for fast roaming in a WiFi network. Both applications require very reliable communication between the fast moving participants and the stationary infrastructure. Based on the high mobility and the specific requirements for the data throughput with very low packet loss, optimal "fast roaming" with the highest WiFi network security is needed. Only with optimisation of the roaming behaviour, and with the very short interruptions associated with it, can the target of low packet loss for these demanding mobile applications be achieved.

References

1) Institute of Electrical and Electronics Engineers, Inc., Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (ANSI/IEEE Std 802.11, 2012 Edition (802.11-2012)), 2012