IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received July 7, 2021, accepted July 20, 2021, date of publication August 12, 2021, date of current version August 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3104331

High-Precision Multipath-Based Indoor Localization Scheme With User Privacy Protection for Dynamic NLoS Environments

ALEXANDRA ZAYETS[1], (Member, IEEE), CHRISTIAN GENTNER[2], (Member, IEEE), AND ECKEHARD STEINBACH[1], (Fellow, IEEE)

[1]Chair of Media Technology, Technical University of Munich, 80333 Munich, Germany
[2]German Aerospace Center, Institute of Communications and Navigation, 82234 Oberpfaffenhofen, Wessling, Germany

Corresponding author: Alexandra Zayets (a.zayets@tum.de)

ABSTRACT High-precision indoor localization systems (ILSs) are critical for applications such as human smartphone navigation, autonomous robotics and automated warehouse and factory design. This paper presents a novel fingerprinting-based ILS, which features a decimeter-level localization accuracy, the ability to function in a constantly changing non line-of-sight (NLoS) environment, and user privacy protection without the need for heavy computations. The proposed ILS is able to maintain its localization accuracy in a constantly changing environment and to camouflage the user's location by leveraging multipath propagation. The method was successfully tested both by experimental verification using the ultra-wideband communication standard and a ray-tracing simulation. An average localization error of 6 cm is demonstrated for a stationary or slow-moving receiver. An average error of 30 cm is demonstrated for a receiver that is moving at a fast walking pace. The obtained localization accuracy is comparable to the accuracy of the state-of-the-art localization algorithms. At the same time, the proposed approach solves two practical challenges faced by ILSs: robustness to changing environments with moving objects and the high computation requirements of user privacy protection. The high degree of user privacy was evaluated using a set of corresponding metrics.

INDEX TERMS Indoor localization, multipath fingerprinting, camouflage-based privacy protection.

I. INTRODUCTION

The demand for high-precision indoor localization systems (ILS) is growing rapidly. The applications, which critically depend on localization accuracy, include smart-phone based navigation apps, large-scale internet of things (IoT) systems and autonomous robotics. Furthermore, the higher the precision with which the location of the user, IoT sensors and the robots is estimated, the more functions the IoT and robotics systems can perform. The development of the Global Positioning System (GPS) was a breakthrough in the field of positioning. However, it provided m-level accuracy, while many robotics and industrial systems require cm-level precision. Relying on GPS indoors is additionally problematic, since without a line-of-sight (LoS) GPS signals are severely attenuated.

Cm-level localization accuracy has been achieved in [1] by a system of intercommunicating electromagnetic (EM) transceivers. This demonstrates that EM indoor localization systems (ILS) are a suitable alternative to GPS. In addition, the transceiver chips or boards required by the ILSs can be easily integrated into a robot, a smartphone or a communications router. The resulting ILSs also have a suitable range of up to 900m [2]. Despite their high accuracy, state-of-the-art ILSs still face several practical challenges, two of which are addressed in this paper. The first challenge is the deployment of ILS in non line-of-sight (NLoS) and dynamic environments. Most high accuracy ILSs are developed and tested in either LoS or static NLoS environments [1]. However, in reality people and robots move around public buildings and factories, larger furniture and machinery is replaced over time. This severely degrades the accuracy of state-of-the-art ILS [3], [4]. Meanwhile, the second practical constraint is the integration of a low-complexity and secure user privacy protection into the ILSs.

ILSs, that similar to GPS, measure the distances or angles between a receiver and a set of access points (APs) and then calculate the user's location using trilateration, triangulation,

The associate editor coordinating the review of this manuscript and approving it for publication was Fakhrul Alam.

or multilateration [5]–[7] are accurate [2], [8]. However, they require a LoS between the user's device and the APs to function. On the other hand, fingerprinting-based ILSs perform equally well in LoS and NLoS conditions [6]. Therefore, the localization approach developed in this paper is based on fingerprinting. Fingerprinting-based ILS compare a query fingerprint measured by the user to a previously created fingerprint map. The fingerprints themselves can either be based on the received signal strength indicator (RSSI) [6], [9]–[13] or channel state information (CSI). The accuracy of practical RSSI-based ILSs is normally several meters which is insufficient for most robotics and industrial applications. On the other hand, CSI-based fingerprinting systems have been shown to achieve accuracies of up to 1-2 cm in an NLoS environment [1]. However, while conventional CSI-based fingerprinting schemes are accurate in a stationary environment their accuracy decreases significantly if there are changes or moving objects in the environment. If a fingerprint that is calculated from the channel impulse response (CIR) [14] or the channel frequency response (CFR) [1], [15], [16], [16]–[20] and is measured at a fixed location, fluctuates because of changes in the environment, it will no longer be similar to the map entry corresponding to that location. The reasons for this are further explained in Sections IV-I and III. In the author's previous work [21]–[24] the novel multipath component analysis (MCA) localization algorithm is proposed. The MCA uses the multipath delay profile (MDP) of a received signal as a fingerprint and excludes and includes individual multipath components in the calculation of the similarity between a reference and query fingerprint. Therefore, the positioning accuracy of the proposed fingerprinting algorithm is unaffected by moderate changes in the indoor environment. Moreover, this paper also shows that the MDP fingerprint structure and MCA algorithm are uniquely suited to implement user privacy protection.

The second practical requirement for an ILS addressed in this paper is user privacy. If a malicious party knows the location of a user, it can make inferences about the user's health, shopping habits or other private information. It can also uncover trade secrets by tracking the movement of objects inside a factory. The communication messages between the user and the ILS server can easily be encrypted, however this measure will not protect the user from a malicious ILS. This can be the case if the localization system is provided by a party other than the user or factory/warehouse owner. The objective of ILS privacy protection is, therefore, for the user to be able to obtain his or her location from the ILS server without the server knowing what that location is. Unfortunately, existing *K-anonymity* [25]–[32] and *the Paillier cryptosystem* [33]–[39] -based privacy protection algorithms either have an extremely high computational complexity, interfere with the communications infrastructure or do not provide the required level of protection. *Camouflage*-based privacy protection approaches [32], [40]–[42] do not have the above disadvantages. In camouflage-based privacy protection schemes the user creates a number of *fake* fingerprints and sends them to the ILS with the measured fingerprint (see Fig. 5). The ILS does not know which fingerprint corresponds to the true location of the user. We refer to the artificially created fingerprints as *camouflage fingerprints* and to the corresponding locations computed by the ILS as *candidate locations*. This scheme has two additional advantages. Firstly, no changes have to be made to the communication infrastructure and protocol between the user and the ILS server. Secondly, the user's degree of privacy and the scheme's complexity are a function of the number of camouflage fingerprints the user sends to the ILS server. Thus, the scheme allows the user to control the degree of privacy according to his requirements, the available computational power and data transmission volume. However, to the best of the author's knowledge, no camouflage-based privacy protection scheme currently exists for CSI-based fingerprinting. The challenges for implementing camouflage privacy protection for CSI-based fingerprinting are further discussed in Section IV-I.

In this paper the MCA algorithm is extended to include a novel modification of the camouflage-based privacy protection scheme. Unlike the existing schemes, the proposed algorithm is able to generate camouflage CSI fingerprints. This is done by using the MDP as a fingerprint and by creating partial instead of full camouflage fingerprints. In the proposed approach, the user generates partial fingerprints by randomly selecting a subset of the multipath delays in the measured MDP. In addition to the measured partial fingerprints the user also generates partial camouflage fingerprints. The ILS selects multiple candidate locations for each partial fingerprint and returns them to the user, who locally determines his or her true position. As is detailed in Section III-C, a multipath partial fingerprint is much easier to fake than a full or even partial CSI fingerprint. For example, if a subset of CFR of CIR taps is used as a partial fingerprint, that fingerprint might still be unique to a location and give the server an estimate of where the user is. One partial MDP fingerprint however, could be measured at several locations in the environment with equal likelihood. This paper, therefore, demonstrates that the multipath-based MDP fingerprint structure and the MCA algorithm are ideally suited for implementing light-weight and secure privacy protection. In the proposed scheme the user controls the degree of privacy and the exchanged data volume by selecting the number and length of the MDP camouflage fingerprints. It should also be noted, that the communication protocols used by the ILS do not need to be changed to implement this privacy protection scheme. Due to the lack of a standard metric for evaluating ILS privacy, several heuristics are proposed. The initial conference publication [21], presented the core concept of the MCA algorithm and an initial simulation-based validation. In this paper the MCA approach is augmented with a novel privacy protection scheme and fully validated and tested in a ray-tracing simulation and in measurements with the ultra-wideband(UWB) communication standard [2] and the DWM1000 chip [2]. The experimental results obtained in

this paper show an average localization error of 6 cm for a very slow moving robot and a localization accuracy of 30 cm for a robot moving at a fast walking pace. The static measurements were performed with an average distance of 3 cm from each query to the closest reference fingerprint. Therefore, the obtained 5 cm localization accuracy is comparable to the state-of-the-art. At the same time, the proposed system offers additional benefits of privacy and robustness.

The paper is organized as follows. Section II presents the system model. The proposed multipath-based localization scheme is detailed in Section III. The proposed novel privacy protection scheme and the derived evaluation metrics are presented in Section III-C. Section IV-A contains the simulation results. Section IV-F evaluates the algorithms on measurement data. The merit of the proposed approach is compared to the state-of-the-art in Section IV-I. The conclusion is presented in Section V. In this paper, sets are denoted with non-italic bold characters. Vectors and arrays are denoted with bold italic characters.

II. SYSTEM MODEL

This section presents the assumed system model and the ILS requirements. A fingerprinting-based ILS is assumed to be structured as follows. When an indoor localization system (ILS) is installed, certain measurements, or *reference fingerprints* are collected at a set of *reference points* throughout the indoor environment. The reference fingerprints and the corresponding reference points are stored in a *map*. This is referred to as the *off-line* or *training phase* [43]. In the *on-line* phase, the user collects analogous measurements at his location and sends them to the ILS. Note, this communication can occur over any medium, not necessarily over the access points (APs) used for fingerprinting. The ILS server compares the resulting *query* fingerprint to the map. A scalar similarity value is computed for each reference fingerprint stored in the map. This *similarity metric* represents how similar a reference fingerprint is to the query. Typical similarity metrics include the Euclidean distance between two fingerprint vectors [43] and the time reversal resonating strength [1]. The communication between the user, the ILS server and the APs is illustrated in Fig. 1.

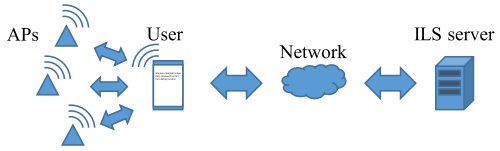


FIGURE 1. Communication between the user, APs and the ILS server.

As an EM wave propagates at the speed of light, the distance a signal travels corresponds to a delay at the receiver. The received signal $r(t)$ is composed of a sum of multiple delayed and attenuated copies of the original signal $s(t)$.

$$r(t) = \sum_k a_k s(t - \tau_k) + z(t), \tag{1}$$

where a_k is the attenuation undergone by the signal along the k-th path from the transmitter to the receiver, and τ_k is its delay. The term $z(t)$ represents random noise added to the signal at the receiver [6]. With $\tau_k = d_k/c$, we obtain

$$r(t) = \sum_k a_k s(t - d_k/c) + z(t), \tag{2}$$

where d_k is the length of the k-th reflected or line-of-sight path and is referred to as the k-th *multipath component*, and c is the speed of light [44]. This is illustrated in Fig. 2 as the signal reflects multiple times from the walls, floors, ceilings and objects before it reaches the receiver. When the obstacle, marked with O, is not present, the signal reaches the receiver with the delays $\{[d^q_{j,1}, \ldots, d^q_{j,4}]\}$. The obstacle blocks the propagation paths $d^q_{j,1}$ and $d^q_{j,2}$ and creates the new propagation paths $d^q_{j,5}$ and $d^q_{j,6}$. Multipath components have been previously used for localization in [8], [45] and for simultaneous localization and mapping (SLAM) in [46]–[48]. In this paper, the set of all multipath components $\{d_k\}$ calculated for a received signal is referred to as a *multipath delay profile (MDP)*.

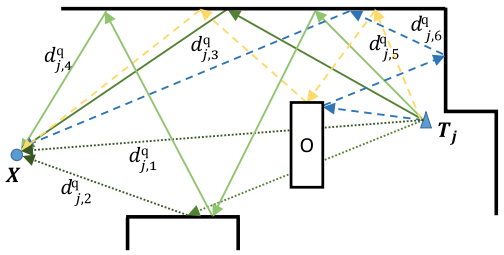


FIGURE 2. Example multipath reflections with and without the obstacle O.

The following assumptions are further made about the system model shown in Fig. 1.

A. ATTACK SCENARIO

the ILS server or a third party accesses the communication messages, calculates and stores the location of the user over time.

B. SYSTEM PROPERTIES

firstly, the ILS server is truthful-but-curious. While it returns the correct locations in response to the user's queries, it may track, analyze and exploit the user's location information. Secondly, the user does not know the indoor geometry or have the fingerprint map. The user may be a human with a smart device or a robot with limited sensors. The user may learn the indoor geometry over time, however, the camouflage fingerprints generated by the user should be believable even when he or she does not have any information about the geometry or environment. Thirdly, the communication

between the user and the server may be intercepted. The location of the user needs to be protected even if the ILS is not encrypting the communication. The ILS may do this to speed up the localization, especially when it is communicating with many users. And forth, there is no point for the ILS server to protect the fingerprint map from the user. The user can collect measurements and construct his or her own map.

C. ILS PERFORMANCE REQUIREMENTS

Firstly, the user should be able to obtain his or her location as accurately as possible. Secondly, the user should be able to obtain his or her location in a dynamic environment. Thirdly, the volume of data exchanged between the user and the ILS server should be as small as possible. The ILS should not be required to send the user the entire fingerprint database. And forth, the computational load on the user should be as low as possible.

D. DESIRED FEATURES OF ILS PRIVACY PROTECTION

Firstly, the ILS should not be able to estimate the location of the user up to a given certainty. The privacy scheme should conceal the general area the user is in, not just the exact coordinates. Secondly, the degree of privacy should be guaranteed regardless of the number of users in the system. Thirdly, the system should be able to guarantee privacy for both moving and stationary users. Forth, no changes, such as an additional encryption layer, should be introduced to the established communication protocols. The localization algorithm and the data exchanged by the user and the ILS can be modified to implement user privacy protection, but not the protocols over which this data is sent. And fifth, the user should not need to hide his identity from the ILS.

III. PROPOSED APPROACH: MULTIPATH COMPONENT ANALYSIS

This section summarizes the MCA algorithm originally proposed in 2017 at the international conference on indoor positioning and indoor navigation [21] and presents the novel privacy protection scheme proposed in this paper.

The MCA algorithm uses multipath delay profile (MDP) fingerprints for the following reason. RSSI and CSI fingerprints aggregate the information about the geometry and material properties into all vector entries. When some feature of the geometry or an object in the environment changes, the power and frequency representations of the channel such as the RSSI and CFR fluctuate unpredictably. This means that a change in the environment will effect all the entries in RSSI and CFR vectors. In that case it is extremely difficult to pinpoint the changes introduced into the fingerprints by a dynamic environment. A CIR is the sum of impulse responses along all of the individual propagation paths. Since these impulse responses overlap, a change on one propagation path will remove, add or change the amplitude of one CIR peak. However, it will also unpredictably effect the magnitude of multiple CIR taps that belong to other propagation paths. On the other hand, the propagation path lengths shown in Fig. 2 cannot fluctuate, as they are tied to physical distances. Individual propagation paths in Fig. 2 can be blocked and new paths can appear as objects move in the indoor environment, however, the rest of the multipath components remain the same and can be used for localization. This makes the MDP a more robust fingerprint than the RSSI and CSI. The proposed localization scheme is illustrated in Fig. 3. The multipath delays are extracted from the measured CIR. After the multipath delays have been extracted, the multipath component analysis (MCA) algorithm is used to calculate the location of a receiver.

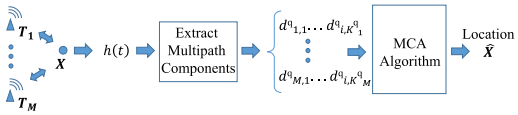


FIGURE 3. Proposed multipath-based localization scheme.

A. MULTIPATH DELAY PROFILE

A multipath delay profile (MDP) is a set of vectors that contain the lengths of all paths that a signal will follow from a query point to each of the transmitters [21]. Two example MDPs $\{[d^q_{j,1}, .., d^q_{j,4}]\}$ and $\{[d^q_{j,3}, \ldots, d^q_{j,6}]\}$ are shown in Fig. 2. The first MDP is produced by the geometry without the obstacle, and the second MDP corresponds to the geometry with the obstacle O. *Reference* MDP fingerprints, $\mathbf{D}_i = \{\boldsymbol{d}_{i1}, .., \boldsymbol{d}_{iM}\}$ with $i = 1 \ldots N$ are measured in the off-line phase of a fingerprinting algorithm at N reference locations $\boldsymbol{X}_i$, with $i = 1 \ldots N$. The vectors $\boldsymbol{d}_{ij} = [d_{ij,1}, .., d_{ij,K_{ij}}]$ contain the lengths of the propagation paths on which the signal travels from the transmitter $\boldsymbol{T_j}$ to the point $\boldsymbol{X}_i$. The *query* MDP $\mathbf{D}^q = \{\boldsymbol{d}^q_1, \ldots, \boldsymbol{d}^q_M\}$ is measured by the user in the on-line phase of the localization algorithm at an unknown location $\boldsymbol{X}^q$. M is the number of transmitters in the system. When a fingerprint contains all of the extracted multipath components, it is referred to it as a *full* fingerprint. A *partial* fingerprint $\mathbf{D}^q_p = \{\boldsymbol{d}^q_{p1} \subseteq \boldsymbol{d}^q_1, \ldots, \boldsymbol{d}^q_{pM} \subseteq \boldsymbol{d}^q_M\}$ is a subset of the multipath components of the full MDP. In Fig. 2, $\{[d^q_{j3}, d^q_{j4}]\}$ is a partial fingerprint of the query fingerprint $\{[d^q_{j1}, .., d^q_{j4}]\}$. This paper demonstrates that the multipath-based fingerprint structure and fingerprint comparison metric proposed in [21] are ideally suited for the implementation of a privacy protection scheme. The localization scheme and multipath component analysis (MCA) algorithm [21] are briefly summarized in the following section.

B. MULTIPATH COMPONENT ANALYSIS (MCA) ALGORITHM

The multipath component analysis (MCA) algorithm proposed in [21] is used to calculate the similarity metric between two fingerprints. Algorithm 1 in Fig. 4 shows its pseudo-code. In this paper, the reference fingerprint with the highest similarity metric value is considered to be the user's location. Techniques such as k-nearest-neighbors (kNN),

Algorithm 1: MCA Localization Algorithm [21]

Data: Query multipath delay profile
$\mathbf{D}^q = \{\boldsymbol{d}_j^q\}, j = 1..M$
transmitters $\{\boldsymbol{T}_j\}, j = 1..M$
fingerprint map $\mathbf{MAP} = \{(\boldsymbol{X}_i, \mathbf{D}_i)\}, i = 1..N$
Parameters: Similarity threshold ε
Result: $\hat{\boldsymbol{X}}$- Estimated location of the receiver

```
for ∀X_i in the fingerprint map do
    for ∀ transmitter T_j do
        d_ij ← D_i(j)
        for ∀ d^q_{j,k} ∈ d^q_j do
            d* ← argmin_{d^q ∈ d_ij} |d^q_{j,k} − d*|
            if |d^q_{j,k} − d*| < ε then
                γ(D^q, D_i|T_j) ← +(ε − |d^q_{j,k} − d*|)^2
            end
        end
    end
end
i ← argmax_i Σ_j γ(D^q, D_i|T_j)
X̂ ← X_i
```

FIGURE 4. MCA Algorithm.

which calculate an average of k reference locations corresponding to fingerprints that are most similar to the query, can be used in the future together with the MCA algorithm to further increase the localization accuracy. The MCA algorithm can be used to calculate the similarity metrics for partial as well as full fingerprints. The MCA algorithm is robust to changes in the environment because it matches individual query multipath delays to the reference fingerprints. Only close matches are included in the calculation of the similarity metric. In this way, propagation paths that disappeared from or were added to the query MDP due to a new obstacle are automatically excluded from the calculation [21]. The similarity metric $\gamma(\mathbf{D}^q, \mathbf{D}_i)$ is calculated individually for each transmitter and then summed up to one value as

$$\gamma(\mathbf{D}^q, \mathbf{D}_i) = \sum_{j=1}^{M} \gamma(\mathbf{D}^q, \mathbf{D}_i|\boldsymbol{T}_j). \tag{3}$$

The MCA algorithm matches multipath components in the vector $\boldsymbol{d}_j^q$ to the multipath components stored in $\boldsymbol{d}_{ij}$. Two distances $d_{j,k}^q$ and d^* are considered matched if the difference $|d_{j,k}^q - d^*|$ is minimized by $d^* \in \boldsymbol{d}_{ij}$ and $|d_{j,k}^q - d^*| < \varepsilon$. This means that d^* is the closest match to $d_{j,k}^q$ from the vector $\boldsymbol{d}_{ij}$. The similarity metric is a measure of how many matches were found and how close they were. Query multipath components which don't have similar counter parts in the reference fingerprint, and thus correspond to changes in the environment, are automatically excluded from the similarity metric calculation and vice versa. For each match, the index k is added to the set $\mathbf{Q}_{ij}$ and $(\varepsilon - |d_{j,k} - d^*|)^2$ is added to the similarity metric

$$\gamma(\mathbf{D}^q, \mathbf{D}_i|\boldsymbol{T}_j) = \sum_{k \in \mathbf{Q}_{ij}} (\varepsilon - |d_{j,k}^q - d^*|)^2 \tag{4}$$

$$\mathbf{Q}_{ij} = \{k | \exists d^* \in \boldsymbol{d}_{ij} : |d_{j,k}^q - d^*| \rightarrow min \cap |d_{j,k}^q - d^*| < \varepsilon\}. \tag{5}$$

In the scenario when $\mathbf{D}^q$ is a full fingerprint, the MCA algorithm returns the user's estimated location. When a partial fingerprint is compared to the map, the algorithm should return κ candidate locations or guesses of the ILS server. The parameters ε and κ are to be chosen empirically. The computation complexity of the MCA algorithm is discussed in [22].

C. PROPOSED PRIVACY PROTECTION SCHEME

This section details the proposed privacy protection scheme and the proposed heuristics for evaluating the degree of location privacy. The privacy protection scheme has to be built into the communication protocol between the user and the server. Its main objective is to allow the user to obtain his or her location from the ILS server, without the server being able to track the user.

A conventional camouflage privacy protection scheme is illustrated on the left in Figure 5. The user generates fake fingerprints and sends them to the indoor localization system (ILS) and the ILS calculates locations of the real and fake fingerprints. This is contrasted to the proposed privacy protection protocol illustrated on the right. N_p partial fingerprints $\{\mathbf{D}_{p1}^q, \ldots, \mathbf{D}_{pN_p}^q\}$ of length np are generated by the user as random subsets of the measured query $\mathbf{D}^q$. For each partial fingerprint, the user then generates N_c fake camouflage fingerprints $\{\mathbf{D}_{c1}^q, \ldots, \mathbf{D}_{c(N_T-N_p)}^q\}$ of the same length. Therefore, a total of N_T partial fingerprints are sent by the user to the ILS. Using the multipath component analysis (MCA) algorithm, the ILS determines κ best matches from the map for each partial fingerprint and returns them to the user. In the following, we refer to the reference fingerprints $\mathbf{D}_{ci}$ selected by the server as the *candidate fingerprints* and to the corresponding locations $\boldsymbol{X}_{ci}$ as the *candidate locations*. The user locally runs the MCA algorithm using the measured fingerprint as the query and the candidate fingerprints as the map. It should be noted, that in a state-of-the-art camouflage scheme, the server receives a number of full fingerprints, some of which are real and some fake. It calculates a location for each fingerprint. The user needs to make sure that the camouflage fingerprints are credible. In a conventional camouflage scheme, the server can compare the created fingerprints to the map, find that they are dissimilar to all map entries and know that they are fake. The proposed scheme differs from the state-of-the-art in that the user only generates the partial and not the complete camouflage fingerprints as in [40]. The server receives fingerprint pieces, some of which are real and some of which are fake. Those fingerprint pieces match multiple reference fingerprints and do not clash with the geometry. Therefore, in contrast to classic camouflage schemes, the server cannot simply pick out the query fingerprints that are dissimilar to the map.

The user can generate the camouflage partial fingerprints in two ways. np multipath propagation distances and transmitter IDs can be randomly generated. This method is summarized in Algorithm 2 in Fig. 6. Alternatively, the user can create the camouflage fingerprints by randomly altering the

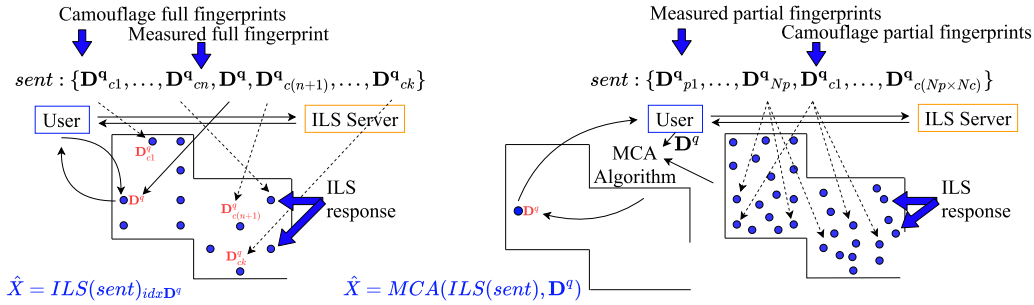


FIGURE 5. Left: Camouflage-based privacy protection, Right: proposed privacy protection protocol.

Algorithm 2: Camouflage Fingerprint Generation I

Data: Measured fingerprint $\mathbf{D}^q = \{\boldsymbol{d}_j^q\}, j = 1...M$

Result: Partial fingerprints to be sent to the ILS $\{\mathbf{D}_{p1}^q, ..., \mathbf{D}_{pN_p}^q, \mathbf{D}_{c1}^q, ..., \mathbf{D}_{c(N_T-N_p)}^q\}$

for $i = 1...N_p$ **do**
  Select random subsets:
  $\mathbf{D}_{pi}^q \leftarrow \{\boldsymbol{d}_{p1}^q \subseteq \boldsymbol{d}_1^q, ..., \boldsymbol{d}_{pM}^q \subseteq \boldsymbol{d}_M^q\}$
  Enforce: $\sum_j |\boldsymbol{d}_{pj}| = np$
end
for $l = 1...(N_T - N_p)$ **do**
  Set random propagation distances:
  $\mathbf{D}_{cl}^q \leftarrow \{[rand_1, ..., rand_{K_j}]\}, j = 1...M$
  Enforce: $\sum_j K_j = np$
end

FIGURE 6. Camouflage fingerprint generation algorithm with random multipath values.

Algorithm 3: Camouflage Fingerprint Generation II

Data: Measured fingerprint $\mathbf{D}^q = \{\boldsymbol{d}_j^q\}, j = 1...M$

Result: Partial fingerprints to be sent to the ILS $\{\mathbf{D}_{p1}^q, ..., \mathbf{D}_{pN_p}^q, \mathbf{D}_{c1}^q, ..., \mathbf{D}_{c(N_T-N_p)}^q\}$

for $i = 1...N_p$ **do**
  Select random subsets:
  $\mathbf{D}_{pi}^q \leftarrow \{\boldsymbol{d}_{p1}^q \subseteq \boldsymbol{d}_1^q, ..., \boldsymbol{d}_{pM}^q \subseteq \boldsymbol{d}_M^q\}$
  Enforce: $\sum_j \left|\boldsymbol{d}_{pj}^q\right| = np$
  for $l = 1...N_c$ **do**
    Shuffle the transmitter IDs:
    $\mathbf{D}_{c(N_c\times(i-1)+l)}^q \leftarrow \{[d_{j1}^q, ..., d_{jK_j}^q]\}$,
    $j = 1...M$
    Enforce: $d_{jk}^q \in \boldsymbol{d}_{pr}^q \in \mathbf{D}_{pi}^q \cap \sum_j K_j = np$
  end
end

FIGURE 7. Camouflage fingerprint generation algorithm with random transmitter IDs.

transmitter IDs of the partial fingerprints $\{\mathbf{D}_{p1}^q, \ldots, \mathbf{D}_{pN_p}^q\}$. The propagation distances in the fingerprints remain the same. The approach is summarized in Algorithm 3 in Fig. 7.

It should be noted that the complexity of a camouflage scheme is defined by the number of camouflage fingerprints, their generation and localization effort. Since in this case the one camouflage fingerprint is generated in constant time and the complexity of the MCA algorithm is linear with the size of the fingerprint database or better [22], the complexity of the proposed privacy protection scheme is $O(N_T \times N + \kappa \times N_T)$. The proposed privacy protection approach has several distinct advantages. The computational load on the user is low, as complex operations do not need to be performed in order to ensure the credibility and wide distribution of the camouflage fingerprints. The real and camouflage partial fingerprints are automatically credible as they contain only a subset of a fingerprint's information and thus are similar to multiple reference fingerprints. Since the transmitter IDs of the camouflage fingerprints are generated randomly, the candidate locations will be located in very different parts of a building. In addition, the user can control the number of candidate locations and the degree of privacy by setting the numbers of total and camouflage partial fingerprints N_T and N_p. The privacy protection approach is possible due to the structure of the MDP fingerprints. In order to apply it to CIR or CFR-based fingerprints, the individual propagation distances need to be extracted and the fingerprints need to be converted to an MDP structure.

It should be noted that in contrast to ILSs using the Paillier cryptosystem, ILSs that use k-anonymity and camouflage-based privacy protection can never fully protect the users privacy. The server can use statistical techniques and analyze all the query data sent by all users. Eventually the ILS can find patterns in the data and identify the user. This also holds for the proposed scheme. On the other hand, while the Paillier cryptosystem fully protects user privacy, it requires heavy computations and a lot of data transfer. The goal of k-anonymity and camouflage-based privacy protection schemes, including the proposed approach, is therefore, to make it as hard as possible for the ILS to track the users, with as little computational load as possible on the users.

D. PROPOSED PRIVACY METRICS

A scalar privacy metric is needed to quantify the performance of the proposed scheme. The authors of this paper are not aware of a general metric applicable to all camouflage privacy protection schemes. Existing privacy protection schemes are often evaluated using specialized metrics. For example, the privacy measure proposed in [29] is specific to the proposed k-anonymity and differential privacy-based scheme. Therefore, two quantitative measures of the degree

of privacy of a stationary user and a metric for evaluating the privacy of a moving user are derived. Since the user's location is protected by the camouflage locations, the distribution of those locations is evaluated to determine the degree of privacy protection. It should be noted, that the metrics derived in this section are easy-to-compute heuristics that estimate the degree of privacy. The metrics do not attempt to derive an exact privacy value. The metrics can also be used to estimate the privacy protection of a k-anonymity scheme, where the ILS server knows only a list of possible user locations.

Figure 8 illustrates four example distributions of candidate points. The top left distribution hides the user's location. In the other three subfigures there are two areas where the user is likely to be according to the distribution of either the candidate points themselves or their occurrence frequency and similarity metric values. Figure 11 shows similar candidate point distributions for a moving user. The following presents four heuristics that can be used to approximate the location privacy of a user.

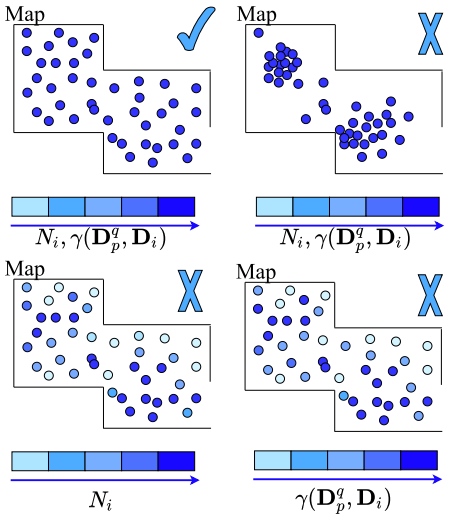


FIGURE 8. Privacy in example candidate point distributions.

1) PRIVACY METRIC 1: NUMBER OF UNIQUE CANDIDATE POINTS

For each partial fingerprint sent by the user the ILS determines κ best matching reference fingerprints. As multiple partial fingerprints are sent by the user, a reference fingerprint can be selected as a match and, thus, picked multiple times. Let N_i be the number of times $\mathbf{D}_i$ is considered "matched" in one localization request.

Statement 1: Let N_i be the number of partial fingerprints sent by the user to the ILS within one localization step, for which the ILS server selected fingerprint $\mathbf{D}_i$ as a candidate. The degree of privacy protection in a system is highest when N_i is equal for all reference fingerprints.

Proof: The higher N_i for a reference point $\boldsymbol{X}_i$, the higher the belief of the ILS that the user is located at $\boldsymbol{X}_i$. If N_i is equal for all reference locations, the ILS cannot prefer any. □

2) PRIVACY METRIC 2: CAMOUFLAGE FINGERPRINT CREDIBILITY ESTIMATE

Proposition 1: The more uniform the distribution of N_i and the more unique candidate fingerprints are calculated by the server, the better the user's privacy is protected.

Proof: If the camouflage fingerprints differ significantly from the reference fingerprints stored in the map, the similarity metric values that ILS server calculates for them will be much lower than for the real query.

Proposition 2: The belief of the ILS server that the user is located at reference point $\boldsymbol{X}_i$ can be approximated as the sum of the similarity metric values, calculated when $\boldsymbol{X}_i$ is picked as a candidate location.

$$\rho(\boldsymbol{X}_i) = \sum\nolimits_{\mathbf{D}_s^q \in \mathbf{L}(\mathbf{D}_i)} \gamma(\mathbf{D}_s^q, \mathbf{D}_i) \tag{6}$$

$$\hat{\rho}(\boldsymbol{X}_i) = \frac{\rho(\boldsymbol{X}_i)}{\sum_{k=1}^{N} \rho(\boldsymbol{X}_k)} \tag{7}$$

$$\mathbf{L}(\mathbf{D}_i) = \{\forall \mathbf{D}_s^q \mid \gamma(\mathbf{D}_s^q, \mathbf{D}_i) \in \ top\ \kappa\ max\ values\}, \tag{8}$$

where $\mathbf{D}_s^q$ are the partial fingerprints sent by the user.

Proof: If $\gamma(\mathbf{D}_p^q, \mathbf{D}_{ci})$ is high for a candidate location $\boldsymbol{X}_i$, the likelihood, that from the point of view of the ILS server $\boldsymbol{X}_i$ is the location of the user, is also high. The same holds for the value N_i in Statement 1. $\rho(\boldsymbol{X}_i)$ combines the two parameters. $\hat{\rho}(\boldsymbol{X}_i)$ is normalized. □

Proposition 3: The entropy $H(\hat{\rho}(\boldsymbol{X}_i))$ can be used as a measure of location privacy of the user.

Proof: According to the definition of entropy, the higher $H(\hat{\rho}(\boldsymbol{X}_i))$ is, the higher the uncertainty of the ILS about the user's location will be. Entropy is also used to measure the degree of privacy in [25], [28] and [32]. □

3) PRIVACY METRIC 3: AMOUNT OF CLUSTERING IN THE SPATIAL DISTRIBUTION OF THE CANDIDATE FINGERPRINTS

The ILS should not be able to tell which general area the user is located in. If the candidate points are located close to each other, the ILS would know the rough location of the user. Therefore, the candidate points should be distributed over as large an area as possible, and the distances between neighboring candidate points should be as large as possible.

Proposition 4: The parameter ω can be used to characterize the spatial distribution of the candidate points, with

$$\omega = \frac{1}{\omega_u} \sum_{k=1}^{N} \sum_{l=1}^{N} \hat{\rho}(\boldsymbol{X}_k) \times \hat{\rho}(\boldsymbol{X}_l) \times \sqrt{d(\boldsymbol{X}_k, \boldsymbol{X}_l)}, \tag{9}$$

$$\omega_u = \frac{1}{N^2} \sum_{k=1}^{N} \sum_{l=1}^{N} \sqrt{d(\boldsymbol{X}_k, \boldsymbol{X}_l)}, \tag{10}$$

where $d(\boldsymbol{X}_k, \boldsymbol{X}_l)$ is the euclidean distance between $\boldsymbol{X}_k$ and $\boldsymbol{X}_l$. N is the number of reference fingerprints in the map.

Proof: Consider the hypothetical distribution of candidate points calculated by an ILS that is illustrated in Fig. 9. If point $\boldsymbol{X}_i$ is shifted to location $\boldsymbol{X}_{i'}$, it is clear that the area

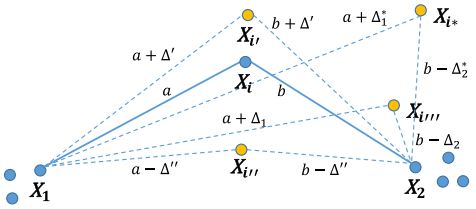


FIGURE 9. Illustration of the proof of Proposition 4. The point X_i is shifted to $X_{i'}$, $X_{i''}$, $X_{i'''}$ and X_{i*}, $a \geq b$.

covered by the candidate points increases. Therefore, the privacy of the user in the system increases. As a privacy estimate ω needs to increase as well and it does so according to Eq. 9. In the same manner, if $\boldsymbol{X}_i$ is shifted to $\boldsymbol{X}_{i''}$, it moves closer to the point clusters around $\boldsymbol{X}_1$ and $\boldsymbol{X}_2$. The candidate points become less spread out in space and the intuitive amount of user privacy and the value of the metric ω decrease. Let $\boldsymbol{X}_i$ be shifted to location $\boldsymbol{X}_{i*}$. As $\Delta_1^* > \Delta_2^*$, $\boldsymbol{X}_i$ was moved is further away from $\boldsymbol{X}_1$ than it was moved closer to $\boldsymbol{X}_2$. In this case, it is difficult to intuitively determine whether the area covered by the candidate points and the location privacy of a user for whom the ILS calculated these candidate locations, increased or decreased. We make the following approximation. We state that, in this case, the change in privacy corresponds to the change in the value of ω. Let $\boldsymbol{X}_i$ be shifted to $\boldsymbol{X}_{i'''}$, so that $\Delta_2 > \Delta_1$. Intuitively, the area covered by the reference points decreases. In the following, we will show that the value of ω decreases as well. It can be easily seen that ω decreases if $\sqrt{a}+\sqrt{b} > \sqrt{a+\Delta_1}+\sqrt{b-\Delta_2}$. As both terms are positive, we will compare their squares.

$$(\sqrt{a+\Delta_1}+\sqrt{b-\Delta_2})^2 = a+b-(\Delta_2-\Delta_1) +2\sqrt{ab-\Delta_2(a-b)-(\Delta_2-\Delta_1)b-\Delta_1\Delta_2} \quad (11)$$

Since $a \geq b$, $\Delta_1 < \Delta_2$, the value of ω decreases. The term $\rho(\boldsymbol{X}_k) \times \rho(\boldsymbol{X}_l)$ is used to only include the distances between likely candidate points into the sum. It is easy to show that, if $\rho(\boldsymbol{X}_i)$ is uniform, $\omega = 1$. □

It should be noted that the similarity metric is used to calculate the above privacy metrics. If the ILS server is using a special metric to compare fingerprints when trying to detect fake ones and that metric is different from the similarity metric used for localization, then the "fake fingerprint detection" metric should be used for privacy evaluation.

4) PRIVACY METRIC 4: PRIVACY OF A MOVING USER

Next, we consider a moving user attempting to localize himself at regular intervals τ_L. We define d_L as the average distance the user moves between two consecutive localization steps. Four example hypothetical candidate point distributions are shown in Fig. 11. In the candidate point distribution on the top left the user's position is well protected. In the examples on the top right and bottom left the ILS server can identify the user relatively quickly, and in the bottom right

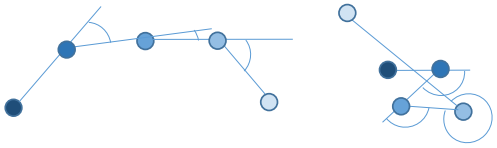


FIGURE 10. Two candidate trajectories. The left trajectory is more likely to be a natural trajectory of the user.

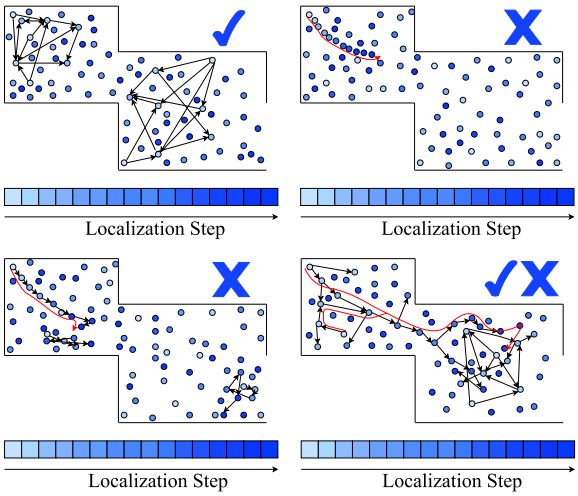


FIGURE 11. Privacy in example candidate point distributions for a moving user.

example the server can eventually identify the user but needs to track many potential trajectories. The guess trajectories of the ILS are marked in black and the identified user trajectory is marked in red.

Statement 2: If $d_L < E[d(\boldsymbol{X}_{c,t}, \boldsymbol{X}_{c,t+\tau_L})]$ *the ILS can easily identify the user among the candidate points.* $E[d(\boldsymbol{X}_{c,t}, \boldsymbol{X}_{c,t+\tau_L})]$ *is the average distance between two candidate locations at time* t *and at time* $t+\tau_L$.

Proof: As illustrated in the top right of Fig. 11, if d_L is small compared to the distances between camouflage fingerprints, the ILS can find the user at a trajectory made up of close-by consecutive candidate points. □

Having the distances between candidate fingerprints in consecutive localization steps smaller or equal to the distance the user moves in one step is a necessary but not sufficient condition to guarantee privacy. If the user is tracked over enough time and the ILS server has infinite resources available, it will eventually be able to identify the user. The ILS can keep track of and analyze all possible trajectories among the candidate points. Over time the ILS will be able to eliminate more and more trajectories as they will have an unnatural shape. Figure 10 shows two trajectories. By evaluating the angles between the line segments, the ILS can identify the left trajectory as valid and the right trajectory as unlikely to belong to a human user. The exact amount of time it would take for the ILS to find the user depends on the sophistication of the pattern recognition algorithms and the computational

power available to the ILS. Therefore, instead of determining whether or not the ILS can find the user, the proposed metric estimates how difficult and computationally expensive it is for the ILS to do so.

Proposition 5: Let $\eta(d)$ be the average number of candidate locations $\boldsymbol{X}_{c,t+\tau_L}$, calculated by the ILS at time $t+\tau_L$, located within a distance d from a candidate location $\boldsymbol{X}_{c,t}$, previously calculated at time t. The parameter $\eta(d_L)$ can be used to characterize the degree of privacy of a moving user.

$$\eta(d) = E\left[\left|\{\forall \boldsymbol{X}_{c,t+\tau_L} \mid d(\boldsymbol{X}_{c,t+\tau_L}, \boldsymbol{X}_{c,t}) \leq d\}\right|\right] \quad (12)$$

Proof: The higher the value of $\eta(d_L)$, the higher the number of candidate trajectories exist with a step size less than d_L. This means there will be more candidate trajectories for the ILS to consider. At time $t+\tau_L$, $\eta(d_L)$ new candidates will be created out of one candidate trajectory, existing at time t. Therefore, the complexity of the tracking procedure for the server will increase exponentially with $\eta(d_L)$. □

IV. EVALUATION RESULTS AND DISCUSSION

This section presents the simulated and experimental validation of the MCA localization algorithm detailed in Section III and the privacy protection scheme proposed in this paper and detailed in Section III-C.

A. SIMULATION SETUP

In the simulation-based evaluation, ray-tracing is used to precisely extract the multipath delay profiles (MDPs) from a model of the 3D indoor geometry. The simulation uses virtual transmitters to recursively calculate the multipath delays at the receiver locations. The methodology is further detailed in [23]. The layers of the communication protocol stack are, therefore, not simulated. In some simulated experiments modeled noise is added directly to the multipath components. The geometry used in the simulation is shown in Fig. 12. The planes are used to represent the walls, ceilings and objects in the room. The positions of the transmitters and the reference and query points are shown he bottom of Fig. 12. Both the query and reference points are down-sampled before being plotted. The MDP calculation is performed twice. The geometry colored in green is used to generate the reference fingerprints. When the query fingerprints are calculated, the obstacles colored in blue are added to the geometry. The similarity threshold ε in the MCA algorithm is set to $1m$.

B. LOCALIZATION PERFORMANCE EVALUATION

Figure 13 shows the localization error obtained with trilateration and the proposed multipath component analysis (MCA) algorithm. The ray-tracing simulation uses virtual transmitters [23] to recursively calculate the multipath delays at the receiver locations. The shortest delay, corresponding to the shortest propagation path, is used to perform trilateration using least-squares. This corresponds to ideal time-of-arrival (TOA) ranging. Signal power-based fingerprinting is not simulated for the following reason. In order to calculate

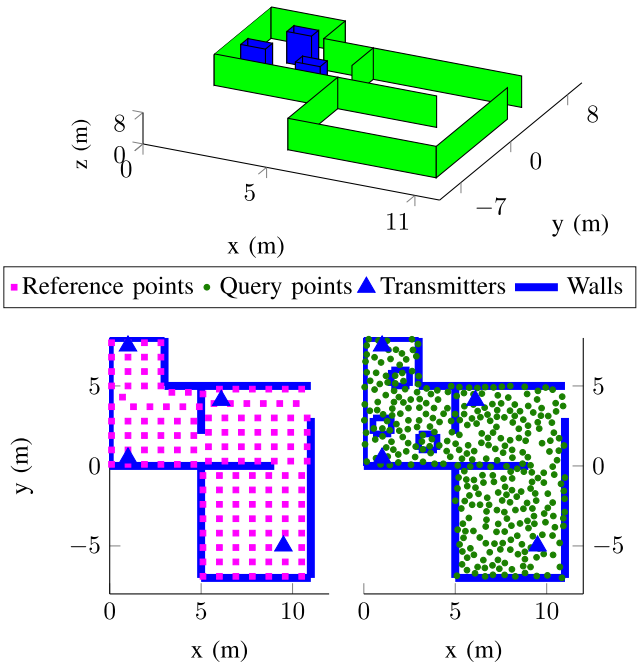


FIGURE 12. Simulation setup. Top: planes representing the indoor geometry (floor and ceiling not displayed). The geometry used for generating the fingerprint maps is colored in green. The three columns, colored in blue, were added to the map before the query fingerprints were generated. Bottom: Transmitter locations and the query/reference points.

realistic RSSI or CFR fingerprints in a ray racing simulation, the signal fading and noise need to be modeled precisely incorporating the material information, interference patterns, antenna parameters. This is currently not possible, the channel fading and signal strength oscillations can be estimated and modeled but those estimates will be imprecise. A signal fading model can be used to compare different CSI-based localization algorithms to each other. However, RSSI and CSI approaches simulated with a fading model cannot be compared to multipath-based schemes simulated with ray-tracing. The figure is generated without noise, noise is added in some of the following experiments. The figure shows that the three obstacles significantly affect the localization accuracy of trilateration-based localization. In order for the trilateration algorithm to work correctly, a LoS needs to exist from the query point to at least 4 of the transmitters. This means that the shadowed area, where localization is not possible, is a combination of several transmitter's shadows. Even in the left most plot where the walls are removed from the rooms, the corners create a large amount of shadowing. The MCA algorithm is shown to be robust against the addition of obstacles. The small amount of error is there because the query points do not coincide with the reference points. The MCA algorithm calculates which reference point the query is closest to and not the exact location of the query.

C. PARTIAL FINGERPRINT LOCALIZATION

Figure 14 shows the localization error obtained when AWGN noise was added to the query and reference

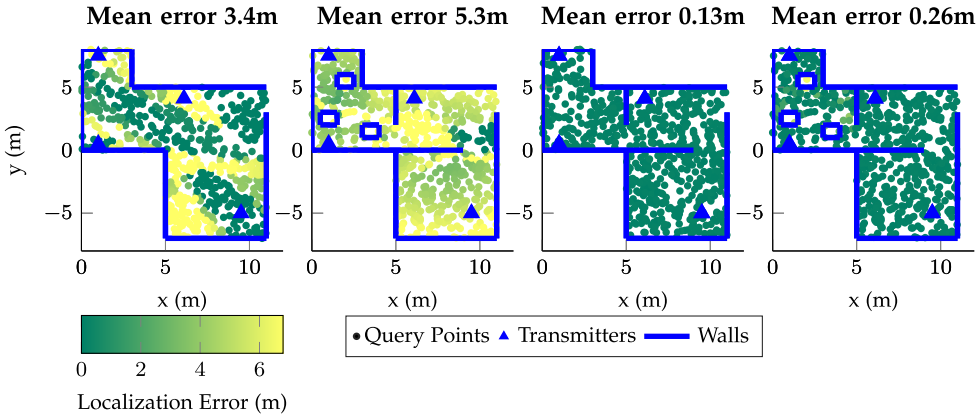


FIGURE 13. Left: Localization error of trilateration walls between the rooms removed. Center Left: Trilateration with obstacles. Center Right: MCA algorithm, reference and query data generated without obstacles. Right: MCA algorithm, obstacles added when the query data was generated. No noise is included in the simulation.

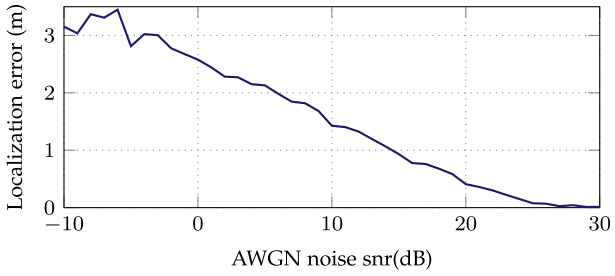


FIGURE 14. Localization error of the MCA algorithm with full fingerprints in the presence of AWGN noise.

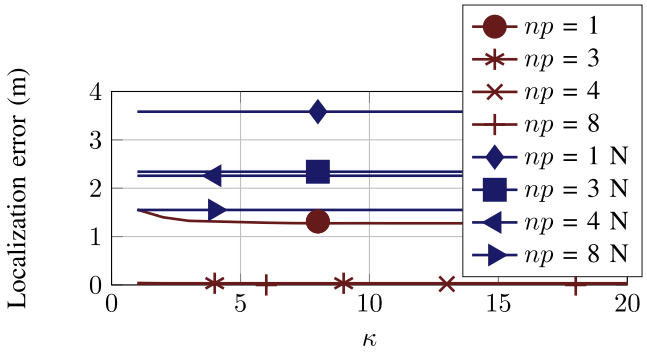


FIGURE 15. Localization accuracy with partial fingerprints. N indicates the presence of noise.

multipath components. Figure 15 shows the average localization error obtained when matching a partial fingerprint to the map. The localization error is evaluated for different values of the partial fingerprint size np and the number of candidates calculated by the ILS for a single partial fingerprint κ. The curves marked with an N show the results after additive white Gaussian noise (AWGN) with $\sigma^2 = 0.25m^2$ was added to the multipath components in the reference and query fingerprints. The results show an expected decrease of the localization accuracy in the presence of noise. They also show that for $\kappa > 3$ the localization accuracy is independent of κ. This shows that using a number of partial query fingerprints instead one full query fingerprint does not decrease the localization accuracy. In the following simulations, we set $\kappa = 3$. It should be noted, that in reality the noise in the multipath components comes from both the environment and the extraction of the multipath components. In a practical system, the noise statistics will, therefore, also depend on the channel and the multipath estimation scheme.

D. PRIVACY EVALUATION FOR STATIONARY USERS

We evaluate the level of user privacy protection in the proposed scheme using the metrics described in Section III-D. Figure 16 shows the results obtained in a simulation without noise. In Figure 17, AWGN with $\sigma^2 = 0.25m^2$ was added to the propagation distances in the reference and query fingerprints. The top figures show the number of candidate fingerprints returned by the indoor localization system (ILS) vs. the number of partial fingerprints sent by the user. It should be noted that the x-axis also controls the algorithm complexity. The black dashed line shows the limit $\kappa \times N_T$. Since the ILS can select the same reference point as a candidate more than once, the number of candidate points begins to saturate for large values of N_T. The two bottom subfigures show the privacy metrics $H(\rho(\boldsymbol{X_i}))$ and ω, derived in Section III-D1. The theoretical upper limits described in Section III-D1 are also plotted. For the curves marked with RF Algorithm 2 is used to generate the camouflage fingerprints, Algorithm 3 is used for curves marked RT.

The results show a trade-off between complexity - the number of partial fingerprints generated by the user, and the amount of privacy protection. They also show that the size of the partial fingerprints np does not significantly affect the degree of privacy protection. The MCA algorithm only searches for the matching propagation distances. It does not penalize the presence of distances in an MDP that were not matched to the reference fingerprint. However, if the ILS used another approach to search for fake fingerprints,

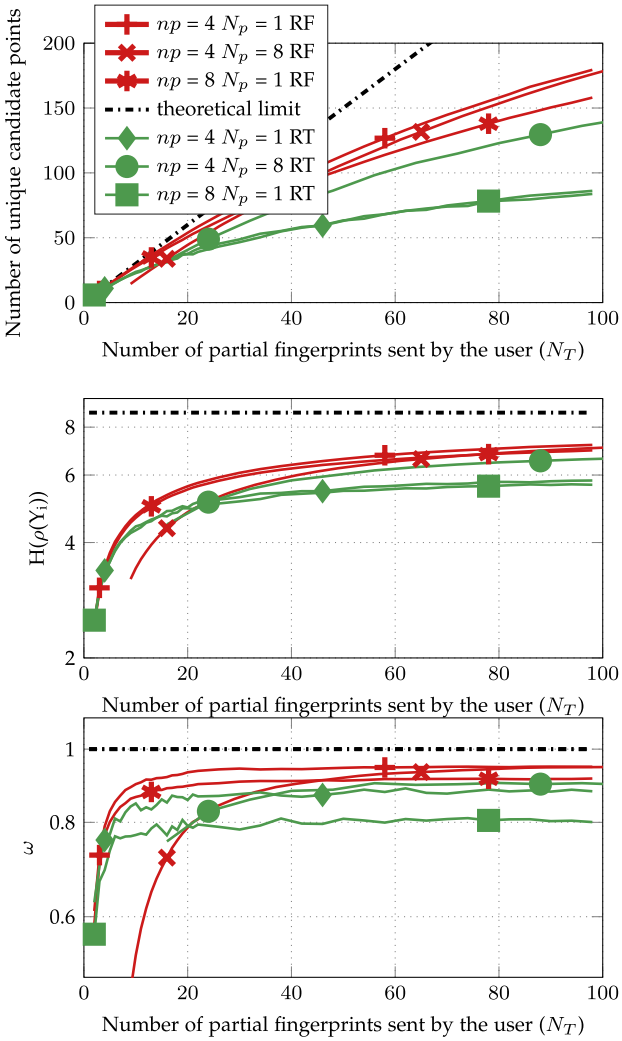


FIGURE 16. Privacy evaluation without noise. Top: number of candidate points received by the user. Middle and bottom: degree of privacy.

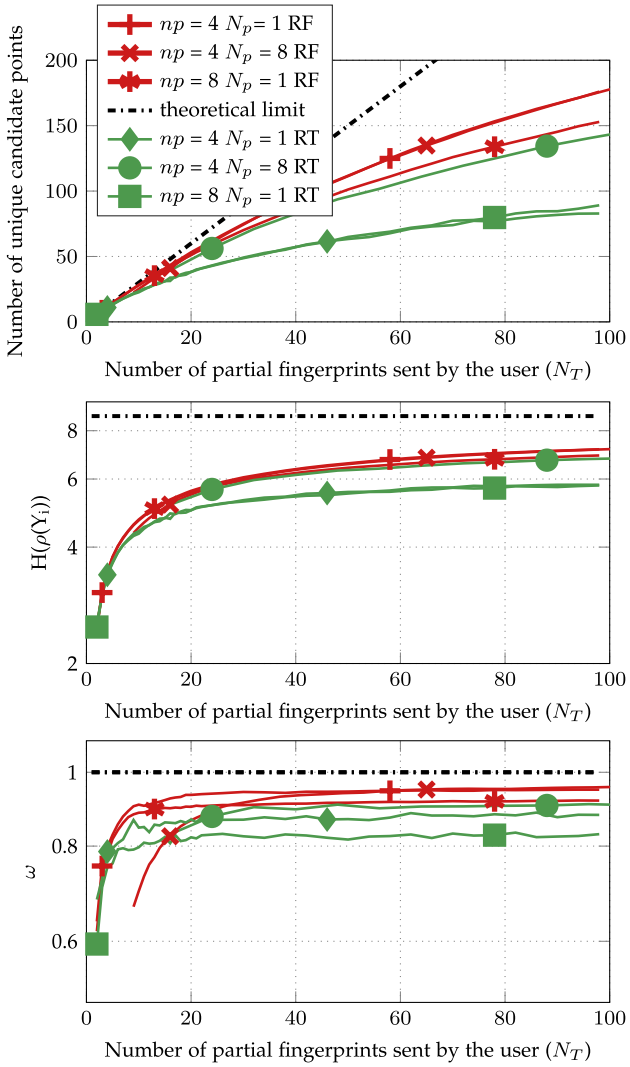


FIGURE 17. Privacy evaluation in the presence of noise. Notation identical to Fig. 16.

the partial fingerprint length np will have a larger effect on privacy. The number of candidates per partial fingerprint is $\kappa = 3$. Our results show that the degree of privacy of the algorithms increased with the value of κ, however, the number of candidate points increased too much. It can be seen from the figures that the degree of privacy increases with N_p when Algorithm 3 is used. This is understandable, as Algorithm 3 creates camouflage fingerprints by randomly changing the transmitter IDs in the *real* partial fingerprints. The higher N_p is, the higher the diversity of the camouflage fingerprints will be. A better localization performance is achieved for a larger number of *real* partial fingerprints N_p as the algorithm becomes more robust against changes in the environment. Figure 2 illustrates that when some of the multipath components appear or disappear due to changes in the indoor environment, the multipath components that remained the same can be used for localization. The larger the number of real partial fingerprints sent by the user to the ILS, the higher the chance that those fingerprints contain the unaltered multipath components. In addition, the obtained results demonstrate that even though the presence of noise predictably decreases the localization accuracy, the degree of privacy protection and system complexity remained largely unaffected.

E. PRIVACY OF A MOVING USER

An average value of the privacy metric $\eta(d)$, introduced in section III-D4, is estimated for an example user trajectory. The simulations were performed without noise. np was set to 4 and N_p to 5. Figure 18 shows the results for the random generation of partial fingerprints (Algorithm 2). In Figure 19, the camouflage fingerprints are generated by randomly changing the transmitter IDs in a *real* partial fingerprint (Algorithm 3). The values of d used to calculate η are shown in the legend. The results again show that better privacy protection was achieved by Algorithm 2.

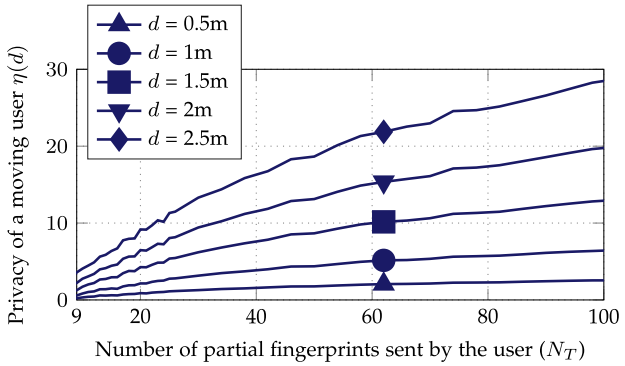


FIGURE 18. Degree of privacy of a moving user. The camouflage fingerprints generated using random multipath delays Algorithm 2.

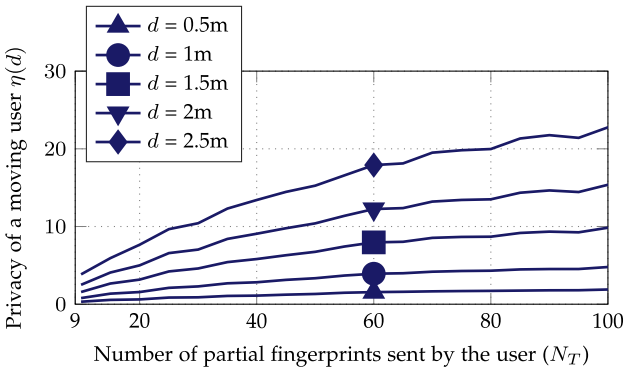


FIGURE 19. Degree of privacy of a moving user. The camouflage fingerprints generated using random transmitter IDs Algorithm 3.

It should be noted that a moving user can also increase his degree of privacy by learning the fingerprint map over time and generating camouflage fingerprints to mimic natural movement patterns. The ILS can find the user by analyzing all possible trajectories in the candidate points over time. Therefore, the presented results and the metric $\eta(d)$ characterize the complexity of the trajectory identification task of the ILS and not the actual degree of privacy of the user.

F. MEASUREMENT SETUP

The hardware setup was developed to test whether enough multipath components can be resolved from a real received signal to apply the MCA algorithm. An experiment also checked whether the MCA algorithm is able function in an environment with a moving object. The measurements are conducted using the Decawave DWM1000 chip[1] with UWB two-way-ranging. The DWM1000 module is attached by a breakout board to the GPIO outputs of a Raspberry Pi 3 B+. A software on the Raspberry Pi communicates by the SPI interface with the DWM1000 chip in order to operate the DWM1000 chip and transfer the time stamps to calculate distance estimates. In our measurement setup, 9 Raspberry Pis are configured as anchors, in the following called APs and one Raspberry Pi is configured as a tag, in the following called receiver. The 9 APs are static and are mounted on the walls at a height of roughly $1m$. The receiver is mobile and is attached to a moving robot or person during various measurements. Figure 20 shows the locations of the APs. For the measurements, the UWB system is configured to a bandwidth of 500 MHz and a carrier frequency of 3.5 GHz.

[1]https://www.decawave.com/product/dwm1000-module/

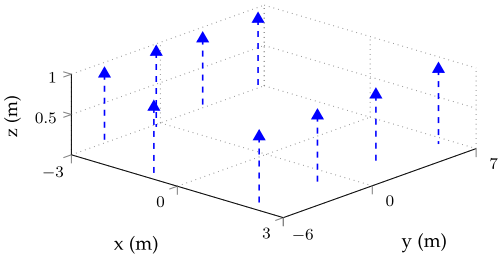


FIGURE 20. Measurement setup, AP locations. APs are mounted on the walls of the room.

As mentioned before, we use a two-way-ranging method to calculate the distance between the receiver and the APs. The receiver is initiating the two-way-ranging method by a ranging request (poll) to one of the APs. The receiver and AP are exchanging four messages, two are sent by the receiver, and two by the AP. The estimated distance is afterwards calculated on the receiver side, see [47]. In addition to the ranging information, the Decawave DWM1000 chip can provide the CIR. The DWM1000 chip includes a large bank of memory that holds the accumulated CIR data which contains complex values representing a $1ns$ sample interval. The receiver software running on the Raspberry Pi accesses this memory after a message from the AP is received. To determine the sparse structure of the CIR, the multipath estimation algorithm called space-alternating generalized expectation-maximization (SAGE) is used [49]. It should be noted, that the current ILS implementation uses active localization. This means that the receiver needs to send messages and actively communicate with the APs to perform CIR estimation. The system can potentially be modified to a passive ILS with multiple tags listening to the messages sent by the APs and performing multipath estimation on the received signals. Different state-of-the-art localization algorithms are implemented on different hardware platforms using software that is generally not published. As the author of this paper does not have access to the software and hardware in question, it was not possible to test the proposed algorithm against the state-of-the-art algorithms in the same environment.

A Vicon motion capturer [50] is used to track the movement of the receiver and obtain the ground truth. Our particular setup consists of 16 infrared sensitive cameras and infrared strobes, and can locate reflectors in the measurement room with a ground area of approximately 10 m by 4 m with an accuracy of less than 1 cm with a sampling rate higher than 100 Hz. We attached a reflector to the receiver, hence,

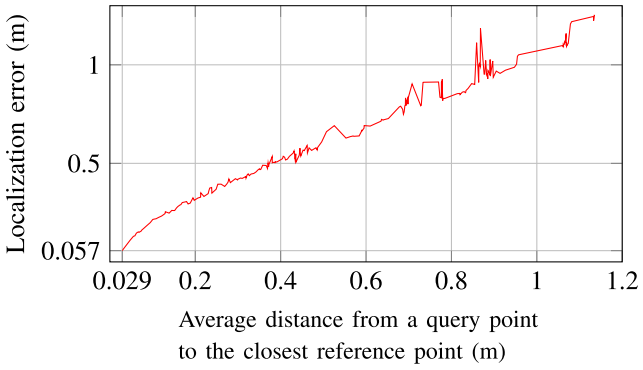


FIGURE 21. Localization error at the query points for different reference fingerprint densities. Static measurements.

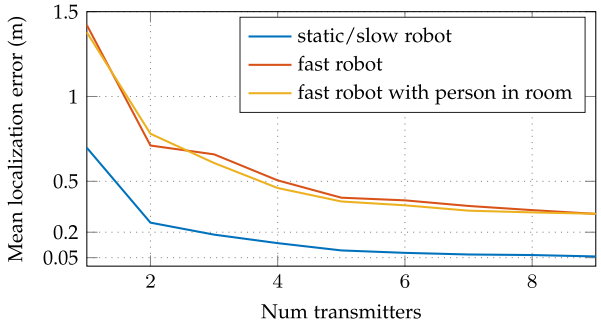


FIGURE 22. Localization error at the query points for different numbers of transmitters.

we were able to obtain the ground truth of the receiver with an accuracy better than 1 cm.

G. EXPERIMENTAL MCA LOCALIZATION PERFORMANCE

Figures 23 - 27 show the localization error obtained at a number of points in the indoor environment. Filled circles correspond to the query points, their color represents the localization error, and empty blue circles correspond to the reference points. All of the experiments use the same reference data. It was collected the following way. A Decawave board is placed on a robot that is moved very slowly along the trajectory shown in Fig. 23. The robot is also stopped and stands still roughly every 30 cm on the trajectory. Since the robot was controlled by hand, this number is approximate. As the robot is moving slowly and stopping, in the following we will refer to these measurements as stationary. The robot is continuously recording fingerprints even when moving. There are a total of 897 reference fingerprints, with 22.4 $fingerprints/m^2$. All of them are located on the trajectory shown in Figure 23. The reference points are averaged such that the distance between two consecutive points is not less than 10 cm. When two reference points are combined their MDPs are also averaged. This is possible since the multipath components are sorted within the MDPs. The mean distance between two reference points on sections where the robot was moving and was not turned or artificially

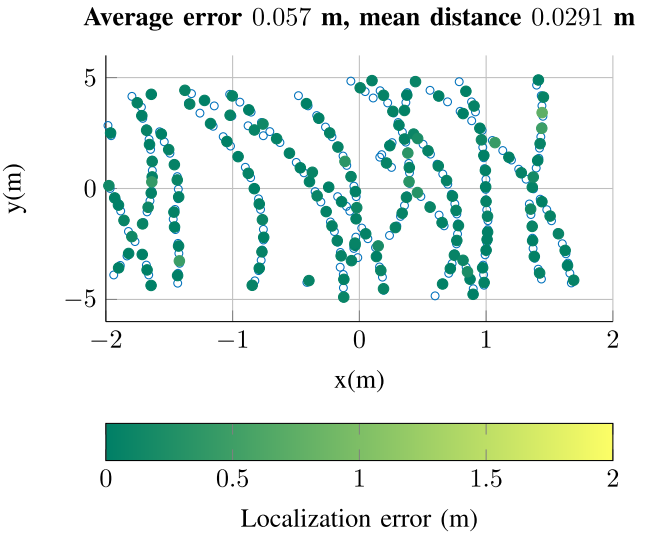


FIGURE 23. Localization error at query points. Near static measurements.

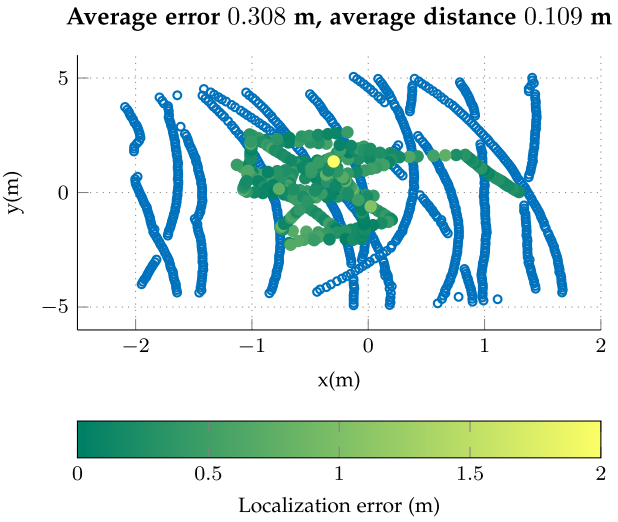


FIGURE 24. Localization error at query points. Query data collected by a moving robot.

re-positioned was 12 cm. The distance between consecutive query fingerprints of a fast moving robot is 15 to 20 cm, for a moving person that number is 12.3 cm. Both the query and reference points are additionally down-sampled when plotting for better visibility. A subset of the stationary data is used as the query data in Fig. 23. While they come from the same measurement series, the sets of query and reference data are different. In Fig. 21 the reference data was further down-sampled while the query data remained the same. The average localization error is plotted as a function of the average distance between the query fingerprints and the closest reference fingerprints. A mean localization error of 0.057 m was obtained for a mean distance of 0.0029 m between the query and closest reference fingerprints. In Fig. 22 the localization accuracy is calculated for the case when the data from a subset of AP is excluded from the calculation. In Fig. 24 the query data was collected by the robot moving slightly

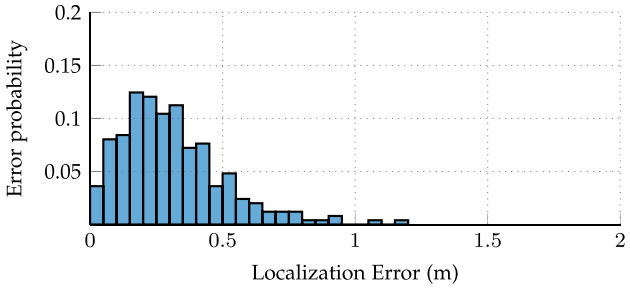


FIGURE 25. Probability distribution of the localization errors. Moving robot Fig. 24.

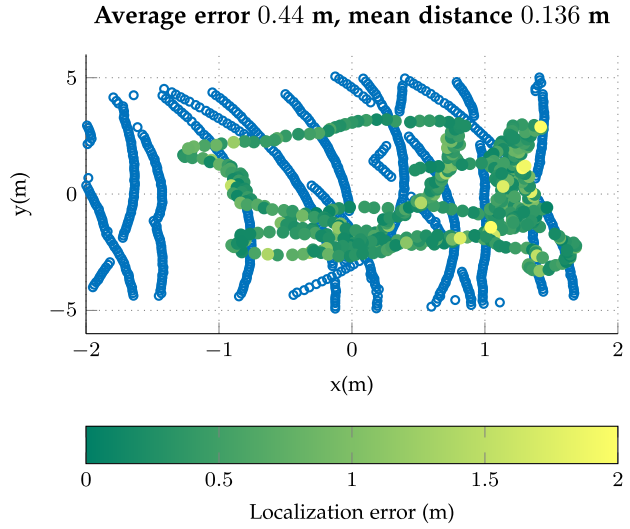


FIGURE 26. Localization error at query points. Query data collected by a moving person.

faster than walking pace. The algorithm localizes the user with an accuracy of 0.308 m. The mean distance from a query to the closest reference point is 0.11 m. The ratio of the mean error to the mean distance increased compared to the static measurements, therefore, the motion of the receiver significantly impacts the localization accuracy. Figure 25 shows the histogram of the distribution of the localization error values. Figure 26 shows the localization error obtained when the query data is collected by a moving person. The increase in localization error corresponds either to the vertical movement of the users hand carrying the receiver or to the fast walking pace of the user. Figure 27 shows the localization error for the case when a person is moving around the room when the query data is collected. The query data is collected by a moving robot. The trajectories in Figs. 24 - 27 are different due to the manual control of the robot.

Figure 21 shows that when the reference and query fingerprints are not identical, the localization error is almost the same as the average distance from the query to the nearest reference fingerprints. Therefore, precise localization with an average error of 5.7 cm is achieved when the robot is stationary or moving slower than a walking pace. The results also show, that the motion of the receiver impacts localization

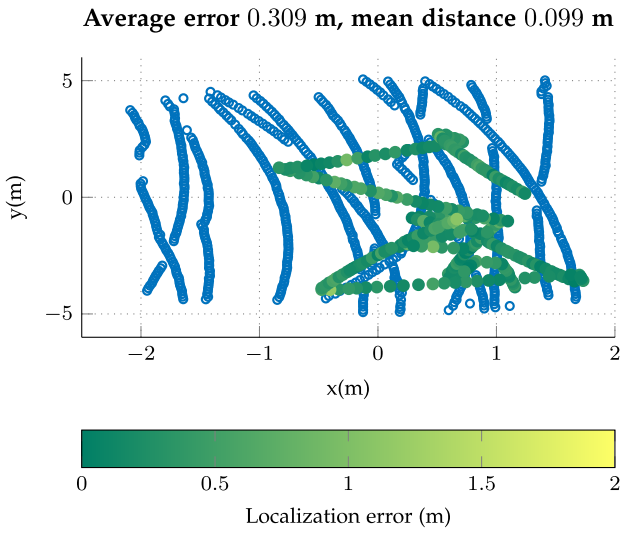


FIGURE 27. Localization error at query points. Query data collected by a moving robot, a person moving around the room during query measurements.

performance. This is most likely because the motion of the receiver changes the CIR estimation and multipath extraction. Figure 26 shows that even when the receiver is moving at a fast walking pace the user is localized with an average error of approximately 30 cm. Fig. 27 shows that the presence and movement of a person in the indoor environment does not affect the localization performance.

H. EXPERIMENTAL PRIVACY EVALUATION

Figure 28 shows the privacy metrics evaluated on the static data. The measurement results mirror the simulated privacy evaluation and validate the effectiveness of the proposed privacy protection scheme.

I. DISCUSSION

The simulation and measurement results demonstrated the high accuracy and effectiveness of the proposed approach. At the same time, the proposed scheme has several additional advantages over the state-of-the-art. Firstly, the proposed scheme maintains its localization accuracy under a moderate amount of changes and movement in the environment. This is not the case for most fingerprinting-based localization schemes and is demonstrated by the experiments in Figs. 13 and 27. The RSSI, which is the received power in dB of a signal that is averaged over a certain sampling period [6], [9]–[13], is very popular and is measured by default by many devices. However, it fluctuates significantly over time due to fading and changes in the environment [3]. Since the RSSI aggregates the whole channel information into one scalar value per AP, it is not possible to identify fingerprint components that correspond to changes in the environment. Classical CSI-based fingerprinting also cannot be used in a dynamic environment. There are several types of CSI fingerprints: parameters of the channel impulse response (CIR) [14], the channel frequency response (CFR) [1], [15],

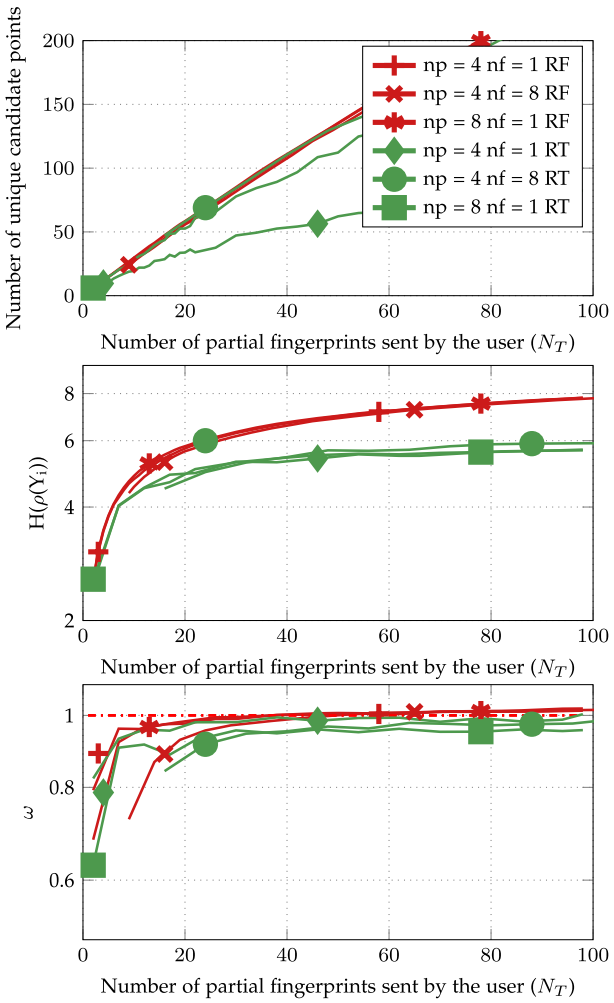


FIGURE 28. Privacy evaluation with measurement data. Notation in Figs.16 and 17.

down-sampled CFR consisting of the received power and phase at each OFDM carrier [16], [16]–[20] and multipath delays extracted from a received signal [51]–[54]. Because CIR and CFR fingerprints include power and fading information, it is not possible to separate the fingerprints into vectors, that correspond to the original geometry, and vectors, that correspond to the changes in the environment. Therefore, a fingerprint measured in a dynamic environment will not be similar to the map entry at its location. It should be noted, that because of the used similarity metrics, classical multipath-based fingerprinting schemes [51]–[54] suffer a similar accuracy decrease in a dynamic environment as CIR and CFR fingerprinting schemes.

The proposed MCA algorithm and MDP fingerprint structure also makes the integration of low-cost privacy protection into the ILS possible. *Camouflage*-based privacy protection has several advantages over the other existing schemes. *K-anonymity*-based privacy protection algorithms [25]–[32] can create user ID collisions and network disruptions. They can also cause an authorized user to be denied access to a private wireless network [26]. In addition, because the user's identity is concealed from the ILS by, for example, replacing the user's IDs or MAC addresses by frequently changing pseudonyms, the degree of privacy of one user strongly depends on the total number of ILS users and their movement patterns [32]. The disadvantage of privacy protection schemes that use *the Paillier cryptosystem* [33]–[39] is that they require the ILS to encode and send the entire fingerprint map to the user. Because in such ILS the server processes encoded data, the privacy of the user is fully secured. However, in this case the computational complexity and transmitted data volume grow linearly with the size of the fingerprint map [33]. This is impractical for most high-precision ILSs, such as [1], that require a very large fingerprint database. Alternative approaches include AP fuzzification [55] and differential privacy [56], and data partitioning [57]. In camouflage-based privacy protection schemes [32], [40]–[42] the user creates a number of *fake* fingerprints and send them to the ILS with the measured fingerprint (see Fig. 5). Several challenges have to be overcome by the state-of-the-art camouflage schemes. When the user moves, the ILS can potentially locate him or her if a candidate location at localization step $n-1$ is close to a candidate location at localization step n. This concept is further illustrated in Fig. 8. Additionally, to the best of the author's knowledge, no camouflage-based privacy protection scheme currently exists for CSI-based fingerprinting. However, as mentioned above, CSI fingerprints are needed for high-precision localization. RSSI fingerprints are easy to fake as they are simple in structure and fluctuate significantly throughout the indoor environment. Believable RSSI fingerprints can be created as vectors of random numbers. However, if camouflage CSI fingerprints are created by randomly generating CIR or CSI taps, the ILS sever can easily identify the resulting fingerprint as fake. Furthermore, the CIR and CFR at a given location are functions of the indoor geometry. Even if a fingerprint sent to the ILS looks 'believable' it needs to be similar to a fingerprint stored in the map. Otherwise the server can identify the camouflage fingerprints as very dissimilar to all of the reference fingerprints stored in the map. Another challenge to be overcome is that if most of the camouflage locations, or points calculated by the ILS, end up in one area, the ILS can infer the general location of the user. The MCA algorithm and MDP fingerprint structure allow the proposed scheme to overcome the above mentioned challenges of localization and privacy protection algorithms.

V. CONCLUSION

This paper presented a multipath-based localization algorithm with decimeter-level accuracy which is robust to changes in the indoor environment. The proposed approach selectively includes and excludes multipath components in the location calculation. The paper also presented a novel privacy protection algorithm. In the proposed privacy-protection scheme, the user sends a number of partial camouflage fingerprints to the ILS and obtains a list of candidate locations. The user locally determines his or her true location. This paper demonstrated that camouflage-based privacy

protection is made possible specifically due to the selected multipath fingerprint structure. Several heuristics for evaluating the degree of user privacy were also developed. The performance of the proposed localization and privacy protection algorithms was demonstrated using simulation and measurement data. The results show that the performance of the proposed privacy-protection algorithm approaches the derived theoretical limits for large numbers of camouflage fingerprints. The results also show that the two algorithms, proposed for camouflage fingerprint generation, present a trade-off between the degree of privacy protection and computational complexity and transmitted data volume.

ACKNOWLEDGMENT

The MCA algorithm is provided by the Technical University of Munich and the hardware setup and the implementation of the SAGE algorithm by the German Aerospace Center (DLR).

REFERENCES

[1] C. Chen, Y. Chen, Y. Han, H.-Q. Lai, and K. R. Liu, "Achieving centimeter-accuracy indoor localization on WiFi platforms: A frequency hopping approach," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 111–121, Feb. 2017.

[2] A. R. J. Ruiz and F. S. Granja, "Comparing Ubisense, BeSpoon, and DecaWave UWB location systems: Indoor performance analysis," *IEEE Trans. Instrum. Meas.*, vol. 66, no. 8, pp. 2106–2117, Aug. 2017.

[3] S. Garcia-Villalonga and A. Perez-Navarro, "Influence of human absorption of Wi-Fi signal in indoor positioning with Wi-Fi fingerprinting," in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Oct. 2015, pp. 1–10.

[4] E. R. Magsino, I. W.-H. Ho, and Z. Situ, "The effects of dynamic environment on channel frequency response-based indoor positioning," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–6.

[5] C. Yang and H.-R. Shao, "WiFi-based indoor positioning," *IEEE Commun. Mag.*, vol. 53, no. 3, pp. 150–157, Mar. 2015.

[6] D. R. Mautz, "Indoor positioning technologies," Habilitation thesis, ETH Zurich, Zürich, Switzerland, Feb. 2012.

[7] Y. Jin, N. O'Donoughue, and J. M. F. Moura, "Position location by time reversal in communication networks," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process.*, Mar. 2008, pp. 3001–3004.

[8] J. Kulmer, S. Hinteregger, B. Großwindhager, M. Rath, M. S. Bakr, E. Leitinger, and K. Witrisal, "Using DecaWave UWB transceivers for high-accuracy multipath-assisted indoor positioning," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2017, pp. 1239–1245.

[9] A. H. Ismail, H. Kitagawa, R. Tasaki, and K. Terashima, "WiFi RSS fingerprint database construction for mobile robot indoor positioning system," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Oct. 2016, pp. 001561–001566, doi: 10.1109/SMC.2016.7844461.

[10] J. Niu, B. Wang, L. Cheng, and J. J. P. C. Rodrigues, "WicLoc: An indoor localization system based on WiFi fingerprints and crowdsourcing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 3008–3013.

[11] C. Liu, A. Kiring, N. Salman, L. Mihaylova, and I. Esnaola, "A Kriging algorithm for location fingerprinting based on received signal strength," in *Proc. Sensor Data Fusion, Trends, Solutions, Appl. (SDF)*, Oct. 2015, pp. 1–6, doi: 10.1109/SDF.2015.7347695.

[12] I. Bisio, F. Lavagetto, A. Sciarrone, and S. Yiu, "A Smart^2 Gaussian process approach for indoor localization with RSSI fingerprints," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[13] X. Du, K. Yang, I. Bisio, F. Lavagetto, and A. Sciarrone, "An AP-centred smart probabilistic fingerprint system for indoor positioning," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.

[14] C. Nerguizian, C. Despins, and S. Affes, "Geolocation in mines with an impulse response fingerprinting technique and neural networks," *IEEE Trans. Wireless Commun.*, vol. 5, no. 3, pp. 603–611, Mar. 2006.

[15] C. Chen, Y. Chen, Y. Han, H.-Q. Lai, F. Zhang, and K. R. Liu, "Achieving centimeter-accuracy indoor localization on WiFi platforms: A multi-antenna approach," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 122–134, Feb. 2017.

[16] Q. Song, S. Guo, X. Liu, and Y. Yang, "CSI amplitude fingerprinting-based NB-IoT indoor localization," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1494–1504, Jun. 2018.

[17] Y. Chapre, A. Ignjatovic, A. Seneviratne, and S. Jha, "CSI-MIMO: Indoor Wi-Fi fingerprinting system," in *Proc. IEEE 39th Conf. Local Comput. Netw.*, Sep. 2014, pp. 202–209.

[18] K. Wu, J. Xiao, Y. Yi, D. Chen, X. Luo, and L. M. Ni, "CSI-based indoor localization," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 7, pp. 1300–1309, Jul. 2013.

[19] X. Wang, L. Gao, S. Mao, and S. Pandey, "CSI-based fingerprinting for indoor localization: A deep learning approach," *IEEE Trans. Veh. Technol.*, vol. 66, no. 1, pp. 763–776, Jan. 2017.

[20] G. Pecoraro, S. Di Domenico, E. Cianca, and M. De Sanctis, "LTE signal fingerprinting localization based on CSI," in *Proc. IEEE 13th Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2017, pp. 1–8.

[21] A. Zayets and E. Steinbach, "Robust WiFi-based indoor localization using multipath component analysis," in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Sep. 2017, pp. 1–8.

[22] A. Zayets and E. Steinbach, "Low-complexity fingerprint matching for real-time indoor localization systems," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2018, pp. 1–7.

[23] A. Zayets, M. Bourguiba, and E. Steinbach, "3D reconstruction of indoor geometry using electromagnetic multipath fingerprints," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2019, pp. 1–7.

[24] A. Zayets and E. Steinbach, "Interpolation and extrapolation of multipath fingerprints using virtual transmitter placement," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–7.

[25] Y. Wang, D. Xu, X. He, C. Zhang, F. Li, and B. Xu, "L2P2: Location-aware location privacy protection for location-based services," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 1996–2004.

[26] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: A quantitative analysis," *Mobile Netw. Appl.*, vol. 10, no. 3, pp. 315–325, Jun. 2005.

[27] D. Yang, X. Fang, and G. Xue, "Truthful incentive mechanisms for k-anonymity location privacy," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2994–3002.

[28] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing," *IEEE Pervasive Comput.*, vol. 2, no. 1, pp. 46–55, Jan. 2003, doi: 10.1109/MPRV.2003.1186725.

[29] P. Zhao, H. Jiang, J. C. S. Lui, C. Wang, F. Zeng, F. Xiao, and Z. Li, "P^3-LOC: A privacy-preserving paradigm-driven framework for indoor localization," *IEEE/ACM Trans. Netw.*, vol. 26, no. 6, pp. 2856–2869, Dec. 2018.

[30] N. Alikhani, V. Moghtadaiee, A. M. Sazdar, and S. A. Ghorashi, "A privacy preserving method for crowdsourcing in indoor fingerprinting localization," in *Proc. 8th Int. Conf. Comput. Knowl. Eng. (ICCKE)*, Oct. 2018, pp. 58–62.

[31] M. Zhou, Y. Liu, W. Nie, L. Xie, and Z. Tian, "Secure mobile crowdsourcing for WLAN indoor localization," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Apr. 2018, pp. 480–485.

[32] X. Liu, K. Liu, L. Guo, X. Li, and Y. Fang, "A game-theoretic approach for achieving k-anonymity in location based services," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2985–2993.

[33] H. Li, L. Sun, H. Zhu, X. Lu, and X. Cheng, "Achieving privacy preservation in WiFi fingerprint-based localization," *Proc. IEEE INFOCOM*, Apr. 2014, pp. 2337–2345.

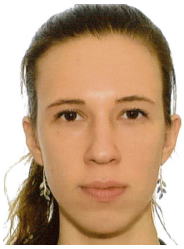
[34] L. Zhang, H. Gao, and O. Kaynak, "Network-induced constraints in networked control systems—A survey," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 403–416, Feb. 2013.

[35] S. Li, H. Li, and L. Sun, "Privacy-preserving crowdsourced site survey in WiFi fingerprint-based localization," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, pp. 1–9, Dec. 2016.

[36] X. Wang, Y. Liu, Z. Shi, X. Lu, and L. Sun, "A privacy-preserving fuzzy localization scheme with CSI fingerprint," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2014, pp. 1–6.

[37] Z. Yang and K. Järvinen, "The death and rebirth of privacy-preserving WiFi fingerprint localization with Paillier encryption," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, Apr. 2018, pp. 1223–1231.

[38] L. Xiang, B. Li, and B. Li, "Privacy-preserving inference in crowdsourcing systems," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Oct. 2017, pp. 1–9.
[39] T. Shu, Y. Chen, and J. Yang, "Protecting multi-lateral localization privacy in pervasive environments," *IEEE/ACM Trans. Netw.*, vol. 23, no. 5, pp. 1688–1701, Oct. 2015.
[40] A. Konstantinidis, G. Chatzimilioudis, D. Zeinalipour-Yazti, P. Mpeis, N. Pelekis, and Y. Theodoridis, "Privacy-preserving indoor localization on smartphones," in *Proc. IEEE 32nd Int. Conf. Data Eng. (ICDE)*, May 2016, pp. 1470–1471.
[41] H. Singh, S. Sarkar, A. Dimri, A. Bhaskara, N. Patwari, S. Kasera, S. Ramirez, and K. Derr, "Privacy enabled crowdsourced transmitter localization using adjusted measurements," in *Proc. IEEE Symp. Privacy-Aware Comput. (PAC)*, Sep. 2018, pp. 95–106.
[42] P. Zhao, W. Liu, G. Zhang, Z. Li, and L. Wang, "Preserving privacy in WiFi localization with plausible dummy locations," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, pp. 11909–11925, Oct. 2020.
[43] F. Lemic, A. Behboodi, V. Handziski, and A. Wolisz, "Experimental decomposition of the performance of fingerprinting-based localization algorithms," in *Proc. Int. Conf. Indoor Positioning Indoor Navigat. (IPIN)*, Oct. 2014, pp. 355–364.
[44] H. Hashemi, "The indoor radio propagation channel," *Proc. IEEE*, vol. 81, no. 7, pp. 943–968, Jul. 1993.
[45] P. Meissner, C. Steiner, and K. Witrisal, "UWB positioning with virtual anchors and floor plan information," in *Proc. 7th Workshop Positioning, Navigat. Commun.*, Mar. 2010, pp. 150–156.
[46] C. Gentner, T. Jost, W. Wang, S. Zhang, A. Dammann, and U.-C. Fiebig, "Multipath assisted positioning with simultaneous localization and mapping," *IEEE Trans. Wireless Commun.*, vol. 15, no. 9, pp. 6104–6117, Sep. 2016.
[47] C. Gentner, R. Pöhlmann, M. Ulmschneider, T. Jost, and S. Zhang, "Positioning using terrestrial multipath signals and inertial sensors," *Mobile Inf. Syst.*, vol. 2017, pp. 1–18, Oct. 2017.
[48] E. Leitinger, F. Meyer, F. Hlawatsch, K. Witrisal, F. Tufvesson, and M. Z. Win, "A belief propagation algorithm for multipath-based SLAM," *IEEE Trans. Wireless Commun.*, vol. 18, no. 12, pp. 5613–5629, Dec. 2019.
[49] B. H. Fleury, M. Tschudin, R. Heddergott, D. Dahlhaus, and K. I. Pedersen, "Channel parameter estimation in mobile radio environments using the SAGE algorithm," *IEEE J. Sel. Areas Commun.*, vol. 17, no. 3, pp. 434–450, Mar. 1999.
[50] Vicon. *Vicon Motion Capture Systems*. Accessed: Jun. 2021. [Online]. Available: https://www.vicon.com/hardware/cameras/
[51] E. Kupershtein, M. Wax, and I. Cohen, "Single-site emitter localization via multipath fingerprinting," *IEEE Trans. Signal Process.*, vol. 61, no. 1, pp. 10–21, Jan. 2013.
[52] S. Chen, J. Fan, X. Luo, and Y. Zhang, "Multipath-based CSI fingerprinting localization with a machine learning approach," in *Proc. Wireless Adv. (WiAd)*, Jun. 2018, pp. 1–5.
[53] L. Chen, X. Yang, P. X. Liu, and C. Li, "A novel outlier immune multipath fingerprinting model for indoor single-site localization," *IEEE Access*, vol. 7, pp. 21971–21980, 2019.
[54] M. N. de Sousa, "Enhanced localization systems with multipath fingerprints and machine learning," in *Proc. IEEE 30th Annu. Int. Symp. Pers., Indoor Mobile Radio Commun. (PIMRC)*, Sep. 2019, pp. 1–6.
[55] Y. Wang, M. Huang, Q. Jin, and J. Ma, "DP3: A differential privacy-based privacy-preserving indoor localization mechanism," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2547–2550, Dec. 2018.
[56] Y. Zhu, Y. Wang, Q. Liu, Y. Liu, and P. Zhang, "WiFi fingerprint releasing for indoor localization based on differential privacy," in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Oct. 2017, pp. 1–6.
[57] K. Järvinen, H. Leppäkoski, E.-S. Lohan, P. Richter, T. Schneider, O. Tkachenko, and Z. Yang, "PILOT: Practical privacy-preserving indoor localization using OuTsourcing," in *Proc. IEEE Eur. Symp. Secur. Privacy (EuroS P)*, Jun. 2019, pp. 448–463.



ALEXANDRA ZAYETS (Member, IEEE) received the Master of Science degree in communications engineering from the Technical University of Munich, Germany, in December 2015, where she is currently pursuing the Ph.D. degree. After this, she joined the Media Technology Group, Technical University of Munich, in February 2016, where she is working as a Member of the Research Staff. Her current research interest includes multipath-based indoor localization.

CHRISTIAN GENTNER (Member, IEEE) received the Dipl.-Ing. (B.A.) degree in electrical engineering from the University of Applied Sciences Ravensburg-Weingarten, in 2006, with a focus on communication technology, and the M.Sc. and Dr.-Ing. (Ph.D.) degrees from the University of Ulm, in 2009 and 2018, respectively. During this study, he received practical experiences at Rohde & Schwarz, Munich. Since 2009, he has been working with German Aerospace Center (DLR), Institute of Communications and Navigation. His current research interest includes indoor positioning.

ECKEHARD STEINBACH (Fellow, IEEE) studied electrical engineering at the University of Karlsruhe, Germany; the University of Essex, Great Britain; and ESIEE, Paris, and received the Engineering Doctorate degree from the University of Erlangen-Nuremberg, Germany, in 1999. From 1994 to 2000, he was a Member of the Research Staff with the Image Communication Group, University of Erlangen-Nuremberg. From February 2000 to December 2001, he was a Postdoctoral Fellow with the Information Systems Laboratory, Stanford University. In February 2002, he joined the Department of Electrical and Computer Engineering, Technical University of Munich, Germany, where he is currently a Full Professor of the Chair of Media Technology. His current research interests include haptic and visual communication, indoor mapping, and localization.