Location-based Handover in Cellular IEEE 802.11 Networks for Factory Automation

Lukasz Wisniewski, Henning Trsek, Ivan Dominguez-Jaimes
inIT - Institut Industrial IT
Ostwestfalen-Lippe University of Applied Sciences
32657 Lemgo, Germany
{lukasz.wisniewski, henning.trsek, ivan.dominguez-jaimes}@hs-owl.de

Anetta Nagy, Reinhard Exel
Institute for Integrated Sensor Systems
Austrian Academy of Sciences
2700 Wiener Neustadt, Austria
{aneta.nad, reinhard.exel}@oeaw.ac.at

Nikolaus Kerö
Oregano Systems - Design & Consulting GesmbH
1030 Vienna, Austria
keroe@oregano.at

Abstract

The use of wireless technologies in Factory Automation is attractive due to several advantages (mobility, cost, etc.); however, to satisfy the requirements of industrial applications, they have to be improved in terms of real-time performance. Handover is a particular weakness in cellular wireless systems, e. g., in IEEE 802.11, since it may introduce delay beyond acceptable bounds. The project "flexWARE - Flexible Wireless Automation in Real-Time Environments" aims at implementing such an infrastructure based on IEEE 802.11. To enhance overall system performance, it offers a localisation service. In this paper we present the flexWARE handover mechanism which exploits localisation to reduce the discovery phase. A performance evaluation, based on simulation and empirical measurements, shows that the mechanism results in a seamless handover for a class of industrial applications.[1]

1. Introduction

Factory automation networks can benefit greatly from the cost-effectiveness and flexibility offered by wireless communication. However, industrial control systems cannot profit from the mobility advantage of wireless system unless the issue of providing real-time (RT) guarantees is solved. This is particularly challenging in cellular WLAN environments as the handover (HO) of a node between different access points is necessary and the HO duration may violate certain deadlines. In order to leverage the mobility possibilities offered by IEEE 802.11 within factory automation networks, it is necessary to develop mechanisms for a seamless HO. Seamless means that there is no degradation on the quality of service (QoS) provided for the industrial RT traffic.

This paper proposes an HO method used within the context of the flexWARE system [4]. The mechanism uses location information to trigger the HO process, thus minimizing the time to accomplish it. Section 2 of this paper describes previous work aimed at reducing the total HO process and earlier proposals for location-based HO management. An overview of localisation techniques in the context of IEEE 802.11 networks is also presented. In Section 3 the proposed location-based HO is described, including the location and clock synchronization execution mechanisms. This is followed by a performance evaluation in Section 4, which is carried out by means of simulation and measurement. Finally, Section 5 concludes the paper with a summary and an outlook about future work.

2. Background

The HO as defined in IEEE 802.11 WLAN [5] is a time consuming process. Hence, several research activities dealing with HO improvements can be found, they are summarized in the remainder of this section. Moreover, as the proposed location-based HO algorithm does not rely on a commercial localisation system (e. g., GPS), this section focuses on most commonly used indoor localisation techniques. A feasible localisation system able to enhance the HO will be discussed.

2.1. Handover Management in WLAN

In general, a HO is required whenever a mobile station (MS) leaves the coverage range of its current access point (AP) to a neighbour AP. In order to maintain the

[1]This research work was financially supported by the EU Project flexWARE under grant number ICT-224350.

data link, the MS will attempt to associate to the new AP by exchanging several management frames related to HO. During this exchange, no user traffic can be exchanged between the AP and the MS. Therefore, the whole HO process needs to be completed as fast as possible in order to avoid any interruption of the data traffic.

The complete HO procedure might be divided into three steps, the *discovery phase*, the *(re)authentication phase* and the *(re)association phase* [2]. The discovery phase is the most time consuming procedure taking up to 90 % of the total HO time [10]. During this phase the MS has to perform an active or passive scan of all available channels (e. g., 13 in the 2.4 GHz band) in order to discover APs in its vicinity. The scanning duration can differ significantly based on the chosen method. For passive scanning the MS is listening for beacon frames on the corresponding channel. As the beacon interval is commonly in the order of hundreds of milliseconds, the scanning procedure of all 13 channels may take several seconds. Whereas for active scanning, the MS sends a *Probe Request* message and waits for a minimum time ($MinChTime$), approx. 10 ms, for a *Probe Response*. If a response is received, the MS remains on this channel for a maximum time ($MaxChTime$), which can be up to 30 ms, and waits for additional responses from other APs. If the MS receives no response within $MinChTime$, it switches immediately to the next available channel. The parameters $MinChTime$ and $MaxChTime$ depend on the particular implementation. After all channels have been scanned, an AP is selected by the MS either based on the Received Signal Strength (RSS) value or on the link quality [6]. The active scanning delay T_{active} can be expressed by the inequality (1), where N is the number of channels [2]. It has been analysed empirically that the active scanning delay of industrial implementations takes in average 2400 ms [16].

$$N \cdot MinChTime \leq T_{\text{active}} \leq N \cdot MaxChTime \quad (1)$$

Several solutions are proposed in the literature which aim at improving the discovery process. The simplest and the most intuitive approach is to decrease the $MinChTime$ and $MaxChTime$ values or to limit the number of channels to be scanned [2]. All other approaches require a priori knowledge about the channel usage of the system. The authors in [6] propose a selective scanning method by means of creating a Neighbour Graph (NG) with potential APs. The drawback of this solution is the graph creation, since this is only possible during the actual HO.

Another approach is presented in [12]. The authors propose an algorithm called *SyncScan*, which requires the APs to send beacon frames in a specific order. By synchronizing the MS to the timing of the beacons, every MS can scan passively by switching to the channel shortly before the known beacon arrival time. *SyncScan* enables a fast and easy recognition of all neighbours and the usage of this knowledge to perform future HOs. However, such an approach results in an increased system complexity due to the precise clock synchronisation needed between all APs and MS's.

Another mechanism is described and evaluated in [13]. It is suggested to use a background scanning of channels interspersing with regular data communication, in order to prepare a list of potential APs for the HO. In contrast to *SyncScan*, the background scan uses an active scanning approach to discover APs, resulting in additional traffic created by probing the channels. The problem is particularly important, if the communication within each cell is scheduled and the MS needs to wait until high priority traffic is sent before scanning is allowed. This might be frequently the case for RT applications.

All approaches mentioned above have in common, that the MS is performing the discovery procedure by passively or actively searching for APs and maintaining a list of candidates. Even though the number of scanned channels have been already reduced, there is still a potential for improving the HO process. For instance, the discovery time can be minimized even further by providing exact information about the new AP. The solution introduced in [9] provides means to configure an ordered list of APs. The MS is supposed to associate to the APs in the configured order along its predefined path. As a consequence the discovery time is decreased to a minimum, because only one channel has to be scanned. However, the lack of flexibility is the main disadvantage of this solution, since the MS has to stick on its predefined path which corresponds to the precompiled list.

Apart from scanning, the second important issue is to initiate the HO process at the right instant. An optimal moment to start the HO process is when the MS has still a relative good connection to the current AP and the signal quality from the new potential AP is sufficient for the communication. This will avoid frame loss before and after the HO due to a low signal quality. The most current wireless devices trigger the HO based on the RSS value, the signal to noise ratio (SNR) or the frame loss ratio (FLR). Making a decision based on these parameters might cause a significant frame loss before the MS decides to change the current association.

2.2. Indoor Localisation Techniques

Precise location of MS's within a wireless network has been a research topic for many years as it opens the doors towards numerous new applications. For indoor localisation usually some of the range localisation techniques are used, because of their superior accuracy compared to other methods. Range methods estimate the distance between two nodes and e. g., triangulation is used for computing the position. They can be divided in three different categories: Angle of Arrival (AoA) measurements, RSS profiling techniques and propagation delay related measurements including Time of Arrival (ToA) and Time difference of Arrival (TDoA). Since the performance of the AoA is rather poor [8], in the following only RSS and

propagation delay related methods will be discussed.

2.2.1. RSS based Methods

These techniques evaluate the location of a node based on RSS measurements. RSS methods can be grouped in manual and automatic ones. The manual group consists of a training (or offline) and an online phase. During the offline phase a radio map is created of the area where the MS may be located by manual walk-arounds. In the online phase the received signal strength of the MS is compared to the map entries and the position is estimated using a proximity search. A well-known example of this category is the RADAR system [1]. The down side of this technique is that in case of environmental changes, the values in the radio map do not fit anymore, and the localisation accuracy decreases significantly. In the automatic RSS techniques the offline phase is omitted. In [11] the authors present an automatic WLAN localisation system which is capable to cope with environmental changes while still achieving an average accuracy of 3.7 m.

2.2.2. Propagation Delay Related Methods

Within this group two techniques are most commonly used: ToA and TDoA. One-way or ToA propagation time measurements provide the difference between the sending time of a signal at the transmitter and the receiving time of the signal at the receiver. This technique requires highly accurate clock synchronization (in the range of 1-3 ns) between the transmitter and receivers, which is not feasible for standard WLAN devices.

TDoA estimates the position by measuring the propagation delay differences at different receivers. In [19] a localisation scheme is described, which is based on TDoA for IEEE 802.11b WLAN. The authors have implemented a localisation system, which deals with more issues: AP synchronization, frame selection and TDoA estimations. The experimental results in an undisturbed environment indicate a localisation accuracy of 2.4 m.

2.3. Location-based Handover Management

The idea to use the knowledge about the location of the MS's to improve the overall performance of the HO is not entirely new, several proposals can be found. The main intention behind them is to select the most suitable AP for a HO, based on the geometry of the system. In [7] a localisation system which is intended to be used to avoid Internet connection interruption in WLAN is presented. For this purpose an AP with two transceivers is used, where one transceiver is exchanging data with the MS's and the second transceiver is used to scan neighbour MS's in the coverage area using a fast passive scan technique. In the proposed system, RSS and TDoA based location estimation techniques were employed in parallel to estimate the location of the MS. In order to achieve the required clock synchronization accuracy for TDoA, it was proposed to use the IEEE 1588 with hardware timestamping. The performance was evaluated using the discrete event simulator OPNET. In the simulated system a RT application (VoIP) was used for testing purposes and the results show that the HO was seamless. The drawback of the proposed solution is that the APs are at the same time used for data exchange and localisation which leads to a contradiction during radio planning. On the one hand, the APs should be placed far enough from each other to have minimum overlapping of the cells and on the other hand, in order to be able to localise the MS's inside the whole area, the cells should almost entirely overlap.

This drawback has been addressed by introducing passive wireless receiver nodes merely listening for wireless data packets, noting their arrival time, and finally forwarding this information to the closet AP. If a sufficient number of these devices is positioned at known locations within the range of every AP, precise TDoA can be implemented without interfering with wireless network topology planning and HO mechanisms.

2.4. Problem definition

To be able to deploy the WLAN standard in industrial applications with demanding RT requirements, it is essential to optimize the HO process. The discovery phase has been identified as being most critical during the whole HO procedure. Hence, a solution which significantly decreases the discovery time, while simultaneously enabling a very flexible and efficient HO based on localisation information, is introduced in this paper.

Most of the existing solutions use a threshold (RSS, SNR or FLR) to trigger the HO process. This always results in unacceptable frame loss before the HO, or the HO might be even triggered incorrectly due to channel fading. The proposed solution approach will help to avoid frame losses during the HO procedure, trigger the HO at the right time and decrease the discovery time to the minimum.

3. Location-based Handover in flexWARE

The flexWARE system architecture [4] is shown in Fig. 1. Its purpose is to enable RT communication between distributed automation devices using a wireless infrastructure. A three-tier centralized approach is used. The functionality of its components is explained below.

- flexWARE Controller (FC). The FC is the centralised point of control which acts as a manager for the whole system. It is also in charge of forwarding RT traffic between backbone and FAPs.
- flexWARE Access Point (FAP). Amongst other functionalities, the FAP acts as a bridge between the wired and the wireless medium.
- flexWARE Node (FN). It interconnects automation devices through a wireless link with the FAP. It can be mobile and roam around different cells within the system.

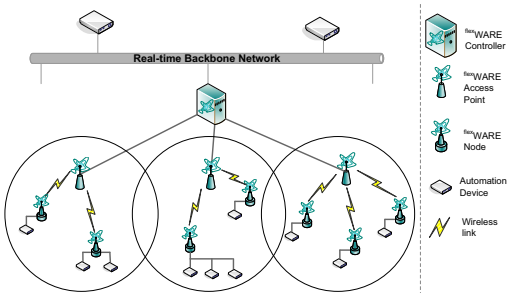

Figure 1. flexWARE System Architecture

All three components play a role in the HO process. In the following subsections, the localisation functionality and the novel location-based HO mechanism for flexWARE are described.

3.1. Localisation in flexWARE

In order to carry out localisation, the initial flexWARE architecture needs to be extended. However, several requirements need to be fulfilled. These included the minimization of the number of frames needed for localisation over the wireless medium and maintaining a traditional design (e. g., radio planning). Keeping these in mind, the TDoA technique was considered as the most suitable amongst the localisation methods mentioned in Section 2. Moreover, this technique can achieve an accuracy of about 1 m without requiring any modifications on the FN.

3.2. The TDoA Technique Analysis

The concept of the TDoA method is shown in Fig. 2. The FN in the center transmits a frame, which is received by multiple receivers (N+1 receivers for N dimensions) with known positions. Using the arrival times at $N+1$ receivers, N propagation delay differences can be obtained. Knowing the propagation speed, the TDoA can be converted to range differences of which each defines a hyperboloid (3D hyperbola) of possible positions of the FN. Finally, the estimated position lies on the intersection of the hyperboloids.

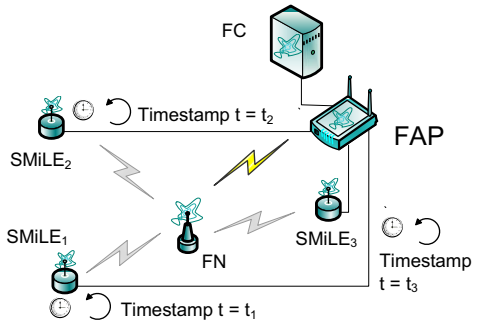

Figure 2. The concept of the TDoA localisation technique

Since dealing with RF propagation, the measured delays and hence the time differences are in the range of nanoseconds. Therefore, it is of utmost importance to keep the timing errors under a few nanoseconds. These errors arise due to loose synchronization between the receiving FAPs or by estimation errors of the wireless frames' arrival times. Although the positional accuracy depends on the intersection angle of the hyperbolas (positional dilution of precision), it can be roughly expected that an inaccuracy of 3 ns causes a localisation error of 1 m.

3.2.1. Localisation Method

The localisation method in flexWARE is based on the National Austrian Research Project ε-WiFi (grant No. 813310/12399) which deals with indoor localisation of IEEE 802.11 wireless networks. Within ε-WiFi a receiver was developed supporting highly accurate hardware timestamping of wireless frames, which will be used for flexWARE as well. The basic method to estimate the TDoA is based on timestamps, which are taken at the receivers in contrast to traditional approaches operating on a general cross-correlation scheme. The inherent advantage of this method is that the data sampled from every receiver need not be transfered to a central cross-correlation unit over a network. Instead timestamps are taken at a specific position that is present in all frames (e. g., at the end of the PLCP CRC). The timestamps together with some identification information are forwarded to a central position calculation server (the FC) which calculates the position. Compared to cross-correlation methods the timestamp method requires only minimal data communication to the FC and hardly any computational power.

The architecture is based on a set of passive receivers consisting of an analogue front-end board called SMart integrated Localisation Extension (SMiLE) board and an Altera Stratix II GX evaluation board. The SMiLE board demodulates, amplifies and finally digitalizes the received data and passes the digital data stream to the FPGA board. The FPGA decodes the frame completely and takes a timestamp which is forwarded to the FC. It has been shown that this architecture is able to timestamp frames with an accuracy of below 1 ns [3]. $N+1$ SMiLE receivers are connected via Ethernet to the FAP (as shown in Fig. 2) forming a localisation cell within the range of the FAP. Although this solution introduces additional cabling, it is deemed as the optimal solution to keep the traffic resulting from synchronization of the SMiLEs and the transmission of the timestamps away from the wireless channel. It has to be noted that the SMiLE boards need to be placed following a particular pattern to ensure signal coverage over the whole area. For example, a grid structure as shown in Fig. 3 can be employed.

3.2.2. Clock Synchronization of the SMiLE Boards

A requirement for TDoA is that all SMiLEs have to be synchronized. Even though state-of-the-art clock synchronization protocols (e. g., PTP defined within IEEE 1588) in conjunction with hardware timestamping can provide significant accuracy, the range of 1 ns is difficult to reach by asynchronous nodes with local oscillators. Expensive high speed digital logic in combination with high grade and expensive oscillators are required to reach ns range. As the amount of SMiLE modules to be

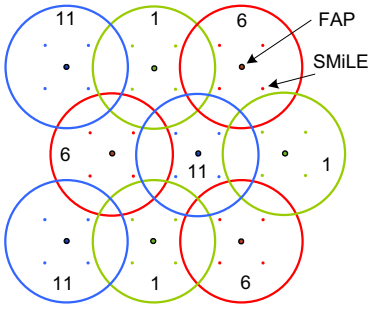

Figure 3. Example of cellular network (802.11b/g non overlapping channels)

distributed can become considerably large, for real world application the production costs for these devices becomes a serious issue as well. Hence, the synchronization is based on a combined approach split into two tasks: adjusting the clock rates by distributing a single frequency over the network similar as proposed by synchronous Ethernet and secondly determining the clock offsets at the SMiLE boards in order to have the same notion of time relative to the FAP.

The frequency distribution is maintained via Ethernet clocking: The SMiLEs belonging to one FAP are connected to a common switch and use the recovered Ethernet clock as their local clock source. As every SMiLE is incrementing the local counter with the same rate, the clock offset between two SMiLEs remains constant.

In the next step the offsets need to be determined. Since the geometry of the system and the signal propagation speed are known, the propagation delays and delay differences from the FAP to the SMiLEs can be calculated. Clearly, if these calculated propagation differences are divided with the signal propagation speed, they can be interpreted as TDoA values. Assuming that the wireless frames sent by the FAP can be timestamped by every SMiLE, measured TDoA values are obtained. Finally, in case one of the SMiLE boards is defined as the reference, it is possible to calculate the clock offsets by comparing the measured and calculated values. These offsets can be stored at the FAP and later used to correct the timestamps creating a virtual common timebase.

3.3. Handover Mechanism in flexWARE

The idea is to coordinate the HO procedure by a central authority, the FC in the flexWARE architecture. Since the FC has the information about the position of all nodes in the system, it will be responsible to trigger the HO whenever necessary. Apart from the knowledge about the position of nodes, it has also knowledge about the resources provided by each AP. It includes information about the coverage area, number of attached FNs and the resource usage. By combining these factors, a reasonable HO decision can be made. All steps of the whole HO procedure are shown in Fig. 4. Whenever the FC calculates the position of the FN, it will make a decision whether the HO should be triggered. The decision will be based on calculating the distance between the FN and the FAP it is currently associated to. The distance will be compared with the coverage map of particular FAP. If a particular position is reached, the FC progresses to the next phase, where it choses a FAP for the HO. In this phase the FC checks the coverage areas of different FAPs with respect to the FN. If more than one FAP has been found, it chooses the optimal FAP with respect to resource utilization. After the one FAP has been chosen, the FC sends a HO trigger frame (HTF) to the FN with information about FAP. The information in the HTF includes the MAC address and channel of the chosen FAP. After the FN receives this frame, it will immediately start the HO by sending its Probe Request according to the parameters extracted from the HTF. In this approach, the FN will only probe one channel, i. e. the discovery procedure is reduced to a minimum.

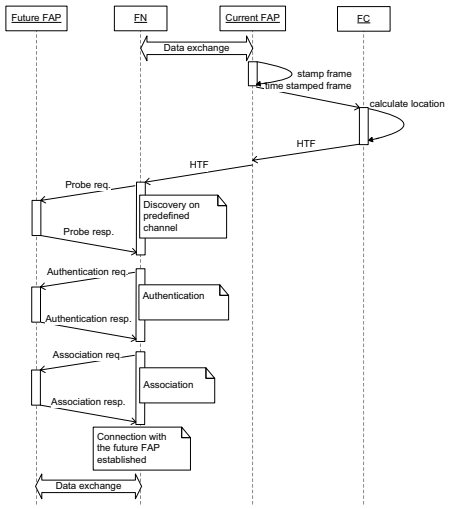

Figure 4. Location based Handover sequence

Although security is not in the scope of this paper, it always has to be considered for wireless systems. A sufficient level of security is provided in flexWARE by a combination of the 802.11i standard [5] and the 802.11r amendment [15]. The latter optimises the handover by incorporating the 4-way handshake into the 802.11 authentication [14], resulting in an identical message exchange between the FAP and the FN as shown in Fig. 4 without extending the HO execution time. Therefore, security mechanisms have not been further considered in this work.

4. Performance Evaluation

In this section the proposed location-based HO and the corresponding HO latency reduction is discussed. Besides a performance evaluation of the proposed system by means of a simulation case study, a detailed localisation accuracy evaluation is presented.

4.1. Localisation Accuracy Evaluation

Since localisation in flexWARE relies on the findings of the the ε-WiFi project, in this section the empirical results

of ε-WiFi are introduced. The goal of the measurements were twofold: on the one hand, the influence of the system itself was tested in a nearly ideal environment without disturbances from surrounding objects and persons. On the other hand, the influences when the same environment was severely disturbed were studied.

In the first case the measured TDoA values remained stable over time, the standard deviation of the TDoA values was approximately 0.2 ns for each receiver pair. The positions were calculated for 6700 measurements and indicated a deviation under 10 cm.

However, the possible accuracy is dependent on inaccuracies in the hardware and the wireless channel. While the former can be measured and compensated (e. g., the dependency of the transceiver IC on amplification, temperature), the wireless channel cannot be determined with the required precision to compensate all effects. Measurements in an outdoor environment showed that in line-of-sight conditions the accuracy is below 1 m. However, in case of severe multi-path channels the accuracy can drop to about 5 m.

4.2. Handover Performance Evaluation

The performance of the proposed HO mechanism is assessed in this section by means of empirical measurements with state-of-the-art devices and a simulation study using the proposed mechanism. Identical parameters have been chosen for both setups. Finally, the achieved results are compared against each other, in order to evaluate our proposed HO mechanism and to show its advantages.

4.2.1. Empirical Measurements

For obtaining HO results which are comparable to the simulation case study outcome, measurements with industrial standard WLAN devices had been conducted. They use a HO based on an AP list (cf. Section 2). Given that a fixed mobility path is used, this method can be almost compared with the flexWARE approach, since the discovery procedure is also limited to one channel. For the measurements, the scenario shown in the Fig. 5 has been used.

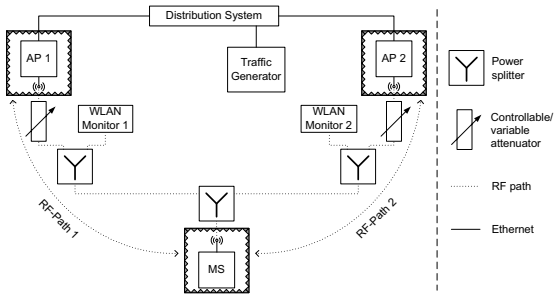

Figure 5. Reproducible environment for the empirical measurements

The test environment consists of an attenuator matrix, RF isolated chambers, capture engines, traffic generators, two APs and one MS. The RT data traffic was generated with a send period of 10 ms. The HO is triggered by increasing the attenuation to its current AP, forcing the MS to perform a HO to the next AP from its list. The HO was triggered 30 times to deliver a sufficient number of results, which will be further compared with the results achieved by simulation.

4.2.2. Simulation Case Study

To evaluate the performance of the newly proposed HO mechanism, a series of simulations have been carried out using OMNeT++ 4.0 [17] and the INET framework.

Model Description The model developed by the flexWARE consortium extends the INET framework by several functionalities like: localisation, clock synchronisation and the HO scheme described in this paper. Because the channel model is not yet implemented we used a simple channel model provided by INET. In this simplified model, no frame errors occur until a predefined distance between FAP and MS is reached, and the coverage resembles a perfect circle. Additionally, the channel is symmetric, i. e., whenever device 1 is able to communicate with device 2, it also works vice versa. For the simulation 1 Mbps was set as bit rate for both data and management frames, i. e., all HO related frames.

Model Validation The HO execution time is calculated as the total time needed to transmit all frames involved in the HO, starting at the time when the Probe Request frame is sent until the association response frame is successfully received at the FN. All FNs transmit according to the Distributed Coordination Function (DCF), which is the MAC mechanism defined in IEEE 802.11 [5]. In DCF each FN has to contend for the medium. After sensing the channel as idle for a distributed inter-frame space (DIFS) duration, the FN has to defer transmission for a random backoff time. This time is drawn from the range [0, CW], where CW is known as the contention window and is expressed in number of time slots ($aSlotTime$). After an unsuccessful transmission, CW is doubled, until a maximum size is reached (CW_{max}). In case of error-free transmission CW does not increase. Hence, the backoff time is drawn from the interval [0, CW_{min}]. Because the backoff time is chosen from a uniform distribution, its mean value ($\bar{t}_{\text{backoff}}$) is calculated using Eq. (2).

$$\bar{t}_{\text{backoff}} = \frac{CW_{\text{min}} - 1}{2} * aSlotTime \qquad (2)$$

Once the FN has gained access to the medium it first transmits a PHY preamble, followed by a PHY header and, finally, the data plus MAC header (called PSDU). To increase reliability, the receiving device sends an acknowledgment (ACK), after a short inter-frame space (SIFS), whenever a reception has been successful. The total transmission time t_{t} of every HO frame (also ACK frames) can

be calculated according to Eq. (3) in which effects such as hardware processing times and propagation delays are not considered. The only exception to Eq. (3) is the Probe Req. that does not require an ACK because it is a Broadcast message [5].

$$t_{\mathrm{t}} = t_{\mathrm{DIFS}} + \bar{t}_{\mathrm{backoff}} + t_{\mathrm{f}} + t_{\mathrm{SIFS}} + t_{\mathrm{ACK}} \qquad (3)$$

Where t_{DIFS}, $\bar{t}_{\mathrm{backoff}}$, t_{f}, t_{SIFS} and t_{ACK} are the time durations of: DIFS, the average backoff, frame transmission, SIFS and ACK frame transmission, respectively. The frame transmission duration, t_{f}, is calculated using Eq. (4), where t_{preamble} and t_{header} are the time durations of the PHY preamble and header respectively. m is the frame's PSDU (in bits). r_{d} is the transmission data rate (bits per second) of the PSDU.

$$t_{\mathrm{f}} = t_{\mathrm{preamble}} + t_{\mathrm{header}} + \frac{m}{r_{\mathrm{d}}} \qquad (4)$$

All frames involved in the HO execution are sent at 1 Mbps, therefore the parameters from the IEEE 802.11b-PHY standard are used (see Table 1).

Table 1. Parameters for IEEE 802.11b [5]

t_{DIFS}	CW_{min}	t_{preamble}	t_{header}	t_{SIFS}	$aSlotTime$
50 μs	31	144 μs	48 μs	10 μs	20 μs

The lengths, expressed in bytes, of every frame (PSDU) needed during the HO are shown in Table 2. These values are used for both, empirical measurements and simulation.

Table 2. Lengths of HO frames ($bytes$)

Probe Req.	Probe Resp.	Auth. Req.	Auth. Resp.	Assoc. Req.	Assoc. Resp.	ACK Frame
93	167	34	34	106	76	14

Using Eqs. (2), (3) and (4), and data from Tables 1 and 2, the average HO execution time is calculated at 8.90 ms. If an application's send period is larger than the HO execution time, the HO may be seamless.

Simulation Scenario The simulation setup is depicted in Fig. 6. Although the system is designed to support a large number of FAPs and FNs, in the simulation setup only one FN and two FAPs were used, where each FAP was in charge of four SMiLE boards for localisation. The FN moved along a linear path with constant speed. The RT traffic is produced by the FN with the send period of 10 ms. The traffic destination is the FC, which captures the arrival time of each RT frame. The HO was triggered 70 times. To check if the HO process is seamless for the RT application, the HO delay was measured as a delay of RT data frames being received by the FC. In our model we used active scanning with adjusted parameters $MinChTime$ and $MaxChTime$ in accordance to [18]. There, the authors have shown that 670 µs is enough time to receive a Probe Response frame. Since the $MinChTime$ needs to be expressed in time units (TU) which are equal to 1024 µs, the minimum possible value which can be used for the $MinChTime$ is 1 ms. Additionally, the authors have shown, that the $MaxChTime$ parameter should be selected according to the traffic load in the cell. Because we expect to receive Probe Response frames only from one FAP and only one station is generating wireless traffic in the scenario, the $MaxChTime$ has been set to 1 ms as well.

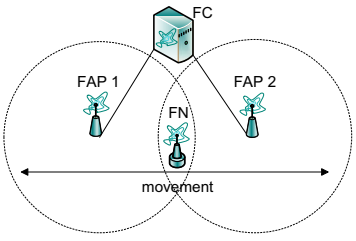

Figure 6. Simulation setup

Based on the results from ε-WiFi , the accuracy of the positioning system was kept under 3 m. This was justified, since the main goal of the simulation was to test effect of the HO on the RT applications.

4.2.3. Results

Fig. 7b shows the results from the empirical measurements. The HO delay varies from 10.6 ms to 49 ms. In average, the HO delay is 23.7 ms. Because the application expects to receive the RT data every 10 ms, the HO can not considered to be seamless.

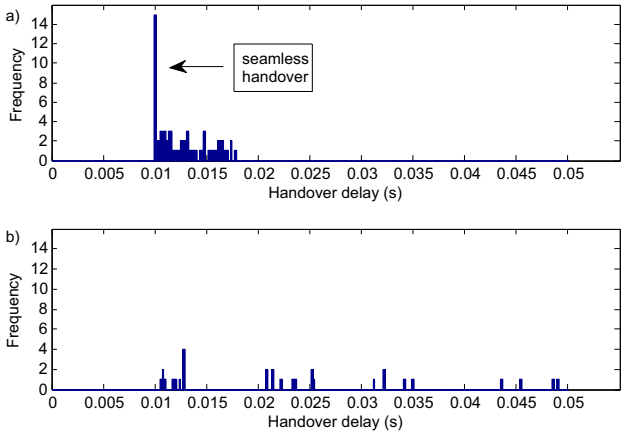

Figure 7. a) Simulation Results and b) Measurement results

The results collected during simulation are presented in Fig. 7a. We observed that 15 out of 70 measured HO delays have no influence on the traffic flow. For the remaining 55 results the HO delay spreads from 10 ms up to almost 18 ms. The reason for this behavior is the HO's start time. Whenever the HO starts just after a new RT data frame is sent, the application will not be affected, because the whole procedure will finish before the next RT

data frame is due to be sent. In such cases the HO is seamless. If a HO begins at a time, in which it is not possible to accomplish the HO procedure before the next RT data frame arrives, the HO will not be seamless. The latency increases when the HO starts closer to the beginning of the next send period. Because in 15 measurements the HO was seamless and the biggest delay was around 18 ms we can assume that HO execution time is approximately 8 ms, which is close to the analytical result presented in Section 4.2.2. If the HO would be scheduled to begin just after the RT data is sent, the HO would always be seamless for our scenario. The results from the simulation are significantly better than the results coming from the measurements, where only one HO was close to be seamless. The difference between simulation results and empirical measurements is caused by an uncertainty of the HO trigger for the latter, resulting in frame transmission errors. Even though the HO's RSS threshold was set to minimize frame losses, communication errors were always present. This is avoided in the simulation by a very precise trigger due to the location information.

5. Conclusion

In this paper, an HO mechanism, proposed within the context of the flexWARE system, is presented. In the proposed location-based HO scheme, an FC informs an FN about the future FAP and when to perform an HO. The FC makes the decision based on a localisation service which provides knowledge about the position of the FN relative to "candidate" FAPs. Furthermore, the FC knows the available resources in every FAP cell and therefore selects the best candidate.

The performance of the proposed HO has been evaluated using simulations and also measurements in a test environment similar to the proposed solution. It is shown, that the HO delay is significantly reduced and that it can be seamless for applications with a send period of 10 ms. However, to be able to always achieve a seamless HO, it is necessary to begin the handover process right after a RT data frame has been sent. Currently, a mechanism is developed that will allow the FN to schedule HO related messages just after RT data, what will result in a seamless HO.

References

[1] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building RF-Based User Location and Tracking System. In *IEEE Infocom*, 2000.

[2] P. S. Choi, J. T. Kwon, and C. Y. Fast-Handoff Support in IEEE 802.11 Wireless Networks. *IEEE Communication Surveys - The Electronic Magazine of Original Peer-Reviewed Survey Articles*, 9(1), mar 2007.

[3] R. Exel, J. Mad, G. Gaderer, and P. Loschmidt. A Novel, High-Precision Timestamping Platform for Wireless Networks. In *ETFA'09: The 14th International Conference on Emerging Technologies and Factory Automation*, pages 1–8, Sep 2009.

[4] flexWARE Consortium. *Architectural Design and Specification*. http://www.flexware.at, 2009.

[5] IEEE. *Std. 802.11-2007 for Information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, June 2007.

[6] H. Kim, S. Park, C. Park, J. Kim, and S. Ko. Selective Channel Scanning for Fast Handoff in Wireless LAN using Neighbor Graph. *Personal Wireless Communications*, 3260:194–203, 2004.

[7] T. Manodham, L. Loyola, and T. Miki. A Novel Wireless Positioning System for Seamless Internet Connectivity based on the WLAN Infrastructure. *Wireless Personal Communications*, 44(3):295–309, 2008.

[8] G. Mao, B. Fidan, and B. D. O. Anderson. Wireless sensor network localization techniques. *Computer Networks: The International Journal of Computer and Telecommunications Networking*, 51(10):2529–2553, July 2007.

[9] H. Merz. Hochverfügbarkeit in Industrial Wireless LAN durch Seamless Roaming. In *Wireless Technologies 11. Kongress*, Sep 2009.

[10] A. Mishra, M. Shin, and W. Arbaugh. An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process. In *ACM SIGCOMM Computer Communication Review*, April 2003.

[11] E. Nett, S. Ivanov, and S. Schemmer. Automatic WLAN Localization for Industrial Automation. In *7th IEEE International Workshop on Factory Communication Systems (WFCS 2008)*, May 2008.

[12] I. Ramani and S. Savage. Syncscan: Practical fast handoff for 802.11 infrastructure networks. In *24th Annual Joint Conference of the IEEE Computer and Communications Societies.*, volume 9, pages 675–684, 2005.

[13] G. Singh, A. P. Atwal, B. Singh, and S. Sohis. Mobility Management Technique for Real Time Traffic in 802.11 Networks. *Journal of Computer Science*, 9(3):390–398, 2007.

[14] A. A. Tabassam, H. Trsek, S. Heiss, and J. Jasperneite. Fast and Seamless Handover for Secure Mobile Industrial Applications with 802.11r. In *5th IEEE International Workshop on Performance and Management of Wireless and Mobile Networks (P2MNET)*, Oct 2009.

[15] A. Treytl, T. Sauter, H. Adamczyk, S. Ivanov, and H. Trsek. Security concepts for flexible wireless automation in real-time environments. In *14th IEEE international conference on Emerging technologies & factory automation, ETFA'09*, pages 1259–1267, Sep 2009.

[16] H. Trsek, A. Pape, and J. Weczerek. Reproduzierbare handover zeiten von zellularen industriellen wlan netzwerken fr die fertigungsautomatisierung. In *Wireless Automation 2009*. 8. VDI Jahrestagung, Lemgo, Germany, Mar 2009.

[17] A. Varga. Using the OMNeT++ discrete event simulation system in education. *IEEE Transactions on Education*, 42(4):11 pp., Nov 1999.

[18] H. Velayos and G. Karlsson. Techniques to reduce the IEEE 802.11b handoff time. In *Proceedings of IEEE ICC*, volume 7, pages 3844–3848, June 2005.

[19] R. Yamasaki, A. Ogino, T. Tamaki, T. Uta, N. Matsuzawa, and T. Kato. TDoA Location System for IEEE 802.11b WLAN. In *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, volume 4, pages 2338–2343, March 2005.