Erfassung und Behandlung von Positionsfehlern in standortbasierter Autorisierung

Philipp Marcus

Dissertation
an der Fakultät für Mathematik, Informatik und Statistik
der Ludwig–Maximilians–Universität München

Tag der Einreichung: 21. Juli 2015

Erfassung und Behandlung von Positionsfehlern in standortbasierter Autorisierung

Philipp Marcus

Dissertation
an der Fakultät für Mathematik, Informatik und Statistik
der Ludwig–Maximilians–Universität München

vorgelegt von
Philipp Marcus

1. Berichterstatterin: Prof. Dr. Claudia Linnhoff-Popien, LMU München
2. Berichterstatter: Prof. Dr. Uwe Baumgarten, TU München
Tag der Einreichung: 21. Juli 2015
Tag der Disputation: 26. November 2015

Eidesstattliche Versicherung

(siehe Promotionsordnung vom 12. Juli 2011 in der Fassung der 1. Änderungssatzung vom 6. Juni 2012, § 8, Abs. 2 Pkt. 5)

Hiermit erkläre ich an Eides statt, dass die Dissertation von mir selbstständig, ohne unerlaubte Beihilfe angefertigt ist.

Philipp Marcus

Danksagung

An dieser Stelle möchte ich Allen danken, die mich auf dem Weg zu dieser Dissertation unterstützt haben. Insbesondere gilt mein Dank Frau Prof. Dr. Linnhoff-Popien. Das besonders freiheitliche und fruchtbare Arbeitsklima am Lehrstuhl hat es mir erst ermöglicht, kreative Ideen zu entwickeln und zu realisieren. Durch die regelmäßigen Lehrstuhlworkshops war die richtige Plattform gegeben, um den eigenen Stand in der Forschungsgruppe kritisch zu diskutieren und voran zu bringen. Mein Dank gilt deshalb auch dem ganzen Team, besonders für die unzähligen inspirierenden Diskussionen und die freundschaftliche Atmosphäre. Insbesondere geht mein Dank hier an Dr. Moritz Kessel, für viele hilfreiche Denkanstöße und Inspirationen. Auch geht besonderer Dank an Lorenz Schauer für die vielen spannenden Diskussionen. Vor allem möchte ich aber meinen Eltern danken, die mich stets auf meinem Weg unterstützt haben. Ihre Unterstützung hat wesentlich dazu beigetragen, dass diese Dissertation möglich wurde. Zuletzt möchte ich meinem sehr guten, langjährigen Freund Sebastian Schießl meinen Dank für die vielen spannenden Diskussionen aussprechen. Seine beeindruckende Fachkenntnis und Auffassungsgabe waren mir stets eine wertvolle Anregung.

Zusammenfassung

Durch die immer größeren technischen Möglichkeiten mobiler Endgeräte sind die Voraussetzungen erfüllt, um diese zum mobilen Arbeiten oder zur Steuerung von industriellen Fertigungsprozessen einzusetzen. Aus Gründen der Informations- und Betriebssicherheit, sowie zur Umsetzung funktionaler Anforderungen, ist es aber vielfach erforderlich, die Verfügbarkeit von entsprechenden Zugriffsrechten auf Nutzer innerhalb autorisierter Zonen zu begrenzen. So kann z.B. das Auslesen kritischer Daten auf individuelle Büros oder die mobile Steuerung von Maschinen auf passende Orte innerhalb einer Fabrikhalle beschränkt werden. Dazu muss die Position des Nutzers ermittelt werden. Im realen Einsatz können Positionsschätzungen jedoch mit Fehlern in der Größe von autorisierten Zonen auftreten. Derzeit existieren noch keine Lösungen, welche diese Fehler in Autorisierungsentscheidungen berücksichtigen, um einhergehenden Schaden aus Falschentscheidungen zu minimieren. Ferner existieren derzeit keine Verfahren, um die Güteeigenschaften solcher Ortsbeschränkungen vor deren Ausbringung zu analysieren und zu entscheiden, ob ein gegebenes Positionierungssystem aufgrund der Größe seiner Positionsfehler geeignet ist.

In der vorliegenden Arbeit werden deshalb Lösungen zur Erfassung und Behandlung solcher Positionsfehler im Umfeld der standortbasierten Autorisierung vorgestellt. Hierzu wird zunächst ein Schätzverfahren für Positionsfehler in musterbasierten Positionierungsverfahren eingeführt, das aus den Charakteristika der durchgeführten Messungen eine Verteilung für den Standort des Nutzers ableitet. Um hieraus effizient die Aufenthaltswahrscheinlichkeit innerhalb einer autorisierten Zone zu bestimmen, wird ein Algorithmus vorgestellt, der basierend auf Vorberechnungen eine erhebliche Verbesserung der Laufzeit gegenüber der direkten Berechnung erlaubt. Erstmals wird eine umfassende Gegenüberstellung von existierenden standortbasierten Autorisierungsstrategien auf Basis der Entscheidungstheorie vorgestellt. Mit der risikobasierten Autorisierungsstrategie wird eine neue, aus entscheidungstheoretischer Sicht optimale Methodik eingeführt. Es werden Ansätze zur Erweiterung klassischer Zugriffskontrollmodelle durch Ortsbeschränkungen vorgestellt, welche bei ihrer Durchsetzung die Möglichkeit von Positionsfehlern und die Konsequenzen von Falschentscheidungen berücksichtigen. Zur Spezifikation autorisierter Zonen werden Eigenschaftsmodelle eingeführt, die, im Gegensatz zu herkömmlichen Polygonen, für jeden Ort die Wahrscheinlichkeit modellieren, dort eine geforderte Eigenschaft zu beobachten. Es werden ferner Methoden vorgestellt, um den Einfluss von Messausreißern auf Autorisierungsentscheidungen zu reduzieren. Ferner werden Analyseverfahren eingeführt, die für ein gegebenes Szenario eine qualitative und quantitative Bewertung der Eignung von Positionie-

rungssystemen erlauben. Die quantitative Bewertung basiert auf dem entwickelten Konzept der Autorisierungsmodelle. Diese geben für jeden Standort die Wahrscheinlichkeit an, dort eine Positionsschätzung zu erhalten, die zur Autorisierung führt. Die qualitative Bewertung bietet erstmals ein binäres Kriterium, um für ein gegebenes Szenario eine konkrete Aussage bzgl. der Eignung eines Positionierungssystems treffen zu können. Die Einsetzbarkeit dieses Analyseverfahrens wird an einer Fallstudie verdeutlicht und zeigt die Notwendigkeit einer solchen Analyse bereits vor der Ausbringung von standortbasierter Autorisierung. Es wird gezeigt, dass für typische Positionierungssysteme durch die entwickelten risikobasierten Verfahren eine erhebliche Reduktion von Schaden aus Falschentscheidungen möglich ist und die Einsetzbarkeit der standortbasierten Autorisierung somit verbessert werden kann.

Abstract

The increasing technical capabilities of mobile devices allow a broad range of new applications. For example, employees are allowed to work mobile or industrial production processes can be remotely controlled via the mobile. For reasons of information security and operational safety, as well as for implementing functional requirements, often the availability of according access rights needs to be restricted to users within an authorized zone. Thus, access to sensitive data can be bound to users within particular offices, or the remote control of industrial machines can be restricted to safe regions within the factory building. For that purpose, the position of the user needs to be determined. Unfortunately, positioning errors in the size of authorized zones can arise during operation. Up to now, there are no approaches that handle those positioning errors when access rights are derived in a way, that minimizes negative consequences of possibly false authorization decisions. Furthermore, there are no methods to analyze the quality of such location constraints in the forefront of their deployment with a specific positioning system. Thus, it is left unclear, if its positioning errors are acceptable in the according scenario.

In order to solve these problems, this thesis presents approaches to comprehend and handle positioning errors in the field of location-based access control. First of all, an error estimator for pattern-based positioning systems is introduced that employes characteristics of conducted position measurements. A probability density function (pdf) is derived in order to model the user's real position. This pdf can be used to derive the probability that a user is within the authorized zone. An algorithm is presented that employes precomputations to derive this probability. It allows for highly increased performance compared to the direct computation. For the first time, a detailed comparison of existing strategies for location-based access control is presented based on decision theory. The risk-based strategy is introduced, which is a novel method that is optimal from decision theory's point of view. Several approaches are presented that allow the assignment of location constraints to access control policies. When enforced, those constraints respect risk stemming from uncertain position measurements and possible damage of false authorization decisions. Feature models are introduced as a generalization of polygons for the specification of location constraints. For each geographic point, those models describe the probability that a required feature can be observed. Furthermore, a method is presented that allows to reduce the impact of measurement outliers on authorization decisions. At last, methods are presented that allow for a qualitative and quantitative rating of positioning systems for a given scenario. The quantitative rating is based on the novel concept of authorization models. Those models

describe the probabiltiy for each geographic point, that a user at this point gets a position estimate that leads to an authorization. The qualitative rating represents a binary criteria to judge the suitability of a positioning system in a given scenario. The applicability of this method is demonstrated by a case study. This case study also brings up the necessity of such an analysis already before location-based access control is deployed. It is shown that for typical positioning systems the damage caused by false authorization decisions can be highly reduced by using the developed risk-based strategy. Finally, this improves the applicability of location-based access control, when positioning errors are non-negligible.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

AfO	Auswerter für Ortsbeschränkungen
BLE	Bluetooth Low Energy
DAC	Discretionary Access Control
EER	Equal Error Rate
FAR	False Acceptance Rate
FN	Falsch-Negativ
FP	Falsch-Positiv
FRR	False Rejection Rate
GPS	Global Positioning System
kNN	k-nächste-Nachbarn
LBS	Location–based Services
MAC	Mandatory Access Control
NFC	Near Field Communication
QQ-Plot	Quantil-Quantil-Plot
RBAC	Role–based Access Control
RN	Richtig-Negativ
RP	Richtig-Positiv
WDF	Wahrscheinlichkeitsdichtefunktion
WFS	WLAN-Fingerprint-Sammler
WLAN	Wireless Local Area Network

Kapitel 1

Einleitung

1.1 Motivation

In den letzten Jahren hat die Bedeutung von mobilen Endgeräten, insbesondere von Tablet-Computern und Smartphones, durch deren technische Möglichkeiten und Verbreitung massiv zugenommen. Solche mobilen Endgeräte besitzen typischerweise eine Konnektivität und Rechenleistung, welche das mobile Arbeiten beinahe uneingeschränkt erlauben. So werden sie vielfach für den mobilen Zugriff auf benötigte Daten, oder auch bei der Digitalisierung von industriellen Fertigungsprozessen eingesetzt. Hier ist eine Verlagerung von Arbeitsschritten auf das mobile Endgerät zu beobachten, wodurch Laufwege eingespart und Arbeitsabläufe detailliert überwacht werden. Auch wird so eine einheitliche Mensch-Maschine-Schnittstelle geboten. Hierdurch entstehen sehr flexibel einsetzbare Systeme, deren Bedienung nicht mehr auf einen stationären Arbeitsplatz oder ein fest verbautes Terminal beschränkt ist. Zusätzlich wird die Bereitstellung von Informationen, Daten oder Diensten in Abhängigkeit vom aktuellen Standort des Nutzers ermöglicht. Denn mit integrierten Empfängern für das Global Positioning System (GPS), Beschleunigungssensoren, Kompass, Gyroskop und Empfängern für Drahtlosnetzwerke, engl. als Wireless Local Area Network (WLAN) bezeichnet, besitzen mobile Endgeräte die nötigen technischen Komponenten und Sensoren, um den Standort des Nutzers zu bestimmen.

In IT-Systemen mit Anbindung solcher mobiler Endgeräte wird die standortbasierte Autorisierung eingesetzt, um die Zugriffsrechte von mobilen Nutzern an geeignete Standorte zu binden. Dazu werden klassische Zugriffskontrollstrategien so erweitert, dass Zugriffsrechte zusätzlich mit Ortsbeschränkungen versehen sind. Die Möglichkeiten zur Definition der Ortsbeschränkungen sind vielfältig. Eine der wichtigsten Methoden ist, dass durch die Ortsbeschränkung eine geographische autorisierte Zone festgelegt wird. Die Ortsbeschränkung ist genau dann erfüllt, wenn sich die geschätzte Position für den Standort des Nutzers innerhalb der autorisierten Zone befindet. Besitzt er das klassische Zugriffsrecht und erfüllt seine Position die Ortsbeschränkung, wird der Nutzer autorisiert. Die standortbasierte Autorisierung erlaubt es also in Abhängigkeit von Positionsschätzungen den Informationsfluss bei der Interaktion eines Subjekts mit einem Objekt zu beschränken. Konkret wird die stand-

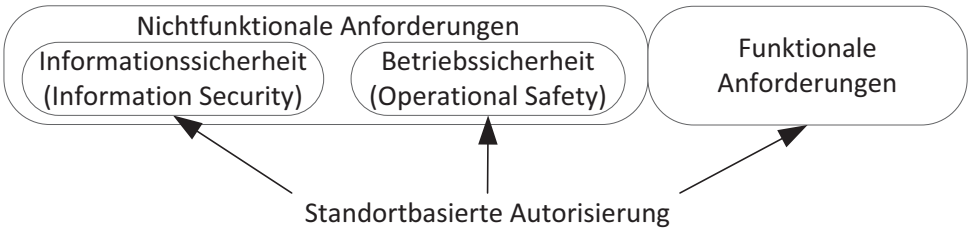


Abbildung 1.1: Die Einordnung der standortbasierten Autorisierung.

ortbasierte Autorisierung in IT-Systemen sowohl zur Realisierung funktionaler als auch nichtfunktionaler Anforderungen eingesetzt. Eine Übersicht zu den Einsatzgebieten ist in Abb. 1.1 dargestellt.

In einer visionären Arbeit schlagen Denning et al. bereits 1996 vor, mittels der standortbasierten Autorisierung die Informationssicherheit (engl. Information Security) in mobil genutzten IT-Systemen zu steigern [45]. Dazu wird die mobile Nutzung auf physisch geschützte Zonen eingeschränkt. Befindet sich ein Subjekt innerhalb dieser Zone, so steigt seine Authentizität, also die Gewissheit über seine wahre Identität. Wird ein mobiles Endgerät gestohlen, so hat der Dieb keine Möglichkeit zur mobilen Nutzung, sofern er nicht auch das physische Zutrittsrecht zur Zone besitzt. Denn es ist ein inhärent schweres Problem einen Ort zu betreten, zu dem man kein Zutrittsrecht besitzt [28]. Zusätzlich würden nach geglücktem Versuch die Mitarbeiter einen Eindringling meist sofort erkennen. Ein Firmengelände, das durch einen Pförtner geschützt wird, ist somit eine geeignete Zone, um darauf den Zugriff auf unternehmensinterne Daten zu beschränken. Für die Tele-Arbeit von Zuhause aus stellt das Haus des Mitarbeiters eine geeignete autorisierte Zone dar. Auch wenn das mobile Endgerät nicht gestohlen wird, so kann darauf ein nicht-autorisierter Nutzer im Zweifelsfall trotzdem unbemerkt vertrauliche Informationen ablesen [37]. Die standortbasierte Autorisierung ermöglicht es, das Anzeigen solcher Informationen auf Räume zu begrenzen, zu denen nur Personen Zutritt haben, die ebenso für die jeweilige Information autorisiert sind.

In soziotechnischen Systemen sind Menschen an der Steuerung oder Überwachung beteiligt. In diesen Systemen ist nach Sommerville die Betriebssicherheit (engl. Operational Safety) gegeben, falls sie bei Menschen oder der Systemumgebung niemals Schaden anrichten [132]. Ein Beispiel sind physische Maschinen in einer Industrieanlage. Diese Maschinen sind zur Einhaltung der Betriebssicherheit oftmals gemäß ISO-13850 konstruiert [68], so dass deren Betrieb nur möglich ist, wenn sich der Nutzer am Bedienstand befindet und dort unverzüglich einen Notausschalter betätigen kann. Ist am Bedienstand eine visuelle Anzeige für Fehler installiert, so kann ein Nutzer diese stets ablesen. Wird in modernen Industrieanlagen jedoch die Bedienung der Maschinen auf mobile Endgeräte verlagert, ist die Anwesenheit am Bedienstand nicht mehr gewährleistet. Damit ein Nutzer im Notfall zur Schadensbegrenzung schnell manuell eingreifen kann, indem er einen Notausschalter drückt, wird die standortbasierte Autorisierung eingesetzt. Das Zugriffsrecht zur mobilen Steuerung wird dabei nur in unmittelbarer Nähe zur Maschine gewährt [100]. Eine entspre-

chend kleine autorisierte Zone schafft hier Abhilfe.

Durch die standortbasierte Autorisierung wird ebenso die Umsetzung standortbezogener funktionaler Anforderungen möglich. Solche Anforderungen definieren, dass das zu implementierende Systemverhalten vom Standort von Subjekten, wie dem Nutzer und Objekten abhängt. Prominentestes Beispiel hierfür sind die standortbezogenen Dienste [85], in der englischen Fachliteratur als Location–based Services (LBS) bezeichnet. Durch die Spezifikation ist dabei entweder statisch oder dynamisch festgelegt, an welchen Orten welcher Informationsfluss stattfinden soll. Wird der Informationsfluss vom Nutzer initiiert, werden diese Dienste als reaktiv bezeichnet. Darunter fallen z.B. Anwendungen zum Finden von Restaurants. Ebenso beschreiben Decker et al. einen persönlichen Notizblock, der die Einträge nur an den Orten anzeigt, an denen sie erstellt wurden [43]. Auch ein vom System initiierter Informationsfluss ist möglich, so dass proaktive Dienste entstehen. Darunter zählen Anwendungen zur automatischen standortbezogenen Benachrichtigung und das Anzeigen von standortbezogener Werbung. Hier soll ein Prozess nur dann autorisiert sein auf dem mobilen Endgerät des Nutzers Werbung anzuzeigen, wenn sich der Nutzer gerade in der Nähe des beworbenen Geschäfts befindet [48].

Zur Auswertung der Ortsbeschränkungen wird zuvor mittels eines Positionierungssystems die Position des Nutzers bestimmt und typischerweise als einfacher Punkt zurückgegeben. Aufgrund schwankender Umwelteinflüsse sowie ungenauer Sensoren sind dabei durchgeführte Positionsschätzungen jedoch mit einem inhärenten Fehler behaftet. Gerade innerhalb von Gebäuden entspricht das Ausmaß dieser Fehler mit existierenden Positionierungnsystemem, wie WLAN-Fingerprinting, oft den Abmessungen von autorisierten Zonen. Somit entsteht Ungewissheit über die wahre Position des Nutzers. Ein Beispiel ist in Abb. 1.2 dargestellt. Die wahre Position des Nutzers (rote Raute) befindet sich in der autorisierten Zone (grüner Bereich). Über die Zeit hinweg unterliegen die Positionsschätzungen (schwarze Kreuzchen) aber Positionsfehlern. Die Positionsschätzungen sind also um die wahre Position des Nutzers statistisch verteilt. Wie später in dieser Arbeit gezeigt wird, ist die Laplace-Verteilung eine geeignete Modellierung für die Fehlerverteilung von WLAN-Fingerprinting. Diese gibt an, wie die wahre Position des Nutzers relativ zur Positionsschätzung verteilt ist. Eine solche Verteilung ist in Abb. 1.3 angedeutet. Der Einsatz der standortbasierten Autorisierung wird dadurch erschwert, dass ihr Betrieb mit größer werdenden Positionsfehlern, sowie kleiner werdenden autorisierten Zonen zunehmend unpraktikabel wird. Denn Falschentscheidungen entstehen, wenn die Positionsschätzung für den Nutzer außerhalb der autorisierten Zone liegt, die wahre Position jedoch innerhalb. Gleiches gilt im umgekehrten Fall, wenn einem Nutzer fälschlicherweise das Zugriffsrecht verwehrt wird, obwohl seine wahre Position innerhalb der autorisierten Zone liegt. Existierende Verfahren zur standortbasierten Autorisierung ignorieren bis auf wenige Ausnahmen die Ungewissheit beim Ableiten von Autorisierungsentscheidungen. Dabei wird die Position des Nutzers als Punkt modelliert und geprüft, ob dieser innerhalb des Polygons der autorisierten Zone liegt. Somit wird von deterministischem Verhalten des Positionierungssystems ausgegangen, obwohl sich deren Fehler nichtdeterministisch verhalten. Nur wenige Verfahren ziehen die Ungewissheit in Betracht, wobei diese einen zuvor bestimmten Schwellwert unterschreiten muss. Die Herleitung und Auswirkung solcher Schwellwerte bleibt bisher of-

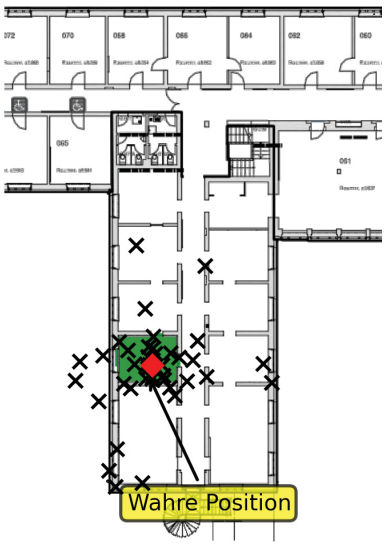


Abbildung 1.2: Positionsschätzungen (x) sind statistisch um die wahre Position (♢) verteilt.

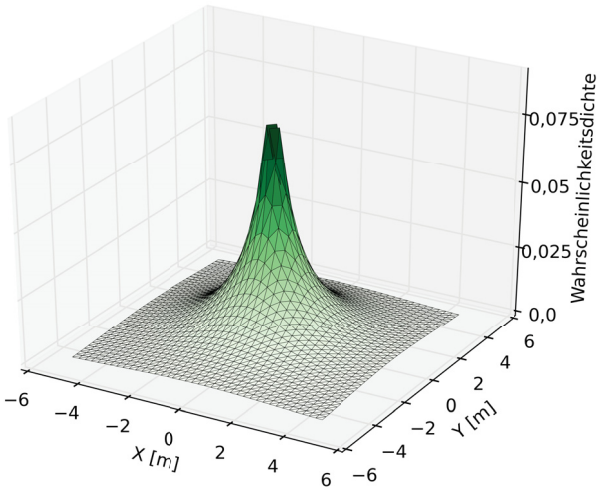


Abbildung 1.3: Beispiel für die statistische Modellierung von Positionsfehlern.

fen. Im schlechtesten Fall realisiert die standortbasierte Autorisierung wegen Falschentscheidungen aufgrund von Positionsfehlern nicht mehr die gewünschte Semantik. Dadurch wird letztlich darüber realisierte Informations- und Betriebssicherheit kompromittiert, ebenso werden entsprechende funktionale Anforderungen verletzt. Dann entstehen unerwünschte Systemzustände die, je nach Anwendungsfall, negative Konsequenzen für Leib und Leben oder finanziellen Schaden mit sich bringen.

Damit die Voraussetzung zur Behandlung von Positionsfehlern geschaffen ist, müssen diese zuverlässig abgeschätzt und ihr Grad der Ungewissheit ermittelt werden. Gerade für Positionierungssysteme innerhalb von Gebäuden existieren dafür bisher nur sehr grobe Techniken. Für WLAN-Fingerprinting, eines der wichtigsten Verfahren, existieren bisher keine Ansätze, die eine geeignete statistische Modellierung für die Position des Nutzers basierend auf den Eigenschaften einer Positionsmessung ableiten. Dadurch ist es bisher nicht möglich, Ungewissheit als Wahrscheinlichkeit auszudrücken, mit welcher sich der Nutzer gerade außerhalb der autorisierten Zone befindet. Ferner werden Verfahren zur standortbasierten Autorisierung benötigt, welche diese Ungewissheit bei Entscheidungen berücksichtigen. Dabei muss auch die Konsequenz aus Falschentscheidungen berücksichtigt werden, die zuvor für jedes Zugriffsrecht quantitativ zu bestimmen ist. Das Ziel im Betrieb ist die Verringerung des erwarteten Schadens aus Falschentscheidungen. Ferner existieren bisher keine Werkzeuge, um bereits vor dem praktischen Einsatz der standortbasierten Autorisierung abzuschätzen, inwiefern ein Positionierungssystem für ein gegebenes Szenario ausreichend ist. Es werden Analysemethoden benötigt um festzustellen, wie sich das Aus-

maß der Positionsfehler auf die Auswertung von Ortsbeschränkungen auswirkt. Werden die Positionsfehler im Vergleich zu den autorisierten Zonen sehr groß, so ist die Einsetzbarkeit des Positionierungssystems nicht mehr gegeben.

Das Ziel der vorliegenden Arbeit ist es, diese kritischen Lücken zu schließen und somit einen wichtigen Beitrag zur Einsetzbarkeit der standortbasierten Autorisierung zu leisten.

1.2 Aufbau der Arbeit

Der Aufbau der Arbeit wird im Folgenden vorgestellt. Kapitel 2 behandelt Grundlagen und verwandte Arbeiten. Dabei wird zunächst auf Positionierungsverfahren und Ansätze zur Abschätzung von Positionsfehlern eingegangen. Darauf folgt der Stand der Technik zur standortbasierten Autorisierung. Abschließend werden existierende Arbeiten zur systematischen Auswahl eines geeigneten Positionierungssystems für standortbezogene Dienste vorgestellt.

In Kapitel 3 folgen Beiträge zur Positionsbestimmung und -verarbeitung. Es wird untersucht, wie sich Positionsfehler im WLAN-Fingerprinting verhalten und wie diese aus den Eigenschaften einer Messung statistisch abgeschätzt werden können. Ferner wird ein Verfahren vorgestellt, welches mittels Vorberechnungen effizient aus solchen Positionsschätzungen die Wahrscheinlichkeit ermittelt, mit der sich der Nutzer innerhalb der autorisierten Zone befindet. Dieser Wert wird bei der Auswertung von Ortsbeschränkungen benötigt. Damit die Position des mobilen Endgeräts stets an die Position des eingeloggten Nutzers gekoppelt ist, wird die Anwendung kontinuierlicher biometrischer Authentifizierungsverfahren vorgeschlagen. Dadurch wird verhindert, dass das mobile Endgerät unbemerkt in die Hände Dritter gelangt. Ansonsten könnte dessen Position als die des eingeloggten Nutzers angenommen werden. Dazu wird ein Anforderungskatalog vorgestellt, den Verfahren erfüllen müssen, damit sie zur Unterstützung von standortbasierter Autorisierung einsetzbar sind.

In Kapitel 4 werden neuartige Ansätze zur Spezifikation und Auswertung von Ortsbeschränkungen vorgestellt. Zunächst werden fünf Strategien zur Auswertung von Ortsbeschränkungen gegenübergestellt. Die Frage der standortbasierten Autorisierung wird dabei als Entscheidungsproblem identifiziert, dessen mögliche Ausgänge unterschiedlichen Nutzen bringen. Es wird die risikobasierte Strategie eingeführt, die den erwarteten Nutzen bei der Autorisierung berücksichtigt. Ebenso wird die erweiterte risikobasierte Strategie vorgestellt, die zusätzlich das bisherige Konzept der polygonalen autorisierten Zonen zu Eigenschaftsmodellen verallgemeinert. Diese beschreiben für jeden Ort die Wahrscheinlichkeit, dass dort eine zur Autorisierung benötigte Eigenschaft gegeben ist. Es wird eine Erweiterung der rollenbasierten Zugriffskontrolle durch Ortsbeschränkungen vorgestellt, wozu die erweiterte risikobasierte Strategie einsetzt wird. Gegenüber existierenden Ansätzen ist dies die erste Ergänzung, die Positionsfehler behandelt. Ebenso wird eine Adaption der risikobasierten Strategie auf Trajektorien vorgestellt. Zu deren Abschätzung werden Partikelfilter eingesetzt. Durch den Ansatz kann kontinuierlich überprüft werden, ob sich der Nutzer innerhalb der autorisierten Zone befindet. Ebenso wird die dynamische Herleitung

von Timeouts eingeführt.

Kapitel 5 behandelt die Analyse der Durchsetzung von Ortsbeschränkungen. Das Ergebnis des Kapitels ist eine Methodik zur Selektion einer geeigneten Konfiguration aus Positionierungssystem und Autorisierungsstrategie zur Durchsetzung einer Ortsbeschränkung. Dazu werden zunächst drei Maße zur quantitativen Bewertung der Eigenschaften von Ortsbeschränkungen eingeführt, die sich in Abhängigkeit von der eingesetzten Konfiguration berechnen. Diese bewerten u.a. die erwartete Verfügbarkeit oder Angreifbarkeit. Ebenso wird eine Methodik vorgestellt, womit für eine gegebene Konfiguration der erwartete Nutzen im Betrieb berechenbar ist. Darauf basierend wird ein Kriterium definiert, das eine binäre Aussage erlaubt, ob eine Konfiguration für die standortbasierte Autorisierung in einem gegebenen Szenario geeignet ist.

Es wird gezeigt, wie die Erfassung und die Behandlung der Positionsfehler die Einsetzbarkeit der standortbasierten Autorisierung deutlich steigert. Gerade für die oben erwähnten mobilen Arbeitsplätze oder die mobile Steuerung von Fertigungsprozessen ist dies ein wesentlicher Schritt. Gleiches gilt für standortbezogene Dienste. Die entwickelten Analysemethoden erlauben eine detaillierte Untersuchung des zu erwartenden Verhaltens bereits vor der Inbetriebnahme. Dadurch ist stets klar, ob ein teureres Positionierungssystem mit kleineren Positionsfehlern einzusetzen ist, oder ob ein vorhandenes System für das jeweilige Szenario ausreicht.

1.3 Zugrundeliegende Vorarbeiten

Ein Teil der Konzepte und Ergebnisse, die in dieser Arbeit vorgestellt werden, sind insgesamt in sieben Vorarbeiten bereits veröffentlicht worden. Die Folgende Liste gibt einen Überblick, in welche Abschnitte die Vorarbeiten eingeflossen sind:

- Abschnitt 3.1 vergleicht einen neu entwickelten Ansatz zur Fehlerschätzung mit der von Marcus et al. in [96] veröffentlichten Vorarbeit. Dr. Moritz Kessel hat dabei den Vorschlag zur Fehlerschätzung auf Basis einer Normalverteilung und des mittleren gewichteten Abstands der kNN von der Positionsschätzung beigetragen. Eigenanteil ist die Evaluationsmethodik mittels der Standardisierung der Fehlervektoren, deren Implementierung und Auswertung.

- Unterabschnitt 3.1.5 basiert auf Marcus et al. [99] und enthält zusätzliche Beispiele und Anmerkungen. Prof. Dr. Claudia Linnhoff-Popien hat bei der Diskussion der Vorarbeit unterstützt.

- Abschnitt 3.2 basiert auf der Vorarbeit von Marcus et al. [96] und enthält eine stark erweiterte Evaluation. Dr. Martin Werner hat das Konvergenzkriterium vorgeschlagen. Zu den Eigenanteilen gehören der Vorschlag ein Kriterium zum Finden der dNN zu suchen, um die Positionsbestimmung zu verbessern, die Implementierung und die Auswertung.

- Abschnitt 3.3 basiert, ausgenommen von Unterabschnitt 3.3.1, auf Marcus et al. [97] und enthält viele zusätzliche Kommentare. Prof. Dr. Claudia Linnhoff-Popien hat bei der Diskussion der Vorarbeit unterstützt.

- Abschnitt 3.4 basiert auf einer starken Überarbeitung der Konzepte, die in Trojahn et al. [141] veröffentlicht wurden, sowie einer Aktualisierung der darin durchgeführten Literaturrecherche. Matthias Trojahn hat maßgeblich zur ursprünglichen Literaturrecherche beigetragen. Deren thematische Strukturierung, sowie der Vorschlag einen solchen Anforderungskatalog zu entwickeln sind Eigenanteil. Die Ausarbeitung des Anforderungskatalogs und die Einordnung der Literatur entstanden in gemeinsamen Diskussionen zu gleichem Anteil.

- Unterabschnitt 4.1.2 enthält eine umfangreiche Erweiterung der Konzepte aus Marcus et al. [98]. Prof. Dr. Claudia Linnhoff-Popien hat bei der Diskussion der Vorarbeit unterstützt.

- Abschnitt 4.2 basiert größtenteils auf Marcus et al. [100] und enthält viele zusätzliche Kommentare und Anmerkungen. Lorenz Schauer und Prof. Dr. Claudia Linnhoff-Popien haben bei der Diskussion der Vorarbeit unterstützt.

- Abschnitt 4.3 basiert größtenteils auf Marcus et al. [95] und enthält viele zusätzliche Kommentare und Anmerkungen. Dr. Moritz Kessel und Prof. Dr. Claudia Linnhoff-Popien haben bei der Diskussion der Vorarbeit unterstützt.

- Abschnitt 5.1 basiert auf den Konzepten und Ergebnissen aus Marcus et al. [99]. Prof. Dr. Claudia Linnhoff-Popien hat bei der Diskussion der Vorarbeit unterstützt.

- Abschnitt 5.2 enthält Teile aus Marcus et al. [98]. Prof. Dr. Claudia Linnhoff-Popien hat bei der Diskussion der Vorarbeit unterstützt.

Kapitel 2

Grundlagen zur standortbasierten Autorisierung

Die Erfassung und Behandlung von Positionsfehlern in standortbasierter Autorisierung bedarf dem Einsatz von Verfahren aus drei Teilbereichen der Informatik. In diesem Kapitel wird für die einzelnen Teilbereiche jeweils der aktuelle Stand der Technik aufgezeigt. Dabei wird besonders auf offene Probleme eingegangen, zu deren Lösung in dieser Arbeit beigetragen wird. Unter diesen Aspekten wird in Abschnitt 2.1 das Themenfeld der Positionsbestimmung und -verarbeitung behandelt. Besonderer Fokus wird dabei auf die Erfassung von Positionsfehlern gelegt. Abschnitt 2.2 stellt die Grundlagen von Zugriffskontrollstrategien und existierende standortbasierte Erweiterungen vor. Ferner werden verwandte Arbeiten aus dem Themenfeld der Spezifikation und Auswertung von Ortsbeschränkungen vorgestellt. Abschließend beschreibt Abschnitt 2.3 verwandte Arbeiten zur Problemstellung, geeignete Positionierungssysteme für ortsbezogene Dienste auszuwählen und stellt den Bezug zur standortbasierten Autorisierung her.

2.1 Positionsbestimmung und Fehlerschätzung

Die Positionsbestimmung beschreibt die Ermittlung der eigenen Position bzgl. der Position eines festen Referenzpunkts bzw. Bezugssystems. Das Ergebnis dieses Prozesses ist eine Positionsschätzung. Dazu werden messbare physikalische Größen ermittelt, mit deren Hilfe die Positionsbestimmung durchgeführt wird. Das eingesetzte System wird als Positionierungssystem bezeichnet. In der vorliegenden Arbeit wird stets davon ausgegangen, dass die Messungen von Nutzerseite aus, mithilfe seines mobilen Endgeräts durchgeführt werden, z.B. einem Smartphone oder Tablet-Computer. Je nach eingesetztem Verfahren kann zusätzlich die Installation von Infrastruktur an den Referenzpunkten oder im Bezugssystem nötig sein. Beispiele hierfür sind das Aufstellen von Funksendern, z.B um als Referenzpunkt zu dienen, das Ausbringen von Strichcodes, oder die Installation von optischen oder akustischen Sendern. Nach Liu et al. kann ein Positionierungssystem unter folgenden Gesichtspunkten bewertet werden [89]:

- Die *Richtigkeit* beschreibt nach ISO 5725-1 die Nähe der Positionsschätzungen zur wahren Position des Nutzers [69].
- Die *Präzision* beschreibt nach ISO 5725-1 die Wiederholbarkeit bzw. Reproduzierbarkeit von Positionsschätzungen [69].
- Die *Komplexität* beschreibt den Rechenaufwand, den ein System zur Positionsbestimmung verursacht. Die benötigte Zeit zwischen zwei aufeinanderfolgenden Positionsbestimmungen bzw. die Positionsbestimmungsrate, sind zwei davon abhängige Größen.
- Die *Robustheit* beschreibt, wie gut das Positionierungssystem mit Abweichungen vom Idealzustand zurechtkommt, z.B. aufgrund defekter Hardware oder unvorhergesehener Hindernisse im Raum.
- Die *Skalierbarkeit* wird unterteilt in geographische und dichtebasierte Skalierbarkeit. Erstere beschreibt, wie gut das System zur Abdeckung größerer Gebiete angepasst werden kann. Letztere beschreibt, wie das System mit einer größer werdenden Anfrage nach Positionsbestimmungen zurecht kommt.
- *Kosten* entstehen zum Einen durch den *Einkauf* der nötigen Infrastruktur und der Bauteile des Positionierungssystems. Der *Installations- und Wartungsaufwand* verursacht ebenso Kosten. Durch den Energiebedarf entstehen ebenso Kosten, da mobile Endgeräte stärkere Akkus benötigen. Auch Infrastrukturkomponenten können öfter neue Batterien benötigen, oder generell hohe *Stromkosten* verursachen. Ebenso kann der *Platzbedarf* im Gebäude oder im mobilen Endgerät als Kostenpunkt betrachtet werden.

Das Konzept der Richtigkeit und Präzision nach ISO 5725-1 wird in Abb. 2.1 veranschaulicht. Die Positionsschätzungen folgen einer Verteilung, deren Mittelwert von der wahren Position abweicht. Das Ausmaß der Streuung um diesen Mittelwert wird als Präzision bezeichnet. Die Entfernung des Mittelwerts von der wahren Position hingegen als Richtigkeit.

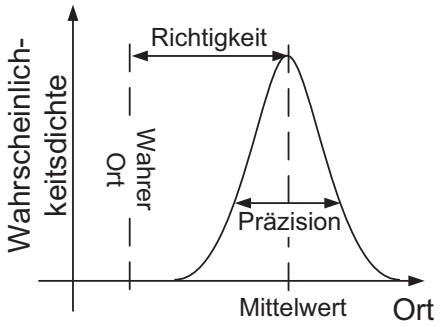


Abbildung 2.1: Richtigkeit und Präzision eines Positionierungssystems nach ISO 5725-1 [69]

Für die standortbasierte Autorisierung ist ein Positionierungssystem mit optimaler Richtigkeit und Präzision ideal, das gleichzeitig eine geringe Komplexität, geringe Kosten, eine hohe Skalierbarkeit und eine hohe Robustheit zeigt. In der Praxis konkurrieren

aber die Ziele einer hohen Richtigkeit und Präzision vor allem mit den Kosten. Bei der Wahl des Positionierungssystems muss somit ein Kompromiss gefunden werden, der auf das jeweilige Szenario abgestimmt ist. In der Literatur existieren nur wenige Arbeiten, die eine Hilfestellung leisten. Ein Überblick wird in Abschnitt 2.3 gegeben. Von der Richtigkeit und der Präzision hängt das Ausmaß der auftretenden Positionsfehler ab. Im Rahmen dieser Arbeit wird in Kapitel 5 ein umfassender Ansatz vorgestellt, welcher die Eignung eines Positionierungssystems für die standortbasierte Autorisierung abhängig von dessen Positionsfehlern und dem Szenario bewertet.

Jedem Positionierungssystem liegt ein bestimmtes Verfahren zugrunde. Im Folgenden wird eine Übersicht zu den wichtigsten Verfahren gegeben, die zur Positionsbestimmung von mobilen Endgeräten eingesetzt werden.

2.1.1 Verfahren zur Positionsbestimmung mobiler Endgeräte

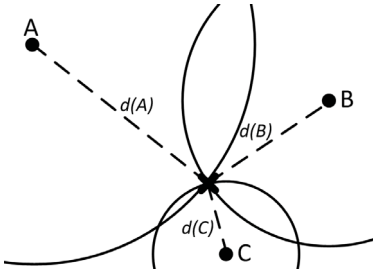
In der Praxis lassen sich Positionierungssysteme nach Fallah et al. im Wesentlichen in vier Klassen einordnen [54]. Im Folgenden werden diese Klassen und die zugehörigen Verfahren vorgestellt.

Verfahren basierend auf Lateration oder Angulation

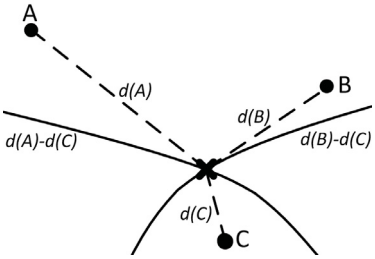
Verfahren zur Lateration bestimmen die Distanz zu mindestens drei Referenzpunkten, was auch Trilateration genannt wird. Liegt die Distanz des Nutzers zu den Referenzpunkten vor, so ist klar, dass er sich auf einem Kreis um den Referenzpunkt herum befindet. Dort wo sich die Kreise schneiden, liegt die geschätzte Position des Nutzers. Dieser Fall ist in Abb. 2.2(a) für einen Nutzer am Ort $\times$ und drei Referenzpunkte A, B und C mit den Distanzen $d(A)$, $d(B)$ und $d(C)$ und zugehörigen Distanzkreisen dargestellt.

Beim Einsatz von mobilen Endgeräten wird in der Regel vorausgesetzt, dass an den Referenzpunkten optische, akustische oder funkbasierte Sender installiert sind, mit denen interagiert werden kann. Durch den Nachrichtenaustausch kann entweder die Ankunftszeit (engl. Time of Arrival) oder die Abnahme der Signalstärke gemessen werden.

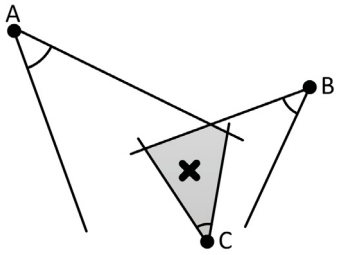
Ist die Ankunftszeit und der Sendezeitpunkt des Signals bekannt, so lässt sich daraus dessen Flugzeit t bestimmen. Darunter wird die Differenz zwischen Sende- und Empfangszeitpunkt verstanden. Zusammen mit der endlichen Ausbreitungsgeschwindigkeit v ergibt sich dann mittels $r = v \cdot t$ der Kreisradius r. Ein Problem hierbei ist, dass die Uhren des Senders und des mobilen Endgeräts genau synchronisiert sein müssen, um keine falschen Flugzeiten zu erhalten. Erschwerend kommt hinzu, dass mit größer werdender Ausbreitungsgeschwindigkeit bereits kleine Messfehler die Flugzeit t und somit den Kreisradius stark verfälschen. Ein Fehler von 1 ms in der ermittelten Flugzeit bewirkt bei der Schallgeschwindigkeit einen Fehler im Kreisradius von ca. 0,34 m, im Gegensatz zu 299,79 km mit der Lichtgeschwindigkeit. Zur Positionsbestimmung in Gebäuden existieren mit Cricket und Drishti zwei Verfahren, die Ultraschall einsetzen [54]. Verfahren, die Infrarot-Licht (z.B. REAL) oder Funkwellen (z.B. mit RFID) einsetzen, benötigen dagegen eine extrem genaue Messung des Empfangs- bzw. Sendezeitpunkts [54]. Die Positionsfehler dieser Ver-



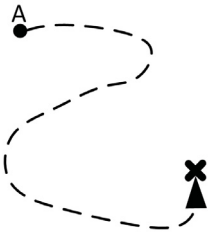
(a) Trilateration (adaptiert aus [89])



(b) Trilateration mit Zeitdifferenzen (adaptiert aus [89])



(c) Ankunftswinkel



(d) Koppelnavigation

Abbildung 2.2: Beispiele zur Ermittlung der eigenen Position (Kreuz) bzgl. der bekannten Position der Referenzpunkte A, B und C.

fahren liegen im Zentimeterbereich, allerdings werden spezielle mobile Empfänger und die aufwendige Ausbringung einer Infrastruktur aus Sendern vorausgesetzt. Mit WLAN-Signalen ist die Lateration auf Smartphones nicht gut möglich [125]. Dies resultiert aus den nichtdeterministischen Interrupts des WLAN-Empfängers.

Eine weitere Methode ist, aus der empfangenen Signalstärke mittels der bekannten Sendestärke und Modellen für die Dämpfung, die das Signal pro Meter erfährt, auf den Kreisradius r zu schließen. Solche Modelle liefern in leeren Räumen perfekte Ergebnisse. Ansonsten können Signale zusätzlich zur Luft auch durch Objekte, wie Gebäude, Bäume und Hügel gedämpft werden [108]. Ein weiteres Problem entsteht, wenn die abgeschickten Signale an solchen Objekten reflektiert werden und sich dann am Ort des Nutzers konstruktiv oder destruktiv überlagern. Grundsätzlich sind hiervon alle funkbasierten Verfahren betroffen, aber gerade beim Einsatz von WLAN in Gebäuden zeigt sich die Problematik besonders stark, so dass die Signalstärke dort kein verlässliches Maß für die Entfernung darstellt.

Betrachtet man das Problem im dreidimensionalen Raum, so werden aus den Kreisen Kugeloberflächen. Im GPS werden Referenzpunkte und Sender durch Satelliten dargestellt, welche die Erde auf bekannten Bahnen umkreisen [151]. Anhand der Flugzeiten, welche die Signale von den Satelliten zum mobilen Endgerät benötigen, werden die Distanzen zu mindestens drei Satelliten bestimmt und Kugeloberflächen gebildet. Diese besitzen maximal zwei Schnittpunkte. Einer davon liegt im Weltraum und einer auf der Erdoberfläche. Letzte-

rer wird dann als Positionsschätzung verwendet. Bei GPS durchlaufen die Signale auf dem Weg vom Satelliten bis zum mobilen Endgerät mindestens 20.000 km und durchqueren dabei die Schichten der Erdatmosphäre. Die Zusammensetzung der Schichten unterliegt ständigen dynamischen Veränderungen, wodurch sich variable Ausbreitungsgeschwindigkeiten ergeben. Für einen fixen Standort ist bei fester Entfernung zu einem Satelliten die Flugzeit des Signals also nichtdeterministisch. Für das klassische GPS wird aktuell garantiert, dass mit professionellen GPS-Empfängern in 95% der Messungen der Fehler innerhalb eines Radius von 7,8 m liegt [62]. Bei Assisted-GPS, was z.B. auch im iPhone 3G unterstützt wird, werden die Rohdaten der empfangenen Signale des Satelliten an einen Server in der Infrastruktur geschickt. Dieser führt dann die Positionsbestimmung aus [151]. Der Vorteil ist, dass dieser Server dazu in der Lage ist, die am mobilen Endgerät gemessene Flugzeit des Signals zu korrigieren. Dazu verwendet er einen stationären Empfänger an einem bekannten Referenzpunkt, wodurch sich die tatsächliche Ausbreitungsgeschwindigkeit berechnen lässt. In einem Experiment von Zandbergen in [151] liegen dabei mit professionellen GPS-Empfängern 95% der Messungen im Radius von 1,3 m um die wahre Position verteilt und mit einem iPhone 3G in 95% der Fälle in einem Radius von 14,4 m.

Zur Flugzeitberechnung muss die Uhr im mobilen Endgerät des Nutzers mit der Uhr der Sender exakt synchronisiert sein. Zu diesem Zweck existiert eine Variante dieses Verfahrens basierend auf Zeitdifferenzen. Hierbei müssen die Uhren der Sender untereinander synchronisiert sein, was in der Regel deutlich einfacher ist, als eine Synchronisation der Sender mit dem mobilen Endgerät. Der Grund ist, dass die Anforderungen an stationäre Sendestationen bzgl. Energie- und Platzbedarf deutlich geringer sind als an mobilen Endgeräte. Somit können präzisere Komponenten verbaut werden. Dieses Verfahren ist in Abb. 2.2(b) skizziert. Hierbei wird ein Signal zweimal gleichzeitig abgeschickt. Einmal von den Sendern an den Referenzpunkten A und C und einmal von den Sendern B und C. Das mobile Endgerät misst jeweils die Differenz der Ankunftszeitpunkte, die direkt proportional zur Differenz der Entfernungen $d(A) - d(C)$ und $d(B) - d(C)$ ist. Da die Position der Referenzpunkte bekannt ist, können nun alle Punkte ermittelt werden, an denen aufgrund der Entfernung zu A, B und C genau eine solche Differenz aus den Signallaufzeiten zu beobachten ist. Dies sind Hyperbeln, wobei zur Positionsbestimmung deren Schnittpunkt verwendet wird.

Treten nun Messfehler beim Radius der Kreise oder Kugeln auf, so entsteht kein Schnittpunkt und somit zunächst keine Positionsschätzung. In der Praxis wird deshalb eine Ausgleichsrechnung durchgeführt. Diese sucht eine Position, die bzgl. der ungenauen Kreise möglichst plausibel scheint. Eine Vorgehensweise hierbei ist es, einen Punkt zu finden, dessen quadratische Abstände zu den Kreisen in der Summe am kleinsten sind. Natürlich kann dieses Problem auch bei den Hyperbeln, beim Verfahren basierend auf Zeitdifferenzen auftreten. Hier wird nach dem gleichen Prinzip verfahren.

Eine weitere Methodik dieser Klasse ist die Angulation. Zur Positionsbestimmung wird hier der Winkel zu den Referenzpunkten anstelle der Distanz verwendet. Dazu werden an den Referenzpunkten Sender vorausgesetzt, die nun einen bekannten Abstrahlwinkel haben. Empfängt das mobile Endgerät die Signale eines solchen Senders, so ist der Sektor, in dem es sich befindet, bekannt. Schneidet man mindestens zwei Sektoren, muss sich der

Nutzer in dieser Schnittfläche aufhalten. Ein Beispiel hierzu ist in Abb. 2.2(c) dargestellt, wobei die Schnittfläche grau hinterlegt ist.

Verfahren basierend auf Koppelnavigation

Moderne mobile Endgeräte, wie Smartphones oder Tablet-Computer, sind mit einer Vielzahl von Sensoren ausgestattet. Darunter befindet sich meist ein Beschleunigungssensor, ein Gyroskop zur Messung der Kreisbewegung und ein Kompass. Bewegt sich ein Nutzer mit seinem mobilen Endgerät, so erfährt dieses durch die Bewegung Beschleunigungen und Drehungen. Daraus lässt sich abschätzen, wie schnell und in welche Richtung sich ein Nutzer bewegt. Über die Zeit betrachtet lässt sich somit der Pfad abschätzen, den der Nutzer zurückgelegt hat. Startet der Nutzer an einem bekannten Referenzpunkt, so erfolgt die Positionsbestimmung, indem ausgehend vom Referenzpunkt der Pfad bis zum Ende verfolgt wird [54]. Dieses Verfahren wird auch als Koppelnavigation (engl. Dead Reckoning) bezeichnet. Ein Beispiel ist in Abb. 2.2(d) gegeben, wobei der Nutzer ausgehend vom Referenzpunkt A einen Pfad abläuft und dessen Ende als seine Position bestimmt wird.

Die Sensoren, die in einem mobilen Endgerät verbaut sind, messen jeweils nur in einem gewissen Toleranzbereich. Somit addieren sich Fehler in der Geschwindigkeit oder im Winkel über die Zeit auf und der Positionsfehler nimmt zu. Deshalb wird auf mobilen Endgeräten die Koppelnavigation mit der zwischenzeitlichen Positionsbestimmung durch Verfahren aus den anderen drei Klassen korrigiert. Eine weitere Möglichkeit ergibt sich, wenn die Landkarte oder der Gebäudeplan bekannt sind. Hier können Fehler auch dadurch eingeschränkt werden, dass die abgeschätzten Pfade nur begehbare Bereiche durchlaufen [54].

Verfahren zur Erkennung der Nähe

Verfahren dieser Klasse erkennen die Nähe des Nutzers zu Erkennungsmarken, die sich an festen Referenzpunkten befinden. Solche Erkennungsmarken können Sender sein, die aktiv akustische, optische oder funkbasierte Erkennungssignale aussenden, oder passive Erkennungsmarken, z.B. Strichcodes (engl. Barcodes), die der Nutzer mit seinem mobilen Endgerät aktiv einlesen muss [54].

Detektiert das mobile Endgerät des Nutzers eine aktive Erkennungsmarke, so ist bekannt, dass der Aufenthaltsort des Nutzers in der davon abgedeckten Zone liegt. Gibt es mehrere konkurrierende aktive Erkennungsmarken, so wird typischerweise die gewählt, deren Signal am stärksten empfangen wird [89]. Eine Methode zur Konstruktion solcher Zonen ist die Erstellung eines Polygons für jede Erkennungsmarke. Die Polygone werden so gewählt, dass genau die Punkte darin enthalten sind, die näher an der zugehörigen Erkennungsmarke liegen, als an einer beliebigen anderen Erkennungsmarke. Solche Polygone werden Voronoi-Zellen genannt. Ein Beispiel ist in Abb. 2.3(a) dargestellt. Hier wird die Erkennungsmarke am Referenzpunkt C am stärksten empfangen, was die Eingrenzung der Position des Nutzers auf die Zelle von C (grau hinterlegt) erlaubt.

Wird eine Erkennungsmarke vom mobilen Endgerät detektiert, ist zunächst nicht bekannt, an welchem Referenzpunkt die Marke liegt. Diese Information wird entweder durch

die Erkennungsmarke selbst bereitgestellt, indem sie ihre Position im aktiv ausgesandten Signal oder im abgelesenen Strichcode enkodiert. Die Erkennungsmarke wird somit zum Referenzpunkt. Andernfalls stellt die Erkennungsmarke einen Identifikator bereit, wobei ihre Position dann aus einer externen Datenbank bezogen wird [54].

Im Folgenden werden exemplarisch drei Verfahren dieser Klasse vorgestellt. Sie werden nach zunehmender Präzision geordnet. Ein mobiles Endgerät, z.B. ein Smartphone, verbindet sich mit einer Basisstation des Mobilfunknetzes, um Telefonie- und Datenverbindungen aufzubauen. Hierfür existieren verschiedene Standards, z.B. GSM, UMTS oder LTE [108]. Jede der Basisstationen besitzt einen eigenständigen Identifikator und eignet sich daher als Erkennungsmarke. Über Datenbanken, wie z.B. die „Unwired Labs' LocationAPI" mit ca. 59 Millionen Einträgen [145], wird schließlich die Position der verbundenen Basisstation abgefragt. Bei GSM und UMTS wird zusätzlich die Rundlaufzeit des Signals zwischen mobilem Endgerät und Basisstation ermittelt, was eine stärkere Eingrenzung der Zelle ermöglicht. Auf einem iPhone 3G liegt in 68% der Messungen der Fehler in einem Kreis mit einem Radius von 827 m [151].

Innerhalb von Gebäuden ergibt sich durch den Bluetooth Low Energy (BLE) Standard eine weitere Möglichkeit zur Erkennung der Nähe [54]. Ein Einsatzgebiet für diesen Standard sind Kleinstcomputer, die aufgrund der Energieeffizienz des Standards über Wochen bis Monate hinweg durch Knopfzellen betrieben werden und nur wenige Zentimeter messen. Diese Kleinstcomputer können als Erkennungsmarken eingesetzt werden und senden Funksignale im 2,4 GHz Bereich. Auf Freiflächen ist dabei im Optimalfall sogar eine Reichweite von über zehn Metern möglich [61]. Ein Beispiel sind die sog. Estimote Beacons [52]. Diese arbeiten in der Rolle eines „Broadcasters" und senden in regelmäßigen Zeitabständen Daten über spezielle Advertisement-Kanäle, bauen aber keine Verbindungen zu anderen Geräten auf [61]. Mobile Endgeräte arbeiten in der Rolle des „Observers" und lauschen auf den Advertisement-Kanälen. Der Referenzpunkt der am stärksten empfangenen BLE-Erkennungsmarke impliziert somit die Zone, in der sich der Nutzer aufhält. Durch die empfangene Signalstärke, die bekannte Sendestärke und ein Signalausbreitungsmodell kann die Distanz zum Referenzpunkt präzisiert und die Zone verkleinert werden. Die Positionsfehler hängen hier stark von der Anzahl der ausgebrachten BLE-Erkennungsmarken und der Umgebung ab, da die schwachen BLE-Signale leicht durch Wände oder Objekte absorbiert werden. Wird das Signal reflektiert und gelangt auf mehreren Wegen zum mobilen Endgerät, so besteht die Gefahr, dass sich die Einzelsignale dort konstruktiv oder destruktiv überlagern und die Distanzmessung verfälschen.

Eine weitere Möglichkeit ist die Ausbringung von Strichcodes, z.B. an den Türschildern in einem Gebäude [54]. Liest ein Nutzer mit seinem mobilen Endgerät den Strichcode ein, bekommt er als seine Position den bekannten Referenzpunkt angezeigt, an dem dieser Strichcode ausgebracht wurde. Nachteile ergeben sich, wenn die Strichcodes schwer zu finden sind. Insbesondere Personen mit Sehschwäche sind davon betroffen. Die Ausbringung der Strichcodes ist dafür relativ kostengünstig, da keine Hardware beschafft werden muss. Die Positionsfehler dieser Methode sind mit wenigen Zentimetern nahezu vernachlässigbar, da das mobile Endgerät zum Einlesen des Strichcodes direkt davor platziert werden muss.

Verfahren basierend auf Mustererkennung

Bei Verfahren dieser Klasse wird ausgenutzt, dass sich an jedem Ort ganz spezifische Beobachtungen von physikalischen Messgrößen machen lassen. Ist im Umkehrschluss die Beobachtung bekannt, so kann auf den zugehörigen Ort geschlossen werden. Solche Verfahren basieren also auf der Wiedererkennung von Mustern.

Vor dem praktischen Einsatz des Verfahrens müssen zunächst Referenzpunkte auf der Karte ausgewählt werden, an denen sogenannte Vormessungen durchgeführt werden [108]. Dieser Prozess wird auch Offline-Phase genannt. Ein wichtiger Unterschied zu den obigen Verfahren ist nun, dass Sender oder Erkennungsmarken nicht an den Referenzpunkten installiert werden müssen. Ihre Position auf der Karte ist beliebig und wird nicht benötigt.

An jedem Referenzpunkt wird durch die Vormessung ein sogenannter Fingerprint (engl. für Fingerabdruck) erstellt und gespeichert, dem die Position des Referenzpunkts fest zugeordnet ist. In diesen Vormessungen kann prinzipiell jede mögliche physikalische Größe erfasst werden, die den Sender oder die Erkennungsmarke am Referenzpunkt charakterisiert. Die Anzahl und Dichte der Referenzpunkte auf der Karte hängt von der Präzision und Richtigkeit ab, die benötigt wird. Sinnvoll ist die Wahl eines Mindestabstands für Referenzpunkte, so dass zwischen beiden Orten eine messbare Abweichung der physikalischen Größe vorliegt.

Die in Frage kommenden physikalischen Größen sind vielfältig. Sind z.B. Ultraschallsender ausgebracht, wird typischerweise die Lautstärke oder der Winkel zu einem Sender gemessen. Andere Ansätze nehmen an jedem Referenzpunkt ein Foto auf, das als Vormessung dient. Auf dem Foto werden markante Bereiche mit starken Kontrastübergängen, z.B. bei Pflanzen oder Türstöcken, durch spezielle Algorithmen erfasst und als Erkennungsmarke betrachtet. Beim späteren Vergleich mit einem anderen Foto werden diese Bereiche wiedererkannt. Ebenso gibt es Ansätze, welche an jedem Referenzpunkt die Charakteristik des Erdmagnetfelds erfassen und als Vormessung verwenden.

Das sogenannte WLAN-Fingerprinting basiert darauf, dass an den Referenzpunkten die Signalstärke von empfangbaren IEEE 802.11 WLAN Access-Points (engl. für Zugriffspunkt) gemessen wird. Diese Access-Points können als Sender an beliebigen Positionen betrachtet werden und sind in heutigen Gebäuden extrem weit verbreitet. Ihr eigentlicher Verwendungszweck ist es, mobilen Endgeräten den Aufbau einer funkbasierten Datenverbindung im 2,4 GHz oder 5,0 GHz Band zu ermöglichen. In den meisten Gebäuden ist deshalb an jedem Referenzpunkt mindestens ein solcher Sender sichtbar ist.

In den letzten Jahren hat sich WLAN-Fingerprinting zum bedeutendsten Verfahren zur Positionsbestimmung in Gebäuden entwickelt [54]. Zum Einen liegt dies daran, dass die Positionsbestimmung über GPS in Gebäuden aufgrund der schwachen Satellitensignale meist nicht möglich ist. Gleiches gilt für Straßenschluchten in Städten, wo zu wenige GPS-Satelliten sichtbar sind. Hier ist WLAN-Fingerprinting ebenso geeignet. Zum Anderen ist die nötige Infrastruktur der Sender, also der WLAN-Access-Points in den meisten Gebäuden ohnehin vorhanden, so dass keine weiteren Investitionen anfallen. Aufgrund der enormen Bedeutung dieses Verfahrens wird in der vorliegenden Arbeit das WLAN-Fingerprinting als laufendes Beispiel für die standortbasierte Autorisierung verwendet. Im Folgenden wird

die Positionsbestimmung auf Basis von Mustererkennung am Beispiel von WLAN-Fingerprinting beschrieben.

Erfassung einer Radiomap Im WLAN-Fingerprinting gibt es zwei Herangehensweisen für die Vormessung der Signalstärken – das diskrete und das probabilistische Fingerprinting. In beiden Fällen wird in der Offline-Phase jedem Referenzpunkt i ein Vektor $\vec{v_i} = (r_1, \ldots, r_n)$ für die Vormessungen zugeordnet, dessen Komponenten $r_1, \ldots, r_n$ den Messwert für die Access-Points $1, \ldots, n$ beschreiben. Die Datenbank, die hierbei entsteht, wird typischerweise als *Radiomap* bezeichnet. Die Access-Points $1, \ldots, n$ können über ihre MAC-Adressen eindeutig identifiziert werden. Die entsprechenden Werte für die Vormessungen werden entweder theoretisch über Ausbreitungsmodelle berechnet, oder empirisch durch manuelle Messungen an den Referenzpunkten ermittelt. Letztere Variante liefert realistischere Ergebnisse, ist aber deutlich zeit- und kostenaufwändiger [78].

Im diskreten Fingerprinting wird jeder Komponente des Vektors genau ein Wert für die Signalstärke zugeordnet, die vom mobilen Endgerät erfasst wird und typischerweise in der Einheit Dezibel Milliwatt (dBm) vorliegt. Ein solcher Vektor hat z.B. die Gestalt:

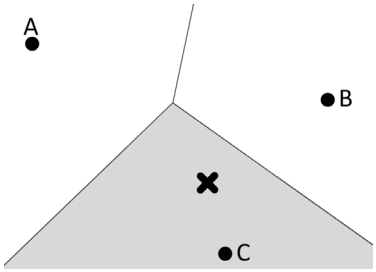
$$\begin{pmatrix} -62 \text{ dBm} \\ -75 \text{ dBm} \\ -54 \text{ dBm} \end{pmatrix} \tag{2.1}$$

Während der Offline-Phase wird für jeden Referenzpunkt $1, \ldots, j$ typischerweise eine ganze Reihe von Vormessungen durchgeführt. Dies ist sinnvoll, da die Signalstärke aufgrund von Umwelteinflüssen an jedem Ort leichten Schwankungen unterliegt, so dass im Vektor der Mittelwert der Messreihe gespeichert wird.

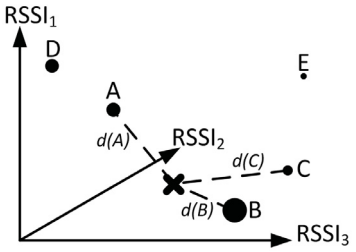
Ausgehend von einer solchen Messreihe betrachtet das probabilistische Fingerprinting, wie die einzelnen Vormessungen verteilt sind. Das Ausmaß der Schwankung wird ebenfalls als ortsabhängige Information betrachtet und mit im Vektor abgespeichert. In vielen Arbeiten wird dazu angenommen, dass die Schwankungen der Signalstärken für jeden Ort einer Normalverteilung folgen. Im Vektor wird dann für jeden Access-Point das Tupel (μ_i, σ_i) abgespeichert. Hier ist μ_i der Mittelwert und σ_i die Standardabweichung, die sich jeweils aus der Anpassung einer Normalverteilung auf die Messreihe bzgl. Access-Point i ergibt. Obiges Beispiel könnte somit folgendermaßen aussehen:

$$\begin{pmatrix} (-62 \text{ dBm}, -5 \text{ dBm}) \\ (-75 \text{ dBm}, -2 \text{ dBm}) \\ (-54 \text{ dBm}, -7 \text{ dBm}) \end{pmatrix} \tag{2.2}$$

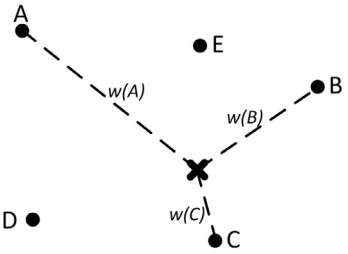
Für den Ort, an dem eine Vormessung $\vec{v}$ durchgeführt wurde, ist $\mathrm{P}(r_i|\vec{v})$ proportional zur Wahrscheinlichkeit, mit welcher Access-Point i mit der Signalstärke r_i messbar ist [127]. Zur Modellierung der Schwankung der Signalstärke werden in der Literatur auch andere Verteilungen als die Normalverteilung verwendet, z.B. die Exponential- oder die Log-Normal-Verteilung. Deren Anwendung ist jedoch weniger weit verbreitet. Deshalb soll sie im Rahmen dieser Arbeit nicht näher betrachtet werden. Für weitere Informationen wird auf Honkavirta et al. [66] verwiesen.



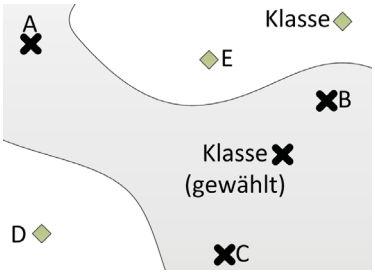
(a) Zellortung



(b) Distanzen im Signalstärkeraum



(c) Szenenanalyse: Regression



(d) Szenenanalyse: Klassifikation

Abbildung 2.3: Verfahren zur Positionsbestimmung basierend auf Zellortung und Szenenanalyse.

Bestimmung der k-nächsten-Nachbarn Die *Online-Phase* startet, nachdem die Vormessungen erfasst wurden. Der Nutzer führt mit seinem mobilen Endgerät eine Messung der Signalstärke der umliegenden WLAN-Access-Points durch und bildet so einen Vektor $\vec{m} = (r_1, \ldots, r_n)$. Im Anschluss werden die Orte der Referenzpunkte bestimmt, deren Vormessungen der aktuellen Messung am ähnlichsten sind. Werden genau k solcher Referenzpunkte bestimmt, werden diese auch als k-nächste-Nachbarn (kNN) im Raum der Signalstärke bezeichnet und später zur Positionsbestimmung verwendet. Typischerweise hat k einen Wert von $3 - 5$ [11,96].

Zur Bestimmung der kNN muss eine Distanz zwischen der Vormessung eines jeden Referenzpunkts und der aktuellen Messung berechnet werden. Dazu werden die Vormessung und die aktuelle Messung jeweils als Punkt in einem Vektorraum betrachtet, dessen Basis sich aus den insgesamt auftretenden MAC-Adressen ergibt. Ein Beispiel ist in Abb. 2.3(b) gegeben. Ausgehend von Referenzpunkten A bis E sind die Vektoren $\vec{v}_A, \ldots, \vec{v}_E$ der diskreten Vormessungen, sowie der Vektor der aktuellen Messung $\vec{m}_\times$ als Punkt im Raum der Signalstärken von drei Access-Points eingetragen.

Die Distanzen $d(A), \ldots, d(E)$ der aktuellen Messung zu den Vormessungen können auf unterschiedliche Arten bestimmt werden. Sind die Vormessungen und die aktuelle Messung einfache Vektoren, wie in (2.1), so ist die euklidische Distanz oder die Manhattan-Distanz anwendbar [89]. Liegen die Vormessungen und die aktuelle Messung entsprechend (2.2)

vor, so eignet sich die Mahalanobis-Distanz.

In Ergänzung zur Abstandsmetrik in Vektorräumen existiert für das probabilistische Fingerprinting eine Möglichkeit, die kNN basierend auf der Likelihood-Funktion zu bestimmen. Ist eine aktuelle Messung $\vec{m}$ gegeben, so kann für jede Vormessung $\vec{v_i}$ bestimmt werden, welchen Wert die bedingte Wahrscheinlichkeitsdichtefunktion (WDF) $\mathrm{P}\left(\vec{m}|\vec{v_i}\right)$ hat [66]. Dieser Wert ist proportional zur Wahrscheinlichkeit, mit der diese Messung am Referenzpunkt der Vormessung $\vec{v_i}$ zu beobachten ist. Sortiert man die Vormessungen anhand dieser Werte, so erhält man eine Liste der kNN.

Bei der Berechnung macht man sich typischerweise das Theorem von Bayes zu Nutze, nach dem dieser Wert der bedingten WDF $\mathrm{P}(\vec{v_i}|\vec{m})$ entspricht [66], denn:

$$\mathrm{P}\left(\vec{v_i}|\vec{m}\right) = \frac{\mathrm{P}\left(\vec{m}|\vec{v_i}\right) \cdot \mathrm{P}\left(\vec{v_i}\right)}{\mathrm{P}\left(\vec{m}\right)} \tag{2.3}$$

Zur einfacheren Berechnung wird üblicherweise angenommen, dass die Signalstärken der Access-Points an jedem Referenzpunkt voneinander unabhängig sind [66]. Somit gilt:

$$\mathrm{P}\left(\vec{m} = (r_1, \ldots, r_n)|\vec{v_i}\right) = \mathrm{P}\left(r_1|\vec{v}_{i1}\right) \cdot \mathrm{P}\left(r_2|\vec{v}_{i2}\right) \cdots \mathrm{P}\left(r_n|\vec{v}_{in}\right) \tag{2.4}$$

Der Wert $\mathrm{P}(\vec{v_i})$ entspricht der Wahrscheinlichkeit, mit der eine Messung $\vec{m}$ am Referenzpunkt der Vormessung $\vec{v_i}$ ausgeführt wird. Da keine näheren Informationen über die Position des Nutzers vorhanden sind, wird dies typischerweise als Gleichverteilung modelliert. Der Wert $\mathrm{P}\left(\vec{m}\right)$ ist ein Normierungsfaktor, für den bei insgesamt j Vormessungen gilt:

$$\mathrm{P}\left(\vec{m}\right) = \sum_{i=0}^{j} \mathrm{P}\left(\vec{m}|\vec{v_i}\right) \cdot \mathrm{P}(\vec{v_i}) \tag{2.5}$$

Unterscheidet sich die Menge der erfassten Access-Points in der aktuellen Messung $\vec{m}$ und in einer Vormessung $\vec{v}_i$, so liegen $\vec{m}$ und $\vec{v}_i$ in unterschiedlichen Vektorräumen. Für die Anwendung der Distanzmaße müssen beide jedoch im gleichen Vektorraum liegen. Im diskreten Fingerprinting hat es sich bewährt, beim Vergleich zweier Vektoren, deren erfasste Access-Points sich unterscheiden, die Signalstärke der fehlenden Access-Points mit einem Pseudowert von -92 dBm bis -100 dBm aufzufüllen. In diesem Bereich endet die Messskala von WLAN-Empfängern für den Endkundenmarkt [51,96]. Im probabilistischen Fingerprinting wird zusätzlich ein Pseudowert für die Standardabweichung der Signalstärke benötigt, der im Verhältnis zur beobachteten Standardabweichungen sehr klein ist, da die Schwankungen mit schwächer werdenden Signalstärken abnehmen [89].

Im praktischen Einsatz ergibt sich das Problem, die beste Anzahl k bei der Ermittlung der kNN zu finden. Hierbei sind aufwendige empirische Untersuchungen nötig. In der vorliegenden Arbeit wird in Abschnitt 3.2 der Ansatz SMARTkNN vorgestellt, der die Anzahl der nächsten Nachbarn dynamisch zur Laufzeit ermittelt und eine empirische Parameterbestimmung erspart. Eine verwandte Arbeit dazu existiert von Roshanaei et al. [118], die eine adaptive Anordnung von Antennen verwenden, um den Ankunftswinkel der WLAN-Signale zu messen. Dadurch kann die Selektion der nächsten Nachbarn auf Sektoren oder

Flächen begrenzt werden. Altintas et al. bestimmen in [4] zunächst aus den Vormessungen eine große Anzahl nächster Nachbarn (z.B. 9). Sie verwenden den k-Means-Algorithmus, um die zugehörigen Referenzpunkte zu clustern. Für die Vormessungen eines jeden Clusters wird im Signalstärkeraum die durchschnittliche Distanz zum Nutzer berechnet. Der ähnlichste Cluster wird schließlich als endgültige kNN-Liste ausgewählt. Shin et al. wählen in [129] nur solche kNN aus, deren Distanz im Signalstärkeraum einen fixen Schwellwert unterschreitet. Diese Kandidaten werden in einem zweiten Schritt nochmals selektiert, indem ihre mittlere Distanz im Signalstärkeraum bestimmt wird. Nur Kandidaten, deren Distanz darunter liegt, werden in die kNN-Liste aufgenommen. Im Gegensatz zu den verwandten Arbeiten wird im Ansatz der vorliegenden Arbeit aus einer langen kNN-Liste sukzessive ein immer längerer Präfix zur Positionsbestimmung verwendet, solange bis die Positionsschätzungen divergieren. Der Vorteil ist, dass keine Schwellwerte im Signalstärkeraum und keine vorherigen empirischen Messungen nötig sind.

Die Positionsbestimmung Nachdem für die aktuelle Messung $\vec{m}$ die Vormessungen bzgl. ihrer Distanz sortiert sind und daraus die kNN ermittelt wurden, erfolgt die Positionsbestimmung. Hierfür gibt es zwei Vorgehensweisen, die numerische und die symbolische Positionsbestimmung.

Bei der numerischen Positionsbestimmung wird die Position μ des Nutzers aus einer Linearkombination der Koordinaten der Referenzpunkte $x_1, \ldots, x_j$ berechnet, die den Vormessungen der kNN-Liste zugeordnet sind [66]:

$$\mu = \left(\sum_{i=1}^{j} w(i) \right)^{-1} \cdot \sum_{i=1}^{j} w(i) \cdot x_i \tag{2.6}$$

Jedes Gewicht $w(i)$ ist dabei positiv und der Faktor vor der Summe normiert die Gewichte, so dass diese in der Summe 1 ergeben. Die Wahl der Gewichtung $w(i)$ ist typischerweise der Kehrwert der oben beschriebenen Distanz, welche die aktuelle Messung im Signalstärkeraum zu einer Vormessung $\vec{v}_i$ hat. Als besonders vielversprechend hat sich hierbei der Kehrwert der quadratischen euklidischen Distanz im Signalstärkeraum erwiesen [96]:

$$w(i) = \left(\frac{1}{\|\vec{m} - \vec{v}_i\|} \right)^2 \tag{2.7}$$

Ein Beispiel zur numerischen Positionsbestimmung ist in Abb. 2.3(c) gegeben. Hier werden, ausgehend vom Signalstärkeraum in Abb. 2.3(b), die Vormessungen an den Referenzpunkten B, A und C als die 3 nächsten Nachbarn ermittelt. Die Position des Nutzers ergibt sich aus der Linearkombination dieser drei Referenzpunkte, die durch $w(B)$, $w(A)$ und $w(C)$ gewichtet sind. Es zeigt sich, dass die Distanz im Signalstärkeraum zwischen einer Vormessung und der aktuellen Messung nicht immer mit der Distanz des zugehörigen Referenzpunkts zur wahren Position des Nutzers korreliert.

Die symbolische Positionsbestimmung ordnet jedem Referenzpunkt eine Klasse zu, beispielsweise den Namen des Raumes, in dem er liegt. Seine exakten Koordinaten werden

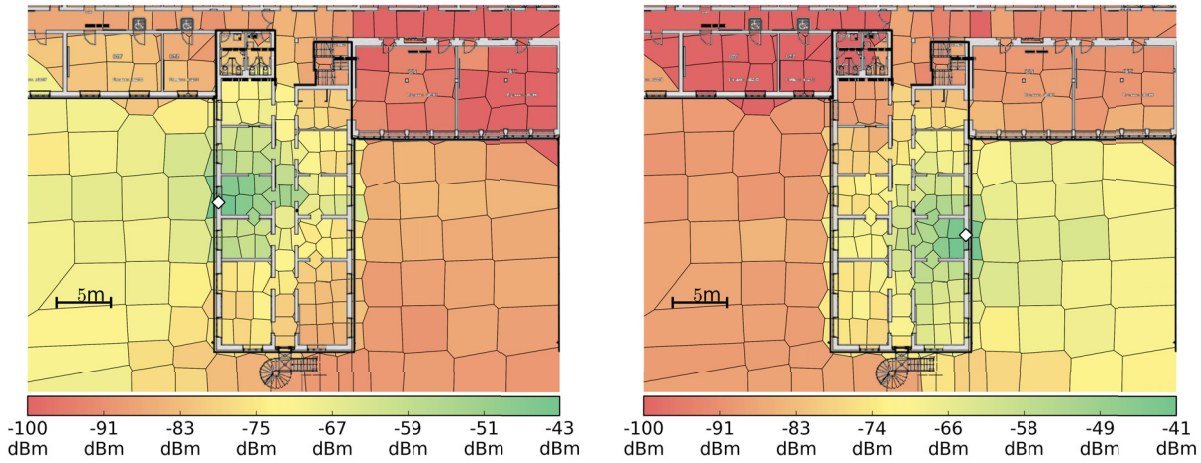
nicht benötigt. Bei der Positionsbestimmung wird nun die Klasse ermittelt, in der die Position des Nutzers liegt. Eine Möglichkeit dazu ist die Untersuchung, welche Klasse in der kNN-Liste vorherrschend ist. Ein Beispiel ist in Abb. 2.3(d) gegeben. Hier ist den Referenzpunkten A, B und C die Klasse $\times$ zugeordnet, welche der symbolische Bezeichner des grauen Bereichs ist. Die Referenzpunkte D und E gehören zur Klasse $\diamondsuit$, die den weißen Bereich bezeichnet. Liegen die drei nächsten Nachbarn aus obigem Beispiel vor, so ist $\times$ die vorherrschende Klasse in der kNN-Liste. Als Resultat ergibt sich die Schätzung, dass sich der Nutzer in der grauen Zone befindet.

Innerhalb von Gebäuden arbeiten Systeme basierend auf WLAN-Fingerprinting sehr präzise im Verhältnis zu dem relativ geringen Kostenaufwand. Eines der ersten Systeme mit numerischen, diskretem Fingerprinting ist RADAR von Bahl et al. [11]. Dabei liegt der Fehler in 90% der Fälle im Umkreis von 5,93–5,97 m. Das Horus-System von Youssef et al. besitzt zwei Ausprägungen [147]. Wird der nächste Nachbar über die Likelihood-Funktion bestimmt und eine numerische Position berechnet, liegt der Fehler in 90% der Fälle im Umkreis von 1,4 m. Durch Verwendung der 6 nächsten Nachbarn wird der Fehler im Schnitt um 13% reduziert. Kessel et al. erzeugen in [72] eine probabilistische Radiomap, indem pro Raum eine Vormessung aus mehreren verteilten Einzelmessungen erstellt wird und ihr der Name des Raumes zugewiesen wird. Über symbolische Positionsbestimmung wird so in 79% der Fälle der korrekte Raum erkannt.

Abschätzung von Positionsfehlern Wird WLAN-Fingerprinting mit symbolischer Positionsbestimmung zur standortbasierten Autorisierung eingesetzt, hängt die Definition der verschiedenen Klassen von den autorisierten Zonen ab. Es entsteht somit eine Abhängigkeitsbeziehung zwischen Positionierungssystem und der standortbasierten Autorisierung. Im WLAN-Fingerprinting mit numerischer Positionsbestimmung gilt dies nicht, weshalb es für den Einsatz zur standortbasierten Autorisierung besonders geeignet ist. Im Folgenden wird auf die Ursachen von Positionsfehlern von WLAN-Fingerprinting mit numerischer Positionsbestimmung und Verfahren zu deren Abschätzung eingegangen.

In der Online-Phase von Verfahren zum numerischen WLAN-Fingerprinting entstehen Positionsfehler aus vielfältigen Gründen. Generell unterliegt jede Messung von WLAN-Signalstärken, die während der Online-Phase durchgeführt wird, einer Reihe von Einflüssen, welche die Auswahl der nächsten Nachbarn und somit die Bestimmung der Position negativ beeinflussen.

Zum Einen muss beachtet werden, dass die empfangene Signalstärke zeitlichen Schwankungen unterliegt, was auch Schwund bzw. Fading genannt wird [108]. Gelangt das Signal mittels Reflexionen über unterschiedlich lange Wege zur Empfängerantenne, tritt also Mehrwegeausbreitung auf, so trifft seine elektromagnetische Welle möglicherweise mit einem gewissen Phasenunterschied am Empfänger ein. Somit entsteht eine zeitliche Dispersion. Im Falle von WLAN-Fingerprinting äußert sich dies insbesondere im Effekt des Small-Scale-Fading, welches am Ort des Empfängers aus der konstruktiven oder destruktiven Überlagerung solcher phasenverschobener Signale entsteht [143]. Innerhalb eines räumlich kleinen Bereichs, der von der Wellenlänge des Signals abhängt, können somit starke Schwankungen



(a) Access-Point mittig links.

(b) Access-Point mittig rechts.

Abbildung 2.4: Darstellung der mittleren gemessenen Signalstärke in dBm bezüglich der aufgezeichneten Fingerprint-Datenbank. Die dargestellten Zellen entsprechen den Voronoi-Zellen der Fingerprint-Datenbank.

der Signalstärke auftreten. Im Fall von WLAN IEEE 802.11g mit 2,4 GHz und einer Wellenlänge von ca. 12 cm kann also innerhalb dieses Gebiets schon eine starke Schwankung beobachtet werden. Innerhalb von Gebäuden sind diese Effekte typischerweise deutlich stärker ausgeprägt als in Außenbereichen, da hier mehr potentielle Flächen zur Reflexion vorhanden sind. Innerhalb eines Raums können somit einzelne Teilbereiche entstehen, die eine gänzlich andere Signalstärkemessung ergeben, als die restlichen Orte [12]. Ist ein solcher Teilbereich nicht durch einen Referenzpunkt in der Fingerprint-Datenbank erfasst, besteht die Gefahr, dass während der Online-Phase eine Messung in einem solchen Teilbereich nicht eindeutig zuzuordnen ist. Bewirkt dies die Wahl einer unpassenden Menge an nächsten Nachbarn, entstehen Fehler bei der Positionsbestimmung. Auf größeren Flächen bzw. Räumen, wie z.B. in Außenbereichen oder Hallen, treten generell aufgrund einer gleichmäßigeren Struktur schwächere Effekte der Mehrwegeausbreitung auf. Somit besitzen auf solch größeren Flächen, die einzelnen Einträge der Fingerprint-Datenbank eine große Ähnlichkeit.

Dies ist für zwei Access-Points in Abb. 2.4 illustriert. Die Grafik ist aus einer Radiomap extrahiert, wobei um jeden Referenzpunkt eine Voronoi-Zelle konstruiert wurde. Die Einfärbung entspricht der gemessenen Signalstärke des Access-Points, der als ♢ dargestellt ist. Klar erkennbar ist, dass die gemessene Signalstärke in den Innenräumen insgesamt heterogener ist. In der Online-Phase kann somit in Außenbereichen eine kleine Abweichung der aktuellen Messung zur Vormessung des nächstgelegenen Referenzpunkts direkt zur Auswahl von solchen nächsten Nachbarn führen, deren Referenzpunkte weit von der wahren Position des Nutzers entfernt liegen und somit größere Fehler verursachen.

Doch auch weitere Einflussfaktoren können die Qualität der Positionsbestimmung be-

einträchtigen. Wird zum Beispiel in der Online-Phase ein anderes mobiles Endgerät als in der Offline-Phase verwendet, ergibt sich ebenfalls eine starke Abweichung der an einem Ort gemessenen Signalstärke, wenn z.B. eine andere WLAN-Antenne oder ein anderer WLAN-Chip verbaut ist. Ein Einflussfaktor für langfristige zeitliche Schwankungen ergibt sich aus den ständigen Veränderungen innerhalb des Trägermediums, also u.a. der Luft oder dem Gebäude [108]. So führt eine unterschiedliche Luftfeuchtigkeit im Falle von WLAN zu einer anderen Absorption und somit zu einer anderen Dämpfung des Signals. Aber auch eine bauliche Veränderung innerhalb des Gebäudes verursacht langfristig eine solche Abweichung. Wird zum Beispiel eine Tür in der Online-Phase geschlossen, die während der Offline-Phase noch geöffnet war, so werden die Signale hierdurch gedämpft und anders als in der Offline-Phase reflektiert. Eine weitere Veränderung ergibt sich auch durch den Ausfall von Access-Points, deren örtliche Verlagerung oder durch Personen, die sich auf dem Pfad des Signals befinden [11].

Wird eine numerische Positionsbestimmung auf Basis der kNN durchgeführt, so ist es für die standortbasierte Autorisierung wichtig, welche Ungewissheit dabei entsteht. Ein Verfahren zur quantitativen Erfassung dieser Ungewissheit im numerischen WLAN-Fingerprinting aus Eigenschaften der durchgeführten Messung in der Online-Phase, wird in dieser Arbeit als Fehlerschätzer bezeichnet. Aktuell existieren in der Literatur nur wenige Fehlerschätzer für WLAN-Fingerprinting.

Eine der ersten Arbeiten stammt von Lemelson et al. [87], die vier Ansätze zur Abschätzung der Richtigkeit von Positionen angeben. Ihre Ansätze sind auf die numerische Positionsbestimmung basierend auf einem nächsten Nachbarn (1NN) ausgelegt. Das Fingerprint-Clustering und das Leave-One-Out-Verfahren verwenden außer der geschätzten Position keine weiteren Eigenschaften.

Im Fingerprint-Clustering wird anhand der Referenzpunkte der Radiomap ein Polygon ermittelt, in dem die geschätzte Position liegt. Die wahre Position des Nutzers wird in diesem Polygon vermutet. Das Polygon wird bestimmt, indem zunächst in Analogie zu Abb. 2.4 die Voronoi-Zellen um alle Referenzpunkte der Radiomap gebildet werden. Anfangs wird jede Voronoi-Zelle als Cluster betrachtet. Iterativ werden jeweils zwei benachbarte Cluster verbunden, wenn die Ähnlichkeit der darin enthaltenen Vormessungen einen vordefinierten Schwellwert überschreitet. Zur Fehlerschätzung im Leave-One-Out-Verfahren wird der Referenzpunkt der Radiomap entfernt, dessen Vormessung der nächste Nachbar ist und der daher auch der geschätzten Position entspricht. Auf der verkleinerten Radiomap werden anschließend m Positionsbestimmungen simuliert, indem für alle m Vormessung des entfernten Referenzpunkts jeweils die geographische Distanz zum zugehörigen nächsten Nachbarn ermittelt wird. Die Fehlerschätzung ist dann die Summe aus deren durchschnittlicher Distanz und dem Doppelten der Standardabweichung dieser Distanzen.

Das Best-Candidate-Set- und das Signal-Strength-Variance-Verfahren verwenden Eigenschaften der aktuellen Messung. Im Ersten gibt es drei Ausprägungen, welche die kNN-Liste verwenden, die anhand der aktuellen Messung ermittelt wird. Die Fehlerschätzung basiert entweder auf der durchschnittlichen oder der maximalen geographischen Distanz des nächsten Nachbarn zu den $k-1$ anderen Referenzpunkten. Eine Alternative ist die Ermittlung der paarweise größten Distanz aus den Referenzpunkten der kNN-Liste. Diese Ausprägun-

gen tendieren mit steigendem k zum Überschätzen der Fehler. Das Signal-Strength-Variance-Verfahren verwendet als Maß zur Fehlerschätzung, wie stark die Empfangsstärke von Access-Points an der wahren Position des Nutzers schwankt. Er muss dafür eine ganze Messreihe aufnehmen, wobei aus den Empfangsstärken für jeden Access-Point die Varianz berechnet wird. Diese dient dann als Maß zur Fehlerschätzung.

Lemelson et al. bewerten in [87] die Qualität ihrer Fehlerschätzer anhand der Fehlerdistanzdifferenz. Dies ist die Abweichung des echten Fehlers vom geschätzten Fehler. Für ihre Verfahren beträgt die Abweichung ca. 2–4 m. Gerade in Gebäuden ist daher keine verlässliche Aussage über die Ungewissheit, mit der sich ein Nutzer in einem Raum befindet, möglich. Ihre Verfahren stellen eher ein Werkzeug zur Klassifikation von ermittelten Positionen als gewiss oder ungewiss dar.

Marcus et al. leiten in [96] eine Normalverteilung aus der kNN-Liste her, indem die durchschnittliche Distanz der Referenzpunkte zur bestimmten Position ermittelt wird. Diese Verteilungen modellieren die Lage der wahren Position relativ zur bestimmten Position. Die Verteilungen werden dabei umso breiter, je breiter die Referenzpunkte gestreut sind. In der Evaluation wird aus den Fehlerschätzungen des Best-Candidate-Set-Verfahrens von Lemelson et al. in [87] eine Normalverteilung hergeleitet. Es zeigt sich, dass diese Darstellung von Positionsfehlern eine bessere Approximation an die Realität ist, als die Darstellung als kreisförmiger Ungewissheitsbereich. Trotzdem wird klar, dass die Statistik der Normalverteilung dazu tendiert, gerade große Fehler zu unterschätzen. Problematisch ist dies beim Einsatz in der standortbasierten Autorisierung, wenn eine zu große Gewissheit über den Aufenthalt in einem bestimmten Raum suggeriert wird. Aufbauend auf diesen Ergebnissen wird deshalb in dieser Arbeit in Abschnitt 3.1 ein Ansatz vorgestellt, der bivariate Laplaceverteilungen aus den Referenzpunkten der kNN-Liste herleitet. Es wird gezeigt, dass Positionsfehler im numerischen WLAN-Fingerprinting so deutlich besser abgeschätzt werden können.

Beder et al. führen in [12] eine Analyse der Radiomap in der Offline-Phase durch, um potentielle Positionsfehler bereits im Vorfeld abzuschätzen. Dabei wird für jede prinzipiell mögliche Position des Nutzers eine Normalverteilung hergeleitet, welche die Fehlervektoren beschreibt, die dort im Betrieb zu erwarten sind. Ihre Überlegung zur Herleitung dieser Verteilung beruht auf der bereits erwähnten Tatsache, dass in Bereichen mit starkem Fading ein großer Positionsfehler entstehen kann (siehe Abb. 2.4). In ihrer Methodik wird für jeden Access-Point anhand der Radiomap eine interpolierte Signalstärkekarte berechnet, worauf der Gradient bestimmt wird (Änderung der Empfangsstärke pro Meter). Zusammen mit einer Normalverteilung für die Schwankung bei der Signalstärkemessung, ergibt sich der Zusammenhang für die Normalverteilung der Fehlervektoren. Ihre Normalverteilung trifft aber nur eine generelle Aussage, die nicht speziell auf der aktuellen Messung beruht und somit nicht alle vorliegenden Informationen berücksichtigt.

Die Arbeit von Beder et al. erlaubt dafür bereits in der Offline-Phase die Identifikation von geographischen Bereichen, in denen kleine Positionsfehler zu erwarten sind. Diese Bereiche sind als Richtschnur für die Definition von autorisierten Zonen verwendbar.

Evennou et al. definieren in [53] eine Normalverteilung um die bestimmte Position und modellieren damit den Fehlervektor. Die Kovarianzmatrix wird dabei in Abhängigkeit von

der Schwankung der Messungen des Nutzers bestimmt, was als Maß für die Konfidenz der Positionsbestimmung verwendet wird. In der Arbeit wird aber nicht beschrieben, wie diese Kovarianzmatrix hergeleitet wird oder wie gut durch die Normalverteilung Positionsfehler abgeschätzt werden.

Moghtadaiee et al. geben in [105] einen Fehlerschätzer an, bei dem der Nutzer mehrere Messungen durchführen muss. In Vorberechnungen wird für die Fingerprint-Datenbank anhand der Referenzpunkte und deren Vormessungen, das durchschnittliche Verhältnis der Distanz zweier Vormessungen im Signalstärkeraum zur geographischen Distanz ihrer Referenzpunkte ermittelt. Dieser Wert wird multipliziert mit der Standardabweichung der Messungen des Nutzers, woraus sich die Fehlerschätzung ergibt. Die Autoren vergleichen den Wert mit der Best-Candidate-Strategie von Lemelson et al. aus [87] und zeigen, dass auf ihren Testdaten im Mittel eine bessere Abschätzung des Fehlers möglich ist. Auch hier besteht das Problem, dass nur ein fester Wert für den geschätzten Fehler und kein statistisches Modell für die reale Fehlerverteilung geliefert wird.

Gao et al. geben in [58] basierend auf einer Positionsschätzung ein Konfidenzintervall für mögliche Positionsfehler an. Aus Vorberechnungen basierend auf der Radiomap wird in der Offline-Phase ein Modell (Normalverteilung) für jede mögliche Positionsschätzung vorberechnet, welches die dortige Schwankung der Signalstärke der Access-Points modelliert. Für die Positionsschätzung x des Nutzers wird diese Verteilung ermittelt, woraus 1000 Stichproben als Pseudo-Messungen des Nutzers gezogen werden (engl. Bootstrapping). Jede Einzelne wird als Messung im Prozess der Positionsbestimmung verarbeitet und die Distanz zu x bestimmt, was der Länge des Fehlervektors entspricht. Aus allen Fehlervektoren wird das 2,5% und das 97,5% Quantil ermittelt und als Grenzen für ein 95% Konfidenzintervall angegeben. Die Intervallgrenzen geben zwar ein Gefühl für das Ausmaß eines Fehlers, sie erlauben aber keine Aussage darüber, wie wahrscheinlich es ist, dass sich ein Nutzer innerhalb einer autorisierten Zone befindet.

Aktuell existiert also kein Verfahren, das anhand der durchgeführten Messung eines Nutzers eine verlässliche statistische Modellierung des Fehlervektors liefert. Denn entweder werden skalare Werte zurückgegeben oder Gleichverteilungen verwendet, die eine zu starke Vereinfachung der Realität darstellen. Wie oben erwähnt, wird deshalb in Abschnitt 3.1 dieser Arbeit ein Verfahren vorgestellt, das aus der kNN-Liste einer Messung des Nutzers eine Laplaceverteilung zur Modellierung des Fehlervektors herleitet.

2.1.2 Die Verarbeitung von Positionsschätzungen

Um Positionsfehler in der standortbasierten Autorisierung zu berücksichtigen, muss zunächst ermittelt werden, wie wahrscheinlich sich der Nutzer innerhalb der autorisierten Zone befindet. Dazu wird eine statistische Verteilung für die wahre Position des Nutzers benötigt, z.B. die oben genannte Laplaceverteilung. Integriert man die WDF dieser Verteilung über die autorisierte Zone, erhält man die Aufenthaltswahrscheinlichkeit, also die Wahrscheinlichkeit, mit der sich der Nutzer tatsächlich innerhalb der autorisierten Zone befindet. Da dieser Prozess sehr rechenintensiv ist [130], werden Verfahren benötigt, um diesen Wert effizient bestimmen zu können.

Ardagna et al. gehen in [7] davon aus, dass die standortbasierte Autorisierung Anfragen autorisiert, bei denen die Aufenthaltswahrscheinlichkeit des Nutzers innerhalb der autorisierten Zone einen vordefinierten Schwellwert überschreitet. Die Positionsschätzung wird als WDF modelliert, die als Gleichverteilung innerhalb eines Kreises vorliegt. In ihrem Ansatz berechnet sich die Aufenthaltswahrscheinlichkeit aus dem Prozentsatz des Kreises, der die autorisierte Zone überdeckt. Positionierungssysteme, deren Statistik durch eine Normal- oder Laplaceverteilung besser beschrieben wird, unterstützt der Ansatz nicht. Darüber hinaus werden auch keine Benchmark-Ergebnisse für diese Art der Auswertung angegeben.

Shin et al. setzen in [130] ebenfalls das Überschreiten eines Schwellwerts voraus. Hier wird eine Normalverteilung als WDF vorausgesetzt. Der Beitrag der Arbeit ist ein Filter, der anhand der WDF der Positionsschätzung mit geringem Rechenaufwand ermittelt, ob der Schwellwert sicher über- oder unterschritten wird. Dazu werden Grenzregionen um autorisierte Zonen gelegt und zusätzlich wird die WDF zu einer Gleichverteilung auf einer quadratischen Fläche vereinfacht. Die numerische Integration ist nur für ungewisse Fälle nötig.

Viele verwandte Arbeiten existieren im Bereich der Auswertung von Abfragen an Datenbanken bewegter Objekte [67]. Solche Abfragen werden auch als räumliche Abfragen bezeichnet (engl .Spatial Queries). In der Datenbank werden dabei Objekte zusammen mit ihrem unscharfen Ort abgelegt. Ein Abfragetyp ist die Bestimmung der k nächsten bekannten Position relativ zu einem definierten geographischen Ort. Dabei werden k Objekte ermittelt, die sich mit der größten Wahrscheinlichkeit innerhalb einer bestimmten Entfernung um diesen Ort befinden. Bereichsabfragen finden hingegen die Objekte, die sich wahrscheinlicher als ein Schwellwert innerhalb eines geographischen Bereichs befinden.

Ein Ansatz, der sich mit räumlichen Anfragen auf rechteckigen Bereichen befasst, stammt von Tao et al. [26]. Die Auswertung erfolgt hier basierend auf einem Monte-Carlo-Verfahren, wobei Stichproben aus der WDF gezogen werden, deren Lage dann relativ zum Bereich untersucht wird. Die Autoren erwähnen, dass die Auswertung solcher Anfragen für allgemeine WDFs sehr rechenaufwendig ist und durch Anwendung von Filtern auf ein Minimum reduziert werden soll.

Chen et al. optimieren in [22] die Auswertung von probabilistischen Bereichsanfragen durch die Anwendung eines Ausschlussverfahrens. Dazu wird für die WDF eines Objekts mit ungewisser Position ein Katalog von p-Grenzen berechnet. Eine p-Grenze ist eine Gerade, welche den Definitionsbereich der WDF in zwei Bereiche teilt, so dass im ersten Teil die Wahrscheinlichkeit p und im zweiten Teil die Wahrscheinlichkeit $1 - p$ liegt. Die Abfrage, ob sich der Nutzer mit einer höheren Wahrscheinlichkeit als p' in einer Zone befindet, wird pauschal negativ beantwortet, wenn die Zone in einem Bereich bzgl. der p-Grenzen liegt, in dem schon eine geringere Wahrscheinlichkeit als p' liegt.

Cheng et al. stellen in [25] einen Ansatz vor, mit dem für eine Menge von Objekten mit ungewisser Position bestimmt wird, ob sie mit größerer Wahrscheinlichkeit als p die kNN zu einer Region sind. Zur Verringerung der nötigen numerischen Integrationen werden auch hier Filter eingesetzt.

Bordogna et al. realisieren in [19] eine Bereichsabfrage, die alle Nutzer mit ungewisser

Position bestimmt, die sich innerhalb eines bestimmten Radius um einen Punkt befinden. Die ungewisse Position wird als Kreis modelliert. Überlappen beide Kreise, so ist der Nutzer in der Ergebnismenge enthalten. Hier wird ebenfalls keine Abschätzung möglicher Fehler angegeben oder die Performanz untersucht.

Eine konzeptionelle Arbeit stammt von Liu et al. [90], die verschiedene Ortsprädikate definieren, um eine topologische Beziehung zwischen einem sich bewegenden Punkt und einer statischen Region zu erkennen. Diese Prädikate werden nur logisch definiert, jedoch wird keine effiziente Auswertungsmöglichkeit angegeben.

Insgesamt existieren nur wenige Arbeiten, die eine Bereichsanfrage effizient auswerten können und die Aufenthaltswahrscheinlichkeit eines Nutzers als Ergebnis liefern. Dabei werden oft unrealistische Annahmen über die WDF des Nutzers getroffen. Soll die WDF für die Position des Nutzers über die autorisierte Zone integriert werden, ist unter der Annahme von beliebig geformten autorisierten Zonen eine geschlossene Lösung nicht möglich. Numerische Methoden müssen zum Einsatz kommen, die im praktischen Einsatz sehr rechenintensiv sind und hohe Antwortzeiten der standortbasierten Autorisierung verursachen. Die praktische Einsetzbarkeit der standortbasierten Autorisierung wird dadurch beeinträchtigt.

Zur Lösung dieses Problems wird in dieser Arbeit in Abschnitt 3.3 ein Ansatz vorgestellt, der es erlaubt, aus einer WDF des entwickelten Fehlerschätzers effizient die Aufenthaltswahrscheinlichkeit in einer autorisierten Zone zu bestimmen. Die WDF kann dabei der Normal- oder Laplaceverteilung folgen. Der Ansatz erzeugt einen Katalog aus Vorberechnungen, so dass zur Laufzeit lediglich Nachschlageoperationen anstelle von Berechnungen nötig sind.

2.1.3 Die Verfolgung von mobilen Nutzern

Um standortbasierte Autorisierung über ein ganzes Zeitintervall durchzuführen, wird nicht nur eine einzelne Positionsschätzung benötigt, sondern ein kontinuierlicher Strom. Aufgrund von Messausreißern ist es dabei möglich, dass eine Positionsschätzung zum Zeitpunkt t gegenüber einer Positionsschätzung zum Zeitpunkt $t-1$ völlig unplausibel scheint, da ein Nutzer eine solche Strecke in der dazwischenliegenden Zeitspanne nicht zurücklegen kann. Hier schaffen Bayesische Filter Abhilfe. Diese werden zunächst allgemein beschrieben, worauf Partikelfilter als eine Realisierung vorgestellt. Partikelfilter werden in dieser Arbeit für den Ansatz in Abschnitt 4.3 verwendet, um die Trajektorie abzuschätzen, die ein Nutzer während der Ausübung eines standortbezogenen Zugriffsrechts abläuft.

Grundlagen Bayesischer Filter

Bayesische Filter nutzen u.a. zwei Modelle, die beschreiben, wie eine neu bestimmte Position von der aktuell vermuteten Position abweicht (Messmodell) und wie sich ein Nutzer in einer definierten Zeitspanne fortbewegt (Bewegungsmodell). Das Filterproblem besteht darin, jeder möglichen wahren Position x_t für einen Zeitpunkt t eine Wahrscheinlichkeit

Algorithmus 1 Das allgemeine Konzept Bayesischer Filter [136].

Eingabe: Vorherige Vermutung $ver(x_{t-1})$ über die Position und Positionsschätzung m_t
Ausgabe: Vermutung $ver(x_t)$ über die Position x_t zum Zeitpunkt t

```
1: function BAYESISCHER_FILTER( ver(x_{t-1}), m_t )
2:     for each x_t do
3:         ver-quer(x_t) = ∫ P(x_t|x_{t-1}) ver(x_{t-1}) dx_{t-1}
4:         ver(x_t) = η^{-1} P(m_t|x_t) ver-quer(x_{t-1})
5:     end for
6:     return ver(x_t)
7: end function
```

$\mathrm{P}(x_t|m_0, \ldots, m_t)$ zuzuordnen, die unter Betrachtung der bisherigen Messungen $m_0, \ldots, m_t$ und der Annahme über den Ausgangsort des Nutzers am plausibelsten scheint.

Ausgehend von einem Zustand x_{t-1} (z.B. der wahren Position des Nutzers zum Zeitpunkt $t-1$) beschreibt das Bewegungsmodell für jede andere mögliche wahre Position x_t die Wahrscheinlichkeit, mit der sich der Nutzer in der Zeitspanne zu x_t bewegt hat. Ein solches Modell wird im Folgenden als $\mathrm{P}(x_t|x_{t-1})$ notiert.

Das Messmodell beschreibt für einen wahren Ort x_t, wie die durchgeführten Positionsschätzungen um x_t herum verteilt sind. Es wird im Folgenden als $\mathrm{P}(m_t|x_t)$ notiert [136].

Ein Bayesischer Filter ist ein rekursiver Algorithmus, der für einen Zeitpunkt t die Berechnung einer Vermutung $ver(x_t) = \mathrm{P}(x_t|m_0, \ldots, m_t)$ bzgl. der Position x_t des Nutzers erlaubt. Als Eingabe wird die Vermutung $ver(x_{t-1})$ zum Zeitpunkt $t-1$ und die Messung m_t zum Zeitpunkt t benötigt. Intern wird zusätzlich eine Vermutung $\overline{ver}(x_t) = \mathrm{P}(x_t|m_0, \ldots, m_{t-1})$ ohne Einbezug der letzten Messung berechnet. Das Konzept ist vereinfachend in Algorithmus 1 dargestellt [119].

Der Algorithmus arbeitet in einer Schleife jede mögliche wahre Position x_t ab, an der sich ein Nutzer zum Zeitpunkt t befinden kann. Für jeden möglichen Wert x_t wird $ver(x_t)$ bestimmt. Das Ergebnis ist ein Modell für den Zeitpunkt t, das die Vermutung über die wahre Position des Nutzers beschreibt [136].

Zeile 3 wird als Vorhersageschritt bezeichnet. Hier wird eine Summierung bzw. Integration durchgeführt. Für jede mögliche Position x_{t-1} wird mittels $ver(x_{t-1})$ die Wahrscheinlichkeit verwendet, mit der sich der Nutzer zum Zeitpunkt $t-1$ dort befunden hat. Diese wird mit der bedingten Wahrscheinlichkeit aus dem Bewegungsmodell multipliziert, dass sich der Nutzer in der Zeitspanne von x_{t-1} zu einer fixen neuen Position x_t bewegt hat. Addiert (bzw. integriert) man diese Wahrscheinlichkeiten, so ergibt sich die gesamte Wahrscheinlichkeit $\overline{ver}(x_t)$, dass sich der Nutzer an der Position x_t befindet [119,136].

In Zeile 4, dem Korrekturschritt, wird die Vermutung $ver(x_t)$ bestimmt, indem die Wahrscheinlichkeit $\overline{ver}(x_t)$, dass sich der Nutzer zum Ort x_t bewegt hat, mit der Wahrscheinlichkeit multipliziert wird, dort die aktuelle Messung m_t zu tätigen. Damit $ver(x_t)$ in der Summe über alle möglichen x_t eins ergibt, wird das Ergebnis mit einem Normierungsfaktor $\eta = \mathrm{P}(m_t|m_1, \ldots, m_{t-1})$ multipliziert.

Bei der praktischen Implementierung dieses Konzepts müssen einige Entscheidungen

getroffen werden, wodurch sich die einzelnen Ausprägungen ergeben [136]:

- Eine Darstellungsform für $ver(x_t)$. Hier kann auf die parametrische oder parameterfreie Statistik zurückgegriffen werden.
- Eine initiale Vermutung $ver(x_0)$.
- Ein Messmodell, das für das jeweilige Positionierungssystem beschreibt, wie die Positionsschätzungen um die wahre Position verteilt sind.
- Ein Bewegungsmodell, das für die Umgebung des Nutzers eine gute Approximation seiner echten Fortbewegung darstellt.

Eine Variante der Implementierung dieses Filters basierend auf der parameterfreien Statistik ist der Partikelfilter.

Grundlagen zu Partikelfiltern

Im Partikelfilter ist die Darstellungsform von $ver(x_t)$ parameterfrei, d.h. im Gegensatz zur Verwendung von Wahrscheinlichkeitsverteilungen ist hier die Struktur des Modells nicht a-priori festgelegt. Partikelfilter stellen die Verteilung $ver(x_t)$ durch n Stichproben, sogenannten Partikeln $\mathcal{X}_t = \left\langle x_t^{[1]}, x_t^{[2]}, \ldots, x_t^{[n]} \right\rangle$ dar. Jedes Partikel $x_t^{[i]}$ stellt dabei eine konkrete Instanziierung einer möglichen wahren Position des Nutzers dar und beinhaltet zusätzlich zur Position die Informationen über Geschwindigkeit und Orientierung.

Der Schritt der *Vorhersage* wird implementiert, indem ein Bewegungsmodell auf jedes Partikel angewandt wird. Dieses sagt seine neue Position, Orientierung und Geschwindigkeit voraus, stellt also eine Möglichkeit für die Bewegung des Nutzers dar. Daraus ergibt sich die Partikelmenge $\overline{\mathcal{X}}_t$, welche die A–Priori–Verteilung $\overline{ver}$ modelliert.

Für den Schritt der *Korrektur* sind Sequential Importance Resampling und Sequential Importance Sampling zwei gängige Methoden [119]. Im Sequential Importance Resampling wird jedem Partikel $x_t^{[i]}$ eine Gewichtung $w_t^{[i]} = p(m_t|x_t^{[i]})$ entsprechend der Positionsschätzung m_t und des Messmodells $p(m_t|x_t)$ zugewiesen. Die aktualisierte Menge $\mathcal{X}_t$ wird aus der Menge $\overline{\mathcal{X}}_t$ generiert und soll entsprechend $ver(x_t)$ verteilt sein. Dazu werden n Partikel mit Zurücklegen und unter Beachtung der Gewichtungen aus der Menge $\overline{\mathcal{X}}_t$ gezogen. Dieser Schritt wird auch Wiederholungsprobennahme (engl. Resampling) genannt. Aufgrund ihrer Gewichtung und des zufälligen Ziehens kann es vorkommen, dass einige Partikel der Menge $\overline{\mathcal{X}}_t$ nicht in $\mathcal{X}_t$ enthalten sind, andere können dafür mehrfach kopiert worden sein. Dieser Schritt entspricht der Darwinistischen Idee des „Survival of the Fittest“. Wird ein Partikel nicht in die Menge $\mathcal{X}_t$ inkludiert, so *stirbt* es.

Betrachtet man die Partikel der Menge $\mathcal{X}_t$, so lässt sich für jeden Zeitpunkt bestimmen, wo sich dieses Partikel befunden hat. Die Trajektorie eines jeden Partikels stellt daher auch eine Hypothese über die Trajektorie des Nutzers dar. Stirbt ein Partikel, so stirbt damit auch die Hypothese über die Trajektorie des Nutzers. Andere Hypothesen verstärken sich hingegen, wenn Partikel kopiert werden. Das heißt, dass der Partikelfilter im Laufe der Zeit ein genaueres Bild über die Vergangenheit bekommt.

Im Sequential Importance Sampling findet kein Resampling statt. Stattdessen werden die Gewichte iterativ über die Zeit hinweg aktualisiert. Dies kann dazu führen, dass sich nur wenige Partikel in dem Bereich befinden, wo sich der Nutzer mit einer hohen Wahrscheinlichkeit aufhält. Im Allgemeinen werden deshalb mehr Partikel benötigt, was den Rechenaufwand erhöht.

2.2 Zugriffskontrollstrategien und standortbasierte Autorisierung

Nach Eckert [49] gibt es zwei Klassen von Sicherheitsstrategien, die Zugriffskontrollstrategie und die Informationsflussstrategie. Eine Zugriffskontrollstrategie hat das Ziel, die Datensicherheit in einem System zu gewährleisten. Dabei wird festgelegt, welche Zugriffsrechte an agierenden Einheiten erteilt werden, um Daten zu lesen oder zu schreiben. Eine agierende Einheit, z.B. ein Nutzer, kann durch ein Zugriffsrecht an Informationen gelangen, die z.B. in einer Datei gespeichert sind. Eine Informationsflussstrategie ist in einem System für die Informationssicherheit zuständig und hat das Ziel zu gewährleisten, dass diese Informationen nur auf zulässigen Informationskanälen zwischen agierenden Einheiten ausgetauscht werden. In der Praxis werden meist Zugriffskontrollstrategien angewandt [49], weshalb diese im Folgenden detailliert beschrieben werden. Die standortbasierte Autorisierung befasst sich mit der Problemstellung, den Standort von mit dem System agierenden Einheiten dynamisch in Zugriffskontrollstrategien zu berücksichtigen.

Es existieren drei wichtige konkrete Ausprägungen von Zugriffskontrollstrategien, die benutzerbestimmte, die systembestimmte und die rollenbasierte Zugriffskontrollstrategie. Um diese zu beschreiben, müssen zunächst einige Begrifflichkeiten definiert werden.

Die oben erwähnten agierenden Einheiten werden konkret als Subjekte und Objekte bezeichnet. Objekte sind die Einheiten eines Systems, die durch eine Zugriffskontrollstrategie geschützt werden sollen [49]. Typischerweise sind solche Einheiten oftmals ineinander verschachtelt. Eine solche Einheit ist z.B. eine Datei, die Zeilen enthält, die ebenfalls als Einheit betrachtet werden können. Ebenso ist eine mobile Applikation, bestehend aus einzelnen Masken, eine solche Einheit. Die Masken enthalten wiederum einzelne Eingabefelder. Je grobkörniger also die zu schützende Einheit gewählt wird, umso weniger Spielraum besteht, um für deren Bestandteile individuelle Datensicherheit zu gewährleisten. Ein Subjekt ist eine abstrakte Darstellung für die agierende Einheit im System, die Operationen bzw. Aktionen auf Objekte anwendet. Das Subjekt kann einen echten Nutzer des Systems repräsentieren, kann aber auch ein Objekt darstellen, auf das nicht nur Operationen angewandt werden, sondern welches auch selbst Operationen anwendet. Ein solches Subjekt wäre ein Prozess, auf den der Benutzer Operationen anwendet, der aber auch selbst in der Lage ist andere Prozesse zu kontrollieren. Je kleiner die Menge der echten Nutzer ist, die durch ein bestimmtes Subjekt abstrahiert werden, umso feinkörniger ist das Subjekt.

Wendet ein Subjekt eine Operation bzw. Aktion auf ein Objekt an, so wird von einem Zugriff auf das Objekt gesprochen. Diese Zugriffe sind durch die Zugriffskontrollstrategie

zu kontrollieren [49]. Wird einem Nutzer dabei ein Zugriff gewährt, so besitzt er das Zugriffsrecht und gilt für den Zugriff als autorisiert.

Die Datensicherheit wird von der Zugriffskontrollstrategie gewährleistet, indem sie Zugriffsrechte beschränkt. Ein Zugriffsrecht ist eine Operation bzw. Aktion im System, die ein Subjekt auf ein Objekt anwenden darf. Besitzt ein Subjekt ein Zugriffsrecht, so darf es die zugrundeliegende Operation bzw. Aktion anwenden. Es wird dabei zwischen universellen und objektspezifischen Zugriffsrechten unterschieden. Ein universelles Zugriffsrecht erlaubt einem Subjekt die Anwendung der Operation bzw. Aktion im System auf alle Objekte, gilt also universell. Ein objektspezifisches Zugriffsrecht ist eine Operation bzw. Aktion, die ein Subjekt nur auf eine bestimmte Teilmenge der Objekte anwenden darf. Auch hier gilt das Prinzip der minimalen Rechte, das objektspezifische Zugriffsrechte erlaubt, die Operationen bzw. Aktionen für ein Subjekt stärker einzuschränken und genau seinem Aufgabengebiet anzupassen.

Unabhängig davon gilt ein Zugriffsrecht als komplex, wenn das Subjekt eine Operation bzw. Aktion nur anwenden darf, wenn zusätzlich eine Bedingung erfüllt ist. Die standortbasierte Autorisierung ist ein Mittel zur Realisierung komplexer Zugriffsrechte. Dabei können universelle oder objektspezifische Zugriffsrechte in Abhängigkeit von der geographischen Position des Subjekts, des Objekts oder beliebiger weiterer Entitäten, beschränkt werden. Dazu werden Ortsbeschränkungen verwendet, die z.B. eine feste Zone vorschreiben, in der sich ein Subjekt oder Objekt befinden muss, um das Zugriffsrecht zu erlangen. Wird einem einfachen Zugriffsrecht eine Ortsbeschränkung zugeordnet, so wird hieraus ein komplexes Zugriffsrecht. Ein Subjekt darf ein Zugriffsrecht nur anwenden, wenn die Bedingung der zugeordneten Ortsbeschränkung erfüllt ist.

2.2.1 Klassische Zugriffskontrollmodelle

Jede Zugriffskontrollstrategie ist eine Funktion f, innerhalb der, ähnlich einer Blackbox, entschieden wird, ob ein gegebenes Subjekt eine bestimmte Operation bzw. Aktion auf ein konkretes Objekt anwenden darf, indem auf einen Wahrheitswert abgebildet wird [28]:

$$f : \mathit{Subjekt} \times \mathit{Objekt} \times \mathit{Operation} \rightarrow \{\texttt{wahr}; \texttt{falsch}\} \tag{2.8}$$

Die benutzerbestimmte, systembestimmte und die rollenbasierte Zugriffskontrollstrategie beschreiben prinzipielle Möglichkeiten zur Definition dieser Funktion. Konkrete Realisierungen dieser Strategien werden Zugriffskontrollmodelle genannt. Im Folgenden werden die Realisierungen anhand zugehöriger Zugriffskontrollmodelle vorgestellt.

Benutzerbestimmte Zugriffskontrollstrategie

Die benutzerbestimmte Zugriffskontrollstrategie, in der englischen Fachliteratur als Discretionary Access Control (DAC) bezeichnet, geht davon aus, dass jedes Objekt einen Eigentümer hat. Der Eigentümer ist dafür verantwortlich für jedes seiner Objekte solche Zugriffsrechte zu spezifizieren, so dass die Datensicherheit der Objekte gewährleistet ist.

Zugriffsrechte sind somit objektspezifisch. Problematisch sind in der DAC-Strategie Zugriffsrechte auf Objekte, die selbst wieder als Subjekt agieren können. Wird einem Subjekt ein Zugriffsrecht auf ein solches Objekt gewährt, kann es indirekt in Besitz der Zugriffsrechte des Objekts gelangen, wenn dieses selbst als Subjekt agiert [49].

Die wichtigste DAC-Strategie ist die Zugriffskontrollmatrix. Hier wird eine Matrix $M : S \times O \rightarrow 2^{Op}$ definiert, die einem Tupel aus Subjekt und Objekt eine Menge von Operationen zuweist. Die Semantik ist, dass ein Subjekt $s \in S$ eine Operation $op \in Op$ auf ein Objekt $o \in O$ anwenden darf, falls $op \in M(s, o)$. Jeder Eintrag der Matrix beschreibt folglich die Zugriffsrechte von s auf o. In der konkreten Umsetzung sind M, S und O zeitabhängig, da die Matrix durch Operationen zum Hinzufügen bzw. Löschen von Subjekten und Objekten oder durch die Zuweisung bzw. Rücknahme von Zugriffsrechten veränderlich ist. Dieses Modell wird auch als Referenzmonitor bezeichnet.

Ein Beispiel ist in Tab. 2.1 gegeben. Ein Arzt „Dr. Bob“ und eine Krankenschwester „Alice“ dürfen ein Programm `Patientenverwaltung` ausführen (Operation `x`), um eine Krankenakte anzuzeigen. Die Krankenakte liegt in der Datei `krankenakte.txt`, die der Arzt lesen und schreiben (`r` und `w`) darf, Alice darf nur lesen. Hier entsteht eine Inkonsistenz, da Alice mittels des Programms indirekt Schreibzugriff auf die Datei erhält.

Systembestimmte Zugriffskontrollstrategien

In der systembestimmten Zugriffskontrollstrategie, in der englischen Fachliteratur als Mandatory Access Control (MAC) bezeichnet, werden Zugriffsrechte über systemweite Regeln definiert. Dabei werden keine konkreten Subjekte oder Objekte referenziert, sondern Zugriffsrechte für Klassen von Subjekten bzw. Objekten festgelegt. Hier wird von universellen Zugriffsrechten gesprochen. Die MAC-Strategie ist daher ein grundlegend anderer Ansatz als die DAC-Strategie. Beide können können aber kombiniert eingesetzt werden. Dabei dominiert für jede anzuwendende Operation bzw. Aktion immer die restriktivere Strategie. Im Folgenden wird das Bell-LaPadula Modell vorgestellt, eines der bedeutendsten Modelle der MAC-Strategie. Eine gute Übersicht über weitere Strategien findet sich z.B. in Eckert et al. [49].

Im Bell-LaPadula-Modell existiert zunächst eine Zugriffsmatrix M. Zusätzlich wird eine Menge von Sicherheitsmarken und eine Menge von Sicherheitskategorien eingeführt. Für die Sicherheitsmarken existiert eine totale Ordnung $\leq$.

Ein Beispiel aus [49] für typische Sicherheitsmarken sind:

$$unklassifiziert \leq vertraulich \leq geheim \leq strenggeheim \tag{2.9}$$

Außerdem wird eine Menge von Sicherheitskategorien definiert. Ein Beispiel aus [49] ist:

$$\{Arzt, Schwester, Patient, Verwaltung\} \tag{2.10}$$

Basierend auf diesen beiden Mengen wird jedem Subjekt und Objekt eine Sicherheitsmarke und eine Teilmenge aus den Sicherheitskategorien zugeordnet. Ein Beispiel aus [49] für ein solches Tupel ist $(vertraulich, \{Arzt, Schwester\})$ oder auch $(vertraulich, \emptyset)$. Jedes

Objekt / Subjekt	kranken-akte.txt	Patienten-verwaltung
Schwester Alice	r	x
Dr. Bob	r, w	x
Patienten-verwaltung	r, w	

Tabelle 2.1: Zugriffskontrollmatrix am Beispiel der Patientenverwaltung.

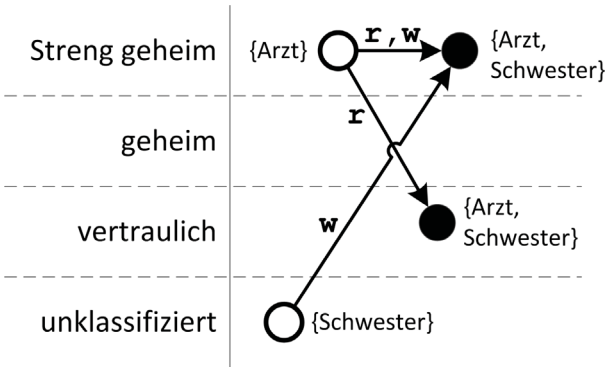


Abbildung 2.5: Bsp. zum Bell-LaPadula Modell, adaptiert aus [49]. Pfeile markieren Zugriffsrechte von Subjekten ∘ auf Objekte •.

Tupel bildet eine eigene Sicherheitsklasse. Die Menge aller möglichen Sicherheitsklassen wird als SC notiert. Auf SC ist eine partielle Ordnung $(SC, \leq)$ definiert. Sind zwei Tupel $X = (A, B)$ und $Y = (A', B')$ aus SC gegeben, so gilt:

$$X \leq Y \;\Leftrightarrow\; A \leq A' \;\wedge\; B \subseteq B' \tag{2.11}$$

Ist ein solches Tupel $X \in SC$ einem Subjekt s zugewiesen, so wird es als die Clearance $\mathrm{sc}(s)$ des Subjekts bezeichnet. Das Tupel, das einem Objekt o zugewiesen ist, wird als die Classification $\mathrm{sc}(o)$ des Objekts bezeichnet.

Um zu entscheiden, ob ein Subjekt s eine Operation op auf ein Objekt o anwenden darf, ob es also das Zugriffsrecht besitzt, prüft das Bell-LaPadula Modell drei Bedingungen [49]:

1. Autorisierung gemäß der Zugriffsmatrix: $op \in M(s, o)$.
2. Die Simple-Security-Eigenschaft: $op = \texttt{lesen} \;\wedge\; \mathrm{sc}(s) \geq \mathrm{sc}(o)$. Ein Subjekt darf die Operation `lesen` auf keine Objekte in einer darüber liegenden Sicherheitsklasse anwenden, auch als „no-read-up“ bezeichnet.
3. Die $\star-$Eigenschaft: $op = \texttt{schreiben} \wedge \mathrm{sc}(s) \leq \mathrm{sc}(o)$. Ein Subjekt darf die Operation `schreiben` auf keine Objekte in einer darunter liegenden Sicherheitsklasse anwenden, auch als „no-write-down“ bezeichnet.

Ein Beispiel zum Bell-LaPadula Modell ist in Abb. 2.5 gegeben. Die Operationen `lesen` und `schreiben` sind mit `r` bzw. `w` abgekürzt. Objekte sind durch gefüllte Kreise und Subjekte durch Kreisränder dargestellt. Eingezeichnet sind alle Zugriffsrechte entsprechend der Clearance und Classification der Objekte und Subjekte.

Es ist von Vorteil, dass die Regeln im Bell-LaPadula Modell effizient überprüft und implementiert werden können. Probleme ergeben sich bei der Integritätsprüfung, wenn z.B.

geschriebene Daten nicht mehr gelesen werden dürfen. Ebenso können nicht alle Szenarien durch das MAC-Modell ausgedrückt werden.

Eine Umkehrung des Bell-LaPadula Modells ist das BiBa-Modell. Dort gilt eine Umkehrung der Simple-Security- und der $\star-$Eigenschaft, indem „no-read-down“ und „no-write-up“ gefordert wird. Bei der Entscheidung zwischen Bell-LaPadula- oder BiBa-Modell ist zu beachten, ob höhere Schichten keine Informationen von tieferen Schichten erhalten dürfen (BiBa), weil diese z.B. unzuverlässig oder fehlerhaft sein können, oder ob tiefere Schichten keine Informationen von höheren Schichten erhalten dürfen (Bell-LaPadula), weil diese z.B. geheime oder vertrauliche Informationen enthalten.

Das Modell zielt darauf ab, die Integrität der Daten zu schützen, indem ein Subjekt aus einer höheren Schicht keine Informationen von kleineren Schutzklassen lesen darf. Ebenso darf ein Subjekt keine Daten in ein Objekt einer größeren Schutzklasse schreiben.

Rollenbasierte Zugriffskontrollstrategien

Die Ausprägung der rollenbasierten Zugriffskontrolle umfasst vier Modelle mit zunehmender Ausdrucksstärke, die erstmals von Sandhu et al. vorgestellt wurden [121,122]. In der englischen Fachliteratur wird diese Ausprägung als Role–based Access Control (RBAC) bezeichnet. Das RBAC_0-Modell ist das elementarste. Es erlaubt die Zuordnung von Zugriffsrechten auf Basis von drei Mengen und zwei Relationen:

- U ist eine Menge zur Repräsentation der angelegten Nutzer (Subjekten) im System.
- R bezeichnet eine Menge von Rollen, die Nutzer einnehmen können.
- P ist eine Menge von Zugriffsrechten, für die Nutzer autorisiert werden können. Ein Zugriffsrecht beschreibt jeweils eine Aktion (dem Prädikat), die auf einem Objekt ausgeführt wird.

Die Relationen zur Formalisierung des Modells:

- $UA \subseteq U \times R$ beschreibt die Rollen, die ein Nutzer einnehmen kann.
- $RP \subseteq R \times P$ beschreibt die Zugriffsrechte, die einer Rolle zugeordnet sind.

Die Relation UA weist Nutzern verfügbare Rollen zu und analog weist RP den Rollen ihre Zugriffsrechte zu. Ein Nutzer u muss zunächst eine RBAC-Sitzung s starten, um Zugriffsrechte zu erlangen und damit seine Aufgaben zu erledigen. Hierbei wählt der Nutzer eine Teilmenge, der ihm gemäß UA verfügbaren Rollen aus und aktiviert diese. Eine Sitzung ist somit formal eine Teilmenge der ihm verfügbaren Rollen. Ist eine ihm verfügbare Rolle r in der Sitzung enthalten, so gilt r als aktiviert. Ohne formale Erweiterungen bleibt im ursprünglichen RBAC-Standard die Menge der verfügbaren Rollen zeitlich konstant, außer der Nutzer stößt manuell die zusätzliche Aktivierung oder die Deaktivierung von Rollen an. Somit bleibt eine Sitzung gültig, bis sie manuell durch den Nutzer beendet wird.

Aktiviert ein Nutzer u eine verfügbare Rolle $r \in R$, so stehen ihm im RBAC_0-Modell alle Zugriffsrechte zur Verfügung, die r zugeordnet sind. Das RBAC_1-Modell ergänzt zusätzlich

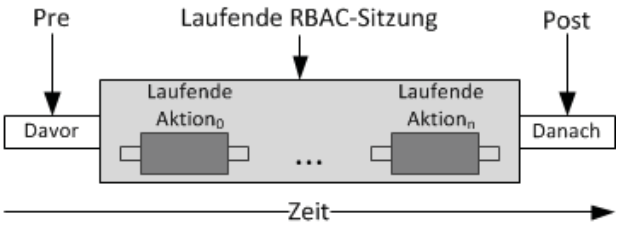


Abbildung 2.6: Darstellung der unterschiedlichen Nutzungsphasen einer Sitzung (adaptiert aus [123]).

die Relation RH, die eine Rollenhierarchie darstellt. Sie besteht aus Tupeln $(r, r') \in R \times R$, die ausdrücken, dass eine Rolle r' einer Rolle r übergeordnet ist. Einem Nutzer mit der Rolle r werden schließlich alle Zugriffsrechte gewährt, die r oder einer übergeordneten Rolle von r zugewiesen sind.

Im RBAC_2-Modell werden ausgehend vom RBAC_0-Modell zusätzlich Beschränkungen zur Funktionstrennung eingeführt (engl. Separation of Duty) [122]. Diese erlauben den wechselseitigen Ausschluss von Rollen. Ziel ist z.B., dass nicht ein und dieselbe Person einen Reiseantrag stellen und genehmigen darf, oder selbst eine Zahlung initiieren und anschließend autorisieren kann [2]. Hierbei wird zwischen dynamischen und statischen Beschränkungen unterschieden. Die statische Funktionstrennung legt Bedingungen für die Definition von UA fest. Sie erlaubt die Modellierung, dass beim Start einer Sitzung für einen Nutzer niemals zwei widersprüchliche Rollen gleichzeitig zur Aktivierung verfügbar sind. Die dynamische Funktionstrennung ist weniger restriktiv und greift erst zur Laufzeit. Zwei widersprüchliche Rollen dürfen hier durchaus zur Auswahl stehen, allerdings dürfen sie innerhalb der gleichen Sitzung nicht beide aktiviert werden. Als Beispiel wird die Rolle Kassierer und Buchhalter genannt, so dass kein Diebstahl aus der Kasse unbemerkt bleibt. In Spezialfällen kann das RBAC_3-Modell gebildet werden, welches das RBAC_1- und RBAC_2-Modell kombiniert. Dieses Modell ist allerdings nicht allgemeingültig, da deren Eigenschaften in gewissen Punkten inkompatibel sind [23].

Chen et al. nutzen in [23] einen sehr intuitiven Ansatz zur Darstellung der Semantik für RBAC_1-Modelle. Eine konkret modellierte Richtlinie wird hierbei als gerichteter, azyklischer Graph $\mathcal{P} = (V, E)$ betrachtet. Für die Menge der Knoten gilt $V = U \cup R \cup P$. Die Kanten ergeben sich als $E = UA \cup RP \cup RH$, also aus der Vereinigung der definierten Relationen. Gemäß der graphbasierten Semantik ist eine Rolle r für einen Nutzer u beim Start einer Sitzung verfügbar, sofern ein Autorisierungspfad $\langle u, \ldots, r \rangle$ in $\mathcal{P}$ existiert.

2.2.2 Das Konzept der Nutzungskontrolle

Die Ausführung von Operationen oder Aktionen, die ein Subjekt durch ein Zugriffsrecht auf ein Objekt anwendet, nimmt, je nach deren Typ, eine längere Zeit in Anspruch. Die alleinige Überprüfung auf ein nötiges Zugriffsrecht beim Start der Operation ist dann nicht mehr ausreichend.

Zur Lösung dieses Problems sind Strategien zur Nutzungskontrolle geeignet, wie z.B.

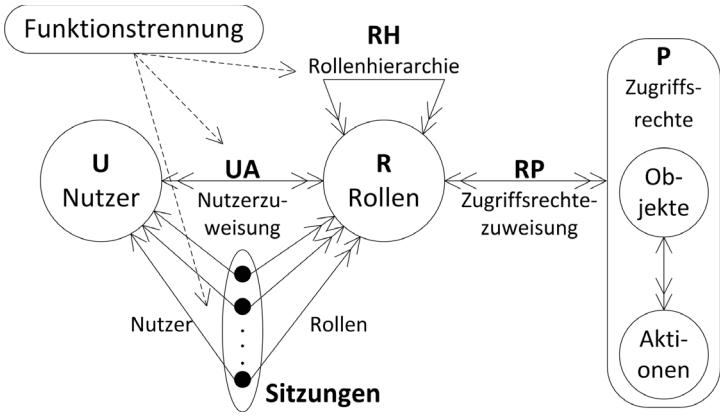


Abbildung 2.7: Das $RBAC_3$-Modell (adaptiert aus [122]).

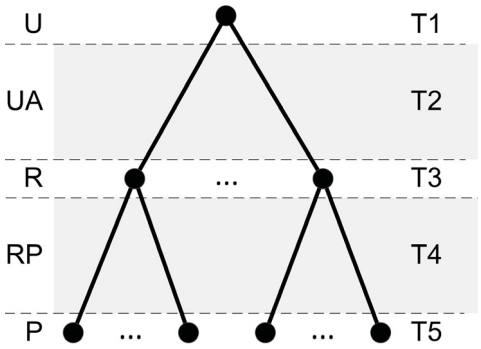


Abbildung 2.8: Ansatzpunkte T1 bis T5 zur standortbasierten Erweiterung von RBAC.

UCON von Sandhu et al. [123]. Grundsätzlich unterteilt UCON die Dauer der Ausführung einer Operation in drei Abschnitte: pre-authorization, ongoing usage und post-authorization. In UCON wird jedem Subjekt und Objekt eine Menge von zeitlich veränderlichen Attributen zugewiesen. Aus deren Belegung leiten sich die Zugriffsrechte ab. Solche Attribute können auch den Standort eines Nutzers modellieren, um kontinuierliche standortbasierte Autorisierung zu implementieren [35,37]. Aktuell existieren jedoch keine Arbeiten, die dabei Positionsfehler berücksichtigen.

Das RBAC-Modell ist mittels UCON abbildbar [109]. Für eine laufende Sitzung s, in der aktuell $Aktion_0, \ldots, Aktion_n$ angewandt werden, ist diese Modellierung schematisch in Abb. 2.6 dargestellt. Bei der Anwendung auf RBAC teilt UCON den Lebenszyklus von Sitzungen oder angewandten Operationen in die drei oben genannten Abschnitte. Im ursprünglichen RBAC werden Operationen in einer solchen Modellierung stets im Kontext einer laufenden Sitzung angewandt.

2.2.3 Standortbasierte Autorisierung

Durch die Zuordnung von Ortsbeschränkungen an Zugriffsrechte entstehen komplexe Zugriffsrechte. Wie oben erwähnt, definieren die Ortsbeschränkungen, in der engl. Fachliteratur als Location Constraints bezeichnet, Voraussetzungen an die Position des Nutzers, des Subjekts oder weiterer Entitäten. Ein Zugriffsrecht wird nur erteilt, sofern die Positionen den Voraussetzungen der Ortsbeschränkung des Zugriffsrechts genügen, wodurch die standortbasierte Autorisierung realisiert wird [93]:

$$f : \mathit{Subjekt} \times \mathit{Objekt} \times \mathit{Operation} \times \mathit{Positionen} \rightarrow \{\texttt{wahr}; \texttt{falsch}\} \tag{2.12}$$

Es entsteht eine Verfeinerung von (2.8), die nur dann `wahr` ergibt, wenn die Positionen bestimmten Voraussetzungen genügen. Je nach Art der geforderten Voraussetzungen werden

Ortsbeschränkungen nach Shin et al. [130] in vier Klassen eingeteilt:

- Statisch-Statisch (SS): Sowohl Subjekt als auch Objekt sind statisch. Ein Beispiel sind Szenarien der Machine-to-Machine-Kommunikation mit unbeweglichen Maschinen.
- Mobil-Statisch (MS): Das Subjekt ist mobil, das Objekt statisch. Ortsbeschränkungen dieser Klasse beschränken Zugriffsrechte abhängig vom aktuellen Standort des Nutzers und der fixen Position des Objekts.
- Statisch-Mobil (SM): Das Subjekt ist statisch, das Objekt ist mobil. Diese Variante ist vor allem bei Maschine-to-X-Ansätzen interessant, wobei X für eine bewegliche Maschine oder einen mobilen Nutzer steht.
- Mobil-Mobil (MM): Das Subjekt und das Objekt sind mobil. Die Ortsbeschränkungen dieser Klasse stellen Voraussetzungen an die Standorte des Subjekts und des Objekts. Werden in der Voraussetzung beide Standorte in Bezug gesetzt, entsteht eine Interaktionsbeschränkung [8].

Fordert die Voraussetzung der Ortsbeschränkung, dass sich die Positionen innerhalb einer autorisierten Zone befinden, erfolgt die Prüfung der Voraussetzung mittels Geo-Fencing. Nach Ravada et al. [112] bezeichnet Geo-Fencing:

> „[...] Geo-fencing [...] identifies the qualified point and area pairs using a virtual perimeter for a real-world geographic area“

Frei übersetzt befasst sich Geo-Fencing also damit, Paare aus Punkten und Zonen zu finden, wobei die Zonen ein reales geographisches Gebiet begrenzen, so dass zwischen beiden Geometrien eine vordefinierte Bedingung erfüllt ist. Beispielsweise kann dies bedeuten, dass der Punkt einen Mindest- oder Maximalabstand entweder über- bzw. unterschreitet oder in der Zone enthalten ist. Der letzte dieser Fälle ist die Grundlage für die meisten existierenden Arbeiten zur standortbasierten Autorisierung in der Literatur. Für Ravada et al. ist Geo-Fencing ein noch offenes Forschungsfeld ohne dominierende Lösungen.

Verallgemeinert man die Betrachtungsweise von standortbasierter Autorisierung und Geo-Fencing, so kann anstatt des geographischen Raums auch ein aufgespannter Merkmalsraum betrachtet werden, in dem autorisierte Bereiche definiert werden. So besteht die Möglichkeit zu fordern, dass die Temperatur des Nutzers in einem bestimmten Intervall liegt, oder dass die Lautstärke einen gewissen Pegel nicht überschreitet. Ebenso ist es denkbar, dass nur autorisiert wird, wenn der Nutzer z.B. gerade stillsteht.

Für diese Arten von Informationen wird von Dey et al. in [47] der Begriff des Kontexts eingeführt. Kontext wird folgendermaßen charakterisiert:

> „Context is any information that can be used to characterize the situation of an entity. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves.“

Die Nutzerposition ist als Kontext einzuordnen und bis auf wenige Ausnahmen der einzig beachtete Kontext bei der Erweiterung von Zugriffskontrollmodellen.

Erweiterung von RBAC Der mit Abstand größte Teil der Arbeiten zur standortbasierten Autorisierung stellt eine Erweiterung von RBAC dar [122]. Selten sind diese Erweiterungen ganz allgemein auf Kontext bezogen und unterstützen z.B. eine Autorisierung in Abhängigkeit der Aktivität des Nutzers oder der Prozessorauslastung seines Rechners. Im Folgenden sollen diese RBAC-Erweiterungen im Hinblick auf die Möglichkeit zur standortbasierten Autorisierung untersucht werden.

Überträgt man die Semantik von Ortsbeschränkungen in RBAC auf den graphbasierten Ansatz von Chen et al. [23], so wird klar, dass die Ortsbeschränkungen dazu eingesetzt werden, die möglichen Autorisierungspfade einzuschränken. Dazu muss mindestens eine der sechs Mengen U, R, P, UA, RP, RH von der gelieferten Positionsschätzung abhängig gemacht werden, da somit auch die Kanten und Knoten im Graphen eingeschränkt werden. Wird z.B. die Zuordnung einer Rolle an einen Nutzer aus der Menge UA entfernt, so verschwinden automatisch alle Autorisierungspfade, die diese Rolle passieren. Eine Übersicht zu diesen fünf Ansatzpunkten zur standortbezogenen Erweiterung von RBAC ist in Abb. 2.8 dargestellt.

Viele Ansätze beziehen sich lediglich auf die Einschränkung der Menge R und sind gemäß obiger Klassifikation T3-Ansätze. Kumar et al. definieren in [84] CS-RBAC (Context-Sensitive RBAC) und ordnen Nutzern und Objekten Eigenschaften zu, die z.B. den jeweiligen Standort beschreiben. Die Einschränkung der Verfügbarkeit einer Rolle aus R erfolgt mit booleschen Ausdrücken, die auf Basis der Eigenschaften des aktuellen Nutzers und des angefragten Objekts ausgewertet werden. Bertino et al. entwickeln in [15] mit GEO-RBAC einen der wichtigsten Ansätze, der als MS-Ansatz einzustufen ist. Rollen können hier so begrenzt werden, dass sie nur zur Verfügung stehen, wenn der Standort des Nutzers in ihrer zugewiesenen autorisierten Zone – einem Polygon – liegt. Diese Rollen sind hier konkrete Instanzen von abstrakten Rollen. Ähnlich einer Schnittstellenbeschreibung geben abstrakte Rollen vor, welchen Typ die autorisierten Zonen ihrer Instanzen haben dürfen. Als solche Typen sind z.B. Stadt, Straßennetz oder Stadtteil genannt. Auch abstrakten Rollen können Zugriffsrechte zugewiesen werden. Liegt der Nutzerstandort in der autorisierten Zone einer solchen instanziierten Rolle, werden alle Zugriffsrechte der übergeordneten abstrakten Rolle vererbt. Dies vereinfacht die Spezifikation, wenn ein Zugriffsrecht z.B. in allen autorisierten Zonen vom Typ „Stadt“ verfügbar sein soll. Damiani et al. schlagen in [37] ferner vor, GEO-RBAC zu einem MM-Ansatz zu erweitern, da oftmals auch der Ort des Objekts von Bedeutung ist. Dies soll realisiert werden, indem die Zugriffsrechte der Menge P anstelle der Rollen R zonenbasiert bereitgestellt werden. GEO-RBAC wird somit zu einem T5-Ansatz transformiert. Aich et al. präsentieren in [3] ebenfalls einen T3-Ansatz, der die Spezifikation von zeit- und zonenbasierten Bedingungen zur Beschränkung von Rollen erlaubt. Einer Rolle werden Bedingungen zugewiesen, die mit dem logischen UND- bzw. ODER-Operator verknüpft werden können.

In der Literatur werden auch reine T4-Erweiterungen vorgestellt, welche die Relation RP ortsabhängig gestalten. GRBAC, einer der ersten Ansätze überhaupt, stammt von Covington et al. [30] und schränkt die Relation RP mithilfe von Umgebungsrollen (engl. Environmental Roles) ein. Umgebungsrollen bilden eine separate Hierarchie und werden automatisch aktiviert, wenn Kontextgrößen eine Anforderung erfüllen. Ein Beispiel ist eine

Umgebungsrolle „*obergeschoss*“, die aktiviert wird, wenn sich die Kinder im Obergeschoss befinden [31]. Für jedes Element e aus RP wird nun festgelegt, welche Umgebungsrollen aktiviert sein müssen, damit e in RP enthalten ist. Hansen et al. stellen mit SRBAC (Spatial RBAC) in [63] ebenso einen T4-Ansatz vor, der abhängig vom Ort des Nutzers die Elemente in RP beschränkt.

Auch reine T5-Erweiterungen sind in der Literatur vorhanden, welche die Elemente der Menge P ortsabhängig beschränken. Strembeck et al. erweitern RBAC in [135] so, dass Bedingungen an dynamischen Kontext der Umgebung, z.B. die Temperatur, oder Bedingungen an den Kontext des zugreifenden Subjekts, z.B. das Alter oder eben dessen Standort formuliert werden können. Diesen Bedingungen werden Zugriffsrechte der Menge P zugewiesen, so dass Elemente darin nur enthalten sind, wenn deren zugeordnete Kontextbedingung erfüllt ist.

Viele Arbeiten verfolgen einen hybriden Ansatz und sind nicht eindeutig einer der fünf Kategorien zuzuordnen. Chandran et al. definieren mit LoT-RBAC (Location- and Time-RBAC) in [21] einen Ansatz, der eine T2-, T3- und T4-Erweiterung darstellt. Der Ansatz erlaubt es, die Mengen R und UA in Abhängigkeit vom Standort des Nutzers zu verkleinern. Ferner wird es unterstützt, zur Umsetzung von MM-Szenarien die Relation RP in Abhängigkeit vom Standort des angefragten Objekts zu definieren. Ray et al. stellen mit LRBAC (Location-aware RBAC) in [114] eine Arbeit vor, die als T3- und T5-Ansatz einzustufen ist und die Abbildung von SM-, MS- und MM-Szenarien erlaubt. Dabei wird einer Rolle aus R eine Zone als Ortsbeschränkung zugewiesen, wenn es gefordert ist, dass sich der Nutzer in der Zone befindet damit die Rolle verfügbar und in R enthalten ist. Eine entsprechende Einschränkung auf der Menge P ist ebenfalls möglich, wobei der Standort des angefragten Objekts innerhalb einer definierten Zone liegen muss. Toahchoodee et al. stellen in [137] eine Arbeit vor, die ebenfalls SM-, MS- und MM-Szenarien unterstützt und als T2-, T4- und T5-Ansatz einzuordnen ist. Die Elemente der Relationen UA und RP sind dabei Abhängigkeit vom Nutzerstandort. Die Menge P wird auf Basis des Standorts des Objekts begrenzt. Ulltveit-Moe et al. beschreiben in [144] einen T3- und T5-Ansatz, der aus einer Erweiterung von SRBAC entsteht, um zusätzlich den Ort des Objekts zu berücksichtigen. Chen et al. stellen in [23] zur Umsetzung von standortbasiertem RBAC ein Standardmodell vor, sowie ein Starkes, ein Schwaches und ein Modell, basierend auf vertrauenswürdigen RBAC-Elementen. Das Standardmodell ist ein T1-, T3- und T5-Ansatz, wobei für U, R und P ein Zeitraum und eine Zone angegeben werden können. Der Ort des Nutzers muss im Schnittbereich der Zonen liegen und der Zugriffszeitpunkt in der Schnittmenge der definierten Zeitintervalle. Das starke Modell erweitert den Ansatz um Beschränkungen auf UA und RP. Im schwachen Modell sind jedoch nur U und P ortsabhängig definiert. Das Modell der vertrauenswürdigen RBAC-Entitäten fordert, dass auf einem Autorisierungspfad ab Erreichen eines solchen Elements alle Beschränkungen ignoriert werden. Zur Präzision der Semantik beim Einsatz von Rollenhierachien aus RBAC_1 wird eine semantikerhaltende Transformation von Beschränkungen der Menge R zu Beschränkungen auf UA vorgeschlagen.

Die meisten Modelle ignorieren, dass die Anwendung einiger Operationen eine längere Zeitdauer beansprucht und zwischenzeitlich die Ortsbeschränkung nicht mehr erfüllt sein

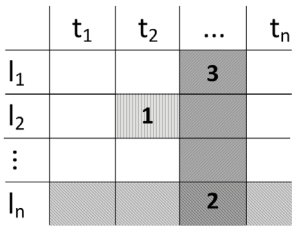


Abbildung 2.9: Schema zur Veranschaulichung der von Ray et al. in [115] vorgestellten ortsbasierten Funktionstrennung.

könnte. Daher zielen einige Arbeiten darauf ab, das oben beschriebene Konzept der Nutzungskontrolle auf RBAC-Modelle zu übertragen. Abdunabi et al. schlagen in [1] einen T2-, T4-, T5-Ansatz vor. Dies ist einer von zwei Ansätzen, die Möglichkeiten zeigen, während einer laufenden RBAC-Sitzungen eine Änderung des Nutzerstandorts zu berücksichtigen. Hier wird nicht beschrieben, welche Folgen daraus für die Semantik der RBAC-Sitzung entstehen. Kirkpatrick et al. erweitern in [77] GEO-RBAC zu einem T3-Ansatz namens Prox-RBAC, womit Ortsbeschränkungen für Rollen über eine zeitliche Dauer hinweg gefordert werden können. Rollen werden während einer Sitzung automatisch aktiviert und deaktiviert, wenn ihre Ortsbeschränkung verletzt ist. Wird ein Zugriffsrecht auf einer Rolle genutzt und kommt es zu einer Verletzung von deren Ortsbeschränkung bis zu einem gesetzten Timeout, so wird die Nutzung beendet.

SRBAC von Hansen et al. [63] ist die erste ortsbezogene RBAC-Erweiterung, die eine ortsbezogene Funktionstrennung realisiert, um die Zuweisung und Aktivierung sich widersprechender Rollen zu verhindern (wechselseitiger Ausschluss). Die Funktionstrennung wird als Beschränkung (x, y) auf jeweils zwei Rollen x und y definiert. Die statische ortsbezogene Funktionstrennung beschränkt den Entwurf der Richtlinie, so dass kein Nutzer an einem Ort l beide Rollen x und y besitzen darf. Das schließt auch das Aktivieren der beiden Rollen in aufeinanderfolgenden Sitzungen aus. Die dynamische ortsbezogene Funktionstrennung ist schwächer und schließt das gleichzeitige Aktivieren von x und y nur innerhalb einer laufenden Sitzung aus. Die ortsbezogene Funktionstrennung wird durch Ortsbeschränkungen auf UA realisiert, indem die gleichzeitige Zuweisung bzw. Aktivierung sich widersprechender Rollen verhindert wird.

STRBAC von Ray et al. [115] ist der umfangreichste Ansatz zur standortbasierten Funktionstrennung und berücksichtigt zusätzlich das aktuelle Zeitfenster. Dazu wird zwischen zwei Rollen oder zwei Zugriffsrechten x und y eine Beschränkung (x, y) zur statischen Funktionstrennung definiert. Insgesamt gibt es vier Varianten, deren Auswirkungen im Folgenden mithilfe von Abb. 2.9 veranschaulicht werden. Die Spalten umfassen Zeitfenster und die Zeilen umfassen verschiedene geographische Zonen. Die gefärbten Bereiche beschreiben Orts- und Zeitbereiche, für die sich zwei Rollen oder Zugriffsrechte x und y gegenseitig ausschließen.

Fall 1 in Abb. 2.9 stellt dar, dass sich x und y nur in einem Zeitfenster t_2 am Ort l_2 widersprechen. Es muss sichergestellt werden, dass kein Nutzer zu dieser Zeit an diesem Ort beide Rollen oder beide Zugriffsrechte annehmen darf. Fall 2 verwirft den konkreten

Zeitpunkt t_2 und fordert pauschal, dass x und y am Ort l_n zu jeder Zeit widersprüchlich sind. Fall 3 verwirft hingegen die Forderung nach einem konkreten Ort und sagt aus, dass x und y zu einem gegebenen Zeitpunkt an jedem Ort widersprüchlich sind. Fall 4 ist der stärkste Fall und beschreibt, dass x und y zu jeder Zeit und jedem Ort widersprüchlich sind. Dies entspricht der klassischen Funktionstrennung, die unabhängig von Ort und Zeit ist. Es werden auch Beschränkungen zur dynamischen Funktionstrennung nach demselben Prinzip eingeführt, welche die Rollenaktivierung in der gerade laufenden Sitzung des Nutzers beschränken.

Aich et al. schlagen in [2] für ESTARBAC ebenso die zeit- und ortsgebundene Funktionstrennung vor und greifen im Wesentlichen die oben genannten Konzepte auf. Die Mengen R und P sind ortsabhängig beschränkt, so dass jeder Rolle und jedem Zugriffsrecht eine Zone zugeordnet ist. Die Beschränkungen zur Funktionstrennung (x, y) werden wie im klassischen RBAC auf Paaren x, y von Rollen oder Zugriffsrechten definiert. Die Schlussfolgerung der Autoren lautet, dass während der Spezifikation der autorisierten Gebiete bereits die Beschränkungen zur Funktionstrennung beachtet werden sollen. Insbesondere dürfen sich die autorisierten Zonen zweier sich ausschließender Rollen bzw. Zugriffsrechte nicht schneiden, damit es nicht zu Konflikten kommt.

Erweiterung von MAC und DAC Verglichen mit RBAC, erweitern nur wenige Arbeiten das DAC- und MAC-Modell um Ortsbeschränkungen. Youssef et al. adaptieren in [148] das DAC-Modell so, dass mobile Nutzer für Händler mit einem Regelkatalog festlegen können, zu welchen Zeiten und in welchen Gebieten sie den Standort des Nutzers z.B. für Werbezwecke auslesen dürfen. Ardagna et al. schlagen in [8] einen allgemeinen Ansatz zur standortbasierten Autorisierung vor, der auf das DAC- oder MAC-Modelle angepasst werden kann.

Dabei werden Zugriffsregeln bestehend aus booleschen Ausdrücken definiert. Nur wenn alle Ausdrücke zu `wahr` auswerten, wird ein Zugriff über die Regel autorisiert. Neben einem zu erfüllenden Ausdruck für den Nutzer (Subjekt), eine Aktion (Prädikat) und die angefragten Daten bzw. Ressourcen (Objekt), wird zusätzlich ein Ausdruck bestehend aus Ortsbeschränkungen definiert. Die beschriebenen Ortsbeschränkungen fordern z.B. den Aufenthalt in einer Zone, einen max. oder min. Abstand dazu, oder beschränken den erlaubten Abstand zu einer anderen beweglichen Entität. Finnis et al. präsentieren in [56] mit LoPSIL einen Ansatz, der am DAC-Modell angelehnt ist. Dabei wird durch eine Richtlinie für Android-Applikationen genau festgelegt, in welchen Zonen einzelne Android-Berechtigungen gewährt werden. Der Zugriff auf das Kamerabild oder den Nutzerstandort steht dann nur berechtigten Anwendungen zur Verfügung. Die Richtlinie wird mit einem eigenen Compiler mit den `.class`-Dateien der Applikation verwoben, wodurch deren Quellcode entsprechend der Vorgaben manipuliert wird.

Ray et al. stellen in [113] eine echte Erweiterung des MAC-Modells um Ortsbeschränkungen vor. Geographischen Zonen werden dabei auch Schutzstufen zugewiesen, die bei deren räumlicher Schachtelung nicht kleiner werden dürfen. Für Nutzer und Objekt kann jeweils für die Operationen `lesen` bzw. `schreiben` eine Zone angegeben werden, in der

sich ein Nutzer bzw. Objekt befinden muss. Zusätzlich wird sichergestellt, dass Nutzer und Objekte keine Zone betreten, die eine restriktivere Schutzstufe als sie selbst besitzt. Decker et al. implementieren in [43] einen Ansatz auf Basis des DAC-Modells, der es erlaubt, die Operationen `lesen` und `schreiben` auf Dokumenten für einzelne Nutzer oder Nutzergruppen in Abhängigkeit vom Erstellungsort des Dokuments zu begrenzen. Da das DAC- und MAC-Modell nach Osborn et al. auch mittels RBAC realisiert werden kann, ist es nachvollziehbar, dass in der Literatur die allgemeineren RBAC-Erweiterungen vorherrschend sind [107].

Arbeitsabläufe mit Ortsbeschränkung Neben der Erweiterung des MAC-, DAC- und RBAC-Modells existieren in der Literatur auch ortsbasierte Erweiterungen für Arbeitsabläufe, engl. als Workflows bezeichnet. Die Grundidee ist hierbei, dass die nächsten erlaubten Zugriffsrechte vom gerade genutzten Zugriffsrecht abhängen, wodurch die zeitliche Abfolge von Aktionen festgelegt wird [10]. Decker et al. haben Workflows für mobile Nutzer in Anlehnung an RBAC angepasst und führen dazu Ortsbeschränkungen ein [41,42,44]. Ihre Ansätze erlauben das Einschränken von Rollenzuweisungen auf bestimmte Zonen. Ferner kann für Aktionen rollenspezifisch festgelegt werden, auf welche Zone ihre Ausführung zu beschränken ist. Ebenso können Aktionen auf Zonen begrenzt werden, in denen zuvor eine andere bestimmte Aktion ausgeführt wurde. So kann modelliert werden, dass ein Fernsehtechniker den Anschluss des TV-Geräts und das Testen des Empfangs am gleichen Ort ausführt, der aber erst zur Ausführung des Arbeitsablaufs bekannt ist. Ein Nachteil der Ansätze von Decker ist, dass das räumliche Bewegungsmuster während der Ausführung einer Aktion des Arbeitsablaufs nicht berücksichtigt wird. Marcus et al. stellen deshalb in [94] einen Ansatz vor, der für das Voranschreiten zu einer Folgeaktion fordert, dass der Nutzer eine zuvor bestimmte Sequenz an Zonen durchlaufen hat. Garzon et al. definieren einen ähnlichen Ansatz in [117]. Auch hier sind jeder Aktion fixe Zonen zugeordnet. Folgen zwei Aktionen im Arbeitsablauf aufeinander, wird eine maximale Zeitspanne gesetzt, innerhalb der ein Nutzer von der Zone der vorherigen Aktion die Zone der nächsten Aktion erreichen muss.

Anforderungen und Implementierungen Nach Bhatti et al. muss ein standortbasiertes Autorisierungsmodell drei Eigenschaften erfüllen [17]: Die benutzerfreundliche Spezifikation von Ortsbeschränkungen (Intuitivität), die problemlose Erweiterbarkeit auf viele Nutzer und Rollen (Skalierbarkeit) und die Möglichkeit zur Implementierung mit existierenden Standards (Reduzierbarkeit). Ein Nachteil der oben genannten theoretischen Modelle ist die fehlende Erprobung in der Praxis. Somit ist aktuell nicht ausreichend genau untersucht, inwiefern diese Eigenschaften durch die einzelnen Modelle zur standortbasierten Autorisierung erfüllt werden [37,115]. Nach Chen et al. liegt dies vor allem daran, dass sich diese Modelle viel zu stark auf die Syntax der Spezifikationen konzentrieren, anstatt ihre Semantik detailliert zu beleuchten [23]. Wichtig ist auch die praktische Erprobung der Richtlinien-Spezifikation, der Implementierung, der Fälschungssicherheit von Positionsschätzungen, Nutzungskontrolle nach dem Zeitpunkt der Autorisierung und der Wartung

bzw. Aktualisierung von standortbasierten Zugriffskontrollmodellen [36]. Ebenso spielt die Energieeffizient eine wichtige Rolle [120].

Einige Arbeiten zeigen auch Erkenntnisse aus der praktischen Umsetzung: Damiani et al. stellen in [37] einen ersten Schritt zur praktischen Realisierung des oben genannten GEO-RBAC vor, wobei einige Schwachstellen bemerkt werden. Eine davon ist, dass Zugriffsrechte oftmals über einen längeren Zeitraum verwendet werden und somit kontinuierlich überprüft werden müsste, ob der Standort des Nutzers noch innerhalb der geforderten Zone liegt. Es wird erkannt, dass eine Art Nutzungskontrolle, wie z.B. UCON von Sandhu et al. [123], eingeführt werden muss und statt einzelner Punkte, die Trajektorien von Nutzern beachtet werden müssen. Bhatti et al. stellen in [17] eine Implementierung zur benutzerfreundlichen Modellierung von Richtlinien für GEO-RBAC vor. Ferner bilden sie GEO-RBAC-Richtlinien auf X-GTRBAC [18] ab, einen bereits implementierten XML-basierten RBAC-Ansatz, welcher die technische Ausführung übernimmt. Kirkpatrick et al. realisieren in [76] ebenfalls GEO-RBAC und bemerken dabei, dass die Verifikation von Positionsschätzungen ein Problem darstellt. Sie realisieren das System mittels XACML, einem offenen XML-basierten Standard, um die Durchsetzung von Zugriffskontrollmodellen zu spezifizieren [116].

Auch der Ansatz von Cruz et al. [33] setzt Standards zur Implementierung eines zuvor von Cirio et al. veröffentlichten T3-Ansatzes ein [27]. So wird die RBAC-Richtlinie als OWL-DL Ontologie modelliert und mittels eines Reasoners hergeleitet, welche Zugriffsrechte ein Nutzer hat. Seine aktuelle Zone wird in Form eines Attributs dargestellt, dessen Wert aus einer Menge von Zonen stammt, die zuvor über die Google Maps API definierten wurden.

Auch Ulltveit-Moe et al. [144] erkennen den Bedarf zur Übertragung auf existierende Standards und implementierten standortbasiertes RBAC auf Basis von GeoXACML des Open Geospatial Consortium [102], einer Erweiterung von XACML. GeoXACML ist konzipiert als statisch-statisch-Ansatz zum Schutz von geospatialen Datenbankeinträgen, denen jeweils eine Zone zugeordnet ist. Der Zugriff auf Einträge wird dann in Abhängigkeit von deren Zone gewährt. Ryoo et al. implementieren einen energieeffizienten Ansatz, um den Aufenthalt in Zonen von Grundstücksgröße zu erkennen [120]. Dabei wird die GPS- und WLAN-Positionierung nur ausgeführt, wenn die stromsparend gemessenen Werte des Beschleunigungssensors oder der Mobilfunkempfangsstärke eine Ortsänderung vermuten lassen.

Sichere Positionsbestimmung Beinahe keine der existierenden Arbeiten zur standortbasierten Autorisierung geht auf die Positionsbestimmung und deren Absicherung gegen Manipulationen ein [1,3,15,21,23,57,83,115,135]. Häufig wird vorausgesetzt, dass die Positionsbestimmung von einem nicht näher bestimmten, „sicheren“ und „vertrauenswürdigen“ Anbieter durchgeführt wird [8,30,63,113,148]. Decker et al. erkennen, dass die Positionsverifikation ein noch zu lösendes Problem für das Gebiet der standortbasierten Autorisierung darstellt [40]. Bertino et al. schlagen vor, dass neben der Positionsbestimmung selbst auch überprüft werden muss, ob sich das mobile Endgerät noch in den Händen des Nutzers be-

findet [16]. Kirkpatrick et al. realisieren in [76] die Verifikation von GPS-Positionen mittels der Nahfeldkommunikation, engl. Near Field Communication (NFC). Dazu wird der NFC-Sender im mobilen Endgerät verwendet und ein manipulationsgeschützter NFC-Leser in der autorisierten Zone installiert. Die Reichweite von NFC beträgt nur wenige Zentimeter, so dass hier erheblicher Aufwand durch eine flächendeckende Ausbringung von Lesern entsteht. Ulltveit-Moe et al. bemerken in [144], dass z.B. GPS-Positionen von mobilen Endgeräten, durch unbemerkt installierte Root-Kits oder manipulierte Treiber des GPS-Moduls, absichtlich zum Angriff der standortbasierten Autorisierung gefälscht werden können. Die Wirkung von Antivirenprogrammen sei hier nicht ausreichend, weshalb das komplette Betriebssystem und alle Treiber durch Methoden des Trusted Computing geschützt werden müssen [50]. Gilbert et al. stellen einen Ansatz vor, der im Betriebssystem die Softwarekomponenten zur Positionsbestimmung mittels Trusted Computing schützt [59,60].

He et al. schlagen in [64] mehrere Lösungen zur Positionsverifikation vor. Zum Einen können Verfahren zur Distanzbegrenzung verwendet werden, wie z.B. das ECHO-Protokoll von Sastry et al. [124]. Dabei wird die Infrastruktur um Verifikationsknoten erweitert, die über Funk- und Ultraschallverbindung mit dem mobilen Endgerät des Nutzers kommunizieren können. Nachdem dieses mittels Funk-Broadcast z.B. seine GPS-Position und die Antwortzeit verbreitet hat, die es zur Erstellung einer Antwort auf Anfragen benötigt, meldet sich ein naher Verifikationsknoten über Funk mit einer Nonce. Diese wird über Ultraschall vom mobilen Endgerät zurückgeschickt. Anhand der angegebenen Antwortzeit und Position sowie dem selbst gemessenen Übertragungsende der Antwort wird im Verifikationsknoten überprüft, ob die darüber berechnete Distanz zum Nutzer der Distanz zur GPS-Position entspricht. Hier wird Ultraschall eingesetzt, da bei der Laufzeitmessung von Funksignalen wegen deren hoher Ausbreitungsgeschwindigkeit zu große Zeitschwankungen durch das nichtdeterministische Verhalten der Systeminterrupts beim Senden und Empfangen des Echos entstehen. Dies konnte von Schauer et al. in Tests mit WLAN und handelsüblichen Smartphones bestätigt werden [125]. Neben der Positionsverifikation schlagen He et al. auch den Einsatz einer Plausibilitätsprüfung vor [64]. Dabei wird über die IP-Adresse auf den Standort des mobilen Endgeräts geschlossen. Dieser wird anschließend mit dem behaupteten, z.B. über GPS gemessenen Standort verglichen. Trotz der Ansätze existiert noch keine vorherrschende Lösung für handelsübliche mobile Endgeräte wie Smartphones oder Tablet-Computer, mit denen eine Positionsverifikation möglich ist. Zum Einen, weil nur die wenigsten Endgeräte den Einsatz von Trusted Computing unterstützen, zum Anderen, weil Lösungen wie das ECHO-Protokoll zu hohe technische Voraussetzungen an die Infrastruktur und die Endgeräte stellen.

Der Umgang mit Positionsfehlern Ein Kritikpunkt an den oben aufgeführten Arbeiten ist die Tatsache, dass der Einfluss von Positionsfehlern weder bei der Spezifikation, noch bei der Durchsetzung von Ortsbeschränkungen für Zugriffskontrollmodelle berücksichtigt wird. Decker et al. beschreiben in [40], dass der Umgang mit Positionsfehlern eine wichtige Eigenschaft von standortbasierter Autorisierung ist. Werden solche Fehler nicht berücksichtigt, so wird ein Nutzer auch dann autorisiert, wenn eine sehr große Ungewissheit

bzgl. seiner Position herrscht. Ansätze, die den Positionsfehler bei der Durchsetzung der standortbasierten Autorisierung nicht berücksichtigen, werden in der restlichen Arbeit als naive Autorisierungsstrategien bezeichnet. Dabei fordert eine Ortsbeschränkung, dass die Position des Nutzers innerhalb einer polygonalen autorisierten Zone liegt. Die Auswertung erfolgt über Punkt-in-Polygon-Tests.

Ein erster Schritt zur Berücksichtigung der Positionsfehler sind die schwellwertbasierten Autorisierungsstrategien. Dabei wird vorausgesetzt, dass der Standort des Nutzers nicht als Punkt, sondern in Form einer WDF beschrieben ist. Adragna et al. stellen in [8] den ersten Ansatz vor, der Positionsfehler durch die Einführung von Schwellwerten berücksichtigt. Dabei wird zuerst ermittelt, mit welcher Wahrscheinlichkeit p sich der Nutzer innerhalb der autorisierten Zone befindet. Daraus wird versucht, eine binäre Entscheidung mithilfe eines oberen und eines unteren Schwellwerts abzuleiten. Übersteigt p den oberen Schwellwert, wird angenommen, dass sich der Nutzer innerhalb der Zone befindet. Unterschreitet p den unteren Schwellwert, wird angenommen, dass sich der Nutzer außerhalb der Zone befindet. Liegt p zwischen den beiden Schwellwerten, muss die Positionsschätzung bis zu einer maximalen Anzahl wiederholt werden, bis das Kriterium erfüllt ist. Wird innerhalb der maximalen Versuche kein geeigneter Wert von p erhalten, so trifft ihr Algorithmus keine Aussage bzgl. der Autorisierung. Zu kritisieren ist, dass jede Anfrage aber trotzdem letztendlich entweder autorisiert oder abgewiesen werden muss. Das größte Problem ist jedoch, dass keinerlei Anhaltspunkte gegeben werden, wie die Schwellwerte zu setzen sind und hier lediglich auf Experten für deren Abschätzung verwiesen wird. Das Abschätzen von Positionsfehlern und die Berechnung des Wertes p werden von Ardagna et al. in [8] ebenfalls nicht behandelt.

Shin et al. stellen in [130] ausgehend von Ardagna et al. [8] eine erweiterte Lösung vor, deren Fokus auf der effizienten Ermittlung von p liegt. Ihr zugrundeliegendes standortbasierte Zugriffskontrollmodell basiert auf dem DAC-Modell und erlaubt die Spezifikation einzelner Regeln. Diese beschreiben, welches Subjekt auf welchem Objekt welche Aktion ausführen darf. Hierbei kann sowohl für das Subjekt, als auch das Objekt eine autorisierte Zone und ein zugehöriger Schwellwert spezifiziert werden. Für Subjekt und Objekt wird der Wert p berechnet. Überschreitet der jeweilige Wert den zugewiesenen Schwellwert, wird die Regel zur Autorisierung führen. Die Autoren erwähnen, dass die Wahl des Schwellwerts davon abhängt, wie sicher die Umgebung für die Ausführung einer zugrundeliegenden Aktion sein muss. Weshalb nicht immer ein Schwellwert von 100% gewählt wird, um maximale Sicherheit zu erreichen, ist unklar. Der Wert p wird in ihrem Ansatz ermittelt, indem die ungewisse Positionsschätzung als Kreis statt Punkt dargestellt wird. Dieser Kreis ist letztlich eine WDF mit einer Gleichverteilung innerhalb eines Kreises. Der Radius des Kreises hängt vom Positionsfehler, der maximalen Bewegungsgeschwindigkeit des Nutzers und der Zeit ab, die seit der Positionsbestimmung verstrichen ist. Hier wird auch nicht beschrieben, wie ein solch diskreter Wert für den Positionsfehler zu ermitteln ist. Auch Ulltveit-Moe et al. gehen in [144] ähnlich vor, wobei die Positionsschätzung ebenso als Kreis modelliert wird. In ihrem Ansatz wird lediglich gefordert, dass dieser Kreis die autorisierte Zone schneidet. Eine Forderung über die Größe der Schnittfläche, also über den Wert p, wird nicht aufgestellt.

Die dritte Klasse bilden Ansätze der risikobasierten Autorisierungsstrategie. Die grundlegende Idee ist, dass jeder Nutzer Attribute besitzt, z.B. seine Kompetenz eine bestimmte Aufgabe zu erledigen, oder seinen aktuellen Standort. An ein solches Attribut können Anforderungen gestellt werden, denen ihr aktueller Wert genügen muss, damit der Nutzer eine Autorisierung erlangt. Nur wenige Arbeiten existieren bisher, welche das Risiko betrachten, das aus einer Autorisierung mit ungewissem Standort des Nutzers folgt.

Cheng et al. weisen in [24] jeder einzelnen vertraulichen Information, die der Nutzer durch Autorisierung erlangen kann, einen monetären Wert zu. Zusätzlich wird für den Nutzer eine Wahrscheinlichkeit bestimmt, mit der er die Information auf die er zugreifen möchte, mutwillig oder unabsichtlich veröffentlichen wird. Das Risiko einer Autorisierung wird in diesem Ansatz aus dem Produkt der Wahrscheinlichkeit und dem Wert der Information berechnet. Der Zugriff wird nicht autorisiert, sofern das Risiko einer Autorisierung größer ist, als das Risiko einer Ablehnung.

Krautsevich et al. schützen Dokumente in [81] vor dem Zugriff, falls mittels Ortsbeschränkung zugeordnete autorisierte Räume während der Zeitspanne der Nutzung verlassen werden. Ihr Ansatz berücksichtigt keine Positionsfehler, so dass zu Beginn einer Autorisierung der Raum des Nutzers exakt feststeht. Positionsschätzungen treffen in deren Ansatz nur alle 15 min ein, so dass zwischenzeitlich über eine Markov-Kette abgeschätzt wird, wie wahrscheinlich sich der Nutzer noch im autorisierten Raum befindet. Dazu wird für jedes Paar von benachbarten Räumen modelliert, wie wahrscheinlich ein Nutzer innerhalb einer Minute den Raum wechselt. Für jeden Zeitpunkt wird dann entschieden, ob die Autorisierung zurückgezogen, oder nochmals verlängert wird. Dazu wird das Risiko beider Entscheidungen verglichen und diejenige mit dem geringen Risiko gewählt. Auch hier ist Risiko das Produkt aus der Wahrscheinlichkeit und den monetären Kosten. Eine fortwährende Autorisierung ist Richtig-Positiv, wenn der Nutzer noch im autorisierten Raum ist, oder Falsch-Positiv, wenn der Nutzer den Raum schon verlassen hat. Wird die Autorisierung eingestellt, ist die Entscheidung Richtig-Negativ, wenn der Nutzer tatsächlich nicht mehr im autorisierten Raum ist, oder eben Falsch-Negativ. Allen vier Fällen werden monetäre Kosten zugewiesen, die positiv sind, wenn das Unternehmen durch den jeweiligen Fall profitiert und negativ, wenn es dadurch Verlust erfährt. Problematisch an diesem Ansatz ist, dass bekannt sein muss, wie wahrscheinlich ein Nutzer pro Minute den Raum wechselt. Ebenso wird nicht erläutert, wie die vier Kosten systematisch hergeleitet werden können.

Marcus et al. stellen in [95] einen Ansatz vor, der ebenso für die gesamte Nutzungsdauer risikobasiert überprüft, ob sich der Nutzer noch in einer autorisierten Zone befindet. Ausgehend von der letzten Positionsschätzung bestimmt dieser Ansatz mithilfe eines Partikelfilters eine pessimistische Abschätzung der Wahrscheinlichkeit, mit der ein Nutzer den Raum zwischenzeitlich verlassen hat. Eine vorgegebene Modellierung der Übergangswahrscheinlichkeiten wie in [81] wird nicht benötigt. Auch hier werden wieder vier Kosten definiert, so dass ausgehend von dieser Wahrscheinlichkeit eine risikobasierte Autorisierung möglich ist.

Krautsevich et al. stellen in [82] einen zweiten allgemeinen Ansatz vor, der die kontinuierliche risikobasierte Autorisierung auf Basis der Werte von veränderlichen Attributen erlaubt. Als ein solches Attribut wird der Standort des Nutzers vorgeschlagen. Dabei wird

auch beschrieben, dass Ungewissheit durch Messfehler auftreten kann. Es wird ähnlich zu ihrer Arbeit in [81] ein Modell vorgestellt, das für jeden Zeitpunkt nach der Autorisierung die Wahrscheinlichkeit beschreibt, dass die Bedingung an das Attribut noch erfüllt ist. Auch hier werden vier Kosten für mögliche Ausgänge der Autorisierungsentscheidung verwendet, um das Risiko zu berechnen. Autorisiert wird, wenn die erwarteten Kosten einer Autorisierung einen Schwellwert übersteigen. Es wird gezeigt, wie dieser Schwellwert gewählt werden muss. Auch hier bleibt offen, woher die Kosten stammen. Es wird lediglich erläutert, dass diese aus gesammelten statistischen Daten berechnet werden können. Offen bleibt, wie groß die Ungewissheit über den Standort des Nutzers im Mittel sein darf und welche Qualität der Autorisierung mit zunehmender Ungewissheit aus Positionsfehlern noch möglich ist.

Aktuell existiert in der Literatur keine Gegenüberstellung dieser drei Strategien. Dadurch ist unklar, wann welche Strategie gewählt werden soll. Insbesondere ist nicht geklärt, ab wann ein Positionierungssystem nicht mehr für den Einsatz zur standortbasierten Autorisierung geeignet ist und ob sich diese Grenze für die einzelnen Strategien unterscheidet. Unterschiedliche Zugriffsrechte können unterschiedliche Sicherheitsrelevanz haben. In existierenden Arbeiten wird stets auf einen Experten verwiesen, der darauf aufbauend den Schwellwert oder die Kosten herleitet. Eine konkrete Methodik wird jedoch nicht vorgeschlagen.

Diese wichtigen Punkte stellen gegenwärtig ein großes Problem beim Einsatz von standortbasierter Autorisierung dar. In dieser Arbeit wird deshalb in Abschnitt 4.1 eine umfassende Gegenüberstellung der drei Strategien auf Basis der Entscheidungstheorie vorgestellt. Dabei wird das bisherige Konzept der monetären Kosten verallgemeinert und durch abstrakten Nutzen abgelöst. Es wird eine Systematik nach von Neumann et al. vorgestellt [111], die zur systematischen Herleitung des Nutzens eingesetzt wird. Abschnitt 5.2 stellt schließlich eine Methodik vor, wie für die einzelnen Strategien zu bestimmen ist, ob sich ein Positionierungssystem für ein bestimmtes Szenario eignet.

2.3 Die Qualität standortbasierter Autorisierung

Wird ein konkretes Positionierungssystem zur Realisierung von standortbasierter Autorisierung eingesetzt, ist die Auswertung von Ortsbeschränkungen unmittelbar von dessen Positionsfehlern betroffen. Je kleiner dabei die autorisierten Zonen im Vergleich zur Präzision und Richtigkeit des Positionierungssystems werden, umso größer wird die Ungewissheit über die Position des Nutzers. Befindet sich ein Nutzer außerhalb der autorisierten Zone, könnte seine Positionsschätzung trotzdem innerhalb dieser Zone liegen. Umgekehrt könnte seine Positionsschätzung außerhalb liegen, obwohl sich der Nutzer innerhalb der Zone befindet.

Wie „gut“ funktioniert also die Durchsetzung einer Ortsbeschränkung mit einem konkreten Positionierungssystem? Wie groß darf eine autorisierte Zone sein, wenn z.B. GPS eingesetzt wird? Benötigt wird ein qualitatives Maß für die Einsetzbarkeit eines Positionierungssystems. Dieses muss ausdrücken, ob das Positionierungssystem aufgrund seiner

Positionsfehler für die Auswertung einer gegebenen Ortsbeschränkung prinzipiell geeignet ist. Durch ein quantitatives Maß wird es möglich, die Eignung von prinzipiell geeigneten Positionierungssystemen zu vergleichen. Liegen mehrere prinzipiell geeignete Positionierungssysteme vor, so kann ein solches Positionierungssystem für die Ortsbeschränkung gefunden werden, welches einen guten Kompromiss zwischen seinen Kosten und seiner quantitativen Eignung darstellt.

Damiani et al. erkannten im Jahr 2006, dass ein Maß für die Qualität von standortbasierter Autorisierung benötigt wird, falls Positionsfehler auftreten [34]. Bisher existieren in der Literatur dazu jedoch keine Ansätze. Verwandte Arbeiten existieren im Bereich der LBS. Dabei werden ganz allgemein Anforderungen für Positionierungssysteme spezifiziert, so dass ein LBS im Betrieb ein gewünschtes Maß der Einsetzbarkeit erreicht. Es wird nicht quantitativ bemessen oder berücksichtigt, wie sich einzelne Aspekte im Verhalten des LBS in Abhängigkeit vom Positionierungssystem ändern. Eine formale Herleitung der Anforderungen aus Eigenschaften des LBS, wie z.B. der Zone, in welcher der LBS eingesetzt werden darf, oder der benötigten Sicherheit, wird nicht berücksichtigt.

Martin-Escalona et al. stellen in [101] MILCO vor, eine Middleware zur Auswahl des kostengünstigsten prinzipiell geeigneten Positionierungssystems für einen gegebenen LBS mit zusätzlich definierten Anforderungen. Diese Anforderungen sind der maximal erlaubte Positionsfehler und die akzeptable Verzögerung bis eine Position vorliegt. Iterativ überprüft die Middleware alle verfügbaren Positionierungssysteme und wählt das kostengünstigste aus, welches die beiden Anforderungen erfüllt. Offen bleibt, woher der Entwickler des LBS den tolerierbaren maximalen Positionsfehler und die Verzögerung für ein zugrundeliegendes Positionierungssystem kennt. Hier zählt bei zwei prinzipiell geeigneten Positionierungssystemen nur, welches kostengünstiger ist. Es wird keine quantitative Bewertung des Verhaltens des LBS mit einem konkreten Positionierungssystem durchgeführt.

Filjar et al. definieren in [55] Mindestanforderungen an ein Positionierungssystem ausgehend von einem LBS. Diese umfassen die horizontale und vertikale Richtigkeit, die Verzögerung bis eine Positionsschätzung vorliegt, den Energiebedarf und die Kosten. Ähnlich zu Martin-Escalona wird iterativ ein Positionierungssystem gesucht, das diesen Anforderungen genügt. Auch hier wird nicht quantitativ bemessen, wie sich der LBS mit diesem Positionierungssystem im Betrieb verhalten wird. Die Spezifikation der Anforderungen ist wieder subjektiv und nicht formal aus den Eigenschaften des LBS herleitbar.

Machaj et al. definieren in [91] als Anforderungen ebenso die horizontale und die vertikale Richtigkeit, die Verzögerung, bis eine Positionsschätzung vorliegt und zusätzlich die erreichbare Positionierungsfrequenz. Für einen gegebenen LBS muss ein Experte jedem dieser Faktoren eine skalare Gewichtung zuweisen und eine obere Schranke für den maximal erlaubten Wert angeben. Für jedes verfügbare Positionierungssystem wird dann bestimmt, wie stark die einzelnen Faktoren die erlaubte obere Schranke überschreiten. Aus diesen Differenzen wird anschließend die gewichtete Summe zur Bewertung des Positionierungssystems gebildet. In diesem Ansatz wird aber nicht beschrieben, welche Gewichtungen und welche oberen Schranken im Betrieb zum gewünschten Verhalten des LBS führen.

Dhar et al. definieren in [48] als Anforderung an ein Positionierungssystem die Richtigkeit, die Antwortzeit und die Robustheit, wenn damit ein konkreter LBS betrieben werden

soll. Die Anforderung an jede dieser Größen wird individuell für jeden LBS in Textform spezifiziert. Sie sollen den Entwurf und den Betrieb der Positionierungsinfrastruktur unterstützen. Die Autoren geben aber kein Maß zur quantitativen Bewertung an, wie gut ein LBS mit einem spezifischen Positionierungssystem im Betrieb arbeiten wird.

Ardagna et al. stellen in [9] einen Ansatz zur standortbasierten Autorisierung auf Zonen vor. Neben der Verzögerung bis zum Vorliegen einer Positionsschätzung wird zusätzlich als Anforderung ein Schwellwert spezifiziert. Dieser legt fest, wie gewiss mit einem konkreten Positionierungssystem im Mittel entscheidbar sein muss, ob sich ein Nutzer innerhalb oder außerhalb einer autorisierten Zone befindet. Auch hier wird nicht analysiert, welche Auswirkungen auf den Betrieb des LBS entstehen, wenn der Schwellwert zu hoch oder zu niedrig gewählt wird.

Im bereits oben beschriebenen Ansatz von Shin et al. [130] wird eine kreisförmige WDF zur Modellierung der Positionsschätzung verwendet. Ein Nutzer ist autorisiert, wenn seine Aufenthaltswahrscheinlichkeit in der autorisierten Zone einen vordefinierten Schwellwert übersteigt. Für sicherheitskritische Zonen werden hohe Schwellwerte gewählt. Dabei wird nicht darauf eingegangen, wie der Schwellwert die Eignung eines Positionierungssystems beeinflusst. Treten nämlich zu große Positionsfehler und somit zu große Kreise auf, überschreitet die Aufenthaltswahrscheinlichkeit den Schwellwert nicht mehr.

Bisher existiert keine Methodik, die für gegebene Positionierungssysteme das Verhalten eines LBS zur Laufzeit voraussagt und eine vergleichende Bewertung erlaubt. Der Betreiber des LBS kann derzeit erst nach Inbetriebnahme erkennen, ob die standortbasierte Autorisierung, mit einem gegebenen Positionierungssystem, entsprechend seiner Anforderungen durchsetzbar ist.

Kapitel 3

Positionsbestimmung und -verarbeitung

In diesem Kapitel werden Beiträge zur Positionsbestimmung und -verarbeitung vorgestellt. Die Positionsbestimmung ist Grundvoraussetzung für die Anwendung standortbasierter Autorisierung. In Gebäuden wird dabei überwiegend WLAN-Fingerprinting eingesetzt, was, wie jedes andere Positionierungssystem auch, inhärenten Positionsfehlern unterliegt. Solche Positionsfehler können in Gebäuden von der Größe autorisierter Zonen sein. Damit die Ungewissheit über die aktuelle Position bei der standortbasierten Autorisierung berücksichtigt werden kann, muss das Ausmaß dieser Positionsfehler erfasst und verarbeitet werden.

Zur Verbesserung der Einsetzbarkeit von WLAN-Fingerprinting für die standortbasierte Autorisierung in Gebäuden wird in Abschnitt 3.1 ein neuartiger Fehlerschätzer vorgestellt. Dieser ermittelt aus den Charakteristika der durchgeführten Messung eine WDF für den Standort des Nutzers. Um die Ungewissheit zu berücksichtigen, kann die standortbasierte Autorisierung auf Basis dieser WDF durchgeführt werden, anstatt eine einzelne Koordinate als Position zu verwenden. Es wird gezeigt, dass der entwickelte Fehlerschätzer deutlich bessere Abschätzungen liefert als existierende Ansätze und somit wesentlich zur Einsetzbarkeit beiträgt.

Ferner wird in Abschnitt 3.2 eine Verbesserung von WLAN-Fingerprinting vorgestellt, welche die dynamische Bestimmung der Anzahl der nächsten Nachbarn erlaubt. Dadurch entfällt eine vorherige empirische Ermittlung dieser Größe für neue Einsatzorte. Grundlage ist die iterative Erhöhung der Anzahl der verwendeten nächsten Nachbarn in der Positionsbestimmung bis eine Divergenz der Positionen eintritt.

Um die abgeleitete WDF des Fehlerschätzers bei Autorisierungsentscheidungen zu berücksichtigen, ist die Aufenthaltswahrscheinlichkeit des Nutzers innerhalb der autorisierten Zone ein zentrales Maß. Diese wird durch numerische Integration bestimmt, welche jedoch im Betrieb und während der Analyse des Autorisierungsverhaltens starken Rechenaufwand verursacht. Ferner ist eine exakte Bestimmung der Aufenthaltswahrscheinlichkeit unmöglich, da die gelieferte WDF nur eine statistische Modellierung ist. In Abschnitt 3.3 wird deshalb ein Approximationsverfahren vorgestellt, welches gegenüber der direkten Anwendung der numerischen Integration nur Leseoperationen auf vorberechneten Matrizen durchführt. Es wird gezeigt, dass dessen Antwortzeit deutlich kürzer ist und der berechnete Näherungswert innerhalb einer Fehlerschranke liegt, die zur standortbasierten Autorisierung keinen

wesentlichen Nachteil darstellt.

Wird ein mobiles Endgerät gestohlen oder weitergegeben, so erscheint dessen Position weiterhin als die Position des eingeloggten Nutzers. Zur Erkennung solcher Situationen werden auf dem mobilen Endgerät typischerweise biometrische Authentifizierungsverfahren eingesetzt. Diese stellen sicher, dass der eingeloggte Nutzer sein mobiles Endgerät selbst bedient. Die Position des mobilen Endgeräts entspricht dann der Position des Nutzers. In Abschnitt 3.4 wird ein Anforderungskatalog an biometrische Authentifizierungsverfahren vorgestellt, um deren Einsetzbarkeit im Umfeld der standortbasierten Autorisierung zu gewährleisten.

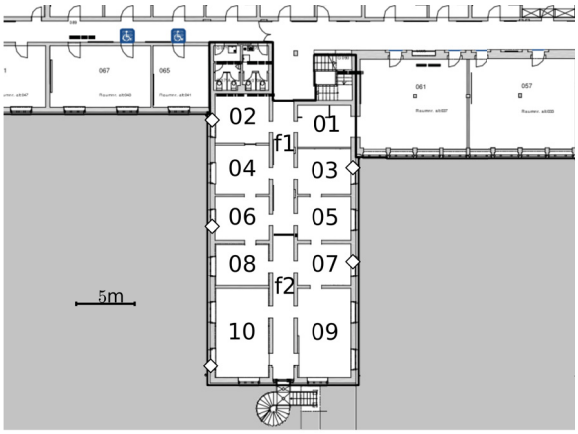
3.1 Ein Fehlerschätzer für WLAN-Fingerprinting

Für die standortbasierte Autorisierung ist die Erfassung und Modellierung von Positionsfehlern von zentraler Bedeutung, um diese behandeln zu können. Im Folgenden wird deshalb ein neuartiger Ansatz vorgestellt, der eine mitlaufende Fehlerschätzung im Betrieb von numerischem WLAN-Fingerprinting erlaubt. Dieser Ansatz erweitert eine gemeinsame Vorarbeit mit Dr. Moritz Kessel und Dr. Martin Werner, die in Marcus et al. [96] publiziert und von Kessel [71] aufgegriffen wurde. Anstelle der in [96] und [71] verwendeten Normalverteilungen zur Modellierung von Positionsfehlern wird ein neuartiger Fehlerschätzer vorgestellt, welcher Laplace-Verteilungen erzeugt. Anhand einer stark erweiterten Testumgebung wird gezeigt, dass diese Vorgehensweise dem bisherigen Ansatz überlegen ist.

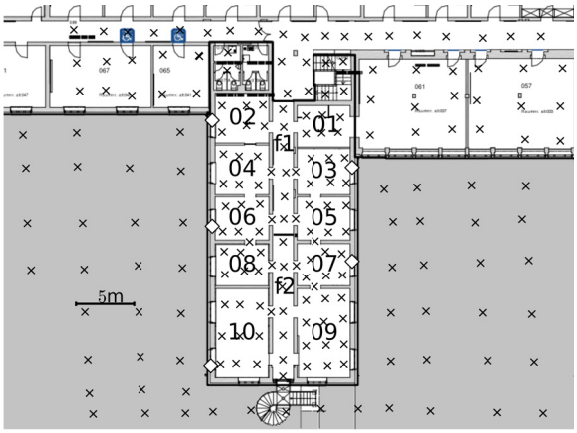
3.1.1 Die Testumgebung

Als Ausgangsbasis für die nachfolgenden Überlegungen und die Evaluation der entwickelten Konzepte wurde zunächst in einer Offline-Phase eine umfassende Fingerprint-Datenbank aus 824 Fingerprints erstellt, die insgesamt eine Fläche von 1730 m^2 abdeckt. Ausgangspunkt ist der Gebäudeplan in Abb. 3.1(a). Räumen sowie dem Flur sind Bezeichner zugewiesen, wobei der Flur auf Höhe des Übergangs von 08 nach 06 in f1 und f2 geteilt ist und sich bis zur Höhe des oberen Endes von 01 erstreckt. Die Messungen wurden unter Android 2.3 mit einem HTC Desire Smartphone durchgeführt. Hierzu wurde ein möglichst gleichmäßiges Raster über den Gebäudeplan gelegt. An jedem Rasterpunkt wurden insgesamt 4 Fingerprints aufgezeichnet, wobei jeweils in eine der vier Himmelsrichtungen geblickt wurde. Jeder einzelne Fingerprint repräsentiert einen Vektor aus Signalstärken der dort empfangbaren Access-Points, die jeweils aus 20 Einzelmessungen gemittelt wurden. Als Access-Points wurden insgesamt 5 Cisco WAP4410N installiert. Die erstellte Fingerprint-Datenbank ist in Abb. 3.1(b) dargestellt. Die 5 Access-Points sind als weiße Rauten eingezeichnet.

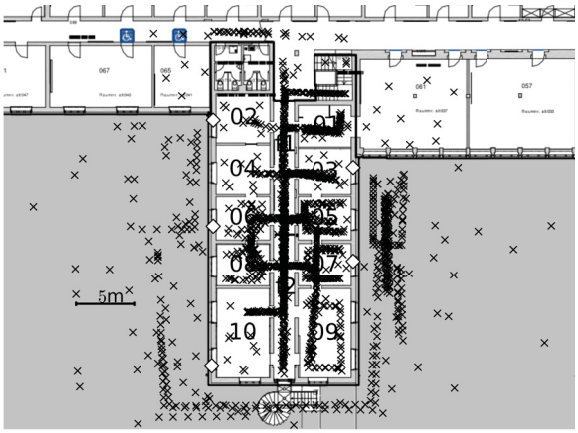
Zusätzlich wurden 2449 Testmessungen erstellt, die ohne eine Mittlung von Einzelmessungen entstanden, da die Erfassung von 20 Einzelmessungen im praktischen Einsatz aufgrund des Zeitaufwands von 5-10 s als unrealistisch anzusehen ist [104]. Der Grund dafür ist, dass während der aktiven Suche (Active Scan) nach Access-Points alle Frequenzbänder



(a) Gebäudeplan und benannte Bereiche



(b) Fingerprint-Datenbank



(c) Testdaten

Abbildung 3.1: Darstellung benannten Bereiche, sowie der Orte, an denen Messungen für die Fingerprint-Datenbank erstellt wurden und der Orte der separat erfassten Testdaten.

sequentiell durchlaufen werden und pro Frequenz jeweils ca. 20-40 ms verstreichen, während auf Antworten (Probe Response) am WLAN-Interface gehorcht wird. Die aufgezeichneten Testdaten setzen sich zum Einen aus 2249 Fingerprints zusammen, deren jeweilige örtliche Grundwahrheit aus der Interpolation zwischen Referenzpunkten von 60 abgegangenen Trajektorien bestimmt wurde. Zum Anderen wurden 200 Testmessungen an festen Orten erstellt. Die Gesamtheit der Testdaten ist in Abb. 3.1(c) dargestellt. Bei der Erstellung der Testdaten und der Fingerprint-Datenbank wurden ausschließlich die Signalstärke der 5 installierten Access-Points beachtet.

Um WLAN-Fingerprinting zur standortbasierten Autorisierung einsetzen zu können, sind Rahmenbedingungen einzuhalten, die für andere Anwendungsfälle nicht zwingend sind. So muss die Fingerprint-Datenbank nicht nur die autorisierten Zonen abdecken, sondern ebenfalls deren Umgebung. Da die Funkreichweite der vorhandenen Access-Points

nicht nur die autorisierte Zone umfasst, kann ein Angreifer ansonsten von außerhalb das System irreführen und eine Autorisierung erwirken. Wird nur die autorisierte Zone durch die Fingerprint-Datenbank abgedeckt, besteht bei der Wahl der kNN aus der Menge der Fingerprints keine andere Möglichkeit als Fingerprints zu wählen, die innerhalb der autorisierten Zone liegen. Ein Angreifer außerhalb der autorisierten Zone hat dann die Möglichkeit eine Positionsschätzung zu erhalten, die innerhalb liegt. Im Rahmen der standortbasierten Autorisierung basierend auf Punkt-in-Polygon-Tests führt dies zu einer Falsch-Positiv-Entscheidung. Zur Lösung dieses Problems wird vorgeschlagen, zunächst die Menge der Access-Points zu ermitteln, die innerhalb der autorisierten Zone an mindestens einem Punkt eine Signalstärke im Messbereich aufweisen. Im nächsten Schritt werden die Abdeckungsflächen dieser Access-Points vereinigt. Die resultierende Fläche muss durch die aufzunehmende Fingerprint-Datenbank abgedeckt werden. Dadurch erhöht sich der Aufwand eine Fingerprint–Datenbank aufzunehmen, wofür aber die Erkennung von Angreifern außerhalb der autorisierten Zone möglich wird.

Um eine Positionsbestimmung frei von systematischen Fehlern zu erlauben, müssen die aufgezeichneten Fingerprints innerhalb der ermittelten Abdeckungsfläche gleich verteilt sein. Eine weitere Besonderheit beim Einsatz von numerischem WLAN-Fingerprinting zur standortbasierten Autorisierung ist, dass die aktuelle Blickrichtung des Nutzers nicht beachtet werden darf. Wird diese über den Kompass des mobilen Endgeräts ermittelt und die Fingerprint-Datenbank vor der Suche nach den kNN damit gefiltert [11,72], hat ein Angreifer die Möglichkeit durch einfaches Drehen seines mobilen Endgeräts die Positionsbestimmung erheblich zu beeinflussen. Denn die Dämpfung des menschlichen Körpers gegenüber WLAN-Signalen beträgt ca. $5 - 9$ dBm [11,70], wodurch er die Wahl der kNN beeinflussen und von außerhalb fälschlicherweise eine Position innerhalb der autorisierten Zone erhalten kann. Im Anwendungsfall zur standortbasierten Autorisierung muss deshalb zur Verringerung von Angriffsmöglichkeiten auf die blickrichtungsbasierte Filterung der Fingerprint-Datenbank verzichtet werden.

3.1.2 Positionsfehler von WLAN-Fingerprinting

Um ein geeignetes Schätzverfahren anzugeben, muss zunächst untersucht werden, wie die Fehler um die tatsächliche Nutzerposition verteilt sind. Hierzu wird für jeden Eintrag der Testdaten aus Abb. 3.1(c) eine Positionsbestimmung basierend auf der Fingerprint-Datenbank aus Abb. 3.1(b) durchgeführt. Dabei wird die Blickrichtung des Nutzers ignoriert, um die Angriffsmöglichkeiten im Einsatzszenario der standortbasierten Autorisierung zu verringern. Aus der Fingerprint-Datenbank werden jeweils die 4 nächsten Nachbarn im Signalstärkeraum über deren euklidische Distanz bestimmt. Fehlende Einträge werden hierbei mit dem Wert -100 dBm ergänzt, so dass zu vergleichende Vektoren die gleiche Dimension besitzen, wie von Kessel et al. in [72] vorgeschlagen. Die Positionsschätzung μ wird schließlich aus dem gewichteten Mittel der 4 nächsten Nachbarn entsprechend (2.6) bestimmt. Aus den so ermittelten Positionsschätzungen werden die realen Fehlervektoren ausgehend von der wahren Position des Nutzers ermittelt und in der restlichen Arbeit als $\vec{f} = \binom{f_x}{f_y}$ notiert. Die wahre Position des Nutzers wird in der restlichen Arbeit als *gtp* abgekürzt,

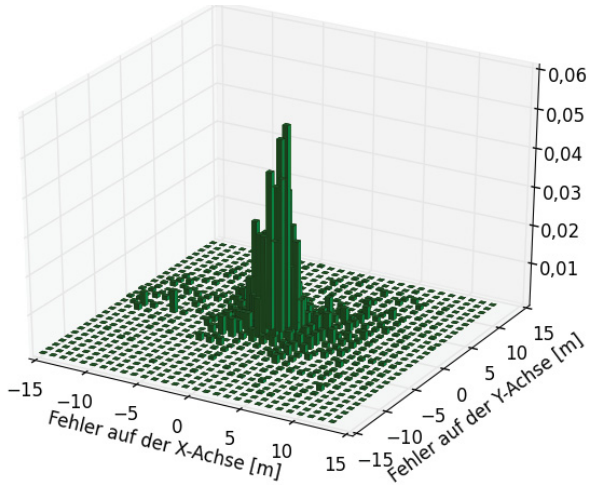


Abbildung 3.2: Histogramm der beobachteten Fehlervektoren der Positionsbestimmung relativ zur wahren Position des Nutzers. Die einzelnen Klassen umfassen jeweils einen Bereich von 1×1 m.

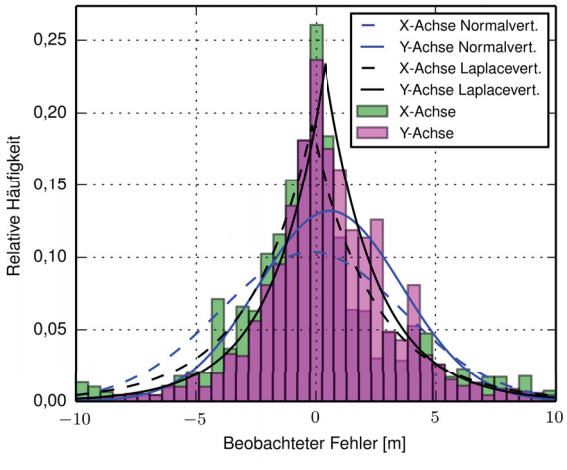


Abbildung 3.3: Verteilung der echten Position des Nutzers um die geschätzte Position für beide Achsen. Die Fehler lassen sich gut durch eine Laplaceverteilung beschreiben.

in Anlehnung an den engl. Begriff der Ground Truth Position. Die Richtigkeit des Positionierungssystems beträgt 0,62 m und berechnet sich aus der euklidischen Norm des Mittelwerts der Fehlervektoren. Die Länge der Fehlervektoren beträgt über alle Testdaten hinweg im Mittel 2,39 m. Dieser Wert ist in Abhängigkeit vom Teilbereich der Testumgebung in Abb. 3.4 dargestellt. Die Gesamtheit der Fehlervektoren zeigt Abb. 3.2 in Form eines dreidimensionalen Histogramms.

Das Histogramm zeigt, dass die Streuung der Fehler auf der X-Achse etwas breiter als auf der Y-Achse ist, so dass eine leichte Korrelation zwischen den Fehlern auf beiden Achsen besteht. Offensichtlich folgt dies jedoch aus dem asymmetrischen Aufbau der Testumgebung, worin die Access-Points auf der Y-Achse auf die Länge des Flurs verteilt ein breiteres Gebiet abdecken, als auf der X-Achse. Allgemeinen ist jedoch von einem symmetrischen Aufbau auszugehen, so dass im Folgenden angenommen wird, dass die Fehler auf auf X- und Y-Achse unkorreliert sind. Hieraus folgt jedoch im Allgemeinen nicht, dass die Fehler stochastisch unabhängig sind.

Die achsenspezifischen Verteilungen sind in Abb. 3.3 als Histogramme dargestellt, wobei für jede Achse die beste Anpassung (engl. Best-Fit) einer Normal- und einer Laplaceverteilung angetragen ist. In einer früheren von Marcus et al. in [96] veröffentlichten Untersuchung wurde mittels Leave-One-Out-Kreuzvalidierung auf einer Fingerprint-Datenbank mit 316 Einträgen und ähnlicher Testumgebung festgestellt, dass die Fehler annähernd normal verteilt sind. Diese Hypothese kann für die oben beschriebene Testumgebung mit einer mehr als doppelt so großen Fingerprint-Datenbank und realen Testdaten nicht gehalten werden. Im Gegensatz dazu zeigt sich, dass die Fehlerverteilung auf den realen Testdaten deutlich besser durch eine univariate Laplaceverteilung approximiert werden kann. Deren

WDF lautet [80]:

$$g_{\mu,\lambda}(x) = (2\lambda)^{-1} \exp\left(\frac{-|x-\mu|}{\lambda}\right) \tag{3.1}$$

Sie hängt vom Lageparameter μ und dem Skalenparameter λ ab.

3.1.3 Die Abschätzung von Positionsfehlern

Im Folgenden wird ein Fehlerschätzer basierend auf Laplaceverteilungen vorgestellt. Dessen Leistungsfähigkeit wird verglichen mit dem zuvor von Marcus et al. in [96] entwickelten Fehlerschätzer, der auf Normalverteilungen basiert und bisher noch nicht auf einem umfangreichen Testdatensatz evaluiert wurde. Die eingesetzte Evaluationsmethodik ist eine Weiterentwicklung der Evaluationsmethodik aus [96].

Möglichkeiten zur Fehlerschätzung

Das Ziel eines Fehlerschätzers für WLAN-Fingerprinting ist, für eine Positionsschätzung $\mu = \binom{\mu_x}{\mu_y}$ eine WDF anzugeben, welche die Lage der wahren Position *gtp* bzgl. der Positionsschätzung μ beschreibt. Zur Angabe einer solchen WDF ergeben sich zwei Herangehensweisen. Zum Einen kann aus der Fehlerverteilung der Gesamtdaten, wie in Abb. 3.3 dargestellt, eine Laplace- oder Normalverteilung angepasst und universell für alle Positionsschätzungen eingesetzt werden. Deren Kovarianzmatrix spezifiziert dann zusammen mit einer konkreten Positionsschätzung μ die WDF. Diese Verteilung ist jedoch nur auf der Gesamtheit der abgedeckten Fläche die beste Wahl, da innerhalb einzelner Bereiche bzw. Räume unterschiedliche Fehlerverteilungen beobachtet werden. Die Standardabweichung der Länge der beobachteten Fehlervektoren ist in Abb. 3.4 dargestellt. In den Bereichen *02*, *05*, sowie in *08* und *Außerhalb* sind größere Werte zu beobachten, als im Bereich *Gesamt*. Auch die anderen Bereiche unterscheiden sich bzgl. der Standardabweichung voneinander. Somit ist die Einführung eines mitlaufenden Fehlerschätzers gerechtfertigt, welche die Zweite der erwähnten Herangehensweisen darstellt. Ein solcher mitlaufender Fehlerschätzer verwendet als zusätzliche Information die Referenzpunkte $l_1, \cdots, l_k$ der kNN und ihre Gewichte $w_1, \ldots, w_k$, die zur Berechnung von μ entsprechend (2.6) verwendet wurden.

Fehlerschätzung durch Normalverteilungen

Der von Marcus et al. in [96] entwickelte Fehlerschätzer σ_{m4} ermittelt für eine Positionsschätzung μ eine WDF, die beschreibt, wie die unbekannte wahre Position *gtp* um μ verteilt ist. Da der wahre Fehlervektor $\vec{f}$ unbekannt ist, wird für dessen Beschreibung eine Zufallsvariable $\mathbf{F}$ eingeführt. Die WDF, welche der Fehlerschätzer herleitet, ist die WDF dieser Zufallsvariablen $\mathbf{F}$. Der Ansatz aus [96] basiert auf der Annahme, dass $\mathbf{F}$ einer Normalverteilung folgt, also $\mathcal{N}(\mu, \Sigma) \sim \mathbf{F}$ gilt. Zusätzlich wird zur Vereinfachung angenommen, dass die Richtigkeit vernachlässigbar ist, d.h. keine systematischen Fehler im Positionierungssystem vorliegen.

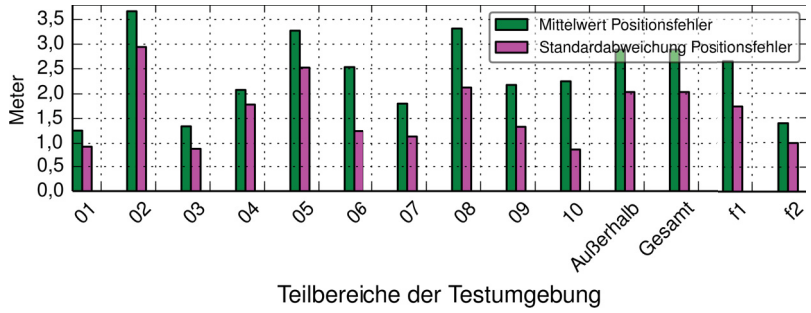


Abbildung 3.4: Mittelwerte und Standardabweichung der Positionsfehler für die Teilbereiche der Testumgebung.

Als WDF wird eine bivariate Normalverteilung hergeleitet. Deren Dichte ist rotationssymmetrisch aufgrund der Annahme, dass die Fehler auf X- und Y-Achse unkorreliert sind. Zur Angabe der WDF wird eine Kovarianzmatrix $\Sigma = \begin{pmatrix} \sigma_{m4}^2 & 0 \\ 0 & \sigma_{m4}^2 \end{pmatrix}$ zusammen mit der Positionsschätzung μ verwendet. Die allgemeine WDF der bivariaten Normalverteilung mit Mittelwert $\mu = \binom{\mu_x}{\mu_y}$, Korrelationskoeffizient φ und Varianzen σ_x und σ_y lautet [106]:

$$g(x,y) = \frac{1}{2\pi\sigma_x\sigma_y\sqrt{1-\varphi^2}} \cdot \exp\left(\frac{(x-\mu_x)^2/\sigma_x^2 - 2\varphi(x-\mu_x)(y-\mu_y)/\sigma_x\sigma_y + (y-\mu_y)^2/\sigma_y^2}{2(1-\varphi^2)}\right) \quad (3.2)$$

Der Wert σ_{m4} wird ausgehend von der Positionsschätzung μ, sowie den Referenzpositionen $l_1, \ldots, l_k$ der kNN und deren Gewichten $w_1, \ldots, w_k$ bestimmt:

$$\sigma_{\mathrm{m4}}(\mu, l_1, l_2, \ldots, l_k) = \sum_{i=1}^{k} w_i \|\mu - l_i\|_2 \quad (3.3)$$

Hier beschreibt σ_{m4} also die mittlere absolute Abweichung der Referenzpositionen $l_1, \ldots, l_k$ der kNN von der Positionsschätzung μ. Diese Methodik berücksichtigt keine Charakteristika der Fingerprint-Datenbank, wie z.B. deren Dichte oder Abdeckungsbereich und kann daher nicht speziell für ein gegebenes Szenario kalibriert oder angepasst werden.

Die WDF der Zufallsvariable $\mathbf{F}$ des Fehlervektors lautet für ein gegebenes μ und Kovarianzmatrix $\Sigma = \begin{pmatrix} \sigma_{m4}^2 & 0 \\ 0 & \sigma_{m4}^2 \end{pmatrix}$:

$$wdf_{\mathbf{F}|\mu,\Sigma}^{normal}(f_x, f_y) = \frac{1}{2\pi\sigma_{m4}^2} \cdot \exp\left(-\frac{(f_x-\mu_x)^2 + (f_y-\mu_y)^2}{2\sigma_{m4}^2}\right) \quad (3.4)$$

Dieser Ansatz wird im Folgenden mit einem neu entwickelten Verfahren verglichen, welches Laplaceverteilungen zur Beschreibung von $\mathbf{F}$ und somit zur Abschätzung des unbekannten wahren Fehlervektors $\vec{f}$ generiert.

Fehlerschätzung durch Laplaceverteilungen

Die symmetrische bivariate Laplaceverteilung entsteht nach Kotz et al. aus der univariaten Laplaceverteilung, indem diese gleichmäßig entlang einer Ellipse in zwei Dimensionen gespreizt wird [80]. Im Allgemeinen gilt für die WDF einer solchen Verteilung mit Mittelwert $\mu = \binom{\mu_x}{\mu_y}$, Korrelation ϱ und Kovarianzmatrix $\Sigma = \begin{pmatrix} \sigma_1^2 & \sigma_1\sigma_2\varrho \\ \sigma_1\sigma_2\varrho & \sigma_2^2 \end{pmatrix}$:

$$g_{\mu,\Sigma}(\bar{x} = x - \mu_x, \bar{y} = y - \mu_y) = \frac{1}{\pi\sigma_1\sigma_2\sqrt{1-\varrho}} \cdot K_0\left(\sqrt{\frac{2\left(\bar{x}^2/\sigma_1^2 - 2\varrho\bar{x}\bar{y}/\left(\sigma_1\sigma_2\right) + \bar{y}^2/\sigma_2^2\right)}{1-\varrho^2}}\right) \tag{3.5}$$

Hierbei ist K_0 die modifizierte Besselfunktion dritter Art für $\lambda = 0$ [80]. Gegeben sei eine Positionsschätzung μ. Unter der oben gegebenen Annahme, dass die Fehler auf der X- und Y-Achse unkorreliert sind ($\varrho = 0$) und für die Varianzen $\sigma_1 = \sigma_2 = \sigma$ gilt, d.h. dass diese den gleichen Wert σ besitzen, folgt aus (3.5) für die WDF von $\mathbf{F}$:

$$wdf^{laplace}_{\mathbf{F}|\mu,\sigma}(f_x, f_y) = \frac{1}{\pi\sigma^2} \cdot K_0\left(\frac{\sqrt{2}}{\sigma}\sqrt{\left(f_x - \mu_x\right)^2 + \left(f_y - \mu_y\right)^2}\right) \tag{3.6}$$

Im nächsten Schritt wird basierend auf der Positionsschätzung eine Vermutung für die Länge r des wahren Fehlervektors $\vec{f}$ erzeugt und mittels der Maximum-Likelihood-Methode [110] der plausibelste Wert σ zur Angabe der WDF einer Laplaceverteilung bestimmt.

Die Vermutung r entspricht der Summe aus dem oben eingeführten σ_{m4} und einer Kalibrierungskonstante Δ. Zur Bestimmung von Δ werden zufällig 10% der Einträge des Testdatensatzes entnommen und deshalb in der späteren Evaluation nicht mehr berücksichtigt. Auf den so gezogenen N Testdaten wird für jeden Eintrag i die Differenz aus der Länge des realen Fehlervektors $\vec{f_i}$ und dem abgeschätztem $(\sigma_{m4})_i$ berechnet. Der Wert Δ ergibt sich als Erwartungswert dieser Differenzen:

$$\Delta = \frac{1}{N} \cdot \sum_{i=0}^{N} \left(\left\|\vec{f_i}\right\| - (\sigma_{m4})_i\right) \tag{3.7}$$

Für die in Unterabschnitt 3.1.1 beschriebene Testumgebung gilt $\Delta = 0{,}49$ m. Im Allgemeinen ist dieser Wert stark von der Umgebung sowie der Fingerprint-Datenbank abhängig und muss vor der Inbetriebnahme des Fehlerschätzers individuell ermittelt werden. Denn eine unterschiedliche Dichte an aufgezeichneten Fingerprints, die Anzahl k der verwendeten kNN sowie die bauliche Beschaffenheit des Gebäudes beeinflussen den Zusammenhang zwischen wahrem Fehlervektor und dem ermittelten σ_{m4}.

Um die Likelihood-Funktion möglichst einfach angeben zu können, wird zunächst (3.6) in Polarkoordinaten mit Ursprung bei der Positionsschätzung μ transformiert [106]:

$$wdf^{laplace}_{\mathbf{F}|\mu,\sigma}(r, \varphi) = \frac{1}{\pi\sigma^2} \cdot K_0\left(\frac{\sqrt{2}}{\sigma}r\right) \tag{3.8}$$

Da die zugrundeliegende WDF rotationssymmetrisch ist, hängt der Funktionswert nicht vom Winkel φ ab, weshalb $wdf^{laplace}_{\mathbf{F}|\mu,\sigma}(r,\varphi)$ durch $f(r)$ abgekürzt wird. Hier muss beachtet werden, dass $\int_0^\infty f(r)\,\mathrm{d}r \neq 1$, da $f(r)$ nur die Wahrscheinlichkeit beschreibt, dass die wahre Position *gtp* im Radius r und einem beliebigem Winkel liegt. Um die Abhängigkeit vom Winkel zu beseitigen, wird die Eigenschaft von WDFs verwendet, dass $\int_{x\in A} wdf(x)\,\mathrm{d}x = 1$ gilt:

$$\int_0^\infty \int_0^{2\pi} f(r)\cdot r\,\mathrm{d}\varphi\mathrm{d}r = \int_0^\infty \underbrace{2\pi r\cdot f(r)}_{\equiv wdf^{laplace}_{\mathbf{F}|\mu,\sigma}(r)}\,\mathrm{d}r = 1 \tag{3.9}$$

Der zusätzliche Faktor r im Integral entsteht durch die Integration in Polarkoordinaten. Für die gesuchte WDF gilt nach Einsetzen von (3.8):

$$wdf^{laplace}_{\mathbf{F}|\mu,\sigma}(r) = 2\pi r\cdot f(r) = 2\pi r\cdot\frac{1}{\pi\sigma^2}\cdot K_0\left(\frac{\sqrt{2}}{\sigma}r\right) \tag{3.10}$$

Im Folgenden wird der neuartige Ansatz vorgestellt, die Maximum-Likelihood-Methode anzuwenden, um für eine Positionsschätzung μ, sowie die Referenzpunkte $l_1,\ldots,l_k$ der verwendeten kNN und deren Gewichte $w_1,\ldots,w_k$ den Parameter σ einer WDF $wdf^{laplace}_{\mathbf{F}|\mu,\sigma}(r)$ abzuschätzen. Dabei wird analog zum Normal-Fehlerschätzer vereinfachend angenommen, dass die Richtigkeit des Positionierungssystems bei der Ableitung der WDF vernachlässigbar ist.

Für eine gegebene Positionsschätzung μ wird das σ gewählt, welches die Wahrscheinlichkeit maximiert, den Radius $r = \sigma_{m4} + \Delta$ zu beobachten. Unter der Annahme, dass r mit der Länge des echten, aber unbekannten Fehlervektors $\vec{f}$ korreliert, ergibt sich als Likelihood-Funktion für σ basierend auf (3.10):

$$\mathcal{L}_r(\sigma) = wdf^{laplace}_{\mathbf{F}|\mu,\sigma}(r) \tag{3.11}$$

Der Wert σ, für den der Wert von $\mathcal{L}(\sigma)$ maximal wird, ist der plausibelste Parameter für die gesuchte WDF und wird im Folgenden als σ_{mls} bezeichnet. Er stellt die Maximum-Likelihood-Schätzung dar:

$$\sigma_{mls} = \arg\max_{\sigma\in\mathbb{R}^+}\mathcal{L}_r(\sigma) \tag{3.12}$$

Für eine Positionsschätzung μ ergibt sich schließlich entsprechend (3.6) aus der Lage der Referenzpositionen der verwendeten kNN und deren Gewichten als WDF für $\mathbf{F}$ die Funktion $wdf^{laplace}_{\mathbf{F}|\mu,\sigma_{mls}}(f_x,f_y)$.

3.1.4 Evaluation des Fehlerschätzers

Bei der Evaluation mitlaufender Fehlerschätzer mittels der Testdaten ergibt sich das Problem, dass zu jeder abgeschätzten WDF i nur eine Stichprobe von $\mathbf{F}_i$ existiert, nämlich der wahre Fehlervektor $\vec{f_i}$ von μ_i zur zugehörigen wahren Position gtp_i des Nutzers. Daraus kann keine Aussage über die Qualität einer WDF getroffen werden. Deshalb wird zur

Evaluation die Erweiterung eines Verfahrens vorgestellt, dessen ursprüngliche Idee von Marcus et al. in [96] publiziert wurde. Dabei wird für jede Messung i aus den Testdaten, der bekannte Fehlervektor $\vec{f_i}$ mittels des geschätzten σ standardisiert. Somit entsteht für jede Testmessung aus dem real beobachteten Fehlervektor $\vec{f_i}$ ein standardisierter Fehlervektor $\overline{\vec{f_i}}$. Die Erweiterung der Evaluation basiert auf der Darstellung der Fehlervektoren in Polarkoordinaten und untersucht in Quantil-Quantil-Plots (QQ-Plots), inwiefern diese der bivariaten Standardnormalverteilung bzw. -laplaceverteilung folgen. Die Darstellung in Polarkoordinaten erlaubt es gegenüber der bisherigen Evaluation aus [71,96] mit kartesischen Koordinaten anhand der QQ-Plots eine Aussage zu treffen, ob Fehler über- oder unterschätzt werden.

Eine Zufallsvariable gilt als standardisiert, wenn ihr Erwartungswert 0 und ihre Varianz 1 ist [110]. Eine Zufallsvariable Y wird folgendermaßen in eine standardisierte Zufallsvariable Y transformiert:

$$X = \frac{Y - \mathrm{E}(Y)}{\sqrt{\mathrm{Var}(Y)}} \tag{3.13}$$

Die Wurzel aus der Varianz ist bekanntlich die Standardabweichung. Für den Fehlerschätzer σ_{m4}, der gemäß obiger Annahmen bivariate Normalverteilungen mit Korrelation $\varrho = 0$ als WDF für $\mathbf{F}$ liefert, gilt für die Kovarianzmatrix $\Sigma = \begin{pmatrix} \sigma_{m4}^2 & 0 \\ 0 & \sigma_{m4}^2 \end{pmatrix}$. Zur Evaluation des Fehlerschätzers σ_{m4} wird zunächst jeder real auf den Testdaten aufgetretene Fehlervektor $\vec{f_i}$ durch die zugehörige Fehlerschätzung $(\sigma_{m4})_i$ standardisiert:

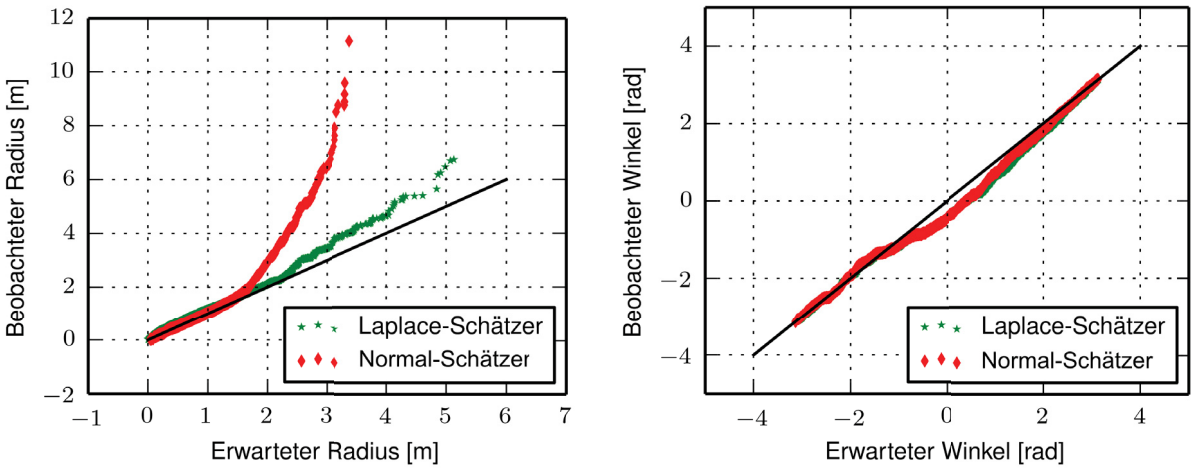
$$\overline{\vec{f_i}^{normal}} = \frac{\vec{f_i}}{(\sigma_{m4})_i} \tag{3.14}$$

Nach Kotz. et al. [80] besitzt die symmetrische bivariate Laplaceverteilung entsprechend (3.5) die Kovarianzmatrix $\Sigma = \begin{pmatrix} \sigma_1^2 & \sigma_1\sigma_2\varrho \\ \sigma_1\sigma_2\varrho & \sigma_2^2 \end{pmatrix}$. Für den vorgestellten Laplace-Fehlerschätzer gilt, wie oben erläutert, die Annahme $\sigma_{mls} = \sigma_1 = \sigma_2$ und $\varrho = 0$. Für die vom Laplace-Fehlerschätzer gelieferten Verteilungen ergibt sich somit die Kovarianzmatrix $\Sigma = \begin{pmatrix} \sigma_{mls}^2 & 0 \\ 0 & \sigma_{mls}^2 \end{pmatrix}$. Analog zu (3.14) wird ebenfalls für den Laplace-Fehlerschätzer jeder reale Fehlervektor $\vec{f_i}$ der Testdaten durch die zugehörige abgeschätzte Standardabweichung $(\sigma_{mls})_i$ standardisiert:

$$\overline{\vec{f_i}^{laplace}} = \frac{\vec{f_i}}{(\sigma_{mls})_i} \tag{3.15}$$

Für jedes Element i der Testdaten liegt dann der real beobachtete Fehlervektor in zwei standardisierten Versionen vor – einmal mit σ_{m4} und einmal mit σ_{mls} standardisiert. Für jede dieser Mengen wird die Entsprechung zur Standardnormal- bzw. zur Standardlaplaceverteilung untersucht. Dazu werden zwei QQ-Plots eingesetzt [14].

Bei N Testdaten werden dazu N Stichproben aus der Standardnormal- bzw. der Standardlaplaceverteilung entnommen. Für jedes Testdatum werden die Polarkoordinaten berechnet, also der Radius als Entfernung zum Ursprung μ, sowie der zugehörige Winkel. Gleiches erfolgt für die standardisierten Fehlervektoren bzgl. deren Ursprung $\binom{0}{0}$. In Abb.



(a) Radien (b) Winkel

Abbildung 3.5: QQ-Plots zur Visualierung des Verhaltens der Fehlerschätzer.

3.5(a) sind die Längen der standardisierten Fehlervektoren der Testdaten, gegen Stichproben aus der zugehörigen Standardverteilung angetragen. In 3.5(b) sind die zugehörigen Winkel der standardisierten Fehlervektoren gegen die Winkel der Stichproben angetragen. Für beide Fehlerschätzer ist diese Visualisierung nahezu identisch, da sich der Winkel der Testdaten bei der Standardisierung nicht ändert.

Aus dem Grad, zu dem die angetragenen Werte der eingezeichneten Gerade folgen, lassen sich Rückschlüsse über die Qualität des jeweiligen Fehlerschätzers ziehen. Zum Einen, ob die Fehler eher über- oder unterschätzt werden und zum Anderen, ob die Normal- bzw. Laplace-Verteilung des eingesetzten Fehlerschätzers zu den realen Fehlern passt.

Wie gut der verwendete Typ der Verteilung die realen Fehler beschreibt, lässt sich aus der Krümmung der Kurve interpretieren, welcher die eingetragenen Datenpunkte folgen. Kommen lange Vektoren bei den Stichproben aus der zugehörigen Standardverteilung seltener vor als unter den zugehörigen standardisierten Vektoren, so folgen die Datenpunkte einer Kurve mit positiver Krümmung. Dies ist für den Fehlerschätzer σ_{m4} klar erkennbar. Die Datenpunkte zum Laplace-Fehlerschätzer folgen hingegen einer kaum gekrümmten Kurve, was die Annahme über die Eignung der Laplace-Verteilung untermauert.

Darüber hinaus lässt sich erkennen, ob die geschätzten Werte σ_{m4} bzw. σ_{mls} den Fehler über- oder unterschätzen. Dazu wird untersucht, ob die Datenpunkte einer Geraden mit größerer bzw. kleinerer Steigung als der Referenzgeraden mit $m = 1$ folgen. Sind die geschätzten Fehler σ_{m4} bzw. σ_{mls} zu klein, liegen die Datenpunkte im QQ-Plot in Abb. 3.5(a) oberhalb der Geraden. Dies ist für den Fehlerschätzer σ_{m4} klar erkennbar, wohingegen der Laplace-Fehlerschätzer die Fehler deutlich geringer unterschätzt. In welchem Bereich der Radien die Fehler unter- oder überschätzt werden, hängt stark mit der Annahme über die zugrundeliegende Verteilung zusammen. So wird im Verlauf für σ_{m4} in Abb. 3.5(a) deutlich, dass gerade große Fehler stark unterschätzt werden. Der Laplace-Fehlerschätzer bildet

diese deutlich besser ab.

Der QQ-Plot in Abb. 3.5(b) erlaubt hingegen eine Aussage darüber, ob die Modellierung der WDF als rotationssymmetrische Verteilung mit Korrelation $\varphi = 0$ und Kovarianzen von 0 gerechtfertigt ist. Da die Testdaten für beide Fehlerschätzer identisch sind, ergibt sich nahezu der gleiche Verlauf. Es zeigt sich, dass die Winkel der beobachteten Fehlervektoren im Wesentlichen gleich verteilt auf dem Intervall $[-\pi; \pi]$ sind. Lediglich im Bereich $\left[-\frac{\pi}{2}; \frac{\pi}{2}\right]$ liegen zu wenige der real beobachteten Fehlervektoren. Die Modellierung der WDF der Fehlerschätzer über eine rotationssymmetrische Verteilung ist also aus Sicht der Winkelverteilung kein wesentlicher Nachteil.

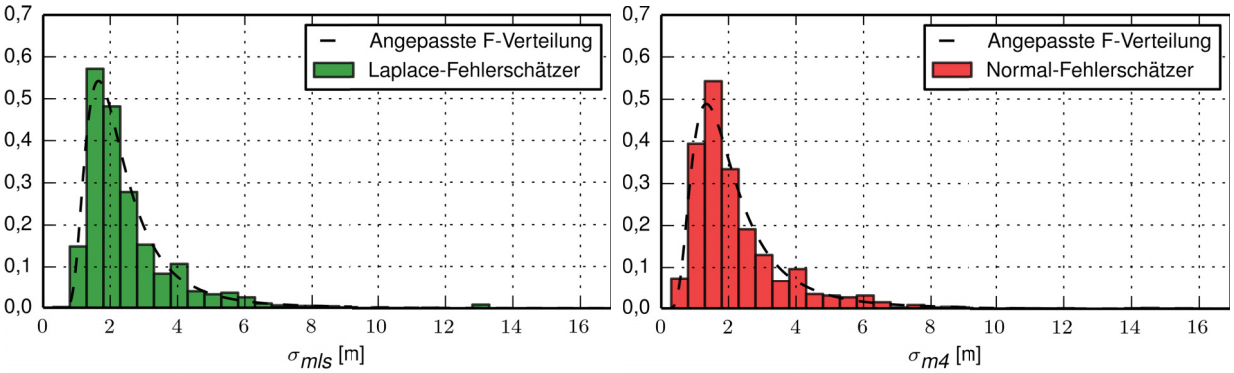
Gegenüber dem ursprünglichen Ansatz von Marcus et al. aus [96] bietet der hier vorgestellte Ansatz des Laplace-Fehlerschätzers gerade im Bereich großer Fehler eine deutlich genauere Abschätzung. Für die Anwendung zur standortbasierten Autorisierung ist dies wichtig, da autorisierte Zonen häufig von Außenbereichen umgeben sind, welche durch die Fingerprint-Datenbank abgedeckt werden müssen, jedoch größere Positionsfehler hervorbringen. Je besser diese Fehler abgeschätzt werden, umso weniger Falschentscheidungen entstehen, wenn standortbasierte Autorisierung unter Beachtung dieser Fehlerschätzungen betrieben wird. Der hier vorgestellte Ansatz bietet als Erweiterung die Übertragbarkeit auf andere Szenarien, indem eine Kalibrierungskonstante eingeführt wird. Die mittlere gewichtete Abweichung der kNN von der Positionsschätzung kann hierdurch je nach Szenario so kalibriert werden, dass plausible Fehlerschätzungen entstehen. Gegenüber Marcus et al. [96] ist die Verbesserung der Analyse in den QQ-Plots wichtig, die bisher noch nicht anhand der Radien und Winkel, sondern nur für die X- und Y-Achse separat durchgeführt wurde. Im Falle von Normalverteilungen ist dies legitim, da X- und Y-Werte der Stichproben stochastisch unabhängig sind. Im Falle von Laplaceverteilungen ist dies aber nach Kotz et al. nicht mehr gegeben [80], so dass die QQ-Plots mithilfe der Radien und Winkel erstellt werden. Zusätzlich wird so, wie oben gezeigt, nachvollziehbar, ob der Fehlerschätzer zum Über- bzw. Unterschätzen tendiert und inwiefern die gewählte Verteilung die wahren Fehlervektoren beschreibt.

3.1.5 Theoretische Modellierung von Positionierungssystemen

Ist für ein Positionierungssystem ein Fehlerschätzer gegeben, so liefert die Verteilung der zurückgegebenen Fehlerschätzungen eine Aussage darüber, wie sich dieses Positionierungssystem im Betrieb mit standortbasierter Autorisierung verhält, sofern hierbei die geschätzte WDF berücksichtigt wird.

Liegt ein Fehlerschätzer vor, der wie auch oben dargestellt symmetrische, bivariate WDFs mit Kovarianzmatrizen $\Sigma = \left(\begin{smallmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{smallmatrix}\right)$ generiert, kann die Verteilung der geschätzten Werte für σ das Autorisierungsverhalten beeinflussen. Im Folgenden wird der Ansatz basierend auf Marcus et al. [99] vorgestellt, die Verteilung der abgeschätzten Werte σ als das theoretische Modell des Positionierungssystems zu verwenden. Die relative Häufigkeitsverteilung ist für den oben vorgestellten Laplace- und den Normal-Fehlerschätzer in Abb. 3.6 dargestellt.

Hierbei zeigt sich, dass die beiden Verteilungen ähnlich sind, allerdings die gelieferten



(a) Laplace-Fehlerschätzer (b) Normal-Fehlerschätzer

Abbildung 3.6: Die relative Häufigkeitsverteilung der geschätzten Fehler σ_{m4} bzw. σ_{mls} für den Normal- bzw. Laplace-Fehlerschätzer mit angepasster F-Verteilung beschreiben.

	Laplace-Fehlerschätzer		Normal-Fehlerschätzer	
	Histogramm	**F-Verteilung**	**Histogramm**	**F-Verteilung**
Erwartungswert	2,4999 m	2,4934 m	2,2927 m	2,2822 m
Varianz	2,1466 m	2,1991 m	2,8184 m	2,7570 m

Tabelle 3.1: Varianz und Erwartungswert der Fehlerschätzungen.

Werte für σ beim Laplace-Fehlerschätzer in Abb. 3.6(a) etwas weniger breit gestreut sind, als beim Normal-Fehlerschätzer in Abb. 3.6(b). In beiden Fällen lässt sich an die dargestellte relative Häufigkeitsverteilung sehr gut eine F-Verteilung anpassen, welche somit die geschätzten Werte von σ beschreibt. Die WDF der F-Verteilung mit m Freiheitsgraden im Zähler und n Freiheitsgraden im Nenner lautet [110]:

$$F(x) = \begin{cases} \frac{\Gamma\left(\frac{m+n}{2}\right)}{\Gamma\left(\frac{m}{2}\right)\Gamma\left(\frac{n}{2}\right)} \left(\frac{m}{n}\right)^{m/2} x^{\frac{m}{2}-1} \left(1+\frac{m}{n}x\right)^{-\frac{m+n}{2}} & \text{falls } x > 0 \\ 0 & \text{falls } x \leq 0 \end{cases} \tag{3.16}$$

Hierbei sei Γ die Gammafunktion.

In beiden Fällen stimmen die Varianz und der Erwartungswert der jeweiligen relativen Häufigkeitsverteilung bis auf eine Nachkommastelle mit der Varianz und dem Erwartungswert der dafür angepassten F-Verteilung überein. Die genauen Werte zeigt Tab. 3.1.

Die jeweils angepasste F-Verteilung, welche die vom Fehlerschätzer gelieferten Werte für σ beschreibt, wird im Folgenden $\mathrm{F}_{fehler}^{Laplace}$ bzw. $\mathrm{F}_{fehler}^{Normal}$ genannt. Diese theoretische Modellierung eines Positionierungssystems ist nicht auf WLAN-Fingerprinting beschränkt. Für die Verteilung der Fehlerschätzungen eines anderen Positionierungssystems wird jedoch eine passende Verteilung benötigt, die dann als F_{fehler} dient. Zu beachten ist, dass dieses Modell ein Positionierungssystem über die Verteilung von Fehlerschätzungen beschreibt. Dabei gelten die vereinfachenden Annahmen, dass das Positionierungssystem eine maximale Richtigkeit besitzt und die Fehlerschätzungen in dem Sinne perfekt sind, als dass sie

bei der oben durchgeführten Analyse im QQ-Plot exakt der Ursprungsgeraden folgen. Wie später gezeigt wird, sind Fehlerschätzungen ein wesentlicher Faktor, um Positionsfehler in der standortbasierten Autorisierung zu behandeln. Für ein gegebenes Szenario hängen daher die Autorisierungsentscheidungen stark von der Verteilung F_{fehler} ab.

Hightower et al. verwenden in [65] ein Infrarot-Positionierungssystem mit kleinen Empfängern, für welches eine statische Normalverteilung $\Sigma = \left(\begin{smallmatrix} 2{,}3\ m & 0 \\ 0 & 2{,}3\ m \end{smallmatrix}\right)$ verwendet wird, die aus den Spezifikationen des Herstellers abgeleitet wurde. Zandbergen et al. zeigen in [150], dass auch für GPS mit professionellen Empfängern eine solche statische Verteilung mit $\Sigma = \left(\begin{smallmatrix} 2{,}008\ m & 0 \\ 0 & 2{,}008\ m \end{smallmatrix}\right)$ angegeben werden kann. Natürlich ist diese Verteilung nicht immer die beste Fehlerschätzung, da die Lage der Satelliten, atmosphärische Einflüsse, Mehrwegeausbreitung usw. variieren und somit auch der Fehler abhängig von Zeit und Ort schwankt. Auf dem iPhone 3G wurden mit Assisted-GPS selbst unter idealen Bedingungen drei bis viermal größere Fehler festgestellt, so dass im Mittel $\Sigma = \left(\begin{smallmatrix} 7{,}7\ m & 0 \\ 0 & 7{,}7\ m \end{smallmatrix}\right)$ eine passende Modellierung darstellt [151]. Für die Verteilung der Länge von GPS-Fehlervektoren wird die Verwendung einer Log-Normal- oder einer Rayleigh-Verteilung nahegelegt aber nicht bestätigt [150].

Für GPS kann näherungsweise auch eine Verteilung F_{fehler} angegeben werden, so dass die in dieser Arbeit entwickelten Konzepte auch auf GPS anwendbar sind:

$$\mathrm{F}_{fehler}^{GPS}(\sigma) = \begin{cases} 1 & \text{falls } \sigma = 7{,}7\ m \\ 0 & \text{sonst} \end{cases} \tag{3.17}$$

Diese Verteilung beruht auf dem mittleren horizontalen Fehler, den Zandbergen et al. in [151] bei der Positionsbestimmung mit Assisted-GPS auf dem iPhone 3G beobachten konnten.

3.2 Die dynamische Berechnung der nächsten Nachbarn

In der Positionsbestimmung mittels numerischem WLAN-Fingerprinting hat die Anzahl k der verwendeten nächsten Nachbarn aus der Fingerprint-Datenbank einen erheblichen Einfluss auf den mittleren und maximalen Positionsfehler. Ausgehend von einer aktuellen Messung m der Signalstärken der sichtbaren Access-Points, wird aus den ermittelten k nächsten Nachbarn der gewichtete Schwerpunkt gebildet und als Positionsschätzung zurückgegeben.

Vor der Ausbringung eines solchen Systems zur WLAN-Positionsbestimmung muss also ein fixer Wert für k bestimmt werden. Im Allgemeinen hängt dieser Wert von der aufgezeichneten Fingerprint-Datenbank und der Umgebung ab, so dass dessen Bestimmung empirisch erfolgen muss und zusätzlichen Aufwand verursacht. Ein in der Literatur gängiger Wert ist $k = 4 - 6$ [11,72,147]. Auf der oben beschriebenen Testumgebung zeigt ein Wert von $k = 4$ mit numerischem, diskretem WLAN-Fingerprinting die besten Ergebnisse. Ist dieser Wert bestimmt, muss er stets aktualisiert werden, wenn z.B. die Fingerprint-Datenbank durch die Aufnahme zusätzlicher WLAN-Fingerprints vergrößert wird. Ein anderes

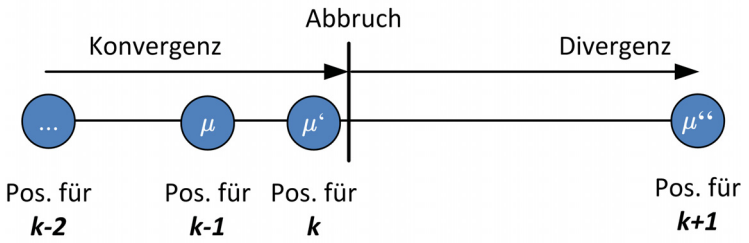


Abbildung 3.7: Die Anzahl k der verwendeten nächsten Nachbarn wird bestimmt, indem k solange erhöht wird, bis die gegenseitigen Abstände der Positionsschätzungen zunehmen.

Problem ergibt sich, wenn das abgedeckte Gebiet sehr heterogen bezüglich der Dichte von aufgezeichneten Fingerprints, der Anzahl sichtbarer Access-Points oder gebäudespezifischer Eigenheiten ist. In solchen Fällen ist die Angabe eines globalen Wertes für k nicht zwangsläufig flexibel genug, um unterschiedlichen Gegebenheiten gerecht zu werden. Aber auch in sehr gleichförmigen Umgebungen, wie der oben vorgestellten Testumgebung, kann ein dynamisch bestimmtes k den mittleren Fehler reduzieren.

Im Folgenden wird SMARTkNN vorgestellt, dessen Konzept in einer gemeinsamen Vorarbeit mit Dr. Martin Werner und Dr. Moritz Kessel entstand und in Marcus et al. [96] vorab veröffentlicht wurde. Der Ansatz erlaubt das numerische, diskrete WLAN-Fingerprinting mittels einer dynamisch bestimmten Anzahl von verwendeten nächsten Nachbarn. Der Ansatz wird auf der Fingerprint-Datenbank und den Testdaten aus Abb. 3.1 evaluiert, welche gegenüber der Fingerprint-Datenbank mit 316 Fingerprints und den 64 Testdaten in [96] deutlich umfangreicher sind.

Die grundlegende Idee des entwickelten Algorithmus ist in Abb. 3.7 dargestellt. Iterativ wird der Wert k inkrementiert und eine darauf basierende Positionsschätzung durchgeführt. Zentral für die Abbruchbedingung der Iteration sind die gegenseitigen Abstände der Positionsschätzungen μ, μ' und μ'', die für $k-1$, k und $k+1$ bestimmt werden. Sobald nämlich die Distanz von μ' zu μ'' größer wird als die zuvor beobachtete Distanz von μ zu μ', bricht die Iteration ab und liefert μ' als Positionsschätzung.

Diese Vorgehensweise ist formal in Algorithmus 2 in Pseudo-Code angegeben. Zunächst wird die Positionsschätzung μ für $k-1$ mit der Position des ersten nächsten Nachbarn initialisiert. Daraufhin wird der aktuelle Wert für k auf den Parameter min_k gesetzt, der die minimale Anzahl der nächsten Nachbarn vorschreibt, die als Ergebnis erlaubt ist. Dieser Wert min_k muss zwingend größer als 1 sein, denn ansonsten würde zwischen μ und μ' sofort der Abstand 0 erreicht werden, so dass der Algorithmus stets die Positionsschätzung für $k = 1$ als Ergebnis liefert. In der Schleife wird iterativ für steigende Werte von k die Positionsschätzung μ' und μ'' für k bzw. $k+1$ bestimmt. Über die Prozeduren `hole_NN` werden zunächst die WLAN-Fingerprints ermittelt, welche die k bzw. $k+1$ nächsten Nachbarn darstellen. Für diese wird jeweils über die Prozedur `gewichteter_Schwerpunkt` die Positionsschätzung μ' bzw. μ'' ermittelt. Nun wird geprüft, ob die euklidische Distanz $\|\mu' - \mu\|_2$ von μ' zu seinem Vorgänger μ kleiner ist als die euklidische Distanz $\|\mu'' - \mu'\|_2$ von μ' zu seinem Nachfolger μ''. Ist dies der Fall, so terminiert die Schleife und gibt die

Algorithmus 2 WLAN-Positionsbestimmung mit dynamisch bestimmten nächsten Nachbarn.

Eingabe: WLAN-Fingerprint m, minimale Anzahl nächster Nachbarn min_k
Ausgabe: Positionsschätzung basierend auf WLAN-Fingerprint m

```
function SMARTkNN(m, min_k)
    μ ← gewichteter_Schwerpunkt(hole_NN(1, m))      ▷ 1NN als letzte Pos. speichern
    k ← min_k                                        ▷ Initialisierung
    while k < |fingerprints| do                      ▷ k darf Maximalwert nicht übersteigen
        kNN' ← hole_NN(k, m)
        μ' ← gewichteter_Schwerpunkt(kNN')
        kNN" ← hole_NN(k + 1, m)
        μ'' ← gewichteter_Schwerpunkt(kNN")
        if ‖μ'' − μ'‖2 < ‖μ' − μ‖2 then              ▷ Fortfahren solange Pos. konvergieren
            μ ← μ'                                   ▷ Für nächste Iteration aktualisieren
            k ← k + 1                                ▷ Für nächste Iteration erhöhen
        else
            return μ
        end if
    end while
    return μ
end function
```

Positionsschätzung μ' basierend auf dem aktuellen k als Ergebnis zurück. Der Algorithmus terminiert ebenfalls, wenn k den maximal möglichen Wert erreicht, welcher der Anzahl $|fingerprints|$ der Einträge in der Fingerprint-Datenbank entspricht.

Entsprechend des beschriebenen Abbruchkriteriums liefert der Algorithmus das erste lokale Optimum als Positionsschätzung zurück. Weitere Positionsschätzungen für ein größeres k werden nicht gefunden. Zur Bewertung dieser Einschränkung wird die Optimalstrategie eingeführt. Diese ermittelt für jeden Eintrag der Testdaten das k, dessen zugehörige Positionsschätzung den kleinsten Fehler bzgl. der wahren Position aufweist. Sie stellt deshalb eine theoretische Schranke für die minimal möglichen Positionsfehler von Ansätzen zur dynamischen Bestimmung der verwendeten nächsten Nachbarn dar. Da im realen Betrieb die wahre Position nicht bekannt ist, handelt es sich um eine fiktive Strategie.

Der SMARTkNN-Algorithmus wurde auf der Fingerprint-Datenbank aus Abb. 3.1(b) gegen die Testdaten aus Abb. 3.1(c) evaluiert. Hierbei wurden als untere Grenze für k jeweils die Werte $min\_k \in \{2,3,4\}$ untersucht und mit der Positionsbestimmung basierend auf einem fixem $k = 4$ und der Optimalstrategie verglichen. Hierdurch kann sowohl für die Strategie mit fixem k, als auch für SMARTkNN die Abweichung zum Optimalverhalten untersucht werden. Die Ergebnisse bezüglich der Positionsfehler sind in Tab. 3.2 aufgeführt. Da die Fingerprint-Datenbank auch Außenbereiche abdeckt, sind die Positionsfehler größer als in Ansätzen, die auf Gebäude beschränkt sind.

Verglichen mit der Positionsbestimmung basierend auf einem fixem $k = 4$ kann SMART-

Methode	Mittelwert der Fehler	Maximaler Fehler	Standard-abweichung
fixes $k = 4$	3,02 m	17,81 m	2,48 m
dynamisches $k \geq 4$	2,99 m	13,25 m	2,44 m
dynamisches $k \geq 3$	3,02 m	14,16 m	2,53 m
dynamisches $k \geq 2$	3,20 m	15,64 m	2,78 m
optimales k	2,00 m	7,46 m	1,78 m

Tabelle 3.2: Evaluationsergebnisse des SMARTkNN-Algorithmus.

kNN in der durchgeführten Evaluation den mittleren Fehler von 3,02 m auf 2,99 m reduzieren. Ferner kann durch SMARTkNN für $min\_k = 4$ der maximale Fehler von 17,81 m auf 13,25 m gesenkt werden, wobei gleichzeitig auch die Standardabweichung der Fehler sinkt. Eine untere Schranke von $min\_k = 2$ oder $min\_k = 3$ konnte jedoch keine besseren Ergebnisse im Vergleich zum fixen $k = 4$ liefern. Die Abweichung zur Optimalstrategie ist für SMARTkNN und der Positionsbestimmung mit fixem k in Abb. 3.8 als kumulative Fehlerverteilung dargestellt. Hierbei zeigt sich, dass SMARTkNN mit $min\_k = 4$ die Optimalstrategie am besten approximiert.

Einen genaueren Einblick in die Verteilung der dynamisch gewählten Werte für k gibt Abb. 3.9 in Form eines Histogramms. Hierbei ist für SMARTkNN mit drei verschiedenen Startparametern min_k, sowie für die Optimalstrategie die relative Häufigkeitsverteilung der gewählten Werte für k abzulesen. Die optimale Anzahl von k ist über ein breites Intervall gestreut, wohingegen SMARTkNN höchstens 12 nächste Nachbarn wählt. Generell zeigt das Histogramm, dass SMARTkNN mit $min\_k = 2$ und $min\_k = 3$ die schlechteren Ergebnisse vorwiegend deshalb erreicht, da zu häufig ein lokales Optimum bei $k = 2$ bzw. $k = 3$ vorliegt und die Suche beendet wird. Diese lokalen Optima bewirken oft größere Positionsfehler als die Positionen, die für ein größeres k gefunden werden.

Die Anzahl der Iterationen bzw. Schleifendurchläufe in SMARTkNN verursacht nur begrenzten Mehraufwand gegenüber der Strategie mit einem fixem k, da entsprechend Abb. 3.9 maximal ein Wert von $k = 12$ dynamisch bestimmt wurde. Darüber hinaus liegt die rechnerische Komplexität des numerischen WLAN-Fingerprintings in der Berechnung der Distanzen im Signalstärkeraum der durchgeführten Messung m zu den Einträgen in der Fingerprint-Datenbank, sowie der Sortierung der Einträge nach der Distanz. Diese Aufgaben können bereits vor Eintritt in die Schleife ausgeführt werden, so dass in den einzelnen Durchläufen lediglich ein Präfix der Länge k der sortierten Liste gebildet und darauf basierend die Position berechnet wird.

Ein interessanter Aspekt ist die mittlere Anzahl der kNN. Die SMARTkNN-Strategie mit $min\_k = 4$ zeigt dabei einen Mittelwert von 5,80 und eine Standardabweichung von 1,27. Hieraus lässt sich folgern, dass vorwiegend Werte von $k = 4$ bis $k = 8$ gewählt wurden. Für $min\_k = 2$ bzw. 3 ergibt sich ein Mittelwert für k von 3,42 bzw. 4,73. Die Optimalstrategie zeigt schließlich einen Mittelwert für k von 13,43 bei einer Standardabweichung von 15,06.

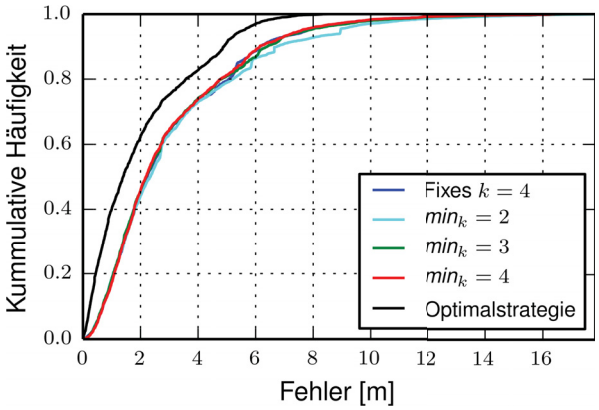


Abbildung 3.8: Die kumulative Fehlerverteilung von SMARTkNN verglichen mit der Optimalstrategie und fixem $k = 4$.

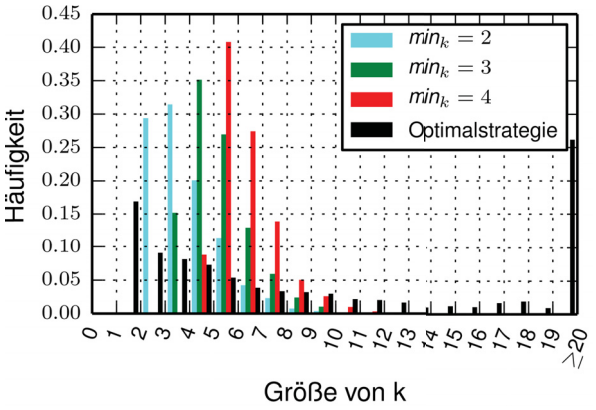


Abbildung 3.9: Die relative Häufigkeitsverteilung der gewählten Anzahl k an nächsten Nachbarn für SMARTkNN und die Optimalstrategie.

Zusammenfassend folgt, dass durch den SMARTkNN-Algorithmus die vorherige empirische Ermittlung des optimalen Werts für die Anzahl k der zu verwendenden nächsten Nachbarn eingespart werden kann. Der mittlere und der maximale Positionsfehler gegenüber der Verwendung von fixen 4 nächsten Nachbarn konnte auf dem umfangreichen Testdatensatz sogar reduziert werden. Trotzdem entsteht in SMARTkNN die Abhängigkeit von dem neuen Parameter min_k. Generell sollte dieser Wert ausreichend hoch gewählt werden, so dass kein Abbruch durch zu frühe lokale Optima eintritt. Ein Wert von $min\_k \geq 4$ kann als Richtschnur angenommen werden. So entsteht keine Gefahr der frühzeitigen Terminierung bei lokalen Optima mit $k = 2$ oder $k = 3$, welche meist größere Positionsfehler aufweisen.

3.3 Auswertung von Positionsschätzungen

Grundvoraussetzung für Modelle zur standortbasierten Autorisierung ist, dass Zugriffsrechte einem Nutzer nur gewährt werden, sofern er die zugrundeliegenden Ortsbeschränkungen erfüllt [28]. Je nach angewandter Autorisierungsstrategie werden diese Ortsbeschränkungen auf Basis der Aufenthaltswahrscheinlichkeit des Nutzers innerhalb der autorisierten Zone ausgewertet [8]. Zur Ermittlung dieser Wahrscheinlichkeit ist die WDF nötig, welche die Ungewissheit über die tatsächliche Nutzerposition modelliert. Existiert ein Positionierungssystem mit hinreichender Richtigkeit und Präzision, so entsteht Ungewissheit hauptsächlich durch veraltete Messungen, da sich der Nutzer zwischenzeitlich fortbewegt haben kann. In der vorliegenden Arbeit wird angenommen, dass diese Messungen zwar aktuell sind, die auftretenden Positionsfehler jedoch verglichen mit der Größe der autorisierten Zonen nicht vernachlässigt werden können.

Liegt die WDF für den Nutzerstandort vor, ist für die Bestimmung der Aufenthaltswahrscheinlichkeit deren rechenintensive numerische Integration über die autorisierte Zone nötig. Die Berechnung wird insbesondere dann zum Flaschenhals, wenn viele Anfragen zu

beantworten sind, beispielsweise zur Analyse des Verhaltens der Ortsbeschränkung eines Zugriffsrechts, oder wenn die Antwortzeit eine wichtige Rolle spielt. Gegenüber Ansätzen zur standortbasierten Autorisierung, die Positionsfehler ignorieren, ist der zusätzliche Berechnungsaufwand bisher ein großer Nachteil.

Zur Verbesserung der Antwortzeit wird im Folgenden ein Ansatz basierend auf Marcus et al. [97] vorgestellt. Diese Vorarbeit wird durch eine neu entwickelte Abschätzung der Fehlerschranke in Unterabschnitt 3.3.1 ergänzt.

Der Ansatz erlaubt es, auf Basis der WDF für die Nutzerposition die Aufenthaltswahrscheinlichkeit in der autorisierten Zone zu approximieren. Dabei ist die Annahme, dass eine Berechnung des exakten Werts aufgrund der statistischen Modellierung der WDF nicht erforderlich ist. Es wird ein Katalog aus vorberechneten Matrizen erzeugt, worüber mittels Leseoperationen der Näherungswert ermittelt wird. Die Antwortzeit gegenüber der direkten Berechnung mittels numerischer Integration wird dadurch auf Kosten eines größeren Fehlers erheblich verkürzt. Es wird gezeigt, dass der Näherungswert innerhalb einer Fehlerschranke liegt, die keinen wesentlichen Nachteil für die standortbasierte Autorisierung darstellt.

Im folgenden Unterabschnitt wird zunächst auf die Annahmen des Verfahrens eingegangen. Anschließend wird das entwickelte Konzept der Kachelmatrix als vorberechnete Datenstruktur eingeführt. Das entwickelte Verfahren zur Parkettierung von autorisierten Zonen mit den zugeordneten Kacheln wird detailliert beschrieben. Anschließend wird die Fehlerschranke diskutiert und schließlich in Unterabschnitt 3.3.2 die Laufzeitverbesserung gegenüber der bisherigen Verfahrensweise untersucht.

3.3.1 Effiziente Berechnung der Aufenthaltswahrscheinlichkeiten

Grundlage für die Bestimmung der Aufenthaltswahrscheinlichkeit ist die WDF einer Positionsschätzung (μ, Σ) und wird z.B. durch den in Abschnitt 3.1 beschriebenen Fehlerschätzer bereitgestellt. Hierbei beschreibt $\mu = (\mu_x, \mu_y)$ den Mittelwert und Σ die Kovarianzmatrix.

Die Anwendung des entwickelten Verfahrens wird im Folgenden für Normalverteilungen vorgestellt, ist aber ohne weiteres auf Laplace- oder Gleichverteilungen übertragbar. Wie oben beschrieben, existiert in den vom Fehlerschätzer gelieferten WDFs keine Korrelation zwischen X und Y, wodurch sie eine rotationssymmetrische Visualisierung besitzen.

Im vorliegenden Ansatz wird diese Eigenschaft für eine Vereinfachung des Problems genutzt, indem lediglich der Teil der Verteilung berücksichtigt wird, der innerhalb eines vordefinierten Quantils liegt. Für Normalverteilungen mit einer Kovarianzmatrix $\Sigma = \left(\begin{smallmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{smallmatrix}\right)$ gelten die in Tab. 3.10 aufgeführten und in Abb. 3.11 visualisierten σ–Quantile. Wird im Falle von Normalverteilungen für die Auswertung nur der Teil der WDF berücksichtigt, der innerhalb des 3σ–Quantils liegt, so sind die berechneten Aufenthaltswahrscheinlichkeiten hierdurch maximal mit einem absoluten Fehler von 1,11% behaftet. Dieser ergibt sich aus dem Anteil der WDF, der außerhalb dieses Quantils liegt. Generell ist für den entwickelten Ansatz ein solches $n\sigma$–Quantil zu wählen, so dass die resultierende Fehlerschranke des Verfahrens im tolerierbaren Bereich liegt. Der Verlauf der Verteilung innerhalb des gewählten $n\sigma$–Quantils wird im Folgenden als Ungewissheitsbereich bezeichnet.

σ–Quantil	Anteil innerhalb
1σ	0,39346934
2σ	0,86466472
3σ	0,98889100
4σ	0,99966454

Abbildung 3.10: σ–Quantile der bivariaten, symmetrischen Normalverteilung.

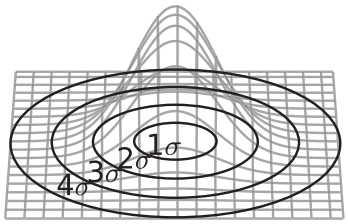


Abbildung 3.11: Visualisierung der σ–Quantile der bivariaten, symmetrischen Normalverteilung.

Gegeben sei nun eine rechteckige autorisierte Zone $\mathcal{Z}$, deren untere linke Ecke die Koordinaten (x_1, y_1) und deren rechte obere Ecke die Koordinaten (x_2, y_2) besitze. Gegeben sei eine WDF $wdf^{normal}_{\mathbf{F}|\mu,\Sigma}(x, y)$ des Normal-Fehlerschätzers. Die Aufenthaltswahrscheinlichkeit $p_{\mathcal{Z}}$ des Nutzers innerhalb von $\mathcal{Z}$ berechnet sich als (adaptiert aus Shin et al. [131]):

$$p_{\mathcal{Z}} = \int_{\max(x_1,\mu_x-n\sigma)}^{\min(x_2,\mu_x+n\sigma)} \int_{\max(y_1,\mu_y-\sqrt{(n\sigma)^2-(x-\mu_x)^2})}^{\min(y_2,\mu_y-\sqrt{(n\sigma)^2-(x-\mu_x)^2})} wdf^{normal}_{\mathbf{F}|\mu,\Sigma}(x, y)\mathrm{d}y\ \mathrm{d}x \tag{3.18}$$

Das im Folgenden vorgestellte Verfahren beruht auf der effizienten Approximation von (3.18). Dazu werden universelle Kachelmatrizen vorberechnet.

Die Berechnung von Kachelmatrizen

Vor der Anwendung des Verfahrens erfolgt die Berechnung einer Menge von Matrizen. Eine solche Matrix wird im Folgenden als Kachelmatrix bezeichnet. Die Vorberechnung einer Kachelmatrix erfolgt stets für eine feste Fehlerschätzung $\sigma \in [0; \infty]$.

Um eine endliche Zahl an Kachelmatrizen zu erhalten, wird zunächst eine Teilmenge $[0; \sigma_{max}]$ bestimmt. Nur für Werte von σ, die in diesem Intervall liegen, wird das Verfahren eine Antwort berechnen können. Für einen Wert σ_{max} lässt sich somit die Antwortwahrscheinlichkeit α des Verfahrens angeben:

$$\alpha = \int_0^{\sigma_{max}} \mathrm{F}_{fehler}(\sigma)\ \mathrm{d}\sigma \tag{3.19}$$

Das entspricht genau der Wahrscheinlichkeit, mit welcher der Fehlerschätzer ein $\sigma \in [0; \sigma_{max}]$ erzeugt. Hierbei stammt F_{fehler} aus Unterabschnitt 3.1.5 und modelliert die Verteilung der Fehlerschätzungen für ein gegebenes Positionierungssystem. Ist ein Wert α einzuhalten, so kann mittels (3.19) das zugehörige σ_{max} ermittelt werden. Mit einer Wahrscheinlichkeit von $1 - \alpha$ wird das entwickelte Verfahren mit einer Positionsschätzung aufgerufen, dessen Fehlerschätzung σ nicht innerhalb dieses Intervalls liegt. In diesem Fall wird auf die herkömmliche direkte Anwendung der numerischen Integration zurückgegriffen.

Mit steigendem σ nimmt die maximal mögliche Aufenthaltswahrscheinlichkeit einer WDF in $\mathcal{Z}$ ab. Sei eine Ortsbeschränkung gegeben, welche fordert, dass die Aufenthaltswahrscheinlichkeit $p_{\mathcal{Z}}$ einen Schwellwert überschreitet. Der kleinste Wert σ, für den keine

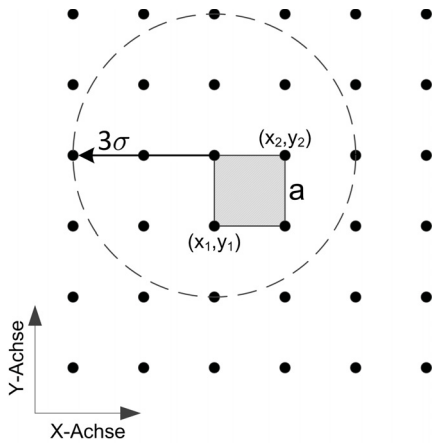


Abbildung 3.12: Eine kleine Kachel mit Seitenlänge a wird in einem Gitter zentriert. Die Gitterkonstante entspricht a.

WDF gefunden werden kann, die den Schwellwert übersteigt, ist eine geeignete Grenze σ_{max}.

Das ermittelte Intervall $[0; \sigma_{max}]$ wird diskretisiert, so dass konkret feststeht, für welche Werte σ eine Kachelmatrix vorberechnet wird. Die Granularität der Diskretisierung ist ein wesentlicher Einflussfaktor für den maximalen absoluten Fehler des Verfahrens.

Im Folgenden wird beschrieben, wie die Kachelmatrix für einen konkreten Wert σ vorberechnet wird. Dazu wird ein Gitter mit Gitterkonstante a eingeführt, wobei die Gitterpunkte als potentielle Werte μ einer Fehlerschätzung betrachtet werden. In dem Gitter ist eine quadratische Kachel mit Seitenlänge a zentriert.

In der Vorberechnung wird nun iterativ um jeden Gitterpunkt μ_i, eine WDF gelegt, z.B. die bivariate Normalverteilung $wdf^{normal}_{\mathbf{F}|\mu,\sigma}(x, y)$. Diese WDF wird jeweils über die Kachel integriert, um die Aufenthaltswahrscheinlichkeit zu erhalten. Die erhaltenen Werte für die einzelnen Gitterpunkte bilden die Einträge der Kachelmatrix. Diese Vorgehensweise ist in Abb. 3.12 visualisiert. Für einen Gitterpunkt ist die verwendete WDF beispielhaft mit ihrem 3σ–Quantil dargestellt, wobei das 3σ–Quantil durch seine Konturlinie dargestellt ist. Die Gitterkonstante a wird unabhängig vom 3σ–Quantil gewählt, so dass in diesem Beispiel $\frac{a}{3\sigma} = \frac{1}{2}$ gilt.

Die Anzahl der Gitterpunkte ist limitiert durch das 3σ–Quantil der WDF. Denn wie oben beschrieben, wird unter Inkaufnahme eines Fehlers nur der Teil der WDF betrachtet, der innerhalb dieses Quantils liegt. Sei eine fiktive Kachel gegeben, deren untere linke Ecke bei (x_1, y_1) und deren rechte obere Ecke bei (x_2, y_2) liegt. Dann sind die Entfernungen der Gitterpunkte auf der X-Achse durch das Intervall $[x_1 - 3\sigma; x_2 + 3\sigma]$ und auf der Y-Achse durch $[y_1 - 3\sigma; y_2 + 3\sigma]$ beschränkt.

Zu beachten ist, dass der Parameter a und somit die Seitenlänge der fiktiven Kacheln nicht beliebig klein gewählt werden können. Denn dann werden auch die Aufenthaltswahrscheinlichkeiten in der Kachel beliebig klein. Somit können ab einer systemabhängigen Grenze arithmetische Unterläufe aufgrund der Fließkommaarithmetik auftreten. Anderer-

seits erlaubt die Wahl einer kleineren Seitenlänge a einen geringeren Fehler aus der Anwendung des Verfahrens.

Für jede Kachelmatrix wird zusätzlich das entsprechende Integralbild (engl. Summed Area Table) berechnet. Dies ist die Grundlage für eine spätere Optimierung des Verfahrens auf konstante Komplexität $\mathcal{O}(1)$. Das Integralbild I ist eine Matrix mit der gleichen Dimensionalität wie die zugehörige Kachelmatrix K. Für ein Element $I(i,j)$ des Integralbildes berechnet sich sein Wert aus der zugehörigen Kachelmatrix: $I(i,j) = \sum_{i'=0}^{i} \sum_{j'=0}^{j} K(i',j')$ [32]. Das Integralbild beschreibt also für jedes Element (i,j) die Summe aller Einträge der Kachelmatrix, deren Indizes kleiner oder gleich i bzw. j sind.

Die Parkettierung von autorisierten Zonen

Liegt im Betrieb eine Positionsschätzung $\left(\mu, \Sigma = \left(\begin{smallmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{smallmatrix}\right)\right)$ vor, so dient das entwickelte Verfahren zur Abschätzung der Aufenthaltswahrscheinlichkeit $p_{\mathcal{Z}}$ des Nutzers innerhalb einer autorisierten Zone $\mathcal{Z}$. Zur Bestimmung von $p_{\mathcal{Z}}$ wird zunächst aus dem Katalog der Kachelmatrizen diejenige ausgewählt, die für das aktuell vorliegende σ vorberechnet wurde. Ist eine solche Kachelmatrix aufgrund der Diskretisierung des Bereichs möglicher Formparameter nicht vorhanden, werden die beiden Kachelmatrizen ausgewählt, die für den nächst größeren und nächst kleineren Formparameter σ_+ bzw. σ_- berechnet wurden. Beide werden als Repräsentanten zur Abschätzung von $p_{\mathcal{Z}}$ verwendet und der Mittelwert aus beiden Abschätzungen als Ergebnis zurückgegeben.

Filterung von Anfragen Aufgrund der Voraussetzung, dass nur der Anteil der Verteilung berücksichtigt wird, der innerhalb des 3σ–Quantils liegt, kann ein Filterschritt erfolgen. Dieser beantwortet Anfragen unmittelbar mit dem Ergebnis 0% sofern die Distanz des Mittelwerts μ der WDF zur Zone $\mathcal{Z}$ auf der X- oder Y-Achse größer gleich 3σ ist. Wie oben beschrieben gilt für den maximalen Fehler hieraus ca. der Wert 1,11%. Für eine rechteckige autorisierte Zone $\mathcal{Z}$ mit unterem linken Eckpunkt (x_1, y_1) und oberem rechten Eckpunkt (x_2, y_2) lautet die Filterbedingung für $i \in \{+, -\}$:

$$\texttt{anfrage\_filtern} \Leftrightarrow \mu_x \leq x_1 - 3\sigma_i \vee \mu_x \geq x_2 + 3\sigma_i \vee \mu_y \geq y_2 + 3\sigma_i \vee \mu_y \leq y_1 - 3\sigma_i \quad (3.20)$$

Nur wenn σ_+ und σ_- den Filter passieren, wird das Verfahren angewandt. Ansonsten wird 0% als Ergebnis zurückgegeben.

Parkettierung mit Kacheln Passiert die Positionsschätzung den Filter, wird das eigentliche Verfahren angewandt. Für jeden der beiden gewählten Formparameter σ_+ und σ_- wird die Aufenthaltswahrscheinlichkeit in $\mathcal{Z}$ basierend auf der zugehörigen Kachelmatrix abgeschätzt.

Grundsätzlich trägt gemäß (3.18) nur der Teil des 3σ–Quantils zum Ergebnis bei, der eine Überlappung mit der autorisierten Zone $\mathcal{Z}$ aufweist. Somit ändert sich die abgeschätzte Aufenthaltswahrscheinlichkeit nicht, wenn $\mathcal{Z}$ auf die Fläche dieser Überlappung verkleinert wird. Entsprechend wird der gleiche Wert für die Abschätzung erhalten, wenn $\mathcal{Z}$ auf das

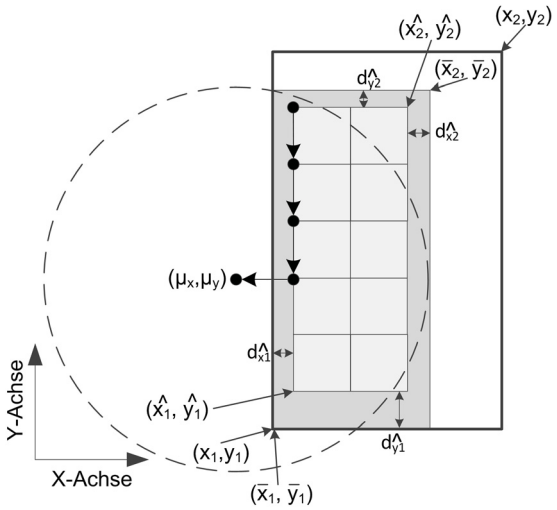


Abbildung 3.13: Eine autorisierte Zone (weiß) und 3σ–Quantil der Fehlerschätzung. Das kleinste umschreibende Rechteck (dunkelgrau) enthält die größte einbeschriebene Parkettierung (hellgrau). Der Vektor $\vec{v_l}$ für die obere linke Kachel ist durch Pfeile skizziert.

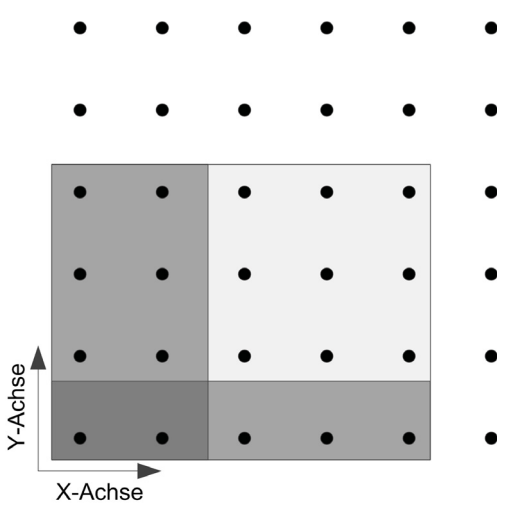


Abbildung 3.14: Visualisierung von (3.26) auf dem Integralbild einer Kachelmatrix. Einzelne Terme der Gleichung sind als farbige Flächen dargestellt.

kleinste umschreibende Rechteck dieser Überlappung reduziert wird. Ein solches Rechteck ist als dunkelgraue Fläche in Abb. 3.13 dargestellt. Dabei besitzt es die linke untere Ecke $(\bar{x_1}, \bar{y_1})$ und die rechte obere Ecke $(\bar{x_2}, \bar{y_2})$. Die linke untere Ecke der zugehörigen autorisierten Zone liegt bei (x_1, y_1) und die rechte obere Ecke bei (x_2, y_2).

Die grundlegende Idee des Verfahrens ist, dieses kleinste umschreibende Rechteck mit jener Kachel zu parkettieren, welche die Grundlage für die Berechnung der gewählten Kachelmatrix ist. Im besten Fall ist die Parkettierung ohne Versatz möglich, so dass die parkettierte Fläche genau der Fläche des kleinsten umschreibenden Rechtecks entspricht. Andernfalls werden zwei Parkettierungen durchgeführt: Die größte Parkettierung, welche der autorisierten Zone noch einbeschrieben ist, sowie die kleinste Parkettierung, welche die autorisierte Zone überlappt. Erstere wird $p_{\mathcal{Z}}$ unter- und letztere überschätzen. In Abb. 3.13 ist die kleinste Parkettierung dargestellt, die dem minimal umgebenden Rechteck noch einbeschrieben ist. Sie besitzt die linke untere Ecke $(\hat{x_1}, \hat{y_1})$ und die rechte obere Ecke $(\hat{x_2}, \hat{y_2})$. Zum linken Rand des minimal umgebenden Rechtecks besteht der Versatz $d_{\hat{x_1}}$, zum rechten Rand $d_{\hat{x_2}}$. Nach unten beträgt der Versatz $d_{\hat{y_1}}$ und nach oben $d_{\hat{x_2}}$. Ausgangspunkt ist hierbei eine WDF für die Position des Nutzers mit einem Mittelwert $\mu = (\mu_x, \mu_y)$ und Kovarianzmatrix $\Sigma = \left(\begin{smallmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{smallmatrix}\right)$. Die Seitenlänge der verwendeten fiktiven Kacheln sei a.

Die größte, der autorisierten Zone noch einbeschriebene Parkettierung wird konstruiert, indem zunächst die untere linke Kachel k in das Rechteck eingepasst wird. Die Lage dieser Kachel wird bestimmt, so dass die Entfernung aller ihrer Ecken zum Mittelwert μ sowohl

auf der X- als auch der Y-Achse jeweils ein Vielfaches von a ist. Iterativ wird nun eine weitere Kachel rechts angehängt, sofern diese noch innerhalb des Rechtecks liegt. Die linke Kachel der darüber liegenden Zeile wird direkt oberhalb der Kachel k gelegt. Diese Reihe wird dann entsprechend zur ersten Reihe iterativ vervollständigt. Dieser Prozess wird solange wiederholt, bis keine weitere Kachel mehr in das kleinste umschreibende Rechteck eingepasst werden kann.

Die kleinste noch überlappende Parkettierung wird erhalten, indem an jeder Seite eine weitere Reihe an Kacheln ergänzt wird, so dass diese das kleinste umschreibende Rechteck überlappen.

Aufenthaltswahrscheinlichkeit aus Parkettierung Sowohl die überschätzende, als auch die unterschätzende Parkettierung besteht aus einzelnen Kacheln l_i und deckt insgesamt jeweils eine Fläche $\bigcup_i l_i$ ab. Für beide Parkettierungen wird im nächsten Schritt die Aufenthaltswahrscheinlichkeit $\mathrm{P}(\bigcup_i l_i)$ des Nutzers in der zugehörigen parkettierten Fläche $\bigcup_i l_i$ ermittelt. Dieser Wert entspricht der Summe der einzelnen Wahrscheinlichkeiten $\mathrm{P}(l_i)$:

$$\sum_i \mathrm{P}(l_i) = \mathrm{P}(\bigcup_i l_i) \tag{3.21}$$

Dies folgt unmittelbar daraus, dass jedes $\mathrm{P}(l_i)$ basierend auf (3.18) berechnet wird. Jedes einzelne $\mathrm{P}(l_i)$ wird nun aus der zugrundeliegenden Kachelmatrix ausgelesen.

Zum Finden des entsprechenden Eintrags in der Kachelmatrix wird für jede Kachel l_i der Parkettierung ein Vektor $\vec{v_{l_i}}$ berechnet. Dessen Komponenten beschreiben den Quotienten aus *1)* der X- bzw. Y-Distanz der oberen linken Ecke dieser fiktiven Kachel l_i zum Mittelwert μ der Fehlerschätzung und *2)* der Gitterkonstante a. Die errechneten Quotienten sind stets ganze Zahlen, da aufgrund der oben beschriebenen Parkettierung die Distanzen auf der X- und Y-Achse jeweils Vielfache von a sind. Wird in der Kachelmatrix der Index des Gitterpunktes bestimmt, der in der Vorberechnung die obere linke Ecke der fiktiven Kachel markiert hat, so kann durch Anwendung von $\vec{v_{l_i}}$ auf diesen Index der Index des für $\mathrm{P}(l_i)$ passenden Elements in der Kachelmatrix erhalten werden. Somit lassen sich die Einzelwerte $\mathrm{P}(l_i)$ erhalten und in (3.21) zur Berechnung von $\mathrm{P}(\bigcup_i l_i)$ anwenden.

Bezogen auf das Beispiel in Abb. 3.13 ergibt sich für die obere linke Kachel der Parkettierung der Vektor $\vec{v_{l_i}} = (-3, -1)$. Zur Bestimmung von $\mathrm{P}(l_i)$ muss zunächst der Index in der Kachelmatrix bestimmt werden, dessen entsprechender Gitterpunkt bei der Vorberechnung auf der oberen linken Ecke der zentrierten fiktiven Kachel platziert war, wie oben in Abb. 3.12 dargestellt. Der gesuchte Wert $\mathrm{P}(l_i)$ ergibt sich durch Anwenden von $\vec{v_{l_i}}$ auf diesen Index und entspricht dem Element in der Kachelmatrix, das drei Zeilen unterhalb und eine Spalte links von diesem Index liegt.

Sowohl für den auf- als auch den abgerundeten Formparameter σ_+ bzw. σ_- wird das Aufsummieren der $\mathrm{P}(l_i)$ jeweils für die kleinste einbeschriebene und die größte umschreibende Parkettierung durchgeführt, so dass vier Werte $p_\perp^{\sigma_-}$, $p_\perp^{\sigma_+}$, $p_\top^{\sigma_-}$ und $p_\top^{\sigma_+}$ erhalten werden. Das Symbol $\perp$ soll hierbei für die größte einbeschriebene Parkettierung stehen und $\top$ entsprechend für die kleinste umschreibende Parkettierung. Als Ergebnis für die Berechnung auf

der gewählten Kachelmatrix für σ_- bzw. σ_+ wird schließlich der Mittelwert $p_- = \frac{p_\perp^{\sigma_-} + p_\top^{\sigma_-}}{2}$ bzw. $p_+ = \frac{p_\perp^{\sigma_+} + p_\top^{\sigma_+}}{2}$ zurückgegeben. Die endgültige Abschätzung berechnet sich schließlich als $0{,}5 \cdot (p_+ + p_-)$.

Ist die größte einbeschriebene bzw. die kleinste überlappende Parkettierung gegeben, so stammen die einzelnen Werte $\mathrm{P}(l_i)$, die aus der Kachelmatrix zur Berechnung von $\mathrm{P}(\bigcup_i l_i)$ ausgelesen werden, aus einer Teilmatrix. Diese umfassen den Bereich von $spalte_{start}$ bis $spalte_{ende}$ und von $reihe_{start}$ bis $reihe_{ende}$ der Kachelmatrix. Formal berechnen sich diese verwendeten Indizes für die größte einbeschriebene Parkettierung mit Versatz $d_{\hat{x_1}}$ nach links, $d_{\hat{x_2}}$ nach rechts, $d_{\hat{y_1}}$ nach unten und $d_{\hat{y_2}}$ nach oben, folgendermaßen:

$$spalte_{start} = (n\sigma + (\hat{x_1} - \mu_x)) \text{ div } a \tag{3.22}$$
$$spalte_{ende} = (n\sigma + (\hat{x_2} - a - \mu_x)) \text{ div } a \tag{3.23}$$
$$reihe_{start} = (n\sigma + (\hat{y_1} - \mu_y)) \text{ div } a \tag{3.24}$$
$$reihe_{ende} = (n\sigma + (\hat{y_2} - a - \mu_y)) \text{ div } a \tag{3.25}$$

Hierbei bezeichnet div die Division mit Rest. Die Indizes für die kleinste umschreibende Parkettierung ergeben sich direkt aus diesen Indizes durch Vergrößerung bzw. Verkleinerung um 1.

Laufzeitverbesserung durch Integralbilder Die Anzahl der Anfragen an eine Kachelmatrix und der durchzuführenden Additionen hängt somit von der Größe des kleinsten umschreibenden Rechtecks und dem Parameter a ab. Durch die oben bereits eingeführten Integralbilder kann das Verfahren jedoch derart optimiert werden, dass eine konstante Komplexität von $\mathcal{O}(1)$ erreicht wird. Ausgehend von der Darstellung als Integralbild ergibt sich die Aufenthaltswahrscheinlichkeit innerhalb der parkettierten Fläche als:

$$\mathrm{P}(\bigcup_i l_i) = I(spalte_{ende}, reihe_{ende}) + I(spalte_{start}, reihe_{start}) - I(spalte_{start}, reihe_{ende}) - I(spalte_{ende}, reihe_{start}) \tag{3.26}$$

Die hierbei verwendeten Indizes bezeichnen genau die Indizes der 4 Elemente der Kachelmatrix, welche die Grenzen der herangezogenen Teilmatrix beschreiben. Dieses Konzept wird in Abb. 3.14 zusätzlich für die Werte $spalte_{start} = 2$ bis $spalte_{ende} = 4$ und $reihe_{start} = 1$ bis $reihe_{ende} = 3$ verdeutlicht.

Die bei diesem Verfahren auftretenden Fehler hängen maßgeblich von den gewählten Parametern a, $n\sigma$ und der Diskretisierung des Intervalls $[0; \sigma_{max}]$ ab. Die Abschätzung der entstehenden Berechnungsfehler ist Voraussetzung für die praktische Anwendung.

Abschätzung von Berechnungsfehlern

Im Folgenden werden theoretische Konzepte zur Abschätzung einer Fehlerschranke des vorgeschlagenen Algorithmus vorgestellt und diskutiert. Insgesamt hängen die auftretenden Fehler von folgenden Parametern ab:

- Genauigkeit der Vorberechnung in den Kachelmatrizen
- Fehler durch unter- oder überschätzende Parkettierung
- Fehler durch Rundung auf Radius einer verfügbaren Kachelmatrix
- Fehler durch ausschließliche Betrachtung des $n\sigma$–Quantils

Im Folgenden wird die Herleitung des maximalen Fehlers des Verfahrens beschrieben, der bei Anwendung auf die WDF einer konkreten Positionsschätzung (μ, Σ) entstehen kann.

Abschätzung der Fehler Wie oben beschrieben, werden während der Abschätzung der Aufenthaltswahrscheinlichkeit vier Werte anhand der Einträge in den Kachelmatrizen bestimmt:

- $p_{\perp}^{\sigma_-}$: Berechnung basierend auf σ_-, dem zu σ nächst kleineren Formparameter für den eine Kachelmatrix vorliegt und der unterschätzenden (größten einbeschriebenen) Parkettierung.
- $p_{\top}^{\sigma_-}$: Berechnung basierend auf σ_- für die überschätzende (kleinste überlappende) Parkettierung.
- $p_{\perp}^{\sigma_+}$: Berechnung basierend auf σ_+, dem zu σ nächst größeren Formparameter für den eine Kachelmatrix vorliegt und der unterschätzenden (größten einbeschriebenen) Parkettierung.
- $p_{\top}^{\sigma_+}$: Berechnung basierend auf σ_+ für die überschätzende (kleinste überlappende) Parkettierung.

Der kleinste dieser berechneten Werte ist $p_{min} = \min\left(\{p_{\perp}^{\sigma_-}, p_{\top}^{\sigma_-}, p_{\perp}^{\sigma_+}, p_{\top}^{\sigma_+}\}\right)$ und der größte entsprechend p_{max}. Für die Berechnung eines jeden $p_i \in \{p_{\perp}^{\sigma_-}, p_{\top}^{\sigma_-}, p_{\perp}^{\sigma_+}, p_{\top}^{\sigma_+}\}$ ergibt sich ein Fehler aufgrund der Genauigkeit der Vorberechnung in der verwendeten Kachelmatrix. Jedes p_i berechnet sich, wie oben erläutert, als Summe einer Teilmatrix der Kachelmatrix bzw. über ihr Integralbild. Die hierbei aufsummierten Werte wurden bei der Vorberechnung der Kachelmatrix über Verfahren der numerischen Integration jeweils mit einer dafür festgelegten absoluten Fehlerschranke ϵ_K vorberechnet. Der insgesamt entstehende Fehler ϵ_i für p_i ist direkt proportional zur Anzahl der aufsummierten Werte aus der Kachelmatrix und somit zur Anzahl der verwendeten Kacheln in der Parkettierung. Die aus ungenauen Vorberechnungen entstehende Fehlerschranke für p_{min} sei ϵ_{min} und die für p_{max} entsprechend ϵ_{max}.

Bei der Berechnung eines jeden p_i wurde nur das $n\sigma$–Quantil der WDF betrachtet, wodurch die Werte p_i höchstens um die Wahrscheinlichkeit $\epsilon_{n\sigma}$ zu klein sein können, die auf den Bereich außerhalb des $n\sigma$–Quantils entfällt. Dieser Fehler $\epsilon_{n\sigma}$ ergibt sich entsprechend Tab. 3.10.

Für den gesuchten Sollwert $p_{\mathcal{Z}}$ muss gelten:

$$p_{min} - \epsilon_{min} \leq p_{\mathcal{Z}} \leq p_{max} + \epsilon_{max} + \epsilon_{n\sigma} \tag{3.27}$$

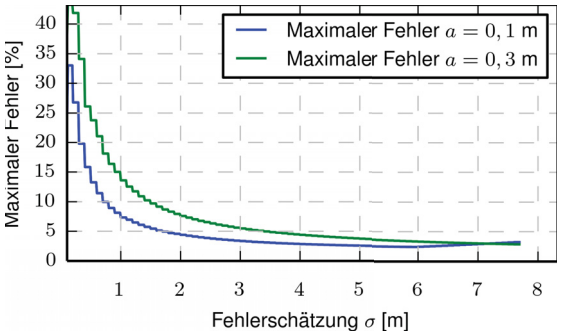


Abbildung 3.15: Der mögliche Beitrag einer über- bzw. unterschätzenden Parkettierung zum Gesamtfehler für Kachelmatrizen mit $a = 0{,}1$ m und $a = 0{,}3$ m und einer Normalverteilung aus der Positionsfehlerschätzung.

Vor der Anwendung des Verfahrens muss eine Aussage getroffen werden, ob die gewählten Parameter für die vorberechneten Kachelmatrizen ausreichend genaue Ergebnisse liefern, d.h. für die Anwendung mit dem zugrundeliegenden Schätzer von Positionsfehlern geeignet sind. Dazu muss der maximale Fehler ermittelt werden, der unter Verwendung der vorberechneten Kachelmatrizen prinzipiell möglich ist.

Analyse der maximalen Fehler Bisher wurde betrachtet, wie sich das Fehlerintervall und somit der maximale Fehler für eine konkrete WDF berechnet. Bei WDFs mit gleicher Kovarianzmatrix ergibt sich, abhängig von deren Mittelwert μ, jeweils ein anderes Fehlerintervall. Im Folgenden wird vorgestellt, wie sich der maximale Fehler berechnet, der für eine WDF mit Kovarianzmatrix $\Sigma = \left(\begin{smallmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{smallmatrix}\right)$ unter Verwendung der vorberechneten Kachelmatrizen auftreten kann.

Zur Analyse des maximalen Fehlers einer WDF mit fixer Kovarianzmatrix $\Sigma = \left(\begin{smallmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{smallmatrix}\right)$ aber unabhängig von μ, wird zunächst σ_- und σ_+ bestimmt. Anschließend werden aus dem Katalog die zugehörigen Kachelmatrizen K_{σ_-} und K_{σ_+} herangezogen. Auf diesen Kachelmatrizen werden alle prinzipiell möglichen 4–Tupel $(p_\perp^{\sigma_-}, p_\top^{\sigma_-}, p_\perp^{\sigma_+}, p_\top^{\sigma_+})$ berechnet, die bei der Anwendung des Verfahrens mit dieser Kachelmatrix auftreten können. Für jedes dieser Tupel wird das Fehlerintervall gemäß (3.27) bestimmt. Aus allen erhaltenen Fehlerintervallen für dieses σ wird schließlich das insgesamt größtmögliche ermittelt.

Zur Verdeutlichung der Größe der auftretenden Fehler wird diese Analyse auf zwei unterschiedlichen Katalogen von Kachelmatrizen durchgeführt, für die jeweils $a = 0{,}1$ m und $a = 0{,}3$ m festgelegt ist. Für das verwendete σ–Quantil gilt $n = 3$ und die Genauigkeit in der Vorberechnung der Kachelmatrizen unterliegt der Fehlerschranke $\epsilon_K = 0{,}1 \cdot 10^{-8}$. Die Ergebnisse sind in Abb. 3.15 dargestellt. Dort ist der maximale absolute Fehler der berechneten Aufenthaltswahrscheinlichkeit in Abhängigkeit von σ angetragen.

Die abgestufte Form ergibt sich aus der Tatsache, dass zur Auswertung einer Fehlerschätzung σ die Kachelmatrizen mit auf- und abgerundetem σ_- bzw. σ_+ verwendet werden. Eine Stufe zwischen zwei Fehlerschätzungen entsteht somit immer dann, wenn dazu ein unterschiedliches Paar σ_- bzw. σ_+ gewählt wird.

Für einen auf einer Kachel mit fester Seitenlänge a basierenden Katalog aus Kachelmatrizen zeigt sich, dass der maximale Fehler mit steigendem σ abnimmt. Dies liegt daran, dass mit steigendem σ die einzelnen Werte in der Kachelmatrix betragsmäßig kleiner werden und somit nur ein kleinerer Fehler durch den entstehenden Versatz aus der größten einbeschriebenen und der kleinsten umschreibenden Parkettierung entstehen kann. Der maximale Fehler konvergiert nicht gegen $\epsilon_{n\sigma}$, da mit steigendem σ die entsprechenden Kachelmatrizen auch mehr Einträge enthalten. Jeder Eintrag unterliegt einem Fehler von $\epsilon_K = 0{,}1 \cdot 10^{-8}$, weshalb der maximale Fehler mit größerem σ wieder zu steigen beginnt, nachdem er ein Minimum durchlaufen hat.

Beim Vergleich der zwei vorberechneten Kataloge von Kachelmatrizen mit $a = 0{,}1$ m und $a = 0{,}3$ m zeigt sich, dass die Vorberechnung auf kleineren Kacheln tendenziell kleinere Fehler liefert. Somit ist mit dem Katalog von $a = 0{,}1$ m und Fehlerschätzungen mit 1,0 m $\leq \sigma \leq$ 7,0 m eine Abschätzung von Aufenthaltswahrscheinlichkeiten mit einem maximalem Fehler von 7% möglich, der für $\sigma \geq 1{,}80$ m sogar unter 5% fällt. Ein solcher maximaler Fehler liegt entsprechend Abschnitt 3.1 im Toleranzbereich des zugrundeliegenden Fehlerschätzers.

Generell ist zu sagen, dass der tatsächliche Fehler deutlich geringer als der maximale Fehler ausfällt. Denn die einzelnen Ergebnisse in der Kachelmatrix können einen kleineren Fehler als ϵ_K besitzen, der Fehler aus $\epsilon_{n\sigma}$ kann nur bei konkaven autorisierten Zonen voll zum Tragen kommen und der maximale Fehler aus dem Versatz von ein- und umschreibender Parkettierung tritt nur als Spezialfall auf.

3.3.2 Evaluation

Dieser Unterabschnitt zeigt die Performanz des vorgestellten Algorithmus im Vergleich zur direkten Anwendung von numerischer Integration zur Berechnung von Aufenthaltswahrscheinlichkeiten aus Ungewissheitsbereichen. Als Vergleichsbasis wird die *dblquad*-Funktion aus SciPy 0.11.0rc2 mit Numpy 1.6.2 und Python 2.7 auf einer Intel Xeon CPU X5650 mit 2,67GHz und 8GB RAM herangezogen.

Für die Evaluation werden als autorisierte Zonen alle benannten Bereiche aus Abb. 3.1(a) und die Fingerprint-Datenbank aus Abb. 3.1(b) verwendet. Als mögliche Positionsschätzungen werden die Testdaten aus Abb. 3.1(c) verwendet, wobei hier der Normal-Fehlerschätzer angewandt wird. Jeder Positionsschätzung wird zufällig eine der autorisierten Zonen zugewiesen und die Aufenthaltswahrscheinlichkeit mittels *dblquad* und des vorgestellten Verfahrens bestimmt. Dabei wurden Kachelmatrizen mit $a = 0{,}1$ m verwendet und der maximale absolute Fehler aus den Werten der Abb. 3.15 ermittelt. Dieser Wert wird auch in *dblquad* als maximaler absoluter Fehler festgelegt.

In Abb. 3.16 ist der Faktor angetragen, um den die Laufzeit durch das entwickelte Verfahren gegenüber *dblquad* reduziert werden kann. Dieser Faktor ist abhängig vom maximalen absoluten Fehler der Berechnung, also dem Betrag, mit dem die Aufenthaltswahrscheinlichkeit maximal über- oder unterschätzt wird. Für die beschriebene Evaluation liegt der Faktor der Laufzeitverbesserung zwischen 150 und ca. 350. Der Grund dieses Verhaltens ist, dass die Laufzeit von *dblquad* massiv zunimmt, wenn eine genaue Berechnung

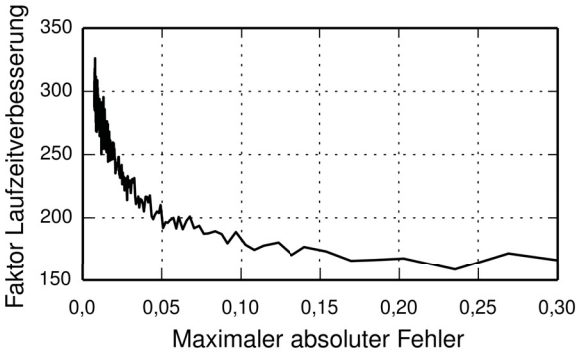


Abbildung 3.16: Zusammenhang der Laufzeitverbesserung gegenüber *dblquad* in Abhängigkeit vom auftretenden maximalen Fehler im beschriebenen Szenario.

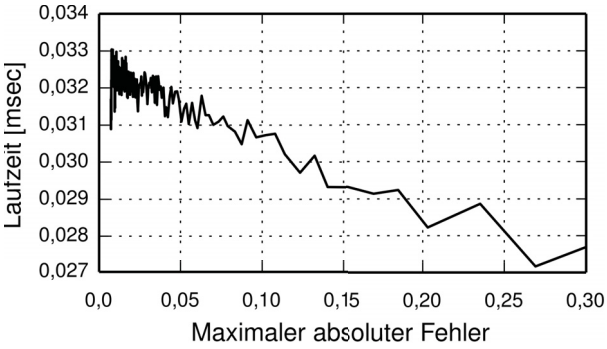


Abbildung 3.17: Die Laufzeit des vorgeschlagenen Verfahrens in Abhängigkeit vom maximalen absoluten Fehler im beschriebenen Szenario.

verlangt wird. Das vorgestellte Verfahren erlaubt somit eine erhebliche Verbesserung der Antwortzeiten von Systemen zur standortbasierten Autorisierung, die jedoch mit einem erhöhten Speicherbedarf einhergeht.

Trotz der theoretischen Komplexität von $\mathcal{O}(1)$ wirkt sich in der Praxis die Größe der verwendeten Kachelmatrix auf die Laufzeit des Verfahrens aus. Die Laufzeit des entwickelten Verfahrens ist in Abb. 3.17 dargestellt. Der Ansatz konnte Anfragen mit einer Verzögerung von 0,027 msec bis 0,033 msec beantworten. Die Ursache der Zunahme der Laufzeit bei kleiner werdendem absolutem Fehler wird klar, wenn nochmals Abb. 3.15 betrachtet wird. Hier zeigt sich, dass mit steigendem σ der absolute Fehler abnimmt. Kleine absolute Fehler werden also unter Verwendung von Kachelmatrizen erreicht, die für ein großes σ berechnet wurden. Die Anzahl der Elemente einer Kachelmatrix hängt, gemäß oben beschriebener Konstruktion, von 3σ ab. Da das verwendete Numpy–Paket aufgrund interner Implementierungsdetails mit größer werdenden Matrizen langsamer wird, steigt in dieser Implementierung auch die Antwortzeit des Verfahrens.

3.3.3 Diskussion

Um die Ungewissheit aus auftretenden Positionsfehlern in der standortbasierten Autorisierung zu berücksichtigen, ist die Aufenthaltswahrscheinlichkeit des Nutzers innerhalb der autorisierten Zone ein zentrales Maß. Ihr Wert wird durch numerische Integration einer WDF für den Standort des Nutzers über die autorisierte Zone ermittelt. In existierenden Ansätzen wird diese Berechnung für jede Anfrage ausgeführt und lediglich durch Filter eingegrenzt. Die Anwendung dieser Integration ist aber sehr rechenintensiv und führt zu hohen Antwortzeiten. In dem vorgestellten Algorithmus wird die numerische Integration aber im Vorfeld durchgeführt, so dass zur Laufzeit lediglich Leseoperationen auf Kachel-

matrizen nötig werden. Zur Vorberechnung der Kachelmatrizen wird das Intervall von Fehlerschätzungen ermittelt, deren WDF noch genügend Aufenthaltswahrscheinlichkeit in der autorisierten Zone besitzen kann, so dass der Nutzer autorisiert wird. Dieses Intervall wird diskretisiert und für die erhaltenen Werte von Fehlerschätzungen jeweils eine Kachelmatrix vorberechnet. Diese speichert für jeden Punkt eines definierten Gitters die Aufenthaltswahrscheinlichkeit innerhalb einer kleinen fiktiven Kachel, die in diesem Gitter zentriert liegt. Während der Auswertung werden relevante Bereiche der autorisierten Zone mit der fiktiven Kachel parkettiert. Die Wahrscheinlichkeit, mit der sich der Nutzer innerhalb der parkettierten Fläche befindet, wird durch eine Sequenz von Leseoperationen auf den vorberechneten Kachelmatrizen ermittelt. Der Algorithmus wurde zu einer konstanten Komplexität $\mathcal{O}(1)$ verbessert, indem die Integralbilder der Kachelmatrizen verwendet werden.

Der vorgestellte Algorithmus zeigt erhebliche Verbesserungen der Antwortzeiten um den Faktor 150–350 gegenüber der direkten Anwendung von numerischer Integration. Es wurde gezeigt, dass der absolute maximale Fehler der berechneten Aufenthaltswahrscheinlichkeit maximal 7% beträgt, sofern die Fehlerschätzung im Intervall von 1,0 m bis 7,0 m liegt. Der Fehler kann grundsätzlich auf Kosten von erhöhtem Speicherbedarf an die Anforderungen des Anwendungsszenarios angepasst werden. Insgesamt erlaubt das vorgestellte Verfahren also einen anwendbaren Kompromiss aus maximalem Gesamtfehler und benötigter Antwortzeit.

3.4 Kopplung von Nutzern und mobilen Endgeräten

Bisher wurde die Ungenauigkeit im Prozess der Messung als Ursache für Positionsfehler betrachtet. Soll jedoch die Position des Nutzers bestimmt werden und nicht die Position des Endgeräts, entsteht ein Problem, wenn der Nutzer das Endgerät nicht in seinen eigenen Händen hält. Die standortbasierte Autorisierung ist davon betroffen, wenn ein Nutzer, nachdem ihm ein Zugriffsrecht gewährt wurde, sein mobiles Endgerät an einen unberechtigten Dritten weiterreicht. Dies hat zur Konsequenz, dass die Autorisierung während der kontinuierlichen Nutzung nicht anhand der Position des betrachteten Nutzers bzw. Subjekts, sondern anhand der Position eines Dritten erfolgt. In einem Szenario in einer modernen Fabrik kann so die Situation entstehen, dass der Sicherheitsbeauftragte auf seinem mobilen Endgerät autorisiert wird, eine Maschine zu steuern. Gibt er dieses an einen anderen, unqualifizierten Benutzer weiter, um selbst z.B. kurz im Nebenraum Pause zu machen, wäre das Zugriffsrecht weiterhin gewährt. Von dem unqualifizierten Benutzer geht jedoch im Ernstfall eine Gefahr aus, da er nicht geschult ist, um auf Notfälle an der zu steuernden Maschine zu reagieren.

Positionsfehler entstehen also auch dann, wenn der vermutete Nutzer eines mobilen Endgeräts dieses selbst gar nicht in den Händen hält. Um dies aber sicherzustellen, muss der Nutzer kontinuierlich während der gesamten Nutzungsdauer eines gewährten Zugriffsrechts authentifiziert werden. Dabei ist es wichtig, dass die Authentifizierung implizit im Hintergrund stattfindet, damit der Nutzer bei der Arbeit mit dem mobilen Endgerät nicht

abgelenkt wird. Grundsätzlich gibt es drei Arten zur Authentifizierung: spezifisches Wissen, Besitz oder körperliche Merkmale. Bei der Authentifizierung mittels spezifischen Wissens muss der Nutzer dieses Wissen aktiv in einem Challenge-Response-Verfahren beweisen, weshalb eine implizite, kontinuierliche Authentifizierung damit nicht möglich ist [49]. Ein Beispiel sind die klassischen Passworteingaben. Bei der Authentifizierung mittels Besitz besteht die Gefahr, dass der Besitz zusammen mit dem mobilen Endgerät gestohlen oder unberechtigt weitergegeben wird. Davon ist auch die erwähnte Authentifizierung mittels spezifischen Wissens betroffen. Eine Lösung des Problems ist die Anwendung von biometrischen Authentifizierungsverfahren, wobei ein Nutzer auf Basis der Eigenheiten seiner körperlichen Merkmale oder seines Verhaltens identifiziert wird. Für die Erfassung dieser Eigenheiten bringen moderne mobile Endgeräte mit ihren integrierten Sensoren die nötige Voraussetzung mit [16]. Dadurch wird es möglich, ohne aktives Zutun des Nutzers zu erkennen, ob er sein mobiles Endgerät noch selbst in der Hand hält, oder ob es z.B. abgelegt, gestohlen oder weitergegeben wurde. Dies ist die Grundlage, um standortbasierte Autorisierung korrekt durchzusetzen, wenn die verwendeten Positionsschätzungen unter Beteiligung des mobilen Endgeräts entstehen.

In der standortbasierten Autorisierung steht durch die autorisierte Zone einer Ortsbeschränkung und dem Zugriffsrecht implizit im Vorfeld fest, an welchen Orten eine gewährte Operation genutzt wird und wie dabei die Eingabe am mobilen Endgerät erfolgt. Aus den Eigenschaften der Orte und der Art der Operation ergeben sich Rahmenbedingungen für die Anwendung biometrischer Authentifizierungsverfahren. Beispielsweise darf die gewählte autorisierte Zone keine lauten Störgeräusche besitzen, um dort die Stimme des Nutzer zu erkennen. Wird die Operation stationär ausgeführt, macht eine Identifizierung über die Gangart keinen Sinn. Ebenso gilt, dass das biometrische Authentifizierungsverfahren sehr energieeffizient arbeiten muss, wenn die Operation über einen langen Zeitraum verwendet wird. Es ist daher eine systematische Aufstellung erforderlich, welche Anforderungen sich durch die standortbasierte Autorisierung für biometrische Authentifizierungsverfahren ergeben. Im Rahmen einer gemeinsamen Vorarbeit [141] mit Matthias Trojahn wurde dazu ein Katalog aus Anforderungen entwickelt, die ein biometrisches Authentifizierungsverfahren beim Einsatz in Verbindung mit standortbasierter Autorisierung erfüllen muss. Existierende Verfahren wurden in einer Literaturrecherche auf diese Anforderungen hin untersucht. Im Folgenden wird eine starke Überarbeitung dieser Konzepte vorgestellt, wobei insbesondere mit der Energieeffizienz und der Reaktionsgeschwindigkeit zwei neue Anforderungen aufgenommen werden, sowie die Messbarkeit und Sensitivität aufgrund zu unscharfer Abgrenzung zur Anwendbarkeit und der Transparenz entfernt werden. Die Literaturrecherche wird auf den neuesten Stand der Technik aktualisiert und bezüglich des geänderten Anforderungskatalogs überarbeitet.

Dazu werden zunächst in Unterabschnitt 3.4.1 die grundlegenden Konzepte der biometrischen Authentifizierung auf mobilen Endgeräten und Smartphones erläutert. In Unterabschnitt 3.4.2 wird daraufhin der überarbeitete Anforderungskatalog an biometrische Authentifizierungsverfahren vorgestellt. In Unterabschnitt 3.4.3 werden in der Literatur vorgestellte biometrische Authentifizierungsverfahren für Smartphones gegen den Anforderungskatalog untersucht und ihre Anwendbarkeit in Verbindung mit standortbasierter

Autorisierung bewertet. In Unterabschnitt 3.4.4 wird an zwei Fallbeispielen die Anwendung des Anforderungskatalogs demonstriert und die Vor- und Nachteile der untersuchten Verfahren diskutiert. Abschließend fasst Unterabschnitt 3.4.5 die gewonnenen Erkenntnisse zusammen.

3.4.1 Grundlagen zur biometrischen Authentifizierung

Der Prozess der biometrischen Authentifizierung gegenüber einem System besteht aus vier Schritten [49]: Der Datenerfassung, der Vorverarbeitung der Daten, der Extraktion von Merkmalen aus den Daten und der Klassifikation basierend auf extrahierten Merkmalen.

Zunächst werden die Daten durch die Sensoren des Smartphones erfasst und durch Filterverfahren von Rauschen befreit. Im nächsten Schritt werden Merkmale aus den Daten extrahiert, so dass physische Eigenheiten einzelner Personen mit einer hohen Diversität erkennbar sind. Geeignete Merkmale sind Eigenschaften der Gangart, die Sprechweise, die Tastenanschläge pro Zeiteinheit, die Geradheit von gezeichneten Linien oder der Druck auf die Tasten [75,88,92]. Im Schritt der Klassifikation verwendet das System die extrahierten Merkmale, um den Nutzer zu authentifizieren. Dazu wird ein Abgleich mit einer Datenbasis durchgeführt, in der die Merkmalsausprägungen der bekannten Nutzer abgelegt sind. Die Authentifizierung ist erfolgreich, wenn die Gewissheit des Systems über die Identität der Person einen vordefinierten Schwellwert überschreitet.

Die verwendete Datenbasis wird im Vorfeld der Ausbringung des Systems in einer separaten Phase erstellt. Die betrachteten biometrischen Eigenheiten einer Person werden dabei mehrmals durch Sensoren abgetastet, vorverarbeitet und für die Berechnung von Merkmalen verwendet. Die Merkmale werden schließlich mit einer Zuordnung zur Person in der Datenbasis abgelegt. Ein Problem der Datenerfassung in dieser Phase ist, dass die biometrischen Eigenheiten der Personen zeitlich nicht konstant sind und somit beim Betrieb des Systems Uneindeutigkeiten auftreten. Beispielsweise hängen die abgespeicherten persönlichen Eigenheiten stark von der gegenwärtigen Verfassung, dem Alter oder der Umgebung ab. Dies erschwert die Identifikation z.B. auf Basis der Anzahl der Rechtschreibfehler oder der Unterschrift einer Person [149].

Im Betrieb des Systems hat dies zur Folge, dass Authentifizierungsversuche gelegentlich ein falsches Ergebnis liefern. Dabei werden zwei Fehlerarten unterschieden: Die Falschrückweisung und die Falschakzeptanz. Die Charakterisierung eines Systems erfolgt zum Einen über die Falschrückweisungsrate, engl. False Rejection Rate (FRR), welche den erwarteten Anteil der fehlschlagenden Authentisierungsversuche einer zuvor erfassten Person im Verhältnis zu allen ihren Authentisierungsversuchen beschreibt [49]. Zum Anderen beschreibt die Falschakzeptanzrate, engl. False Acceptance Rate (FAR), die Wahrscheinlichkeit, mit der eine fremde, nicht zuvor im System erfasste Person fälschlicherweise erfolgreich authentifiziert wird [49]. Wird der oben erwähnte Schwellwert so eingestellt, dass FAR und FRR gleich sind, spricht man von der Gleichfehlerrate des Systems, engl. Equal Error Rate (EER) [49]. Ihr Wert wird typischerweise verwendet, um biometrische Authentifizierungssysteme zu vergleichen.

Aufgrund der Unzuverlässigkeit einzelner biometrischer Merkmale werden zur Authen-

tifizierung oftmals mehrere Merkmale gleichzeitig verwendet. Man spricht dann von einer Fusion von einzelnen Authentifizierungsverfahren und erzielt in der Regel deutlich bessere Ergebnisse [128].

3.4.2 Anforderungen an Authentifizierungsverfahren

In diesem Unterabschnitt wird ein Katalog von Anforderungen an biometrische Authentifizierungsverfahren vorgestellt, die in Verbindung mit der standortbasierten Autorisierung auf Smartphones gelten. Grundsätzlich muss das System dabei kontinuierlich sicherstellen, dass sich der Nutzer innerhalb der autorisierten Zone befindet, während er ein gewährtes Zugriffsrecht nutzt. Es muss daher kontinuierlich überprüft werden, ob der Standort des Smartphones mit dem Standort des eingeloggten Nutzers übereinstimmt. Diese Bedingung wird verletzt, sobald der Nutzer das Smartphone aus den Händen legt. Um diese Situation zu erkennen, eignet sich die kontinuierliche biometrische Authentifizierung.

Damit der Nutzer bei der Arbeit mit dem gewährten Zugriffsrecht nicht gestört wird, muss die Authentifizierung implizit erfolgen. Mittels Wissen ist dies jedoch nicht möglich und die Authentifizierung mittels Besitz hat den Nachteil, dass der Besitz zusammen mit dem Smartphone weitergegeben werden kann. Deshalb kommen biometrische Authentifizierungsverfahren zum Einsatz, an deren Anwendung in Verbindung mit standortbasierter Autorisierung vier Anforderungen gestellt werden: Anwendbarkeit, Energieeffizienz, Reaktionsgeschwindigkeit und Transparenz. Diese Anforderungen sind eine eigene Weiterentwicklung der Anforderungen, die aus einer Zusammenarbeit mit Matthias Trojahn entstanden sind und in Trojahn et al. [141] veröffentlicht wurden:

Anwendbarkeit Eine wichtige Forderung an implizite, biometrische Authentifizierungsverfahren ist die Eigenschaft der Anwendbarkeit innerhalb der autorisierten Zone, in der ein gewährtes Zugriffsrecht genutzt werden soll. Im Allgemeinen ist dies nicht gewährleistet, da die autorisierte Zone spezielle Randbedingungen vorweisen kann, wie z.B. die Lautstärke der Umgebung oder die Helligkeit. Ferner kann die Anwendbarkeit eines Verfahrens in Abhängigkeit von der Art und Weise eingeschränkt sein, mit der während der Nutzung des Zugriffsrechts mit dem Smartphone interagiert wird.

Energieeffizienz Das eingesetzte Verfahren muss energieeffizient arbeiten, um eine Anwendung über die ganze Nutzungsdauer hinweg zu ermöglichen. Dies ist der Fall, wenn der Betrieb des Sensors wenig Leistung benötigt und die Merkmalsextraktion sowie Klassifikation mit geringem Rechenaufwand möglich sind [86]. Ferner muss das Verfahren in möglichst vielen Fällen bzw. Nutzungssituationen niedrige Fehlerraten erlauben, so dass eine Fusion mit weiteren Verfahren unnötig ist und kein zusätzlicher Energiebedarf entsteht. Um niedrige Fehlerraten zu erhalten, muss das zugrundeliegende Merkmal in der jeweiligen Nutzungssituation eindeutig mit dem Smartphone messbar sein.

Reaktionsgeschwindigkeit Um selbst ein kurzes Ablegen oder Weitergeben des Smartphones zu vermeiden, ist die Reaktionsgeschwindigkeit des biometrischen Authentifizierungsverfahrens wichtig. Von einer ausreichenden Reaktionsgeschwindigkeit wird gesprochen, falls die Zeitspanne zwischen zwei Abtastpunkten kürzer ist, als die minimale Zeitspanne nach der Schaden durch das Ablegen oder Weitergeben entstehen kann. Diese Anforderung setzt indirekt voraus, dass das Verfahren kontinuierlich arbeitet.

Transparenz Alle angewandten Authentifizierungsverfahren müssen transparent für den Nutzer sein, um ein Ablenken oder Blockieren während der Arbeit mit dem gewährten Zugriffsrecht zu vermeiden. Das angewandte Verfahren muss daher implizit, also im Hintergrund arbeiten. Fundamental für die Transparenz eines solchen Verfahrens ist die FRR. Denn wird ein Nutzer fälschlicherweise zurückgewiesen, muss das System auf die Authentifizierung mittels spezifischem Wissen oder Besitz zurückgreifen, was die explizite Interaktion des Nutzers erfordert.

An biometrische Authentifizierung werden in einer späteren Arbeit von Li et al. [88] unabhängig von standortbasierter Autorisierung die Anforderungen Kontinuität, Unsichtbarkeit und Leichtgewichtigkeit identifiziert. Da unabhängig von der aktuellen Aufgabe des Nutzers argumentiert wird, ist die Anforderung nach Anwendbarkeit nicht aufgeführt. Die Kenntnis über die zu nutzenden Zugriffsrechte verfeinert somit die Anforderungen. In einer Arbeit von Toledano et al. [138] werden Anforderungen an die Nutzerfreundlichkeit biometrischer Verfahren entwickelt, welche fordern, das Verfahren möglichst transparent zu gestalten. Die Transparenz für biometrische Verfahren wird ebenfalls von Ben–Asher et al. in [13] gefordert, um eine Akzeptanz bei den Nutzern zu erhalten.

3.4.3 Einsetzbarkeit bestehender Verfahren

Neben den körperlichen Merkmalen, die im Unterabschnitt 3.4.1 beschrieben wurden, werden in vielen Verfahren zur biometrischen Authentifizierung auch Verhaltensmerkmale erfasst. Beide Klassen werden bzgl. ihrer spezifischen Merkmale in Abb. 3.18 verglichen. In Verbindung mit standortbasierter Autorisierung können jedoch nicht alle dargestellten Merkmale herangezogen werden. Deshalb sind die Merkmale grau hervorgehoben, die aktuell (Stand 2015) mittels der Sensoren von Smartphones messbar sind. Ferner scheiden aufgrund der speziellen Nutzeroberfläche von Smartphones zusätzlich Authentifizierungsverfahren aus, deren Merkmalserfassung den Nutzer mit speziellen Abfragen ablenkt. Hierunter fällt z.B. die Venen- oder Unterschrifterkennung. Speziell die Verfahren, welche auf Smartphones realisierbar sind, werden im Folgenden qualitativ auf die Einsetzbarkeit in Verbindung mit standortbasierter Autorisierung untersucht. Die Grundlage dafür bildet der definierte Anforderungskatalog. Die Verfahren sind nach den einzelnen Sensoren gruppiert, die zur Erfassung der zugrundeliegenden Merkmale benötigt werden.

Verfahren basierend auf optischen Sensoren Optische Sensoren werden für die biometrische Authentifizierung mittels Gesichts-, Iris- oder Handflächenerkennung benötigt,

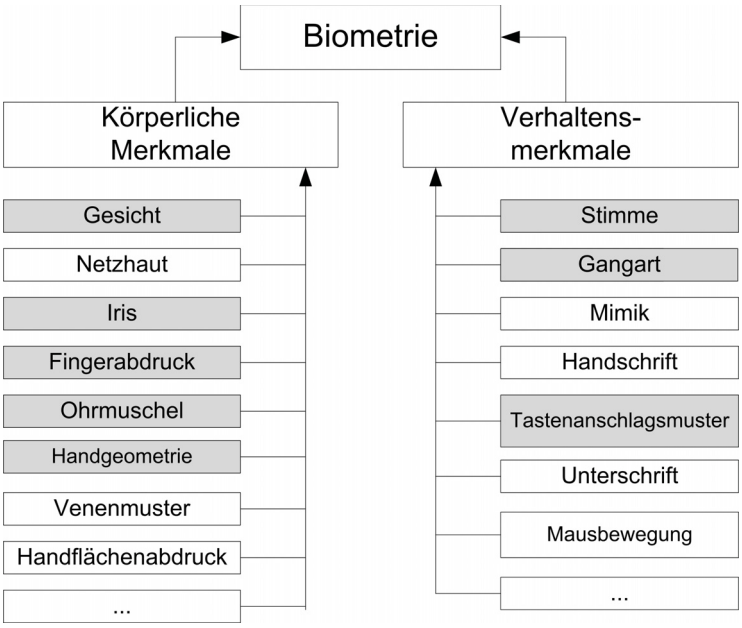


Abbildung 3.18: Klassifikation der Merkmale, die zur biometrischen Authentifizierung verwendbar sind. Solche, die auf dem Smartphone eingesetzt werden, sind grau hervorgehoben (adaptiert aus [141]).

sowie für die Erkennung anhand der Ohrmuschel. Dabei wird die Ohrmuschel kurz vor Annehmen eines Anrufs durch die Frontkamera des Smartphones fotografiert. Gleiches geschieht bei der Handflächenerkennung, kurz bevor das Gerät vom Tisch aufgehoben wird. Beide Ereignisse sind selten, so dass die Handflächen- und Ohrmuschelerkennung nicht anwendbar sind, falls eine hohe Reaktionsgeschwindigkeit gefordert ist.

In solchen Fällen eignet sich die Gesichtserkennung deutlich besser. Hierbei werden spezifische Merkmale der Augen, der Augenbrauen, der Nase usw. für den Prozess der Authentisierung herangezogen [133]. Es wird zwischen der 2D- und der 3D-Gesichtserkennung unterschieden. Die 2D-Gesichtserkennung wird beispielsweise zum automatischen Entsperren von Smartphones seit Android 4.0 eingesetzt [5]. Damit solche Systeme nicht durch vorbereitete Fotos eines bekannten Nutzers irregeführt werden können, gibt es Ansätze wie z.B. KeyLemon [74] zur Erkennung der Lebendigkeit z.B. über Lidschläge.

Voraussetzung zur Anwendung der Gesichtserkennung ist, dass der Nutzer den Bildschirm betrachtet und sein Gesicht im Kamerabild erkennbar ist. Dabei werden Bilder und Videosequenzen zur Authentifizierung erstellt. In Szenarien, in denen die Beleuchtung sehr dunkel oder sehr grell ist, wird die Anwendbarkeit solcher Verfahren massiv erschwert [79]. Abhilfe kann hier das Licht der Bildschirmbeleuchtung des Smartphones schaffen und die Anwendbarkeit, z.B. nachts, verbessern. Tagsüber ist es wichtig, dass das Display reflexionsfrei ist, da das Smartphone ansonsten unnatürlich gehalten werden kann und keine korrekte Gesichtserkennung möglich ist [140]. In Szenarien, in denen nur ein kleiner Teil des Gesichts sichtbar ist, z.B. aufgrund von Schutzkleidung oder spezieller Arbeitsklei-

dung, sind Verfahren zur Gesichtserkennung kaum anwendbar. Eine Ausnahme stellt die Iriserkennung dar, da hierbei nur die Augen deutlich erkennbar sein müssen [39].

Bei der Authentifizierung über Gesichtserkennung erreichten Kim et al. in [75] eine Gleichfehlerrate von 5,09%. Werte dieser Größenordnung sind ausreichend, sofern es sich beim genutzten Zugriffsrecht nicht um eine hochsichere Anwendung handelt und die Energieeffizienz und Nutzbarkeit des Systems im Vordergrund stehen.

Ein Nachteil der Authentifizierung mittels 3D-Gesichtserkennung ist der hohe Rechenaufwand während der Analyse. In einem Experiment von Anjos et al. wurden 3,7 s benötigt, um aus einem solchen Bild eine Entscheidung bzgl. der Authentifizierung abzuleiten [6]. Trewin et al. erreichen mit einer 2D-Gesichtserkennung Antwortzeiten von 2-2,5 s. Diese Zeitspanne erlaubt für Zugriffsrechte zur Dateneinsicht eine ausreichende Reaktionsgeschwindigkeit, um das Ablesen von Daten auf dem Smartphone nach dessen unberechtigter Weitergabe schnell genug zu unterbinden.

Da alle benötigten Informationen im Hintergrund gesammelt werden, muss ein Nutzer im Idealfall nicht aktiv zur Authentifizierung mittels Gesichts- oder Iriserkennung beitragen [126]. Jedoch erfordert die Gesichtserkennung, dass der Nutzer längere Zeit still hält und in die Kamera blickt [88]. Geschieht dies durch den Typ des Zugriffsrechts nicht automatisch, z.B. wenn eine Spracheingabe im Gehen gewährt wird, ist eine transparente Authentifizierung mittels optischer Sensoren erschwert.

Verfahren basierend auf inertialen Sensoren In modernen Smartphones sind mit Beschleunigungssensoren und gyroskopischen Sensoren typischerweise zwei Typen inertialer Sensoren verbaut. Ergänzt werden diese Sensoren oft durch Magnetfeldsensoren, wodurch ein Kompass realisiert werden kann. Das Gyroskop wird zur Messung von Drehungen des Geräts verwendet, wohingegen der Beschleunigungssensor verwendet wird, um Bewegungen des Geräts zu erfassen [20]. Durch deren Anwendung ist es möglich, Verhaltensmerkmale der Nutzer zu erfassen, die zur biometrischen Authentifizierung verwendet werden. Ein Beispiel ist die charakteristische Bewegung des Smartphones während es vom Nutzer bedient wird [29], oder dessen Bewegung während der Nutzer geht [46,92]. Zwei weitere Möglichkeiten bietet die Analyse, wie das Smartphone aufgehoben wird [128], oder wie es beim Entgegennehmen eines Anrufs an das Ohr geführt wird [29].

Die Authentifizierung des Nutzers mittels Gangerkennung ist in solchen Szenarien anwendbar, in denen eine Arbeit mit dem gewährten Zugriffsrecht ein permanentes Gehen ohne längere Pausen erfordert [92]. Darunter fällt die visuelle Kontrolle eines größeren Geländes und das Eintragen von Auffälligkeiten in ein Interface auf dem Smartphone. Legt die Art des Zugriffsrecht jedoch nahe, dass der Nutzer bei der Arbeit damit meist stillsteht, sollte zur Überbrückung der Lücken eine Fusion mit möglichst unterschiedlichen Verfahren durchgeführt werden.

Der Ansatz zur Authentifizierung während des Heranführens des Smartphones an das Ohr von Conti et al. erreicht eine EER von 5,5%, ist allerdings nur in diesen seltenen Fällen anwendbar [29]. Verfahren zur Authentifizierung mittels Gangerkennung zeigen nur eine geringe Diversität zwischen Personen und somit entsprechende Fehlerraten. In einem

Experiment von Derawi et al. mit herkömmlichen Smartphones wird z.B. nur eine EER von 20% erreicht [46]. Hierbei tragen die Testpersonen das Endgerät am Gürtel an der rechten Seite ihrer Hüfte. In einem früheren Experiment von Mäntyjärvi et al. wird mit dedizierten tragbaren Beschleunigungssensoren eine EER von 7% erreicht, wobei die Nutzer das Gerät ebenfalls am Gürtel tragen [92]. In Verbindung mit standortbasierter Autorisierung wird deshalb eine Fusion mit zusätzlichen Verfahren empfohlen. Auch wenn zukünftig aufgrund besserer Sensoren im Smartphone eine niedrigere Fehlerrate erreicht wird, lässt sich sagen, dass aufgrund der Fusion keiner der existierenden Ansätze der Anforderung der Energieeffizienz standhält. Somit kann nur eingeschränkt von dem eigentlich niedrigen Energiebedarf bei der Verwendung und Auswertung von inertialen Sensoren profitiert werden.

Aufgrund ihrer EER können Verfahren basierend auf inertialen Sensoren nur mit eingeschränkter Verlässlichkeit das Weitergeben des Smartphones erkennen. Ferner gilt, dass aufgrund der Abhängigkeit von der Bewegung des Nutzers kaum eine Unterscheidung getroffen werden kann, ob der Nutzer nur stillsteht, oder aber z.B. das Gerät auf einem Tisch abgelegt hat und sich davon entfernt.

Die Authentifizierung mittels Gangerkennung hat den Vorteil der hohen Transparenz für den Nutzer. Die Erfassung und Verarbeitung der Daten findet vollständig im Hintergrund statt, wobei mit seiner Gangart das Merkmal einer Bewegung verwendet wird, die der Nutzer ohnehin ausführt. Allerdings ist die Transparenz des Verfahrens bei längerem Stillstand des Nutzers nicht mehr gegeben, weil dann eine explizite Aufforderung zur Bewegung nötig wird und der Ansatz dadurch nicht mehr implizit arbeitet.

Verfahren basierend auf kapazitiven Touchscreens Anstelle klassischer Tastaturen besitzen moderne Smartphones typischerweise kapazitive Touchscreens, die es erlauben den Anpressdruck und die Größe des Fingerabdrucks zu messen. Beide Merkmale können zur biometrischen Authentifizierung verwendet werden. Dazu existieren Ansätze, in denen der Nutzer Zahlen mit dem Finger auf das Display schreiben muss [140], oder das Tippverhalten bei Eingabe eines Entsperr–Codes analysiert wird [38]. Denkbar ist auch, dass betrachtet wird, mit welchen speziellen Eigenheiten die Steuerung des Smartphones durch Wischgesten erfolgt [128]. Allgemein muss vor Anwendung eines Authentifizierungsverfahrens für Touchscreens zunächst erkannt werden, um welche Art dieser möglichen Interaktionen es sich handelt. Darauf basierend werden dann passende Merkmale aus den aufgezeichneten Daten extrahiert.

Die biometrische Authentifizierung mittels des Tastenanschlagmusters ist in Szenarien anwendbar, in denen der Nutzer während der Benutzung seiner gewährten Zugriffsrechte in kurzen Zeitabständen Eingaben auf dem Touchscreen vornimmt [140]. Bei Wischgesten auf dem Touchscreen spielt die Dauer der ausgeführten Bewegung eine wichtige Rolle für die Klassifikation. Ist also während der Nutzung eines gewährten Zugriffsrechts ein hohes Maß an Interaktion gefordert, sind diese Verfahren sehr gut anwendbar.

Die Klassifikation von erfassten Merkmalen aus der Berührung des Touchscreens ist effizient möglich, so dass z.B. Li et al. auf herkömmlichen Smartphones eine Antwortzeit des Klassifikators von 17 ms erhalten [88]. Wird speziell das Tastenanschlagsmuster beim

Tippen auf dem Touchscreen betrachtet, zeigen bisherige Experimente gute Fehlerraten. So konnten Trojahn et al. eine FAR von 8.31% und eine FRR von 5.26% erreichen [142], was trotzdem eine Fusion mit anderen Verfahren erforderlich macht und somit den Energieverbrauch erhöhen kann. De Luca et al. konnten auf Basis des Tippverhaltens eine FRR von 19% und FAR von 21% beobachten, wobei der Eingabezeitraum hier nur auf das Entsperren des Smartphones begrenzt war. Zur Verbesserung der Fehlerraten durch Fusion wurden in der Literatur unter anderem Stimmerkennung, Bewegungserkennung oder Gesichtserkennung vorgeschlagen [88,140].

Die Anforderung an die Reaktionsgeschwindigkeit kann hier nur erfüllt werden, sofern der Nutzer permanent mit dem Touchscreen seines Smartphone interagiert. Wie oben schon beschrieben, kann die Klassifikation währenddessen extrem performant erfolgen. Li et al. [88] stellen jedoch fest, dass in der Praxis zwischen zwei Gesten typischerweise eine Zeitspanne von 8 - 51 s verstreicht. Eine ausreichend geringe Reaktionsgeschwindigkeit um die Weitergabe des Smartphones und das Ablesen von vertraulichen Daten zu verhindern ist dann nicht mehr gegeben. Somit ist die Reaktionsfähigkeit in Szenarien eingeschränkt, in denen der Nutzer kaum mit dem Touchscreen interagiert, z.B. weil aufgrund des Zugriffsrechts Daten vorwiegend abgelesen und nicht eingegeben werden.

Die transparente Anwendung des Verfahrens ist nur möglich, wenn ein Nutzer tippt oder Gesten verwendet. Die transparente Anwendung dieser Verfahren ist demnach durchaus realisierbar, allerdings wird die Transparenz gebrochen, sobald der Nutzer zur Eingabe oder zu Gesten aufgefordert wird.

Verfahren basierend auf Audiosensoren Audiobasierte Authentifizierung kann entweder durch Sprach- oder Stimmerkennung erfolgen, wobei erstes vom gesprochenen Text und letzteres von der Art abhängt, wie gesprochen wird [128].

In Umgebungen mit hoher Belastung neigen einzelne Nutzer zu Aussprachefehlern, was letztlich Fehler in der Authentifizierung verursacht und somit die Anwendbarkeit einschränkt. Ebenfalls haben Umgebungsgeräusche einen enormen Einfluss auf solche Verfahren [140]. Insbesondere in sehr geräuschvollen Umgebungen kann der menschliche Anteil im aufgezeichneten Audiospektrum nur schwer vom Hintergrundrauschen getrennt werden, sofern der Nutzer nicht sehr laut spricht. Die Anwendbarkeit hängt deshalb von der Geräuschkulisse innerhalb der autorisierten Zone ab.

Da die CPU eine große Datenmenge verarbeiten muss, ist die Anwendung von Stimmerkennung auf Smartphones nicht sehr energieeffizient [86]. Die Fehlerraten liegen im Experiment von Kim et al. [75] mit einer EER von 8,98% und einer Genauigkeit von ca. 95% in der Arbeit von Shi et al. [128] im typischen Bereich. Deshalb ist auch hier eine Fusion mit weiteren Verfahren nötig, was die Energieeffizienz zusätzlich verschlechtert.

Die Reaktionsgeschwindigkeit der Authentifizierung über Stimmerkennung war z.B. im Experiment von Shi et al. mit 2-2,5 s sehr gut, was die Eignung für die meisten Arten von Zugriffsrechten verspricht [128]. Falls die Sprach- oder Stimmerkennung als einziges Verfahren verwendet wird, besteht die Gefahr, dass nur eine niedrige Reaktionsgeschwindigkeit bei gezielten Angriffen erreicht wird. Denn wird das Smartphone weitergegeben und wer-

den gleichzeitig alte Audioaufnahmen eingespielt, ist ein Umgehen des Verfahrens möglich. Somit wird auch hier eine Prüfung auf Lebendigkeit erforderlich, z.B. durch Abgleich der Lippenbewegung.

Sofern der Nutzer permanent bei der Verwendung der gewährten Zugriffsrechte spricht, da er z.B. damit den Zustand von Maschinen bei ihrer visuellen Kontrolle dokumentiert, ist die Anwendung durchaus sinnvoll. Generell ist es jedoch empfehlenswert, die Audiosignale zunächst auf menschliche Stimme zu untersuchen [128] und anschließend erst zu authentifizieren. Falls keine Stimme erkannt wird, so ist zwingend die Fusion mit einem weiteren Verfahren basierend auf einem anderem Merkmal nötig, da ansonsten der Nutzer durch eine Passwortabfrage oder durch die Aufforderung zu sprechen abgelenkt werden müsste [140].

3.4.4 Zwei Fallstudien

Derzeit erfüllt kein Verfahren alle Anforderungen für ein gegebenes Szenario. Somit ist die Fusion einer Menge von biometrischen Authentifizierungsverfahren nötig, um ausreichende Fehlerraten zu erhalten und den Anforderungskatalog zu erfüllen. Im Folgenden zeigen zwei Beispielanwendungen die Bestimmung der Verfahren zur Fusion.

Das erste Szenario sei in einer industriellen Umgebung angesiedelt, beispielsweise einer Fabrik. Hier wird Nutzern durch standortbasierte Zugriffsrechte innerhalb der näheren Umgebung von Maschinen gestattet, diese mittels ihres Smartphones zu steuern. Direkt vor den Maschinen soll den Nutzern ein Blick auf die spezifischen Statusinformationen sowie das Aufzeichnen von Notizen erlaubt werden. Es wird angenommen, dass die Umgebung innerhalb der Fabrikhalle laut und schlecht beleuchtet ist. Durch die Betriebsrichtlinien wird ferner eine spezielle Arbeitskleidung benötigt, die einen Helm und eine Atemschutzmaske umfasst und somit das Gesicht teilweise verdeckt. Deshalb wird die Anwendung von Gesichtserkennung erschwert, da aus Fotos nicht genügend Merkmale extrahiert werden können. Aufgrund des Hintergrundgeräuschs der Maschinen unterliegt auch die Stimmerkennung ähnlichen Problemen. In diesem Szenario wäre deshalb die biometrische Authentifizierung auf Basis von kapazitiven Touchscreens und inertialen Sensoren denkbar. Trotzdem ist es erforderlich, dass der Nutzer öfters durch eine explizite Passworteingabe unterbrochen wird, falls die angewandten Verfahren eine Falschabweisung liefern.

Im zweiten Szenario wird angenommen, dass ein Arzt eine Visite durchführt. Ihm wird durch die standortbasierte Autorisierung das Zugriffsrecht gewährt, die Akte eines Patienten einzusehen, sobald er dessen Zimmer betritt. Dort unterhält sich der Arzt mit dem Patienten und aufgrund der ruhigen Umgebung kann der Arzt über seine Stimme authentifiziert werden. Außerdem wird angenommen, dass er keine Schutzkleidung trägt, die sein Gesicht verdeckt. Hier scheint also eine Fusion aus Stimm-, Gesichts- und Gangerkennung eine sinnvolle Lösung für kontinuierliche und implizite Authentifizierung darzustellen.

3.4.5 Zusammenfassung

In diesem Abschnitt wurde zunächst das Problem identifiziert, dass die Positionsschätzung für einen Nutzer nur gültig ist, sofern er sein Smartphone selbst in der Hand hält. Daher kann die standortbasierte Autorisierung irregeführt werden, wenn das mobile Endgerät unbemerkt in die Hände unberechtigter Dritter gelangt. In diesem Abschnitt wurde deshalb vorgeschlagen, die Position des Nutzers an die Position seines Smartphones durch die Anwendung kontinuierlicher, implizierter biometrischer Authentifizierung zu koppeln. Ausgehend von einer gemeinsamen Vorarbeit mit Matthias Trojahn [141] wurde ein stark überarbeiteter Anforderungskatalog an biometrische Authentifizierungsverfahren vorgestellt, der für den Einsatz mit der standortbasierten Autorisierung gilt. Dabei wurden gegenüber der Vorarbeit durch die Energieeffizienz und die Reaktionsgeschwindigkeit zwei neue Anforderungen eingeführt, die bisher nicht bedacht wurden. Darauf wurde analysiert, zu welchem Grad existierende biometrische Authentifizierungsverfahren für Smartphones diese Anforderungen erfüllen. Die Analyse aus der Vorarbeit wurde auf die neuen Anforderungen übertragen und dem aktuellen Stand der Technik angepasst. Hierbei zeigte sich, dass alle Verfahren jeweils auf sehr spezielle Einsatzszenarien zugeschnitten sind. Somit ergab sich die Empfehlung, je nach den Charakteristika des gewährten Zugriffsrechts und den Umgebungsbedingungen der zugeordneten autorisierten Zone mehrere geeignete biometrische Authentifizierungsverfahren auszuwählen und über entsprechende Algorithmen zu fusionieren. In zwei Fallstudien wurde gezeigt, wie geeignete Verfahren zur Fusionierung ausgewählt werden können. Der Anforderungskatalog an die implizite, kontinuierliche biometrische Authentifizierung und die durchgeführte Analyse erlauben es in zukünftigen Anwendungen der standortbasierte Autorisierung gezielt eine unberechtigte Weitergabe des Smartphones zu erkennen. Eine Kompromittierung der beabsichtigten Semantik wird somit in solchen Fällen deutlich erschwert.

Kapitel 4

Spezifikation und Auswertung von Ortsbeschränkungen

Das folgende Kapitel behandelt Beiträge zur Spezifikation von Ortsbeschränkungen zur Erweiterung klassischer Zugriffskontrollmodelle. Dabei wird insbesondere auf deren Durchsetzung unter Beachtung von Positionsfehlern eingegangen.

Dabei wird in Abschnitt 4.1 zunächst eine umfassende Gegenüberstellung von existierenden standortbasierten Autorisierungsstrategien auf Basis der Entscheidungstheorie vorgestellt. Mit der risikobasierten Autorisierungsstrategie wird eine neue Methodik eingeführt, deren Konzept in dieser Form zur standortbasierten Autorisierung bisher keine Anwendung fand. Wenn Positionsfehler auftreten, sind so erstmals Autorisierungsentscheidungen möglich, die aus entscheidungstheoretischer Sicht rational sind. Die risikobasierte Strategie wird erweitert, so dass das bisher in der Literatur übliche Konzept von Polygonen zur Modellierung von autorisierten Zonen für Ortsbeschränkungen generalisiert wird. Dazu werden Eigenschaftsmodelle eingeführt, welche für jeden Ort die Wahrscheinlichkeit modellieren, dort eine für die Autorisierung gewünschte Eigenschaft zu beobachten. Somit ist eine realistischere Umsetzung von Ortsbeschränkungen als durch Polygone möglich, falls die benötigte Eigenschaft nicht gleich verteilt und zu jeder Zeit innerhalb eines Polygons vorherrscht.

In Abschnitt 4.2 wird eine standortbasierte Erweiterung von RBAC vorgestellt, die Positionsfehler beachtet. Dabei wird das Konzept der erweiterten risikobasierten Autorisierungsstrategie angewandt. Ortsbeschränkungen werden einzelnen Elementen der RBAC-Richtlinie zugewiesen. Es werden 9 Modelle eingeführt, wie innerhalb von RBAC-Sitzungen und der laufenden Nutzung von gewährten Zugriffsrechten auf die Verletzung von Ortsbeschränkungen reagiert werden kann. In der Evaluation wird gezeigt, dass dieser Ansatz dem bisherigen Konzept, Positionsfehler zu ignorieren, deutlich überlegen ist.

In Abschnitt 4.3 wird ein Ansatz vorgestellt, der die risikobasierte Strategie zusammen mit einem Partikelfilter einsetzt. Wird ein gewährtes Zugriffsrecht über einen längeren Zeitraum genutzt, wird so der Einfluss von Messausreißern reduziert. Hierbei wird auf Basis eines Partikelfilters und WLAN-Fingerprinting eine probabilistische Abschätzung der Trajektorie des Nutzers ermittelt und zur Autorisierung verwendet. Im Gegensatz zu existie-

renden trajektorienbasierten Ansätzen wird hierbei die Ungewissheit über die tatsächliche Nutzertrajektorie herangezogen und basierend auf dem Polygon und der risikobasierten Autorisierungsstrategie eine Autorisierungsentscheidung getroffen. Ebenso wird ein Konzept vorgestellt, das dynamisch einen Timeout bestimmt, bis zu dem die nächste Positionsschätzung vorliegen muss. Bisher waren nur statische Timeouts möglich, die nicht die aktuelle Gewissheit über den Nutzerstandort berücksichtigen. In der Evaluation wird gezeigt, dass die getroffenen Autorisierungsentscheidungen deutlich weniger stark von einzelnen Messausreißern beeinträchtigt werden, als dies in existierenden Ansätzen der Fall ist.

4.1 Grundlagen zu Ortsbeschränkungen

Die Aufgabe der standortbasierten Autorisierung ist es, eine Entscheidung über die Autorisierung des Nutzers mit seiner aktuellen Positionsschätzung (μ, Σ) bzgl. der Gewährung eines Zugriffsrechts zu treffen. Hierzu werden Ortsbeschränkungen definiert, mit denen klassische Zugriffskontrollmodelle wie RBAC, DAC oder MAC erweitert werden. Zunächst ist eine Ortsbeschränkung vereinfachend als autorisierte Zone definiert. Um ein Zugriffsrecht zu erhalten ist es erforderlich, dass der Nutzer sowohl durch das klassische Zugriffskontrollmodell, als auch bzgl. der zugeordneten Ortsbeschränkung autorisiert ist. Die Auswertung von Ortsbeschränkungen erfolgt durch eine standortbasierte Autorisierungsstrategie, deren Aufgabe es ist, eine Entscheidung zu treffen und dadurch die Ortsbeschränkung durchzusetzen.

Definition 4.1.1 (Standortbasierte Autorisierungsstrategie)**.** *Gegeben sei eine Elementaraussage* aut *mit dem Wahrheitswert* `wahr`*. Eine standortbasierte Autorisierungsstrategie i ist definiert als Wahrheitswertzuweisung von der Menge $\mathbb{P}$ aller möglichen Positionsschätzungen (μ, Σ) und der Menge $\mathbb{O}$ aller möglichen Ortsbeschränkungen o auf einen Wahrheitswert* aut *zur Autorisierung bzw.* $\neg$aut *zur Ablehnung, so dass gilt:*

$$\text{aut}^i : \mathbb{P} \times \mathbb{O} \mapsto \{\text{aut}; \neg\text{aut}\} \tag{4.1}$$

Eine Ortsbeschränkung o gilt für eine gegebene Positionsschätzung (μ, Σ) als erfüllt, wenn dem Tupel $((\mu, \Sigma), o)$ der Wahrheitswert `wahr` *zugewiesen wird.*

Eine standortbasierte Autorisierungsstrategie wird als Formalismus betrachtet, dessen Entscheidungen die Intention des Entwicklers bzw. des Betreibers der standortbasierten Autorisierung widerspiegeln sollen. In diesem Kapitel werden in der Literatur existierende Autorisierungsstrategien und eine neu vorgestellte, risikobasierte Strategie auf Basis der Entscheidungstheorie gegenübergestellt.

4.1.1 Standortbasierte Autorisierung als Entscheidungsproblem

Eine standortbasierte Autorisierungsstrategie muss ausgehend von einer Ortsbeschränkung und einer Positionsschätzung (μ, Σ) entscheiden, ob die Ortsbeschränkung, die auf einer

Zustand \ **Aktion**	aut = `wahr`	¬aut = `falsch`
Nutzer ist in $\mathcal{Z}$ (p = $p_{\mathcal{Z}}$)	*RP*	*FN*
Nutzer ist nicht in $\mathcal{Z}$ (p = $(1 - p_{\mathcal{Z}})$)	*FP*	*RN*

Tabelle 4.1: Die Entscheidungsmatrix standortbasierter Autorisierung.

polygonalen Fläche $\mathcal{Z} \subset \mathbb{R}^2$ basiert, erfüllt ist. Dabei muss die Entscheidung zwischen den Aktionen aut und ¬aut getroffen werden. Gleichzeitig ist bekannt, dass sich der Nutzer mit Wahrscheinlichkeit $p_{\mathcal{Z}}$ innerhalb von $\mathcal{Z}$ befindet, oder mit Wahrscheinlichkeit $(1 - p_{\mathcal{Z}})$ außerhalb davon. Wird nun eine Aktion $a \in \{\text{aut}; \neg\text{aut}\}$ ausgewählt, so kann diese Entscheidung vier mögliche Ausgänge zur Folge haben. Die Ausgänge für $a = \text{aut}$ sind Richtig-Positiv (RP), falls $gtp \in \mathcal{Z} \wedge a = \text{aut}$ oder Falsch-Positiv (FP), falls $gtp \notin \mathcal{Z} \wedge a = \text{aut}$. Gleichermaßen gilt für die Ausgänge der Aktion $a = \neg\text{aut}$ somit Richtig-Negativ (RN), falls $gtp \notin \mathcal{Z} \wedge a = \neg\text{aut}$ und Falsch-Negativ (FN), falls $gtp \in \mathcal{Z} \wedge a = \neg\text{aut}$. Dieses Problem kann, wie in Tab. 4.1 abgebildet, als klassische Entscheidungsmatrix dargestellt werden. Jeder der Ausgänge ist aus Sicht des Zugriffskontrollmodells unterschiedlich erstrebenswert.

Von Neumann und Morgenstern definieren ein Theorem, das beschreibt, welche Voraussetzungen ein Entscheider erfüllen muss, damit er die Entscheidung für eine Aktion stets rational trifft [110]. Ein solcher Entscheider wird von-Neumann-und-Morgenstern-rational, kurz VNM-rational genannt. Dazu wird das Konzept einer Präferenzrelation auf Lotterien benötigt. Wird eine Autorisierungsentscheidung aut oder ¬aut getroffen, so kann das als die Teilnahme an der jeweiligen Lotterie betrachtet werden. Lotterien sind induktiv definiert und im Falle der standortbasierten Autorisierung gilt nach einer Adaption von Peterson [111]:

1. Alle elementaren Ausgänge *RP*, *RN*, *FP*, *FN* sind eine Lotterie
2. Sind A und B zwei Lotterien, so ist ebenfalls die Situation eine Lotterie, in der mit Wahrscheinlichkeit p der Ausgang A und mit Wahrscheinlichkeit $(1-p)$ der Ausgang B erhalten wird, wobei $0 \leq p \leq 1$ gilt
3. Nichts anderes ist eine Lotterie

Eine Lotterie mit möglichen Ausgängen $S_1, \ldots, S_n$, die mit Wahrscheinlichkeit $p_1, \ldots, p_n$ eintreten, wird notiert als [119]:

$$L = [p_1, S_1; p_2, S_2; \ldots; p_n, S_n] \tag{4.2}$$

Damit ein Entscheider VNM-rational entscheidet, muss der Entscheider eine Präferenzrelation $\succsim$ besitzen, die auf der Menge der möglichen Lotterien der standortbasierten Autorisierung definiert ist und vier Axiome erfüllt. Sind A, B und C Lotterien, so bedeutet

$A \succ B$, dass der Entscheider die Lotterie A gegenüber der Lotterie B präferiert. $A \sim B$ bedeutet, dass beide Lotterien gleich attraktiv für den Entscheider erscheinen. Damit der Entscheider VNM-rational arbeitet, muss diese Ordnung nach von Neumann und Morgenstern vier Bedingungen erfüllen [111]:

1. Vollständigkeit: $A \succ B$ oder $A \sim B$ oder $B \succ A$
2. Transitivität: Falls $A \succ B$ und $B \succ C$, dann $A \succ C$
3. Unabhängigkeit: Für jede Wahrscheinlichkeit $p > 0$ gilt, dass $A \succ B$ genau dann gilt, wenn $[p, A; (1-p), C] \succ [p, B; (1-p), C]$
4. Kontinuität: Falls $A \succ B \succ C$, dann existieren ein p und q, so dass gilt $[p, A; (1-p), C] \succ B \succ [q, A; (1-q), C]$

Im Folgenden wird stets vorausgesetzt, dass der Entwickler der standortbasierten Autorisierung, der in diesem Fall der Entscheider ist, eine Präferenzrelation auf den Lotterien der standortbasierten Autorisierung besitzt, welche diesen vier Axiomen genügt. Er entscheidet somit stets VNM-rational.

Das Theorem nach von Neumann und Morgenstern sagt aus, dass die Präferenzrelation eines Entscheiders genau dann diese vier Axiome erfüllt, wenn eine Funktion U existiert, die von der Menge möglicher Lotterien auf reelle Zahlen im Intervall $[0; 1]$ abbildet und die folgenden Punkte gelten [111,119]:

1. $\mathrm{U}(A) > \mathrm{U}(B)$ genau dann, wenn $A \succ B$
2. $\mathrm{U}(A) = \mathrm{U}(B)$ genau dann, wenn $A \sim B$
3. $\mathrm{U}([p_1, S_1; \ldots; p_n, S_n]) = \sum_i p_i \cdot U(S_i)$, wobei S_i Lotterien seien, und eine Lotterie S_i mit Wahrscheinlichkeit p_i erhalten wird
4. Für jede andere Funktion U', welche die Punkte 1, 2 und 3 erfüllt, existieren Zahlen $a > 0$ und b, so dass gilt $\mathrm{U}'(S) = a \cdot U(S) + b$

Für einen ausführlichen Beweis dieses Theorems sei z.B. auf Peterson verwiesen [111].

Dabei wird davon ausgegangen, dass die Funktion U den erwarteten Nutzen einer Lotterie beschreibt. Ihre Abkürzung U leitet sich vom engl. Utility (Nutzen) ab. Generell kann zwischen Nutzen, Wert und Geldwert unterschieden werden [110]. Der Geldwert bewertet, wie viel Geld der Entscheider, also der Betreiber des Zugriffskontrollmodells, durch den jeweiligen Ausgang gewinnt oder verliert. Der Geldwert ist aber nicht immer die beste Entscheidungsgrundlage, da sich für Menschen typischerweise der Nutzen von Geld logarithmisch zu dessen Betrag verhält [119]. In diesem Fall würde es stark vom Kapital des Betreibers abhängen, wie erstrebenswert die einzelnen Ausgänge sind. Der Wert ist hingegen eher eine objektive, allgemeine Sicht auf die Erbstrebsamkeit eines Ausgangs. Hierbei kann z.B. der moralische Wert eines Ausgangs berücksichtigt werden, was aber nicht unbedingt mit den Zielen des Entscheiders übereinstimmt. Nutzen ist der Wert eines Ergebnisses aus Sicht des Entscheiders unter Berücksichtigung seiner Ziele [110]. Es ist eine abstrakte Größe, die nicht direkt beobachtet werden kann. Per Definition ergibt sich der Nutzen eines Ausgangs daraus, wie wertvoll sein Eintreten für den Entscheider ist.

Jeder VNM-rationale Entscheider verhält sich so, als würde er vor seiner Entscheidung den erwarteten Nutzen der möglichen Aktionen berechnen und sich für die Aktion entscheiden, die den größten erwarteten Nutzen besitzt. Im Falle der standortbasierten Autorisierung sind die möglichen Aktionen aut, also das Autorisieren, bzw. das Ablehnen ¬aut. Das Entscheiden für eine Aktion kann wie ein Ticket für die Lotterie aufgefasst werden. Die beiden zugehörigen Lotterien für die Aktionen aut und ¬aut werden formuliert als:

$$L_{\text{aut}} = [p_{\mathcal{Z}}, RP; (1 - p_{\mathcal{Z}}), FP] \tag{4.3}$$

$$L_{\neg\text{aut}} = [p_{\mathcal{Z}}, FN; (1 - p_{\mathcal{Z}}), RN] \tag{4.4}$$

Hierbei sei $p_{\mathcal{Z}}$ die Wahrscheinlichkeit, dass sich der Nutzer unter seiner aktuellen Positionsschätzung (μ, Σ) in der autorisierten Zone $\mathcal{Z}$ aufhält. Die Definition der Ortsbeschränkung eines Zugriffsrechts erfolgt basierend einer Abbildung U und einer autorisierten Zone $\mathcal{Z}$:

Definition 4.1.2 (Ortsbeschränkung)**.** *Eine Ortsbeschränkung $o \in \mathbb{O}$ ist definiert als ein 2–Tupel $(\mathcal{Z}, \mathrm{U})$, bestehend aus einer polygonalen Fläche $\mathcal{Z} \subset \mathbb{R}^2$ und einer Abbildung* U*, die Lotterien der standortbasierten Autorisierung auf reelle Zahlen im Intervall $[0; 1]$ abbildet, die Punkte 1–4 des oben angegebenen Theorems nach von Neumann und Morgenstern erfüllt und $U(RP) > U(FN) \ \wedge \ U(RN) > U(FP)$ gilt.*

Durch die Forderung der Punkte 1–4 gilt, dass eine VNM-rationale Präferenzrelation auf Lotterien der standortbasierten Autorisierung existiert. Die Forderung $U(RP) > U(FN)$ und $U(RN) > U(FP)$ drückt aus, dass bzgl. der Präferenzrelation $RP \succ FN$ und $RN \succ FP$ gilt. Die Relevanz dieser Forderung wird an zwei kurzen Gegenbeispielen gezeigt.

Angenommen es gelte $RP \prec FN$, dann gilt wegen Eigenschaft 1 der Funktion U entsprechend des Theorems nach von Neumann und Morgenstern auch $U(RP) < U(FN)$, da der Entscheider VNM-rational arbeitet. Liegt ein Positionierungssystem mit größtmöglicher Präzision und Richtigkeit vor, so gilt stets:

$$(gtp \in \mathcal{Z} \Rightarrow p_{\mathcal{Z}} = 1) \wedge (gtp \notin \mathcal{Z} \Rightarrow p_{\mathcal{Z}} = 0) \tag{4.5}$$

Sei $gtp \in \mathcal{Z}$ und $p_{\mathcal{Z}} = 1$. Dann gilt gemäß (4.3) und (4.4) auch $U(L_{\text{aut}}) < U(L_{\neg\text{aut}})$, da $1 \cdot U(RP) < 1 \cdot U(FN)$. Weil ein VNM-rationaler Entscheider stets so entscheidet, dass er mit seinen Aktionen den erwarteten Nutzen maximiert, entscheidet er in diesem Fall für eine Ablehnung ¬aut, obwohl das Positionierungssystem absolut präzise und richtig ist und zu 100% Wahrscheinlichkeit feststeht, dass sich der Nutzer innerhalb der autorisierten Zone befindet.

Analog gilt für das Gegenbeispiel mit $RN \prec FP$, dass $U(RN) < U(FP)$. Sei nun $gtp \notin \mathcal{Z}$ und $p_{\mathcal{Z}} = 0$. Dann gilt $U(L_{\text{aut}}) > U(L_{\neg\text{aut}})$, da $1 \cdot U(FP) > 1 \cdot U(RN)$. Auch hier gilt, dass der Entscheider VNM-rational entscheidet und somit die Aktion aut wählt, obwohl definitiv feststeht, dass sich der Nutzer außerhalb der autorisierten Zone befindet.

Nutzen im Kontext von Ortsbeschränkungen Aus dem Beweis des Theorems von von Neumann und Morgenstern folgt eine Methodik zur Ableitung der Funktion U [111],

die im Folgenden auf das Beispiel der standortbasierten Autorisierung angewandt wird. Zentral für die Herleitung nach von Neumann und Morgenstern ist, dass es keine absolute Skala für Nutzen gibt, sondern eine beliebige Skala definiert werden kann. Zunächst werden der erstrebenswerteste und der ungünstigste Ausgang identifiziert [119]. Diesen werden die Werte $u^{\top} = 1$ bzw. $u_{\perp} = 0$ zugewiesen, sodass eine normierte Skala für den Nutzen erhalten wird. Hieraus bildet sich die sog. Standardlotterie $\overline{L} = \left[p, u^{\top}; (1-p), u_{\perp}\right]$.

Der Nutzen eines jeden weiteren Ausgangs S kann nun bestimmt werden, indem der Standardlotterie die Lotterie $L = [1{,}0\,,\ S]$ gegenübergestellt wird. Hierbei ist ein solcher Wert für p zu wählen, so dass für den Entwickler der Zugriffskontrollstrategie, der in diesem Fall der Entscheider ist, beide Lotterien völlig gleichwertig sind und er keine der beiden präferiert. Dazu muss der erwartete Nutzen entsprechend Punkt 3 des oben angegebenen Theorems nach von Neumann und Morgenstern für beide Lotterien gleich sein:

$$1{,}0 \cdot \mathrm{U}(S) = p \cdot u^{\top} + (1-p) \cdot u_{\perp} \tag{4.6}$$

Liegt eine normierte Skala für den Nutzen vor, so vereinfacht sich (4.6) zu:

$$1{,}0 \cdot S = p \cdot u^{\top} \tag{4.7}$$

Der Nutzen $\mathrm{U}(S)$ von S entspricht also dem zu wählenden Wert p, so dass beide Lotterien aus Sicht des Entscheiders gleich attraktiv sind. Die Werte für den Nutzen liegen auf einer Intervallskala. Somit ist es nicht legitim, das Verhältnis von einzelnen Werten auf dieser Skala zu vergleichen, da die Skala, wie eben gezeigt, beliebig transformiert werden kann. Stattdessen kann stets nur die Größe des Intervalls zwischen zwei Werten zueinander in Bezug gesetzt werden.

Beispiele zur Herleitung des Nutzens Das Herleiten und Transformieren einer Abbildung U für den Nutzen soll im Folgenden an zwei unterschiedlichen Beispielen veranschaulicht werden.

Beispiel 4.1.1 (Sicherer Dienst)**.** *Es soll über die Autorisierung für einen zonenbasierten Dienst entschieden werden, der den Zugriff auf höchst vertrauenswürdige Unternehmensdaten auf einen Raum $\mathcal{Z}$ begrenzen soll. In diesem Beispiel wird angenommen, dass genau die für den Dienst autorisierten Personen auch einen physischen Schlüssel zu diesem Raum besitzen, also zusätzliche Sicherheit durch das Einführen der standortbasierten Autorisierung entsteht. Wird das mobile Endgerät allerdings gestohlen, so kann der Dieb damit nur von außerhalb zugreifen. Der schlimmste aller Ausgänge wäre hier deshalb FP und der erstrebenswerteste Ausgang RP. Es wird daher festgelegt $u^{\top} = \mathrm{U}(RP) = 1{,}0$ und $u_{\perp} = \mathrm{U}(FP) = 0{,}0$.*

Um den Nutzen für die Ausgänge FN und RN zu finden, muss der Entwickler der Zugriffskontrollstrategie zwei Wahrscheinlichkeiten p und p' bestimmen, indem er das Prinzip aus (4.7) anwendet:

$$1{,}0 \cdot \mathrm{U}\,(FN) \;=\; p \cdot \mathrm{U}\,(RP) \tag{4.8}$$

$$1{,}0 \cdot \mathrm{U}\,(RN) \;=\; p' \cdot \mathrm{U}\,(RP) \tag{4.9}$$

Zur Bestimmung von $U(FN)$ muss der Entscheider somit einen Wert p finden, so dass es für ihn gleichwertig scheint, die Lotterie $[1{,}0\,,\ U(FN)]$ oder aber die Standardlotterie $[p, \mathrm{U}(RP); (1-p), \mathrm{U}(FP)]$ zu wählen. Konkret sucht er einen solchen Wert p, so dass er sagen kann:

> *"Ich ziehe gleich viel Nutzen aus einer Autorisierungssituation, die zu 100% Wahrscheinlichkeit den Ausgang FN bringt, oder aus einer Autorisierungssituation, für die ich den exakten Ausgang zwar nicht kenne, aber weiß, dass zu p-Prozent der Ausgang RP und zu $(1-p)$-Prozent der Ausgang FP folgt."*

Wird ein RP nicht oft genug erkannt, so empfinden die Mitarbeiter die standortbasierte Autorisierung als unbrauchbar. Treten die zu vermeidenden Fälle von FP auf, so ist auch der Betreiber dieser Meinung. In diesem Fall wählt der Entscheider also einen Wert $p = 0{,}2$, so dass gilt $\mathrm{U}(FN) = 0{,}2$. Zur Bestimmung von $\mathrm{U}(RN)$ muss entsprechend analog ein Wert p' vom Entwickler abgeschätzt werden. Er wählt schließlich einen Wert von $p' = 0{,}9$, da er den erwarteten Nutzen der Lotterie $[1{,}0\,,\ \mathrm{U}(RN)]$ und den der Standardlotterie mit $[0{,}9\,, U(RP); 0{,}1\,, U(FP)]$ als gleichwertig sieht. Somit gilt $\mathrm{U}(RN) = 0{,}9$.

Beispiel 4.1.2 (Werbedienst)**.** *In diesem Beispiel soll ein zonenbasierter Dienst die Nutzer der mobilen Applikation eines Museums im Kassenbereich $\mathcal{Z}$ über das Angebot informieren, ein erweitertes Ticket zu kaufen. Dieses berechtigt zusätzlich zum Eintritt in eine angegliederte Sonderausstellung. Der Entwickler der Zugriffskontrollstrategie identifiziert den Ausgang RP als den besten, da gewinnversprechendsten und den Ausgang FN als schlechtesten, da potentiell weniger Kunden geworben werden. Nun sind wieder Werte p und p' zu bestimmen, so dass aus Sicht des Entwicklers folgende Gleichungen gelten:*

$$\begin{aligned} 1{,}0 \cdot \mathrm{U}(FP) &= p \cdot \mathrm{U}(RP) \\ 1{,}0 \cdot \mathrm{U}(RN) &= p' \cdot \mathrm{U}(RP) \end{aligned}$$

Hier ist der Ausgang FP insofern schlimm, dass Kunden, die den Kassenbereich bereits verlassen haben, nochmals durch Werbung belästigt werden. Nutzen wird dabei aus dem unrealistischen Fall gezogen, dass ein solcher Kunde zurückkehrt und das Angebot wahrnimmt. Der Entwickler der Zugriffskontrollstrategie wählt also $p = 0{,}2$ wodurch sich $U(FP) = 0{,}2$ ergibt. Für die Wahl von p' gilt, dass aus RN nur der Nutzen gezogen wird, dass die mobile Applikation als nicht störend empfunden wird. Er wählt daher $p' = 0{,}7$, wodurch sich $U(RN) = 0{,}7$ ergibt.

Rationale Autorisierungsentscheidungen Ist U für alle vier Ausgänge bestimmt, so sind auch $U(L_{\mathrm{aut}})$ und $U(L_{\neg\mathrm{aut}})$ aus (4.3) und (4.4) vollständig definiert. Wird eine Autorisierungsentscheidung aut oder ¬aut getroffen, so kann das als die Teilnahme an der jeweiligen Lotterie betrachtet werden. Der erwartete Nutzen der jeweiligen Lotterie wird dann als der erwartete Gewinn aus der Teilnahme verstanden.

Das Ziel einer VNM-rationalen Autorisierungsentscheidung ist es, den erwarteten Nutzen zu maximieren. Somit gilt, dass die Aktion $a^* \in \{\mathrm{aut}; \neg\mathrm{aut}\}$ die rationalste Wahl ist,

deren Lotterie den erwarteten Nutzen maximiert:

$$a^* = \underset{a \in \{\text{aut}; \neg\text{aut}\}}{\arg\max}\ U(L_a) \tag{4.10}$$

Wird nun eine Aktion a^* gewählt, so entsteht als Nutzen einer der Werte U(RP), U(FP), U(RN) oder U(FN), abhängig vom realen Zustand des Nutzers. Befindet sich der Nutzer innerhalb von $\mathcal{Z}$, so ist der maximal mögliche Nutzen, der aus einer Aktion folgen kann, gegeben durch U(RP), da U(RP) > U(FN). Befindet sich der Nutzer außerhalb von $\mathcal{Z}$, so ist der maximal mögliche Nutzen, der aus einer Aktion folgen kann, gegeben durch U(RN), da U(RN) > U(FP).

Die Differenz aus dem Nutzen der gewählten Aktion zu dem jeweiligen maximal möglichen Nutzen wird als Opportunitätsverlust bezeichnet [111]. Befindet sich der Nutzer in der Realität in $\mathcal{Z}$, so gilt $gtp \in \mathcal{Z}$ und für den Opportunitätsverlust folgt:

$$\text{Opportunitätsverlust} = \begin{cases} \text{U}\,(RP) - \text{U}\,(RP) & \text{falls } a^* = \texttt{aut} \\ \text{U}\,(RP) - \text{U}\,(FN) & \text{falls } a^* = \neg\texttt{aut} \end{cases} \tag{4.11}$$

Befindet sich der Nutzer in der Realität außerhalb von $\mathcal{Z}$, so gilt $gtp \notin \mathcal{Z}$ und für den Opportunitätsverlust gilt:

$$\text{Opportunitätsverlust} = \begin{cases} \text{U}\,(RN) - \text{U}\,(FP) & \text{falls } a^* = \texttt{aut} \\ \text{U}\,(RN) - \text{U}\,(RN) & \text{falls } a^* = \neg\texttt{aut} \end{cases} \tag{4.12}$$

Es existieren somit zwei Fälle, in denen kein Opportunitätsverlust auftritt. Je geringer im Mittel der Opportunitätsverlust ist, der aus Entscheidungen einer Autorisierungsstrategie entsteht, umso gewinnbringender bzw. nützlicher ist ihr Einsatz. Somit wird dieser Begriff eine zentrale Rolle bei der Evaluation und Analyse von standortbasierten Autorisierungsstrategien spielen.

4.1.2 Standortbasierte Autorisierungsstrategien

Im Folgenden sollen fünf standortbasierte Autorisierungsstrategien vorgestellt werden, welche das Grundprinzip der standortbasierten Autorisierung auf verschiedene Art und Weise realisieren. Dazu werden die Positiv- und Negativstrategie, die naive Strategie, die schwellwertbasierte Strategie und die risikobasierte Strategie vorgestellt. Die einzelnen Strategien unterscheiden sich in der Menge an Informationen, die zur Entscheidung berücksichtigt werden. Eine Übersicht dazu ist in Abb. 4.1 in Form eines Euler-Diagramms dargestellt. Prinzipiell steht die Abbildung U für den Nutzen, sowie die Positionsschätzung (μ, Σ) zur Verfügung. Wie zuvor in Abschnitt 3.1 eingeführt, ist μ der Mittelwert und Σ die Kovarianzmatrix einer WDF für die Nutzerposition.

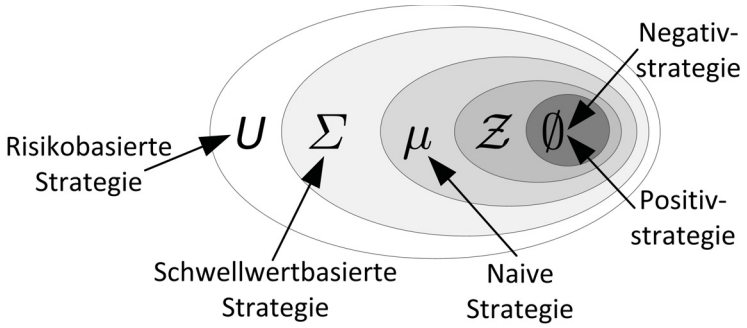


Abbildung 4.1: Die Menge der genutzten Informationen der einzelnen Strategien.

Positiv- und Negativstrategie Die einfachsten Autorisierungsstrategien sind die Positivstrategie und die Negativstrategie, die keine Informationen aus der Positionsschätzung für die Autorisierungsentscheidung verwenden. Die Positivstrategie autorisiert Nutzer an allen Standorten, wohingegen die Negativstrategie alle Anfragen ablehnt. Für die Positivstrategie gilt:

$$\text{aut}^{positiv}(\mu, \Sigma) \Leftrightarrow \texttt{wahr} \tag{4.13}$$

Im Gegensatz dazu entspricht die Negativstrategie dem Fall, dass jeder beliebige Standort des Nutzers zu einer negativen Auswertung der Ortsbeschränkung führt. Unter dieser Auswertungsstrategie wird somit niemals ein Zugriffsrecht gewährt, dem eine Ortsbeschränkung zugeordnet ist:

$$\text{aut}^{negativ}(\mu, \Sigma) \Leftrightarrow \texttt{falsch} \tag{4.14}$$

Beide Strategien sind theoretische Modelle, die in der Praxis nicht eingesetzt werden. Sie dienen lediglich als theoretische Vergleichsgröße zu den nachfolgend vorgestellten Strategien und sind im Allgemeinen in ihrem Verhalten irrational bzgl. ihrer Autorisierungsentscheidung.

Naive Strategie Die naive Strategie löst das Entscheidungsproblem ohne die Berücksichtigung des Nutzens der möglichen Ausgänge. Hierbei wird lediglich die Positionsschätzung μ und die autorisierte Zone $\mathcal{Z}$ verwendet. Ein möglicherweise entstehender Opportunitätsverlust aus einer Falschentscheidung aufgrund von Positionsfehlern wird hierbei außer Acht gelassen. Die naive Strategie ist folglich nur mit einem fiktiven, absolut präzisen und richtigen Positionierungssystem rational. Wie oben beschrieben, wird dieser Ansatz beinahe in allen verwandten Arbeiten zur standortbasierten Autorisierung eingesetzt. In standortbasiertem RBAC werden mittels der naiven Strategie z.B. die Mengen U, R, P und Relationen UA und RP beschränkt [1,21,63,115]. Im Allgemeinen führt diese Strategie lediglich einen Punkt-in-Polygon-Test durch, der prüft, ob die Position μ innerhalb der autorisierten Zone $\mathcal{Z}$ liegt:

$$\text{aut}^{naiv}(\mu, \Sigma) \Leftrightarrow \mu \in \mathcal{Z} \tag{4.15}$$

Der Vorteil dieser Strategie ist der geringe Rechenaufwand zur Herleitung einer Entscheidung und der Effizienz von Punkt-in-Polygon-Tests [112]. Insbesondere ist es für diese

Strategie nicht nötig eine Fehlerschätzung durchzuführen, um Σ herzuleiten. Es fallen keine komplexen numerischen Operationen zur Berechnung von Aufenthaltswahrscheinlichkeiten an.

Der Nachteil der naiven Strategie wird klar, wenn die Autorisierung über den maximal erwarteten Nutzen aus (4.10) mit der Autorisierungsfunktion (4.15) der naiven Strategie verglichen wird. Und zwar wird entsprechend (4.10) bei einer rationalen Autorisierungsentscheidung diejenige Aktion $a \in [\texttt{aut}; \neg\texttt{aut}]$ gewählt, deren Lotterie L_{aut} bzw. $L_{\neg\text{aut}}$ den größten erwarteten Nutzen hat. Damit die naive Strategie VNM-rational arbeitet, müssen alle Randbedingungen so beschaffen sein, dass der erwartete Nutzen aus (4.3) größer ist, als der erwartete Nutzen aus (4.4), falls $\mu \in \mathcal{Z}$ gilt. Ansonsten muss genau das umgekehrte Verhältnis gelten. Dies ist jedoch nur in dem speziellen und unrealistischen Fall erfüllt, wenn folgende Annahme gilt:

$$\mu \in \mathcal{Z} \Leftrightarrow gtp \in \mathcal{Z} \tag{4.16}$$

Aufgrund der Annahme geht die naive Strategie von einer falschen Aufenthaltswahrscheinlichkeit $p_{\mathcal{Z}}{}'$ aus, die von der realen Aufenthaltswahrscheinlichkeit $p_{\mathcal{Z}}$ im Allgemeinen abweicht. Insbesondere ist die Annahme, dass sich der Nutzer zu 100% Wahrscheinlichkeit innerhalb der autorisierten Zone $\mathcal{Z}$ befindet, sofern μ innerhalb von $\mathcal{Z}$ liegt. Andernfalls gilt $p_{\mathcal{Z}}{}' = 0$:

$$p_{\mathcal{Z}}{}'(\mu, \Sigma) = \begin{cases} 1 & \text{falls } \mu \in \mathcal{Z} \\ 0 & \text{sonst} \end{cases} \tag{4.17}$$

Die naive Strategie verhält sich wie ein VNM-rationaler Entscheider, der den erwarteten Nutzen der Lotterien L_{aut} bzw. $L_{\neg\text{aut}}$ mit dem falschen Wert $p_{\mathcal{Z}}{}'$ berechnet, anstelle die korrekte Aufenthaltswahrscheinlichkeit $p_{\mathcal{Z}}$ zu verwenden:

$$\mathrm{U}\left(L_{\text{aut}}\right) = \begin{cases} 1{,}0 \cdot \mathrm{U}\left(RP\right) + 0{,}0 \cdot \mathrm{U}\left(FP\right) & \text{falls } \mu \in \mathcal{Z} \\ 0{,}0 \cdot \mathrm{U}\left(RP\right) + 1{,}0 \cdot \mathrm{U}\left(FP\right) & \text{sonst} \end{cases} \tag{4.18}$$

$$\mathrm{U}\left(L_{\neg\text{aut}}\right) = \begin{cases} 0{,}0 \cdot \mathrm{U}\left(RN\right) + 1{,}0 \cdot \mathrm{U}\left(FN\right) & \text{falls } \mu \in \mathcal{Z} \\ 1{,}0 \cdot \mathrm{U}\left(RN\right) + 0{,}0 \cdot \mathrm{U}\left(FN\right) & \text{sonst} \end{cases} \tag{4.19}$$

Die naive Strategie verhält sich nun so, als dass sie stets die Aktion auswählt, die den größeren erwarteten Nutzen gemäß (4.18) bzw. (4.19) erzeugt. Mit echten Positionierungssystemen gilt die Annahme (4.16) natürlich nicht pauschal, weshalb $p_{\mathcal{Z}}{}' \neq p_{\mathcal{Z}}$ und die Aufenthaltswahrscheinlichkeit über- oder unterschätzt wird. Die Entscheidung aut bzw. ¬aut kann daher von einer VNM-rationalen Entscheidung, die unter Verwendung des korrekten Wertes $p_{\mathcal{Z}}$ ermittelt wird, abweichen.

Ein Beispiel sei eine Ortsbeschränkung mit $U(RP) = U(RN) = 1$ und $U(FP) = U(FN) = 0$. Gegeben sei eine Positionsschätzung (μ, Σ), für die $p_{\mathcal{Z}} \to 0$ und $\mu \in \mathcal{Z}$ gilt. Die naive Strategie autorisiert, da aufgrund der falschen Annahme der erwartete Nutzen einer Autorisierung größer scheint, als der erwartete Nutzen einer Ablehnung. Der tatsächlich

erwartete Nutzen gemäß (4.3) und (4.4) liefert jedoch $U(L_{\neg\text{aut}}) > U(L_{\text{aut}})$, so dass eine Ablehnung die rationalere Wahl ist. Dabei wird der korrekte Wert $p_{\mathcal{Z}}$ verwendet.

Je größer der durchschnittliche Positionsfehler, umso häufiger werden aufgrund der Annahme irrationale Entscheidungen durch die naive Strategie getroffen. Eine Analyse dieses Einflusses erfolgt später in dieser Arbeit.

Schwellwertbasierte Strategie Die schwellwertbasierte Autorisierungsstrategie beachtet zusätzlich die Information über die Aufenthaltswahrscheinlichkeit $p_{\mathcal{Z}}$ des Nutzers in der autorisierten Zone $\mathcal{Z}$. Deren Wert kann ermittelt werden, indem zunächst entsprechend Abschnitt 3.1 eine WDF vom Fehlerschätzer hergeleitet wird, die dann gemäß (3.18) über die autorisierte Zone $\mathcal{Z}$ integriert wird. Hierdurch wird bei der Autorisierungsentscheidung die Ungewissheit über die reale Nutzerposition berücksichtigt und muss einen zuvor definierten Schwellwert übersteigen:

$$\text{aut}^{schwellwert}(\mu, \Sigma) \Leftrightarrow p_{\mathcal{Z}}(\mu, \Sigma) > Schwellwert \tag{4.20}$$

In der Literatur ist dieser Ansatz jedoch nicht häufig vertreten, da oftmals Positionsfehler einfach ignoriert werden. Existierende Arbeiten nehmen keinen Bezug auf die konkrete Herleitung einer geeigneten Fehlerschätzung für Positionsschätzungen [8,82,130]. Die schwellwertbasierte ist gegenüber der naiven Strategie insofern benachteiligt, da sie nur eingesetzt werden kann, sofern eine WDF für die Nutzerposition vorliegt. Ferner entsteht zusätzlicher Aufwand aus der Berechnung von $p_{\mathcal{Z}}(\mu, \Sigma)$. Im Einsatz stellt sich außerdem die Frage, welcher Schwellwert für eine gegebene Ortsbeschränkung eines Zugriffsrechts eine geeignete Größe darstellt. Diese Fragestellung wird in der Literatur nicht ausreichend untersucht, sondern lediglich auf benötigtes Expertenwissen zur Definition solcher Schwellwerte verwiesen [7,8,26,130].

Auch hier besteht das Problem, dass irrationale Entscheidungen getroffen werden können. Übertragen auf die Lotterien (4.3) und (4.4) verhält sich die schwellwertbasierte Strategie nämlich so, als würde der über die Integration der WDF ermittelte Wert $p_{\mathcal{Z}}$ beim Treffen der Entscheidung gemäß (4.10) durch $p_{\mathcal{Z}}{}'$ ersetzt werden:

$$p_{\mathcal{Z}}{}'(\mu, \Sigma) = \begin{cases} 1 & \text{falls } p_{\mathcal{Z}}(\mu, \Sigma) > Schwellwert \\ 0 & \text{sonst} \end{cases} \tag{4.21}$$

Folglich geht die schwellwertbasierte Strategie davon aus, dass sich der erwartete Nutzen der Lotterien L_{aut} und $L_{\neg\text{aut}}$ folgendermaßen ergibt:

$$\mathrm{U}\,(L_{\text{aut}}) = \begin{cases} \mathrm{U}\,(RP) & \text{falls } p_{\mathcal{Z}}(\mu, \Sigma) > Schwellwert \\ \mathrm{U}\,(FP) & \text{sonst} \end{cases} \tag{4.22}$$

$$\mathrm{U}\,(L_{\neg\text{aut}}) = \begin{cases} \mathrm{U}\,(FN) & \text{falls } p_{\mathcal{Z}}(\mu, \Sigma) > Schwellwert \\ \mathrm{U}\,(RN) & \text{sonst} \end{cases} \tag{4.23}$$

Unter dieser Annahme wählt sie die Aktion mit dem größten erwarteten Nutzen.

Es lässt sich zeigen, dass Fälle existieren, in denen die schwellwertbasierte Strategie irrational handelt. Seien eine Ortsbeschränkung gemäß Def. 4.1.2 und eine Positionsschätzung (μ, Σ) gegeben, für die $0 < p_{\mathcal{Z}} < 1$ gilt. Ferner gelte $p_{\mathcal{Z}} > \textit{Schwellwert}$. Für die schwellwertbasierte Strategie gilt somit nach (4.22) und (4.23), dass $\mathrm{U}(L_{\mathrm{aut}}) > \mathrm{U}(L_{\neg\mathrm{aut}})$, weshalb sie autorisiert. Dieses Verhalten ist nicht VNM-rational, falls der tatsächliche erwartete Nutzen, der sich unter Verwendung des korrekten Wertes $p_{\mathcal{Z}}$ anstelle von $p_{\mathcal{Z}}{}'$ ergibt, für $\mathrm{U}(L_{\mathrm{aut}})$ kleiner als der erwartete Nutzen $\mathrm{U}(L_{\neg\mathrm{aut}})$ ist. Dies ist der Fall, wenn unter Verwendung von $p_{\mathcal{Z}}$ die Ungleichung $\mathrm{U}(L_{\mathrm{aut}}) > \mathrm{U}(L_{\neg\mathrm{aut}})$ nicht erfüllt ist. Aus Umformung ergibt sich:

$$\frac{p_{\mathcal{Z}}}{(1-p_{\mathcal{Z}})} > \frac{\mathrm{U}(RN) - \mathrm{U}(FP)}{\mathrm{U}(RP) - \mathrm{U}(FN)} \tag{4.24}$$

Es zeigt sich, dass Werte $\mathrm{U}(RN)$, $\mathrm{U}(RP)$, $\mathrm{U}(FP)$ und $\mathrm{U}(FN)$ existieren, für welche die Ungleichung (4.24) nicht erfüllt ist und somit eine Ablehnung die Aktion mit dem größeren erwarteten Nutzen ist. Die schwellwertbasierte Strategie autorisiert in diesem Fall jedoch unabhängig von U und entscheidet in diesen Fällen nicht VNM-rational.

Risikobasierte Strategie Die risikobasierte Strategie verwendet zusätzlich die Information über die Abbildung U des Nutzens [82,95]. In der Literatur ist sie bisher noch nicht zusammen mit einer WDF für die Fehlerschätzung eingesetzt worden. Sie beruht auf der grundlegenden Idee sich genau für die Aktion $a \in \{\mathrm{aut}; \neg\mathrm{aut}\}$ zu entscheiden, deren Lotterie den größten erwarteten Nutzen bringt. Das Risiko des Opportunitätsverlusts wird somit minimiert. Der erwartete Nutzen der beiden Lotterien berechnet sich hierbei direkt entsprechend (4.3) und (4.4). Der Wert $p_{\mathcal{Z}}$, der dazu von den Lotterien benötigt wird, leitet sich bei dieser Strategie direkt aus der WDF vom Fehlerschätzer ab. Dazu wird die WDF über die autorisierte Zone $\mathcal{Z}$ integriert. Der Nutzer wird schließlich autorisiert, wenn der erwartete Nutzen einer Autorisierung den erwarteten Nutzen einer Ablehnung übersteigt:

$$\mathrm{aut}^{risikobasiert}(\mu, \Sigma) \Leftrightarrow p_{\mathcal{Z}}\mathrm{U}(RP) + (1-p_{\mathcal{Z}})\,\mathrm{U}(FP) > p_{\mathcal{Z}}\mathrm{U}(FN) + (1-p_{\mathcal{Z}})\,\mathrm{U}(RN) \tag{4.25}$$

Der benötigte Rechenaufwand entspricht der schwellwertbasierten Strategie, da ebenfalls eine Fehlerschätzung und die Berechnung der Aufenthaltswahrscheinlichkeit anfallen. Ein weiterer Vorteil dieser Strategie ist, dass kein Schwellwert gewählt werden muss, sondern nur die Abbildung U für den Nutzen benötigt wird. Deren Herleitung kann entsprechend Unterabschnitt 4.1.1 erfolgen. In der Theorie ist der größte Vorteil die Optimalität aus Sicht der Entscheidungstheorie, die jedoch nur erreicht werden kann, sofern die Statistik der Schätzfehler perfekt bekannt ist. Wie sich diese Abhängigkeit von der Qualität des Fehlerschätzers jedoch in der Praxis auswirkt, wird später in Abschnitt 5.2 untersucht.

Aus der risikobasierten Strategie ergeben sich zwei wichtige Eigenschaften.

Satz 4.1.1 (Autorisierungsäquivalenz)**.** *Gegeben seien zwei verschiedene Ortsbeschränkungen o_1 und o_2 mit unterschiedlichen Abbildungen U_1 und U_2 für den Nutzen, der gleichen autorisierten Zone $\mathcal{Z}$, auf die jeweils die risikobasierte Strategie angewendet wird. Sie trifft*

für o_1 die Entscheidung aut_1 *und für o_2 die Entscheidung* aut_2*. Falls es eine positive reelle Zahl $c \in \mathbb{R}^+$ gibt, mit:*

$$\begin{aligned}[U_1(RN) - U_1(FP)] &= c \cdot [U_2(RN) - U_2(FP)] \\ \wedge [U_1(RP) - U_1(FN)] &= c \cdot [U_2(RP) - U_2(FN)]\end{aligned}$$

Dann gilt, dass aut_1 *und* aut_2 *für jede beliebige Positionsschätzung (μ, Σ) die gleiche Autorisierungsentscheidung darstellen:*

$$\Longrightarrow \forall(\mu, \Sigma) : \text{aut}_1(\mu, \Sigma) = \text{aut}_2(\mu, \Sigma)$$

Beweis. Gegeben sei der Wert $p_{\mathcal{Z}}$, der aus (μ, Σ) folgt. Die Autorisierungsentscheidung für o_1 und o_2 ist identisch, falls die Ungleichung in (4.25) in beiden Fällen gleich auswertet. Aus Umformung von (4.25) ergibt sich:

$$\begin{aligned}
p_{\mathcal{Z}}\mathrm{U}(RP) + (1 - p_{\mathcal{Z}})\,\mathrm{U}(FP) &> p_{\mathcal{Z}}\mathrm{U}(FN) + (1 - p_{\mathcal{Z}})\,\mathrm{U}(RN) && \Leftrightarrow \\
(1 - p_{\mathcal{Z}})\,\mathrm{U}(FP) - (1 - p_{\mathcal{Z}})\,\mathrm{U}(RN) &> p_{\mathcal{Z}}\mathrm{U}(FN) - p_{\mathcal{Z}}\mathrm{U}(RP) && \Leftrightarrow \\
(1 - p_{\mathcal{Z}})\,[\mathrm{U}(FP) - \mathrm{U}(RN)] &> p_{\mathcal{Z}}\,[\mathrm{U}(FN) - \mathrm{U}(RP)] && \Leftrightarrow \\
(1 - p_{\mathcal{Z}})\,\underbrace{[\mathrm{U}(RN) - (UFP)]}_{\stackrel{!}{=} t} &< p_{\mathcal{Z}}\,\underbrace{[\mathrm{U}(RP) - \mathrm{U}(FN)]}_{\stackrel{!}{=} u} && \Leftrightarrow \\
(1 - p_{\mathcal{Z}}) \cdot t &< p_{\mathcal{Z}} \cdot u
\end{aligned}$$

Aufgrund der Definition von Ortsbeschränkungen gilt $U(RP) > U(FN)$ und $U(RN) > U(FP)$, weshalb $u > 0$ und $t > 0$ gilt. Somit folgt:

$$\frac{t}{u} > \frac{p_{\mathcal{Z}}}{(1 - p_{\mathcal{Z}})} \tag{4.26}$$

Sei nun $u_1 = [\mathrm{U}_1(RP) - \mathrm{U}_1(FN)]$ und $u_2 = [\mathrm{U}_2(RN) - \mathrm{U}_2(FP)]$. Entsprechend erfolgt die Substitution mit t_1 und t_2. Ist die Prämisse des Satzes erfüllt so gilt:

$$\text{aut}_1(\mu, \Sigma) = \text{aut}_2(\mu, \Sigma) \Leftrightarrow \left(\frac{t_1}{u_1} > \frac{p_{\mathcal{Z}}}{(1 - p_{\mathcal{Z}})}\right) = \left(\frac{t_2}{u_2} > \frac{p_{\mathcal{Z}}}{(1 - p_{\mathcal{Z}})}\right) \tag{4.27}$$

Aufgrund der Prämisse gilt: $t_1/c = t_2$ und $u_1/c = u_2$. Durch Einsetzen und Kürzen von c ergibt sich:

$$\text{aut}_1(\mu, \Sigma) = \text{aut}_2(\mu, \Sigma) \Leftrightarrow \left(\frac{t_1}{u_1} > \frac{p_{\mathcal{Z}}}{(1 - p_{\mathcal{Z}})}\right) = \left(\frac{t_1}{u_1} > \frac{p_{\mathcal{Z}}}{(1 - p_{\mathcal{Z}})}\right) \Leftrightarrow \frac{t_1}{u_1} > \frac{p_{\mathcal{Z}}}{(1 - p_{\mathcal{Z}})} \tag{4.28}$$

□

Sei $u_i := [\mathrm{U}_i(RP) - \mathrm{U}_i(FN)]$ und $t_i := [\mathrm{U}_i(RN) - \mathrm{U}_i(FP)]$. Zwei Ortsbeschränkungen o_1, o_2 verhalten sich in der risikobasierten Strategie gleich, sofern das Verhältnis von u zu t für o_1 und o_2 gleich ist:

Korollar 4.1.1 (Autorisierungsäquivalenz aus Nutzenverhältnis)**.** *Für zwei verschiedene Ortsbeschränkungen o_1 und o_2 mit unterschiedlichen Abbildungen* U_1 *und* U_2 *für den Nutzen, der gleichen autorisierten Zone $\mathcal{Z}$ und den Entscheidungen der risikobasierten Strategie* aut_1 *für o_1 bzw.* aut_2 *für o_2 gilt:*

$$\frac{u_1}{t_1} = \frac{u_2}{t_2} \implies \forall(\mu, \Sigma) : \mathrm{aut}_1(\mu, \Sigma) = \mathrm{aut}_2(\mu, \Sigma)$$

Beweis. Folgt direkt aus der Umformung der Prämisse aus Satz 4.1.1. □

Auch wenn die Prämisse von Satz 4.1.1 erfüllt ist und somit zwei Ortsbeschränkungen stets gleichzeitig autorisiert oder abgelehnt werden, so erzielen sie trotzdem im Allgemeinen einen unterschiedlichen Opportunitätsverlust. Dies folgt direkt aus der Tatsache, dass jede Ortsbeschränkung eine unterschiedliche Abbildung U für den Nutzen haben kann und somit (4.11) bzw. (4.12) andere Ergebnisse liefern.

Der nächste Satz zeigt, dass auch die schwellwertbasierte Strategie in bestimmten Fällen risiko-optimal arbeitet, sofern der richtige Schwellwert gewählt wird.

Satz 4.1.2 (Optimaler Schwellwert)**.** *Für jede Ortsbeschränkung eines Zugriffsrechts existiert ein Schwellwert, so dass für jede fixe Positionsschätzung (μ, Σ) die schwellwertbasierte und die risikobasierte Strategie die gleiche Autorisierungsentscheidung treffen:*

$$\begin{aligned}\forall o \in \mathbb{O}\ \exists \mathit{Schwellwert} \in [0;1]\ \ \forall(\mu, \Sigma) : p_{\mathcal{Z}} > \mathit{Schwellwert} \\ \Leftrightarrow p_{\mathcal{Z}}\mathrm{U}\,(\mathit{RP}) + (1 - p_{\mathcal{Z}})\,\mathrm{U}\,(\mathit{FP}) > p_{\mathcal{Z}}\mathrm{U}\,(\mathit{FN}) + (1 - p_{\mathcal{Z}})\,\mathrm{U}\,(\mathit{RN})\end{aligned} \quad (4.29)$$

Beweis. Ausgangspunkt ist zunächst die Substitution entsprechend des Beweises von Satz 4.1.1 und Umformung des rechten Teils:

$$\forall o \in \mathbb{O}\ \exists \mathit{Schwellwert} \in [0;1]\ \ \forall(\mu, \Sigma) : p_{\mathcal{Z}} > \mathit{Schwellwert} \Leftrightarrow (1 - p_{\mathcal{Z}}) \cdot t\ <\ p_{\mathcal{Z}} \cdot u \quad (4.30)$$

Aus Umformung folgt:

$$\forall o \in \mathbb{O}\ \exists \mathit{Schwellwert} \in [0;1]\ \ \forall(\mu, \Sigma) : p_{\mathcal{Z}} > \mathit{Schwellwert} \Leftrightarrow t < p_{\mathcal{Z}}\,(u + t) \quad (4.31)$$

Die Idee ist, durch Auflösen des rechten Teils nach $p_{\mathcal{Z}}$, den Wert $p_{\mathcal{Z}}$ zu erhalten, ab dem die risikobasierte Strategie autorisiert. Setzt man diesen als Schwellwert ein, ergibt sich das gleiche Verhalten. Die rechte Seite gibt genau dann `wahr`, wenn:

$$\frac{t}{u + t}\ <\ p_{\mathcal{Z}} \quad (4.32)$$

Die Umformung ist stets möglich, da aufgrund der Definition von Ortsbeschränkungen $U(\mathit{RP}) > U(\mathit{FN})$ und $U(\mathit{RN}) > U(\mathit{FP})$ gilt. Setzt man nun den *Schwellwert* entsprechend als $\frac{t}{u+t}$, so verhält sich die schwellwertbasierte Strategie identisch zur risikobasierten Strategie. □

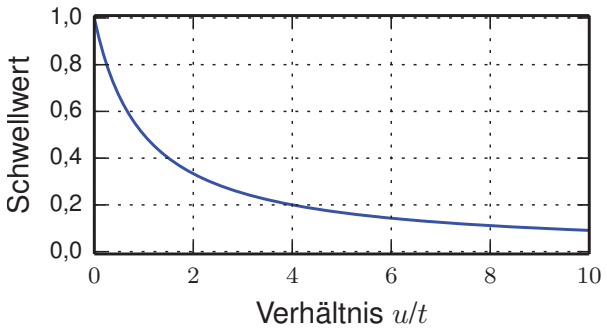


Abbildung 4.2: Benötigte Schwellwerte in Abhängigkeit vom Verhältnis $[\mathrm{U}(RP) - \mathrm{U}(FN)] / [U(RN) - (UFP)] = u/t$, so dass die schwellwert- und die risikobasierte Strategie gleich entscheiden.

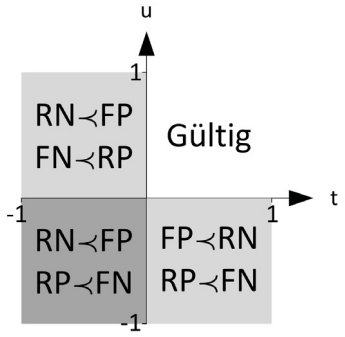


Abbildung 4.3: Gültige Ortsbeschränkungen erfüllen die Bedingung $t > 0$ und $u > 0$.

Der implizierte Schwellwert ist in Abb. 4.2 dargestellt. Krautsevich et al. berechnen in [82] ebenfalls einen optimalen Schwellwert für die schwellwertbasierte Strategie. Das Wissen über den Zusammenhang zwischen schwellwert- und risikobasierter Strategie hat den Vorteil, dass der schwellwertbasierten Strategie ein nachvollziehbarer Schwellwert zugewiesen werden kann. Für dessen Herleitung wird lediglich die Abbildung U für den Nutzen benötigt. Unter dem so ermittelten Schwellwert entspricht die schwellwertbasierte Strategie der risikobasierten Strategie und arbeitet daher aus entscheidungstheoretischer Sicht VNM-rational.

Anhand der Substitutionen u und t sind gültige Ortsbeschränkungen im Kontrast zu den theoretisch möglichen Ortsbeschränkungen in Abb. 4.3 dargestellt. Das besondere an gültigen Ortsbeschränkungen ist, dass u und niemals t negativ sind. Für die Abbildung U für den Nutzen heißt das, dass stets $\mathrm{U}(RP) > \mathrm{U}(FN) \ \wedge \ \mathrm{U}(RN) > \mathrm{U}(FP)$ gilt. Gilt $U(RN) < U(FP)$ würde die Ortsbeschränkung stets autorisieren. Gilt $U(RP) < U(FN)$, würde die Ortsbeschränkung stets ablehnen. Würde $U(RN) < U(FP) \wedge U(RP) < U(FN)$ gelten, so tritt in gewisser Weise eine Inversion der Ortsbeschränkung auf, da eine hohe Aufenthaltswahrscheinlichkeit im Gebiet außerhalb von $\mathcal{Z}$ zur Autorisierung benötigt ist. Wird dieses Gebiet als $\mathcal{Z}$ definiert, so kann die Abbildung U so modifiziert werden, dass die Ortsbeschränkungen gemäß Def. 4.1.2 gültig ist.

Im praktischen Einsatz hängen die schwellwert- und risikobasierte Strategie von der Qualität des Fehlerschätzers für die Nutzerposition ab. Statistisch mangelhafte Fehlerschätzer können schließlich den tatsächlichen Wert von $p_{\mathcal{Z}}$ im Mittel über- oder unterschätzen und somit zu suboptimalen Entscheidungen führen. Diese Thematik wird in Kapitel 5 detailliert behandelt.

Erweiterte risikobasierte Strategie Alle bisher vorgestellten Strategien verfolgten das Ziel, die Autorisierung für ein Zugriffsrecht daran zu koppeln, ob sich der anfragende Nutzer innerhalb einer autorisierten Zone befindet. Die erweiterte risikobasierte Strategie verfolgt hingegen den allgemeineren Ansatz, zu fordern, dass der Standort des Nutzers eine konkrete Eigenschaft besitzt. Im Folgenden wird, basierend auf einer Vorarbeit, die erweiterte risikobasierte Strategie aus Marcus et al. [100] vorgestellt. Anstelle der bisher verwendeten autorisierten Zonen wird eine diskrete Zufallsvariable E eingeführt, welche beschreibt, ob eine für die Autorisierung geforderte Eigenschaft gegeben ist. Um die Wahrscheinlichkeit zu bestimmen, mit der eine konkrete Realisierung e an einem bestimmten Ort x beobachtet werden kann, werden Eigenschaftsmodelle eingeführt:

Definition 4.1.3 (Eigenschaftsmodell)**.** *Ein Eigenschaftsmodell ist definiert als die bedingte Wahrscheinlichkeitsverteilung $P(E|X)$, wobei $P(E = e|X = x)$ für einen Ort x die Wahrscheinlichkeit beschreibt, dass an x die geforderte Eigenschaft e beobachtet werden kann.*

Hierbei gilt zu beachten, dass im Folgenden Verteilungen über eine Zufallsvariable E als $\mathrm{P}(E)$ angegeben werden. Einzelwahrscheinlichkeiten für $E = e$ werden als $\mathrm{P}(e)$ notiert. Die eingeführten Eigenschaftsmodelle werden im Folgenden als Generalisierung des existierenden Polygonkonzepts verwendet, was durch drei unterschiedliche Beispiele verdeutlicht werden soll. Für einen fixen Zeitpunkt kann basierend auf einem Eigenschaftsmodell $\mathrm{P}(E|X)$ und einer Positionsschätzung für einen Nutzer n die Wahrscheinlichkeit bestimmt werden, mit der an seinem Standort die geforderte Eigenschaft tatsächlich zu beobachten ist. Die Verteilung $\mathrm{P}(E)$ ergibt sich dann aus der Marginalisierung des Eigenschaftsmodells bzgl. der WDF aus der Positionsschätzung (μ, Σ) von Nutzer n, welche gemäß (3.6) z.B. durch $wdf^{laplace}_{\mathbf{F}|\mu,\sigma}$ beschrieben ist:

$$\mathrm{P}(e) = \int_X \mathrm{P}(e|X = x) \cdot wdf^{laplace}_{\mathbf{F}|\mu,\sigma}(x)\,\mathrm{d}x \tag{4.33}$$

Somit erlaubt (4.33) die Herleitung der Wahrscheinlichkeit $\mathrm{P}(e)$, mit der am wahren Standort des Nutzers zum Zeitpunkt t, zu dem die Positionsschätzung erstellt wurde, die geforderte Eigenschaft beobachtet werden konnte. Darauf basierend kann die Autorisierungsfunktion als Erweiterung von (4.25) angegeben werden:

$$\begin{aligned} \mathrm{aut}^{risikobasiert+}(\mu, \Sigma) \Leftrightarrow \quad & \mathrm{P}(e)\mathrm{U}\,(RP) + (1 - \mathrm{P}(e))\,\mathrm{U}\,(FP) && (4.34)\\ > & \mathrm{P}(e)\mathrm{U}\,(FN) + (1 - \mathrm{P}(e))\,\mathrm{U}\,(RN) && (4.35) \end{aligned}$$

Dies entspricht (4.25), jedoch wird $p_{\mathcal{Z}}$, also die Aufenthaltswahrscheinlichkeit in $\mathcal{Z}$, durch die Wahrscheinlichkeit $\mathrm{P}(e)$ ersetzt, dass am aktuellen Standort des Nutzers die geforderte Eigenschaft E beobachtet werden kann. Die Spezifikation einer erweiterten Ortsbeschränkung erfolgt dann als Tupel $(\mathrm{P}(E|X), \mathrm{U})$ unter Beibehaltung der Anforderungen an die Funktion U. Die Herleitung von Eigenschaftsmodellen für Zugriffsrechte soll im Folgenden an drei Beispielen verdeutlicht werden.

Beispiel 4.1.3. *Im ersten Beispiel sei ein einzelnes Büro $\mathcal{Z}$ innerhalb eines Gebäudes identifiziert, welches die Eigenschaft $E_{vertraulich}$ erfüllt, dass dort streng vertrauliche Firmendaten eingesehen werden dürfen, da nur Personen der Führungsschicht Zutritt haben. In solchen Fällen sind die Orte mit der nötigen Eigenschaft scharf auf das Polygon des Büros begrenzt. Alle Punkte $x \in \mathcal{Z}$ erfüllen offensichtlich die Eigenschaft, innerhalb des Büros zu liegen, wodurch sich folgende Definition von $P(E_{vertraulich}|X)$ ergibt:*

$$P(e_{vertraulich}|x) = \begin{cases} 1, & falls\ x \in \mathcal{Z} \\ 0, & sonst \end{cases} \tag{4.36}$$

Ein entsprechendes Beispiel ist in Abb. 4.4 dargestellt. Mit diesem Beispiel zeigt sich, wie alle Fälle der risikobasierten Autorisierung auch über die erweiterte risikobasierte Autorisierung abgebildet werden können.

Ist die geforderte Eigenschaft an einem Ort x nicht in allen Fällen zu beobachten, so wird in allen oben beschriebenen Autorisierungsstrategien die benötigte Definition einer autorisierten Zone zu einer schwierigen Aufgabe.

Beispiel 4.1.4. *Gegeben sei ein Zugriffsrecht, das es Mitarbeitern einer Fabrik erlaubt, über ihr mobiles Endgerät eine physisch vorhandene Maschine zu steuern. Ferner schreiben gesetzliche Auflagen vor, dass Mitarbeiter dieses Zugriffsrecht nur verwenden dürfen, falls es von ihrem aktuellem Standort möglich ist, den Notausschalter der Maschine innerhalb einer Zeit von t Sekunden physisch zu erreichen. Unter der Annahme, dass die Schrittgeschwindigkeit von Menschen zufällig verteilt ist, kann keine geeignete autorisierte Zone angegeben werden. Benötigt wird also ein Eigenschaftsmodell $\mathrm{P}\left(E_{erreichbar}|X\right)$, welches für jeden Punkt x auf dem Gebäudeplan beschreibt, mit welcher Wahrscheinlichkeit ein Mensch den Notausschalter von dort aus innerhalb von t Sekunden erreichen kann.*

Ein entsprechendes Eigenschaftsmodell kann in zwei Schritten erstellt werden. Zunächst muss die Lage des Notausschalters auf dem Gebäudeplan identifiziert werden, den ein Nutzer innerhalb einer gewissen Zeit erreichen muss. Im nächsten Schritt wird die Distanz zu diesem spezifischen Punkt für alle anderen Punkte auf der Karte berechnet. Dies ist in Abb. 4.6 dargestellt. Um aus dem Distanzmodell ein Eigenschaftsmodell herzuleiten, muss für jeden Punkt eine minimal geforderte Geschwindigkeit v_{min} bestimmt werden, damit der Notausschalter in maximal t Sekunden erreichbar ist.

Dazu wird zuerst die Distanz des Punkts durch die maximal erlaubte Zeitspanne t dividiert. Für einen beliebigen Punkt x ergibt sich schließlich der Wert von $\mathrm{P}\left(e_{erreichbar}|x\right)$ aus der Überlebensfunktion (engl. Survival Function) einer kumulativen Verteilung für die menschliche Schrittgeschwindigkeit. Im vorliegenden Beispiel wird eine Normalverteilung mit einem Mittelwert von 1,31 $\frac{m}{s}$ und einer Standardabweichung von 0,22 $\frac{m}{s}$ gewählt [103]. Das Eigenschaftsmodell, das sich hieraus aus dem Distanzmodell von Abb. 4.6 mit einem Zeitlimit von 6 s ergibt, ist in Abb. 4.7 dargestellt. Offensichtlich wird in so berechneten Eigenschaftsmodellen nicht berücksichtigt, dass Menschen langsamer werden, wenn Sie um Ecken gehen bzw. dass eine Mindestdistanz zu Wänden eingehalten wird. Trotzdem ergibt sich eine gute Approximation der Wahrscheinlichkeit, den spezifischen Punkt innerhalb der

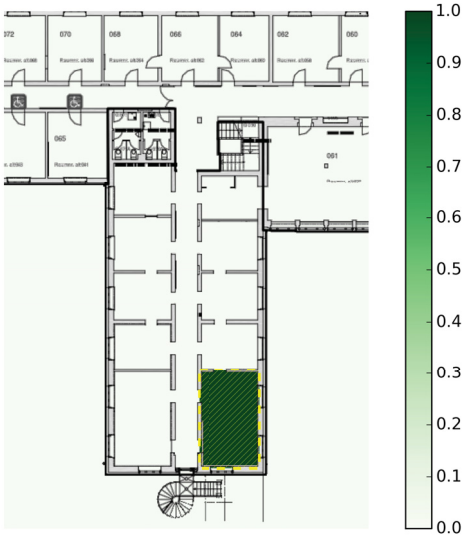


Abbildung 4.4: Gleichförmige Wahrscheinlichkeit von 1,0 innerhalb eines Raumes.

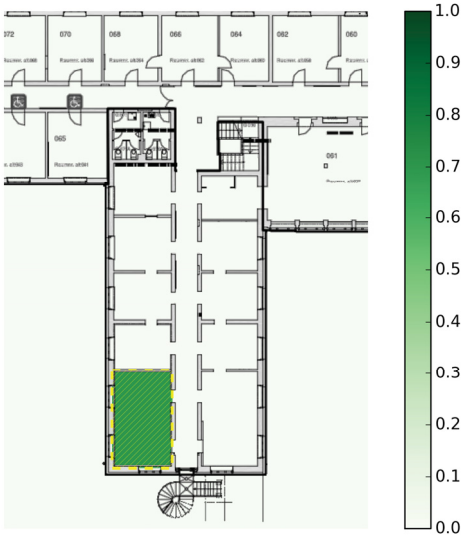


Abbildung 4.5: Gleichförmige Wahrscheinlichkeit von 0,7 innerhalb eines Raumes.

geforderten Zeit zu erreichen. In Abb. 4.7 ist zusätzlich ein Polygon dargestellt, das alle Punkte umschreibt, die eine Wahrscheinlichkeit größer 0,5 *besitzen. Dieses Polygon würde somit eine Möglichkeit zur Modellierung einer autorisierten Zone darstellen, um das gewünschte Verhalten in den oben vorgestellten Ansätzen zur standortbasierten Autorisierung zu approximieren.*

Es sei angemerkt, dass entsprechende Eigenschaftsmodelle auch eingesetzt werden können, wenn vom aktuellen Nutzerstandort z.B. eine Kontrollanzeige auf der physischen Maschine noch ablesbar sein muss. Wendet man statt der Verteilung der Schrittgeschwindigkeiten eine Verteilung der Lesbarkeit in Abhängigkeit von der Entfernung an, so kann auch ein solches Szenario abgebildet werden. Durch das vorgestellte Konzept können nicht nur Ortsbeschränkungen, die aus Arbeitsschutzrichtlinien stammen, zur Herleitung von $P(E|X)$ verwendet werden, sondern auch sicherheitsrelevante Überlegungen.

Beispiel 4.1.5. *In diesem Beispiel wird eine erweiterte Ortsbeschränkung auf einem Eigenschaftsmodell definiert, um die Informationssicherheit in einer Zugriffskontrollstrategie* $\mathcal{A}$ *(z.B. MAC, DAC oder RBAC) zu steigern. Es sei ein Bürogebäude gegeben, worin Büro* $\mathcal{Z}$ *durch eine physische Zutrittskontrolle geschützt ist, z.B. durch eine verschlossene Türe mit zugehörigen Schlüsseln oder RFID–Karten. Befindet sich ein Nutzer innerhalb von* $\mathcal{Z}$*, so ist bekannt, dass er zu dem Personenkreis gehört, der den Schlüssel besitzt. Die Menge der Personen, die physischen Zutritt zu einem Punkt* x *besitzen, ist eine Eigenschaft eines jeden Ortes. Gibt es nun in* $\mathcal{A}$ *ein Zugriffsrecht* b*, so kann Missbrauch entstehen, wenn das mobile Endgerät eines dafür autorisierten und bereits eingeloggten Nutzers gestohlen und zur Ausübung von* b *verwendet wird.*

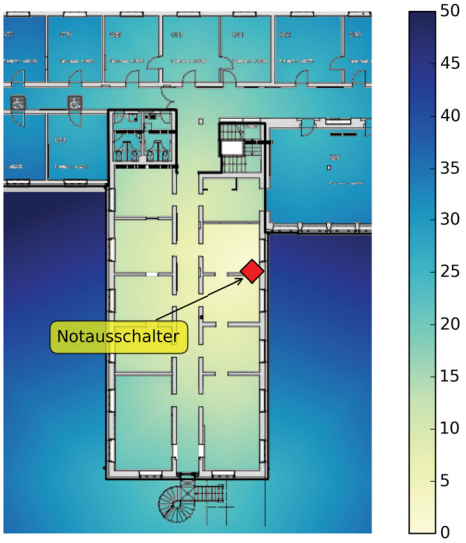


Abbildung 4.6: Entfernungen in Metern zum Notausschalter.

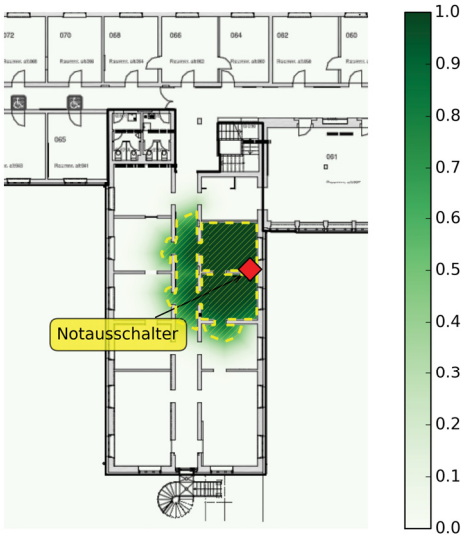


Abbildung 4.7: Eigenschaftsmodell mit einem 50%–Polygon.

Begrenzt man ein Zugriffsrecht b auf das Büro $\mathcal{Z}$, so muss der Dieb ebenfalls die Schlüssel zum Büro $\mathcal{Z}$ besitzen. Die Identität eines solchen Diebes kann also auf den Personenkreis begrenzt werden, der Zutritt zum Büro hat.

Dazu wird ein Eigenschaftsmodell definiert, welches für jeden Ort $x \in \mathcal{Z}$ die Wahrscheinlichkeit beschreibt, dass sich dort eine Person aufhält, die selbst ein Nutzerkonto mit Autorisierung für b besitzt. Alle Nutzerkonten aus $\mathcal{A}$, die für b autorisiert sind, seien im Folgenden als N bezeichnet. Das Eigenschaftsmodell ergibt sich somit aus dem Quotienten der Mächtigkeit der Menge an Personen die ein Nutzerkonto, das für b autorisiert ist und einen Schlüssel für $\mathcal{Z}$ haben und der Mächtigkeit der Menge aller Personen, die physischen Zugang zum Ort x besitzen:

$$P(e|X = x) = \frac{|\{n \in N \,|\, \mathcal{A}\ \texttt{autorisiert}\ n\ \texttt{für}\ b \wedge \texttt{hat\_zugang}(n, x)\}|}{|\{p \in \mathit{Personen} \,|\, \texttt{hat\_zugang}(p, x)\}|} \tag{4.37}$$

Hierbei gilt $N \subseteq$ Personen. Das Prädikat `hat_zugang` *bezeichnet dabei, ob eine real existierende Person die nötigen physischen Schlüssel besitzt, um den Ort x zu betreten und sich dort aufzuhalten. Für den Fall, dass 10 Personen Zugang zu $\mathcal{Z}$ haben, aber davon nur 7 Personen in $\mathcal{A}$ das Zugriffsrecht b zugeordnet ist, stellt Abb. 4.5 das entsprechende Eigenschaftsmodell dar.*

4.2 Die Erweiterung von rollenbasierter Zugriffskontrolle durch Ortsbeschränkungen

Im praktischen Einsatz werden klassische Zugriffskontrollmodelle eingesetzt, um Zugriffsrechte zu modellieren. Eines der verbreitetsten Modellen ist RBAC [121], das standardmäßig jedoch keine Berücksichtigung des Nutzerstandorts erlaubt. Im Folgenden wird deshalb eine Erweiterung von RBAC durch Ortsbeschränkungen vorgestellt, die von Marcus et al. in [100] veröffentlicht wurde. Hierzu wird die erweiterte risikobasierte Autorisierung auf RBAC angepasst. Wie bereits in Unterabschnitt 2.2.1 erklärt, werden im klassischen RBAC einem Nutzer Rollen zugeordnet, die ihn jeweils zur Nutzung einer Menge von Zugriffsrechten autorisieren. Im nächsten Schritt startet der Nutzer eine RBAC-Sitzung und wählt eine Teilmenge der zugeordneten Rollen aus, was ihm schließlich die zugeordneten Zugriffsrechte für die Dauer seiner Sitzung bereitstellt. Im ursprünglich entwickelten Ansatz für RBAC können während einer offenen Sitzung auf einem mobilen Endgerät, z.B. einem Smartphone oder Tablet–Computer, generell von jedem beliebigem Ort Anfragen zur Nutzung von Zugriffsrechten veranlasst werden. Solche Anfragen dürfen aber nicht gewährt werden, falls der Standort des Nutzers nicht wichtige Eigenschaften erfüllt, die für die Benutzung der angefragten Zugriffsrechte erforderlich sind. Beispielsweise kann eine solche Eigenschaft sein, dass sich der Nutzer auf dem Firmengelände befindet, sofern er ein Zugriffsrecht zur Einsicht vertraulicher Unternehmensdaten nutzen möchte. Ebenfalls kann es in einer Fabrikhalle erforderlich sein, das Zugriffsrecht zur Steuerung von physischen Maschinen mittels eines Tablet–Computers auf dafür geeignete Orte zu beschränken. Solche Orte können z.B. genau die sein, von denen der Nutzer den Notausschalter der Maschine innerhalb einer vordefinierten Zeitspanne erreichen kann.

Um diese Semantik zu realisieren, wurden in der Literatur bisher standortbasierte Erweiterungen zu RBAC vorgestellt, die den Nutzerstandort verwenden, um über die Autorisierung von angefragten Zugriffsrechten zu entscheiden. Die meisten dieser Ansätze beschränken die Verfügbarkeit von Rollen oder Zugriffsrechten in RBAC-Richtlinien auf Nutzer innerhalb vordefinierter geographischer Polygone, den autorisierten Zonen. Im praktischen Einsatz mit echten Positionierungssystemen wird die Umsetzung dieser Ansätze jedoch durch das Auftreten von Positionsfehlern erschwert. Bisher wurde in der Literatur noch kein Ansatz vorgestellt, der hierbei den Opportunitätsverlust aufgrund von Positionsfehlern in Autorisierungsentscheidungen berücksichtigt. Ein weiterer Nachteil der existierenden Erweiterungen von RBAC-Richtlinien ist, dass diese lediglich auf Polygonen zur Definition von autorisierten Zonen basieren. Hierdurch wird die Abbildung von Szenarien, wie dem beschriebenen Notausschalter, unnatürlich erschwert.

Aufgrund dieser Lücken wird im Folgenden ein Ansatz zur standortbasierten Erweiterung von RBAC entwickelt, der Positionsfehler berücksichtigt und eine Anpassung der erweiterten risikobasierten Strategie anwendet [100]. Im Folgenden soll dieser Ansatz vorgestellt werden. Anstelle von Polygonen werden einzelnen Elementen einer RBAC-Richtlinie durch Ortsbeschränkungen zwei Informationen zugeordnet. Dies sind jeweils ein Eigenschaftsmodell, als auch eine Abbildung U für ihren Nutzen. Das neue Konzept eines Eigen-

schaftsmodells beschreibt für jeden möglichen Ort x die Wahrscheinlichkeit, mit der eine geforderte Eigenschaft beobachtet werden kann - beispielsweise das Erreichen des Notausschalters innerhalb einer zeitlichen Frist oder der Aufenthalt auf dem Firmengelände. Diese Modelle generalisieren das bisherige Konzept der autorisierten Zonen. Die zugeordnete Abbildung U verhält sich wie oben eingeführt und ist analog für die vier Fälle *RP*, *RN*, *FP* und *FN* definiert. Im Gegensatz zu Arbeiten in der Literatur, in denen Positionsschätzungen als einfache Koordinaten bereitgestellt werden, basiert der entwickelte Ansatz auf der Verwendung von WDFs, wie sie z.B. durch den Ansatz in Kapitel 3.1 bereitgestellt werden. Wird eine solche WDF über das Eigenschaftsmodell integriert, so kann die Wahrscheinlichkeit abgeschätzt werden, mit der am Nutzerstandort die geforderte Eigenschaft beobachtbar ist. Dies erlaubt schließlich den erwarteten Nutzen abzuschätzen, der daraus folgt, das RBAC-Element in der aktuellen RBAC-Sitzung verfügbar oder nicht verfügbar zu machen. Die Ortsbeschränkungen werden schließlich risikobasiert durchgesetzt, indem für jedes RBAC-Element die Entscheidung mit dem größten erwarteten Nutzen gewählt wird.

Der restliche Abschnitt ist folgendermaßen strukturiert: In Unterabschnitt 4.2.1 wird die entwickelte Erweiterung von RBAC um Ortsbeschränkungen und in Unterabschnitt 4.2.2 deren risikobasierte Durchsetzung basierend auf probabilistischen Positionsschätzungen vorgestellt. Ebenfalls wird in Unterabschnitt 4.2.3 diskutiert, wie in einer laufenden Sitzung damit umzugehen ist, wenn zuvor verfügbare RBAC-Elemente aufgrund der Risikoanalyse plötzlich nicht mehr zur Verfügung stehen. Die Effektivität des entwickelten Ansatzes wird in Unterabschnitt 4.2.4 untersucht. Unterabschnitt 4.2.5 fasst die Ergebnisse schließlich zusammen.

4.2.1 Syntaktische Definition von Ortsbeschränkungen

Dieser Unterabschnitt beschreibt, wie RBAC-Richtlinien syntaktisch um die entwickelten Ortsbeschränkungen erweitert werden können. Der Ansatz wird Top–Down erklärt: Zunächst wird die Anwendung von Eigenschaftsmodellen und des Konzepts des Nutzens für RBAC-Elemente definiert. Darauf basierend wird die formale Definition von Ortsbeschränkungen entwickelt.

Eigenschaftsmodelle für RBAC-Elemente

Ein Element i einer RBAC-Richtlinie, z.B. eine Rolle, wird als ortssensitiv bezeichnet, wenn der aktuelle Standort des Nutzers eine gültige Grundlage darstellt, um darüber zu entscheiden, ob i in seiner aktuellen Sitzung zur Verfügung gestellt werden soll. Insbesondere kann die Anforderung, dass sich der Nutzer an einem bestimmten Standort aufhalten muss als sinnvoll bezeichnet werden, wenn der Ort intrinsische Eigenschaften besitzt, die auf natürliche Art zum Element i passen. So könnte die Aktivierung einer Rolle `Mitarbeiter` nur sinnvoll sein, wenn der Standort des Nutzers die Eigenschaft besitzt, dass er auf dem Firmengelände liegt. Ebenso könnte der Betrieb einer physischen Maschine mittels eines mobilen Endgeräts in einer Fabrik nur dann gestattet werden, wenn der Nutzerstandort

die Eigenschaft erfüllt, dass der Notausschalter von dort innerhalb einer vorgegebenen Zeitspanne erreichbar ist. So schreibt z.B. ISO 13850 vor, dass an jedem Bedienstand ein Notausschalter vorhanden sein muss [68]. Folglich muss die mobile Interaktion auf einen Bereich begrenzt werden, so dass durch den Abstand zum Notausschalter kein wesentlich höheres Gefahrenpotential entsteht als an einem stationären Bedienstand. Liegt ein ortssensitives RBAC-Element i vor, so muss für dieses also zunächst ein passendes Eigenschaftsmodell $\mathrm{P}(E_i|X)$ bestimmt werden.

Der Nutzen von RBAC-Elementen

Basierend auf der WDF einer Positionsschätzung und einem Eigenschaftsmodell kann die Wahrscheinlichkeit angegeben werden, mit welcher eine geforderte Eigenschaft am realen Nutzerstandort zum Zeitpunkt t vorliegt. Im Folgenden wird das im Abschnitt 4.1 eingeführte Konzept des Nutzens auf RBAC übertragen. Auch hier gibt es die vier Fälle *RP*, *RN*, *FP* und *FN*. Hierbei entsteht zu jedem Zeitpunkt während einer Sitzung der Nutzen *RP* bzw. *FP* wenn das RBAC-Element (z.B. eine Rolle oder Zugriffsrecht) in einer Sitzung verfügbar ist und der reale Nutzerstandort die geforderte Eigenschaft besitzt bzw. nicht besitzt. Analog ergibt sich die Semantik für *RN* bzw. *FN* für den Fall, dass ein RBAC-Element in einer Sitzung nicht verfügbar ist. Eine Abbildung, die für ein RBAC-Element i den Nutzen in diesen vier Fällen beschreibt, wird im Folgenden als U_i bezeichnet.

Die Erweiterung von RBAC um Ortsbeschränkungen

Für einzelne Elemente der RBAC-Richtlinie werden Ortsbeschränkungen auf Basis des zugehörigen Eigenschaftsmodells und der Funktion U des Nutzens definiert. Im ursprünglichen RBAC-Model werden einem Nutzer n alle Zugriffsrechte gewährt, die über einen Autorisierungspfad erreichbar sind, der nur Rollen in der aktuellen Sitzung von n enthält. Damit diese Semantik beibehalten wird, darf keinem RBAC-Element e mit $e \in RP$ oder $e \in P$ eine Ortsbeschränkung zugeordnet werden. Formal ist eine (erweiterte) Ortsbeschränkung in dem entwickelten Ansatz die Zuweisung eines Eigenschaftsmodells und einer Funktion U des Nutzens an ein RBAC-Element.

Definition 4.2.1 (Erweiterte Ortsbeschränkung)**.** *Eine Ortsbeschränkung für ein RBAC-Element $i \in N \cup NR \cup RH \cup R$ ist definiert als ein 2–Tupel $(P(E_i|X), \mathrm{U}_i)$, bestehend aus einem Eigenschaftsmodell für eine Eigenschaft E und einer Abbildung, welche den vier Fällen RP, RN, FP und FN einen Wert für ihren Nutzen zuordnet. Solche Ortsbeschränkungen werden gegenüber der Definition basierend auf Polygonen als erweitere Ortsbeschränkungen bezeichnet.*

Ein einfaches Beispiel einer ortsbeschränkten RBAC-Richtlinie ist in Abbildung 4.8 dargestellt. Hierbei verlangen die Ortsbeschränkungen, die den Elementen auf dem Autorisierungspfad $\langle n, r_1, \ldots, r_k, p\rangle$ zugeordnet sind, dass die Eigenschaften $E_{r_1}, \ldots, E_{r_k}$ am realen Standort des Nutzers beobachtet werden können, also `wahr` sind. Um nun darüber zu entscheiden, ob ein RBAC-Element i in der Sitzung eines Nutzers zur Verfügung stehen

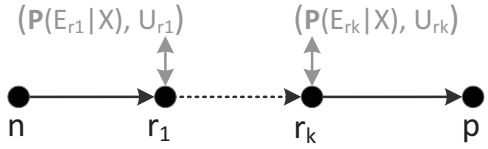


Abbildung 4.8: Auswertung des Autorisierungspfads $\langle n, r_1, \ldots, r_k \rangle$. Die Zugehörigkeit von zugeordnete Ortsbeschränkungen zu Rollen wird durch einen Pfeil dargestellt.

soll, beschränken die zugeordneten Ortsbeschränkungen die Existenz von Autorisierungspfaden basierend auf der aktuellen Positionsschätzung des Nutzers. Diese Durchsetzung der Ortsbeschränkungen wird im nächsten Abschnitt erläutert.

4.2.2 Durchsetzung von Ortsbeschränkungen

In diesem Unterabschnitt wird die Durchsetzung von Ortsbeschränkungen behandelt. Hierbei werden Autorisierungsentscheidungen mittels eines Referenzmonitors hergeleitet, der auf der ursprünglichen RBAC-Richtlinie und den zugeordneten Ortsbeschränkungen aufsetzt. Dem Referenzmonitor wird hierbei ein Datenstrom aus vertrauenswürdigen Positionsschätzungen eines jeden Nutzers mit einer aktiven Sitzung durch ein vertrauenswürdiges und fälschungssicheres Positionierungssystem bereitgestellt. Die Frequenz, mit der Positionsschätzungen bereitgestellt werden, muss hierbei möglichst hoch sein, um die Zeitspanne zu minimieren, in der aufgrund von veralteten Messungen zusätzliche Unsicherheiten über den Nutzerstandort entstehen. Für die Absicherungen von Messungen gegen Fälschungen sei z.B auf Gilbert et al. [59,60] verwiesen.

Ähnlich zum ursprünglichen RBAC, muss jeder Nutzer n vor der Autorisierung zunächst Rollen aktivieren, wenn er seine Sitzung s startet. Hierbei kann eine Rolle r in einer Sitzung s genau dann aktiviert werden, wenn es einen Autorisierungspfad $\langle n, \ldots, r \rangle$ in der darunterliegenden, originalen RBAC-Richtlinie $\mathcal{P} = (V, E)$ gibt. Im nächsten Schritt werden die Ortsbeschränkungen durchgesetzt, indem die Sitzung s auf eine beschränkte Sitzung s' mit $s' \subseteq s$ abgebildet wird. Auf diese Art kann die ursprüngliche Semantik von RBAC beibehalten werden, indem Autorisierungspfade anstatt mit der ursprünglichen Sitzung s mit der beschränkten Sitzung s' gesucht werden. Während der fortwährenden Nutzung einer Sitzung wird dieser Vorgang durch den Referenzmonitor für jede vom Positionierungssystem eintreffende Positionsschätzung wiederholt. In der Konsequenz wird einem Nutzer n im Rahmen seiner Sitzung s die Benutzung eines Zugriffsrechts p nur gewährt, wenn bzgl. der zugehörigen beschränkten Sitzung s' ein Autorisierungspfad $\langle n, \ldots, p \rangle$ existiert. Dieses Verhalten wird in Algorithmus 3 beschrieben. Die darin referenzierten Prozeduren `behandle_sitzungs_verletzung` und `behandle_zugriffsrechts_verletzung` dienen der Behandlung von Verletzungen der Ortsbeschränkungen und werden detailliert in Unterabschnitt 4.2.3 beschrieben.

Im Folgenden wird die Prozedur `aktualisiere_sitzungs_rollen` beschrieben. Diese dient der Konstruktion der beschränkten Sitzung s' aus der ursprünglichen Sitzung s. Die Grundidee ist, dass eine Rolle $r \in s$ auch in s' enthalten ist, wenn ein Autorisierungspfad

Algorithmus 3 Behandlung verletzter Ortsbeschränkungen in laufenden Sitzungen.

Eingabe: Nutzer u, Sitzung s, RBAC-Richtlinie $\mathcal{P}$, Positionierungssystem *loc*
Ausgabe: Durchsetzung der Ortsbeschränkungen für s

```
function DURCHSETZUNG_VON_ORTSBESCHRÄNKUNGEN(u,s,P, loc)
    for each (μ, Σ) geliefert_von loc do
        s' ← AKTUALISIERE_SITZUNGS_ROLLEN(u, s, (μ, Σ), P)        ▷ Durchsetzung
        if s ≠ s' then                                  ▷ Reaktion der Sitzung auf Verletzungen
            BEHANDLE_SITZUNGS_VERLETZUNG(u, s, s', P)
        end if
        for each laufende Nutzung mit Recht p do
            if ∃⟨u, ..., p⟩ ∈ P . ∀i ∈ ⟨u, ..., p⟩ : i ∈ R → i ∈ s' then
                continue                                ▷ Es gibt einen Autorisierungspfad in s'
            else
                BEHANDLE_ZUGRIFFRECHTS_VERLETZUNG(u, s, s', P)
            end if
        end for
    end for
end function
```

$\langle n, \ldots, r\rangle$ existiert, der nur Rollen aus s verwendet und der die zugeordneten Ortsbeschränkungen erfüllt. Aus der Durchsetzung der zugeordneten Ortsbeschränkungen können also mit s ursprünglich mögliche Autorisierungspfade in s' deaktiviert werden. Somit gilt $s' \subseteq s$. Der reale aber dem System unbekannte Zustand, in dem sich der Nutzer zum Anfragezeitpunkt befindet, kann jede auf dem Autorisierungspfad geforderte Eigenschaft entweder erfüllen oder nicht erfüllen. Die Eigenschaften sind also entweder `wahr` oder `falsch`. Die Wahrscheinlichkeit, mit der eine einzelne Eigenschaft am Ort x `wahr` ist, wird durch das Eigenschaftsmodell der Ortsbeschränkung beschrieben. Im Rahmen der Durchsetzung der Ortsbeschränkungen kann ein Autorisierungspfad auch dann deaktiviert werden, wenn zumindest einige der geforderten Eigenschaften aktuell am realen Standort des Nutzers `wahr` sind.

Um zu entscheiden, ob ein Autorisierungspfad die Ortsbeschränkungen erfüllt, werden die Abbildungen U_i für den Nutzen der einzelnen Ortsbeschränkungen herangezogen. Die Annahme ist, dass der Nutzen, wenn ein Autorisierungspfad entweder aktiv bleibt oder deaktiviert wird, davon abhängt, welche Eigenschaften zu diesem Zeitpunkt am realen Nutzerstandort beobachtet werden können. Um zu entscheiden, ob ein Autorisierungspfad in s' aktiviert bleibt oder deaktiviert werden muss, wird für beide Fälle der erwartete Nutzen berechnet. Schließlich wird die Entscheidung getroffen, welche den größten erwarteten Nutzen verspricht.

Sind den Elementen auf einem Autorisierungspfad insgesamt m Ortsbeschränkungen zugeordnet, so ist jede einzelne Eigenschaft $E_1, \ldots, E_m$ im realen Zustand des Nutzers entweder `wahr` oder `falsch`. Der Nutzer befindet sich in der Realität somit, ausgehend von den geforderten Eigenschaften, in einem von 2^m möglichen Zuständen $\sigma_1, \ldots, \sigma_{2^m}$. Formal

stellt jedes σ_i ein m–Tupel dar, welches jeder geforderten Eigenschaft $E_1, \ldots, E_m$ einen booleschen Wert zuweist. Im Folgenden bezeichne $\pi(\sigma_i)$ die Wahrscheinlichkeit, dass ein Zustand σ_i den realen Zustand eines Nutzers darstellt.

Ferner seien die Funktion $u_{RP}(\sigma_i)$, $u_{FP}(\sigma_i)$, $u_{RN}(\sigma_i)$ und $u_{FN}(\sigma_i)$ definiert. Dabei berechnen $u_{RP}(\sigma_i)$ und $u_{FN}(\sigma_i)$ jeweils die Summen aller U(RP) bzw. U(FN) für die Ortsbeschränkungen, die im jeweiligen Zustand σ_i `wahr` sind. Analog berechnen $u_{RN}(\sigma_i)$ und $u_{FP}(\sigma_i)$ die Summen aller U(RN) bzw. U(FP) für die Ortsbeschränkungen, die im jeweiligen Zustand σ_i `falsch` sind. Im Detail durchlaufen $u_{RP}(\sigma_i)$ bzw. $u_{FN}(\sigma_i)$ sequentiell jeden booleschen Wert j im m-Tupel σ_i. Falls $(\sigma_i)_j = \texttt{wahr}$, so wird $\mathrm{U}_j(RP)$ bzw. $\mathrm{U}_j(FN)$ zu ihrem Ergebnis addiert. Die Funktionen $u_{RN}(\sigma_i)$ und $u_{FP}(\sigma_i)$ arbeiten analog, allerdings wird geprüft ob $(\sigma_i)_j = \texttt{falsch}$ gilt. Falls ja, wird entsprechend $\mathrm{U}_j(RN)$ bzw. $\mathrm{U}_j(FP)$ zu ihrem Ergebnis addiert.

Dies erlaubt schließlich den erwarteten Nutzen zu berechnen, entweder für den Fall der Deaktivierung des Autorisierungspfads, oder den Fall, dass er aktiv bleibt:

$$\texttt{nutzen\_deaktivierung} = \sum_{i=1}^{2^m} \left(\pi(\sigma_i) \cdot \left(u_{FN}(\sigma_i) + u_{RN}(\sigma_i)\right)\right) \tag{4.38}$$

$$\texttt{nutzen\_aktivierung} = \sum_{i=1}^{2^m} \left(\pi(\sigma_i) \cdot \left(u_{FP}(\sigma_i) + u_{RP}(\sigma_i)\right)\right) \tag{4.39}$$

Um die ortsbeschränkte RBAC-Richtlinie risikobasiert durchzusetzen, wird in jedem Fall die Entscheidung mit dem größten erwarteten Nutzen getroffen:

$$\texttt{deaktivierung} \Leftrightarrow \texttt{nutzen\_aktivierung} \leq \texttt{nutzen\_deaktivierung} \tag{4.40}$$

Zur Auswertung von (4.38) und (4.39) muss zunächst die Wahrscheinlichkeit $\pi(\sigma_i)$ berechnet werden, die für den Zeitpunkt der Positionsschätzung beschreibt, wie wahrscheinlich σ_i den realen Zustand des Nutzers darstellt. Hierzu muss zunächst das gemeinsame Eigenschaftsmodell des Zustands berechnet werden. Dabei wird angenommen, dass die Ereignisse stochastisch unabhängig sind:

$$\forall x \in X : \mathrm{P}\left(\bigwedge_{j=1}^{m} E_j = (\sigma_i)_j \,|x\right) = \prod_{j=1}^{m} \mathrm{P}\left(E_j = (\sigma_i)_j \,|x\right) \tag{4.41}$$

Der Index j eines potentiellen realen Zustands σ_i soll hierbei die Referenz auf den Wert angeben, der beschreibt ob die Eigenschaft E_j in diesem Zustand `wahr` oder `falsch` ist. Die Vorgehensweise soll an einem kurzen Beispiel verdeutlicht werden. Angenommen es liegt ein Zustand $\sigma_1 = \langle \texttt{wahr}, \texttt{falsch} \rangle$ vor. Das zugehörige gemeinsame Eigenschaftsmodell $\mathrm{P}\left(E_1 = \texttt{wahr} \wedge E_2 = \texttt{falsch} |\, x\right)$ berechnet sich als $\mathrm{P}\left(E_1 = \texttt{wahr}|x\right) \cdot \mathrm{P}\left(E_2 = \texttt{falsch}|x\right)$ für alle möglichen Orte $x \in X$.

Die Wahrscheinlichkeit $\pi(\sigma_i)$ wird schließlich durch Marginalisierung über die Variable X mittels der WDF basierend auf der Positionsschätzung (μ, Σ) des Nutzers ermittelt:

$$\pi\left(\sigma_i\right) = \mathrm{P}\left(\bigwedge_{j=1}^{m} E_j = (\sigma_i)_j\right) = \int_X \mathrm{P}\left(\bigwedge_{j=1}^{m} E_j = (\sigma_i)_j \,|X = x\right) \cdot wdf_{\mathbf{F}|\mu,\sigma}^{laplace}(x)\, \mathrm{d}x \tag{4.42}$$

Zustand \ **Aktion**	aut = `wahr`	¬aut = `falsch`
Eigenschaften $\langle E_1, \ldots, E_m \rangle$ befinden sich im Zustand σ_1 (p = $\pi(\sigma_1)$)	$u_{RP}(\sigma_1) + u_{FP}(\sigma_1)$	$u_{RN}(\sigma_1) + u_{FN}(\sigma_1)$
$\vdots$	$\vdots$	$\vdots$
Eigenschaften $\langle E_1, \ldots, E_m \rangle$ befinden sich im Zustand $\sigma_{(2^m)}$ (p = $\pi(\sigma_{(2^m)})$)	$u_{RP}(\sigma_{(2^m)}) + u_{FP}(\sigma_{(2^m)})$	$u_{RN}(\sigma_{(2^m)}) + u_{FN}(\sigma_{(2^m)})$

Tabelle 4.2: Die erweiterte Entscheidungsmatrix zur standortbasierten Autorisierung.

Zu beachten ist, dass (4.40) eine echte Verallgemeinerung von (4.35) von 2^1 möglichen Zuständen, nämlich $\sigma_1 = \langle \texttt{wahr} \rangle$ und $\sigma_2 = \langle \texttt{falsch} \rangle$, auf 2^m mögliche Zustände darstellt. Dies lässt sich durch Einsetzen und Auflösen leicht nachprüfen. Es ergibt sich somit in Anlehnung an Tab. 4.1 die erweiterte Entscheidungsmatrix, wie in Tab. 4.2 dargestellt. Zur Herleitung der vollständigen beschränkten Sitzung s' muss diese Methodik auf jede Rolle angewandt werden, die in der ursprünglichen Sitzung s aktiv ist. Die vollständige Angabe der Prozedur `aktualisiere_sitzungs_rollen` ist in Algorithmus 4 angegeben.

4.2.3 Der Umgang mit verletzten Ortsbeschränkungen

Die Durchsetzung von Ortsbeschränkungen in einer laufenden Sitzung s bewirkt die Herleitung einer beschränkten Sitzung s', in der möglicherweise weniger Zugriffsrechte zur Verfügung stehen, wie in Unterabschnitt 4.2.2 erläutert. Im Folgenden wird eine Ortsbeschränkung als verletzt bezeichnet, sofern nicht alle Rollen aus der ursprünglichen Sitzung s in der entsprechenden beschränkten Sitzung s' enthalten sind. Darüber hinaus gilt ein Zugriffsrecht p als verletzt, wenn das Zugriffsrecht aktuell genutzt wird, allerdings kein Autorisierungspfad mehr zu p existiert, der ausschließlich Rollen aus s' passiert. Aus diesem Grund erfolgt im oben dargestellten Algorithmus 3 der Aufruf der Prozeduren `behandle_sitzungs_verletzung` und `behandle_zugriffsrechts_verletzung`. Dieser Abschnitt zeigt mögliche Realisierungen dieser Prozeduren auf und diskutiert deren Auswirkung auf die Semantik des Referenzmonitors.

Jede dieser beiden Prozeduren kann grundsätzlich auf drei verschiedene Arten auf eine Verletzung der Sitzung bzw. des Zugriffsrechts reagieren. Entweder durch *fortfahren*, *pausieren* oder *beenden* der laufenden Sitzung bzw. der laufenden Benutzung des Zugriffsrechts. Im Falle der Verletzung von Sitzungen bewirkt das Fortfahren, dass die Sitzung durch die Verletzung der Ortsbeschränkung nicht betroffen ist. Das Pausieren erzwingt jedoch die Sperrung jeglicher weiterer Interaktion des Nutzers. Das Beenden der Sitzung

Algorithmus 4 Algorithmus zur Aktualisierung der aktiven Rollen von Sitzungen.

Eingabe: Nutzer n, Sitzung s, Nutzerposition (μ, Σ), RBAC-Richtlinie $\mathcal{P}$
Ausgabe: Sitzung $s' \subset s$ mit durchgesetzten Ortsbeschränkungen

```
function AKTUALISIERE_SITZUNGS_ROLLEN(n,s,(μ,Σ),P)
    s' ← {}                                              ▷ Initialisiere Ergebnis
    s* ← {r' ∈ R | ∃r ∈ s : (r, r') ∈ RH}                ▷ Entfalte Kind-Rollen
    for each r ∈ s* do                                   ▷ Für alle Rollen der Sitzung
        for each ⟨n, ..., r⟩ ∈ P do                      ▷ Für alle Autorisierungspfade zu r
            E_1, ..., E_m ← EXTRAHIERE_BENÖTIGTE_EIGENSCHAFTEN(⟨n, ..., r⟩)
            σ_1, ..., σ_{2^m} ← EXTRAHIERE_REALE_ZUSTÄNDE(E_1, ..., E_m)

            nutzen_deaktivierung ← Σ_{i=1}^{2^m} (π(σ_i) · (u_FN(σ_i) + u_RN(σ_i)))
            nutzen_aktivierung ← Σ_{i=1}^{2^m} (π(σ_i) · (u_FP(σ_i) + u_RP(σ_i)))

            if nutzen_aktivierung ≥ nutzen_deaktivierung then
                s' ← s' ∪ {r}
            end if
        end for
    end for
return s'
end function
```

terminiert diese, weshalb ein Nutzer vor Anfrage eines neuen Zugriffsrechts zunächst eine neue Sitzung starten muss. Laufende Zugriffsrechte sollen dennoch weitergeführt werden.

Für den Entwurf eines passenden Referenzmonitors ist es unerlässlich, eine passende Implementierung für die beiden Prozeduren zur Behandlung der Verletzung von Sitzungen bzw. Zugriffsrechten anzugeben. Im Folgenden sei die Reaktion der Prozedur `behandle_sitzungs_verletzung` als h_s abgekürzt. Entsprechend ist die Reaktion der Prozedur `behandle_berechtigungs_verletzung` als h_p abgekürzt. Sei $\prec$ eine totale Ordnung auf der Menge möglicher Reaktionen mit *fortfahren* $\prec$ *pausieren* $\prec$ *beenden*. Ferner sei $\sim$ die Äquivalenz zweier Reaktionen.

Um einen passenden Referenzmonitor zur Durchsetzung der Ortsbeschränkungen bereitzustellen, muss also zunächst für die beiden Prozeduren `behandle_sitzungs_verletzung` und `behandle_zugriffsrechts_verletzung` aus den drei Möglichkeiten eine passende Reaktion ausgewählt werden. Die möglichen Kombinationen der vorgestellten Reaktionen definieren eine 3×3–Matrix, die in Abb. 4.9 dargestellt ist. Die möglichen Kombinationen spannen drei semantisch verschiedene Klassen von Referenzmonitoren auf:

1. Die Reaktion h_s, die auf die Sitzung angewandt wird, ist restriktiver als die Reaktion h_p, die auf ein laufendes Zugriffsrecht angewandt wird. Es gilt also $h_p \prec h_s$. Diese Kategorie umfasst die Modelle 2, 3 und 6.

2. Beide Reaktionen sind bezüglich ihrer Restriktivität gleich. Es gilt also $h_p \sim h_s$.

Sitzung / Berechtigung	Fort-fahren	Pausieren	Beenden
Fortfahren	Modell 1	Modell 2	Modell 3
Pausieren	Modell 4	Modell 5	Modell 6
Beenden	Modell 7	Modell 8	Modell 9

Abbildung 4.9: Modelle und Klassen (gleichfarbig), die sich aus den unterschiedlichen Kombinationen der Reaktionen der Prozeduren `behandle_sitzungs_verletzung` und `behandle_zugriffsrechts_verletzung` ergeben.

Diese Kategorie umfasst die Modelle 1, 5 und 9.

3. Die Reaktion h_s, die auf die Sitzung angewandt wird, ist weniger restriktiv als die Reaktion h_p, die auf eine laufendes Zugriffsrecht angewandt wird. Somit gilt $h_s \prec h_p$. Zu dieser Kategorie zählen die Modelle 4, 7 und 8.

In Klasse 1 gilt, dass die Modelle 2 und 3 die laufenden Zugriffsrechte uneingeschränkt fortsetzen, die Sitzung selbst allerdings entweder pausieren oder beenden. Somit ist das Starten neuer Zugriffsrechte entweder gar nicht mehr möglich, oder aber erst nachdem die Ortsbeschränkungen wieder erfüllt sind. Dies ist vor allem dann sinnvoll, wenn nur zum Start eines Zugriffsrechts die Ortsbeschränkungen erfüllt sein müssen. Ein solches Szenario kann vorliegen, wenn es das Zugriffsrecht einem Arbeiter in einer Fabrik erlaubt, mit seinem mobilen Endgerät eine Maschine zu starten. Dabei hat er die Auflage, vor dem Start visuell und aus direkter Nähe zu prüfen, ob genügend Rohstoffe eingelegt wurden. Modell 6 hingegen pausiert das aktuell laufende Zugriffsrecht, bis die Ortsbeschränkungen wieder erfüllt sind und erlaubt innerhalb dieser Sitzung keine neuen Zugriffsrechte mehr. Dadurch lässt sich z.B. abbilden, dass zwar die aktuelle Arbeit fertiggestellt werden soll, aber der Nutzer keine künftigen Zugriffsrechte starten darf, da er die Anforderungen an seinen Standort nicht erfüllt hat.

In Klasse 2 ist die Reaktion, die nach Verletzung der Ortsbeschränkung auf die Sitzung angewandt wird genauso restriktiv, wie die Reaktion, die auf laufende Zugriffsrechte angewandt wird. Im Modell 1 wird hierbei keine zugewiesene Ortsbeschränkung beachtet, was im wesentlichen dem klassischen RBAC-Modell ohne Ortsbeschränkungen entspricht. Laufende Zugriffsrechte und Sitzungen werden ausschließlich durch Einwirkung des Nutzers terminiert. Modell 5 pausiert das laufende Zugriffsrecht und verhindert gleichzeitig das Starten neuer Zugriffsrechte bis die Ortsbeschränkungen wieder erfüllt sind. Modell 9 beendet sowohl das aktuell laufende Zugriffsrecht, als auch die Sitzung. Dies ist die restriktivste Vorgehensweise und sinnvoll, wenn beispielsweise die Menge der selektierten Rollen

in der Sitzung nach einer Verletzung der Ortsbeschränkung keinen Sinn mehr ergibt. So ist eine Rolle denkbar, die in einer medizinischen Umgebung charakterisiert, ob der Nutzer die entsprechenden Schleusen bzw. Waschräume zur Desinfektion durchlaufen hat. Nach Verletzen der Ortsbeschränkung wäre der hygienische Bereich verlassen worden und die Sitzung müsste neu mit initialer Überprüfung gestartet werden.

In Klasse 3 wird auf das aktuell laufende Zugriffsrecht eine restriktivere Reaktion angewandt, als auf die Sitzung. Modell 4 und Modell 7 bewirken dabei, dass während die Ortsbeschränkungen verletzt sind, alle laufenden und während der weiterhin aktiven Sitzung neu gestarteten Zugriffsrechte, sofort pausiert bzw. beendet werden. Im Modell 8 wird das Starten neuer Zugriffsrechte untersagt, bis die Bedingungen wieder erfüllt sind. Wie in Modell 7 werden laufende Zugriffsrechte beendet. Dies ist vor allem dann sinnvoll, wenn z.B. dem Ergebnis aus der Arbeit mit dem Zugriffsrecht nach Verletzung der Ortsbeschränkung nicht mehr vertraut werden kann.

Wie durch die gezeigten Beispiele ersichtlich, ist bei der Implementierung der Prozeduren `behandle_sitzungs_verletzung` und `behandle_zugriffsrechts_verletzung` größte Vorsicht bei der Auswahl der Reaktionen geboten, da die dadurch implizierte Semantik des Referenzmonitors genau auf das jeweilige Anwendungsszenario abgestimmt werden muss.

4.2.4 Performanzanalyse

Wichtigstes Kriterium bei der Evaluation der vorgestellten Erweiterung von RBAC ist der Vorteil gegenüber den RBAC-Erweiterungen, die auf Punkt-in-Polygon-Tests basieren und eine Adaption der naiven Strategie anwenden. Es muss gezeigt werden, dass der Opportunitätsverlust, also die Enttäuschung über den tatsächlich erreichten Nutzen, bei der risikobasierten Erweiterung geringer ist als bei den Ansätzen, welche die naive Strategie adaptieren.

Hierzu wurden zunächst Eigenschaftsmodelle generiert, welche auf den benannten Räumen aus der Testumgebung in Abb. 3.1(b) aufsetzen und deshalb mit den Eigenschaftsmodellen in Abb. 4.5, 4.4 und 4.7 vergleichbar sind.

Die generierten Eigenschaftsmodelle teilen sich auf in fließende und begrenzte Eigenschaftsmodelle. Begrenzte Eigenschaftsmodelle basieren auf der Idee aus Bsp. 4.1.3 bzw. 4.1.5, wobei die Wahrscheinlichkeit, mit der eine Eigenschaft beobachtet werden kann, innerhalb einzelner Räume gleich verteilt mit einem fixen $p \in [0{,}5; 1{,}0]$ ist. Außerhalb der Räume betrage die Wahrscheinlichkeit 0. Da $p \geq 0{,}5$ ist es innerhalb der Räume wahrscheinlicher, dass die geforderte Eigenschaft beobachtet werden kann, als dass dies nicht der Fall ist. Insgesamt wurden 40 begrenzte Eigenschaftsmodelle auf den dargestellten Räumen generiert.

Zusätzlich wurden fließende Eigenschaftsmodelle basierend auf der Idee aus Bsp. 4.1.4 generiert, wobei die Wahrscheinlichkeit abgebildet wird, mit welcher der Nutzer innerhalb einer bestimmten Zeitspanne einen spezifischen Punkt (z.B. Notausschalter) erreichen kann. Insgesamt wurden 40 unterschiedliche fließende Eigenschaftsmodelle generiert, deren zu erreichender spezifischer Punkt jeweils in einem der benannten Räume liegt. Die

zugrundeliegenden maximalen Zeitspannen zur Erreichung des spezifischen Punkts sind gleich verteilt aus dem Intervall [3 s, 15 s] entnommen.

Insgesamt wurden zur Evaluation des Ansatzes 8000 verschiedene mit Ortsbeschränkungen versehe Autorisierungspfade simuliert. Die Simulation erfolgte durch die Kombination von 2 bis 5 Eigenschaftsmodellen, die zufällig aus 80 vorbereiteten Eigenschaftsmodellen gezogen wurden. Damit die erfüllten Autorisierungspfade erfüllbar sind, wurde in jedem Fall zunächst einer der benannten Räume zufällig ausgewählt. Im nächsten Schritt wurde eine zufällige Anzahl an Eigenschaftsmodellen gewählt, welche entweder als begrenztes Eigenschaftsmodell genau auf dem Raum definiert sind, oder im Falle von fließenden Eigenschaftsmodellen, den spezifischen Punkt innerhalb des Raumes liegen haben. Zur Simulation einer Ortsbeschränkung muss jedem Eigenschaftsmodell noch eine Abbildung U für den Nutzen zugeordnet werden.

Untersucht werden soll das Verhalten für solche Ortsbeschränkungen mit $\mathrm{U}(RP) = 1$, $\mathrm{U}(RN) = 1$, $\mathrm{U}(FP) = 0$ und $\mathrm{U}(FN) \in [0;1]$ (Fall 1), sowie Ortsbeschränkungen mit $\mathrm{U}(RP) = \mathrm{U}(RN) = 1$, $\mathrm{U}(FN) = 0$ und $\mathrm{U}(FP) \in [0;1]$ (Fall 2). In diesen Abbildungen U für den Nutzen erzeugen richtige Entscheidungen mehr Nutzen als Falsche. Im Folgenden sei wieder $u := [\mathrm{U}(RP) - \mathrm{U}(FN)]$ und $t := [\mathrm{U}(RN) - \mathrm{U}(FP)]$. Die Ortsbeschränkungen, für deren U der erste Fall gilt, besitzen ein Verhältnis $u/t \in [0;1]$, was sich leicht durch Einsetzen nachprüfen lässt. Für den zweiten Fall gilt $u/t \in [1;\infty]$. Für einen fixen Autorisierungspfad wurde allen Ortsbeschränkungen die gleiche Abbildung U zugewiesen.

Für jede der 8000 Kombinationen von Eigenschaftsmodellen wurde ein entsprechendes Polygon extrahiert, so wie es sehr wahrscheinlich bei der herkömmlichen Definition einer autorisierten Zone verwendet werden würde. Die Extraktion des Polygons erfolgt für einen jeden Autorisierungspfad auf genau dem gemeinsamen Eigenschaftsmodell, in dem alle Eigenschaften `wahr` sind. Als die Grenze des Polygons wurde die 50% Konturlinie gewählt. Somit gilt für alle Punkte, die innerhalb des Polygons liegen, dass die geforderte Eigenschaft dort wahrscheinlicher als 50% beobachtet werden kann. Abb. 4.7 zeigt ein solches Polygon mit gelben Grenzlinien.

Für jede der 8000 Kombinationen wird eine Positionsschätzung erzeugt, indem ein zufälliger Eintrag aus den WLAN-Fingerprinting Testdaten aus Abb. 3.1(c) ausgewählt und die Position und Laplace-Fehlerschätzung berechnet wurde. Für jede Positionsschätzung wurde zufällig bestimmt, welche Eigenschaften am zugehörigen realen Ort des Nutzers `wahr` bzw. `falsch` sind. Die jeweilige Wahrscheinlichkeit hängt dabei vom zugehörigen Wert des zugehörigen Eigenschaftsmodells an dieser Stelle ab.

Abhängig vom Verhältnis u/t wird jeder der 8000 Fälle nun einmal über die vorgestellte risikobasierte Autorisierung und einmal über die existierende naive Strategie autorisiert. Für beide Methoden wurde der dabei auftretende Opportunitätsverlust aufgezeichnet. Die prozentuale Reduktion des Opportunitätsverlusts beim Einsatz des vorgestellten Ansatzes gegenüber der Methodik der existierenden naiven Verfahren ist in Abb. 4.10 dargestellt. Deutlich zeigt sich, dass der Vorteil der erweiterten risikobasierten Strategie für solche Ortsbeschränkungen umso größer ist, je unterschiedlicher u und t sind. Das Minimum liegt bei ca. 10%, so dass der Ansatz selbst im ungünstigsten Fall noch eine Verbesserung gegenüber der naiven Strategie zeigt.

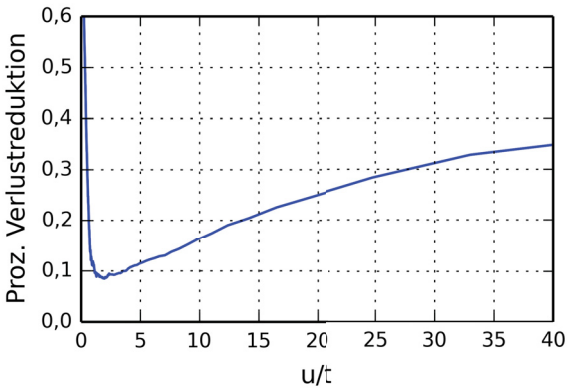


Abbildung 4.10: Die prozentuale Verringerung des Opportunitätsverlusts des vorgestellten Ansatzes gegenüber der bisher eingesetzten naiven Strategie.

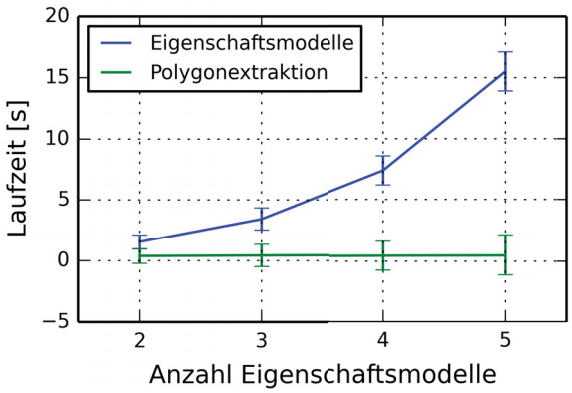


Abbildung 4.11: Laufzeiten mit Fehlerintervall für den vorgestellten Ansatz verglichen mit der naiven Strategie.

Zuletzt wurde auch die Laufzeit beider Ansätze verglichen. Hierzu wurde die benötigte Zeit zur Extraktion eines 50%–Polygons aus einem Eigenschaftsmodell mit der Zeit verglichen, die zur Herleitung der gemeinsamen Eigenschaftsmodelle aller 2^m möglicher realer Zustände benötigt wird. Die Evaluation wurde auf einer Intel Xeon X5650 CPU mit 2,67 GHz und 8 GB RAM durchgeführt. Die Implementierung wurde basierend auf Python 2.7.7 und Numpy 1.7.0 bereitgestellt. Die Ergebnisse der Laufzeitanalyse sind in Abbildung 4.11 dargestellt. Klar zeigt sich, dass die Herleitung von risikobasierten Entscheidungen und der geringere Opportunitätsverlust auf Kosten der Laufzeit gehen. Diese steigt exponentiell mit der Anzahl m der Ortsbeschränkungen, die einem Autorisierungspfad zugeordnet sind, da 2^m gemeinsame Eigenschaftsmodelle hergeleitet werden müssen. Im praktischen Betrieb kann dieser Nachteil teilweise dadurch kompensiert werden, dass die Berechnungen z.B. auf einen performanten Server ausgelagert werden. Eine weitere Möglichkeit ergibt sich aus der baumartigen Struktur der RBAC-Richtlinien, weshalb viele Autorisierungspfade einen gemeinsamen Präfix mit den gleichen Ortsbeschränkungen besitzen. Dies erlaubt die teilweise Vorberechnung von gemeinsamen Eigenschaftsmodellen auf solchen Präfixen. Für einen kompletten Autorisierungspfad müssen dann lediglich die Eigenschaften aus den Ortsbeschränkungen auf dem Suffix berücksichtigt werden.

4.2.5 Diskussion

Mit diesem Ansatz wurde ein Verfahren für standortbasierte RBAC-Richtlinien vorgestellt, welches die Menge der verfügbaren Rollen innerhalb einer Sitzung basierend auf dem Nutzerstandort einschränkt. Dies erlaubt es, die Semantik des klassischen RBAC weiterzuentwickeln, welche ein Zugriffsrecht gewährt, wenn ein Autorisierungspfad in der RBAC-

Richtlinie vom aktuellen Nutzer zum angefragten Zugriffsrecht existiert und dieser nur Rollen passiert, die in der aktuellen Sitzung aktiv sind. Das Konzept wurde umgesetzt, indem einzelnen Elementen der RBAC-Richtlinie Ortsbeschränkungen zugewiesen werden können, die zur Laufzeit risikobasiert durchgesetzt werden. Solche Ortsbeschränkungen bestehen je aus zwei Teilen, einem Eigenschaftsmodell und einer Abbildung U für den Nutzen. Sie können jedem RBAC-Element außer Zugriffsrechten und Zugriffsrechtszuweisungen zugeordnet werden. Das Eigenschaftsmodell hängt hierbei sehr stark von dem RBAC-Element ab, dem die Ortsbeschränkung zugeordnet wurde. Es beschreibt für jeden Ort x die Wahrscheinlichkeit, mit der an diesem Ort die Eigenschaft beobachtet werden kann, die zur Aktivierung des RBAC-Elements am Nutzerstandort vorhanden sein sollte. Solche Eigenschaften können z.B. sein, dass von dem Ort aus der Notausschalter einer Maschine innerhalb einer bestimmten Zeitspanne erreichbar ist, oder dass sich der Ort auf dem Firmengelände befindet. Die Abbildung U beschreibt den Nutzen, der in den vier unterschiedlichen Fällen entsteht: Wenn die Eigenschaft am Ort des Nutzers beobachtbar ist und das Element verfügbar bzw. deaktiviert ist, oder aber wenn die Eigenschaft am Ort des Nutzers nicht beobachtbar ist und das Element verfügbar bzw. deaktiviert ist.

Die Positionsschätzungen werden in Form einer WDF entsprechend zu Abschnitt 3.1 bereitgestellt. Diese werden zusammen mit den Eigenschaftsmodellen verwendet, um die Wahrscheinlichkeit abzuschätzen, mit der am Nutzerstandort die geforderten Eigenschaften zu beobachten sind. Dies erlaubt es, den erwarteten Nutzen und somit den erwarteten Opportunitätsverlust zu bestimmen, den eine Deaktivierung bzw. Aktivierung eines RBAC-Elements in der aktuellen Sitzung verspricht. Die Entscheidung über die Aktivierung bzw. Deaktivierung eines RBAC-Elements für die Sitzung eines Nutzers wird schließlich risikobasiert getroffen, indem die Option mit dem größten erwarteten Nutzen gewählt wird.

In den standortbasierten Erweiterungen zu RBAC, die in der Literatur existieren, wird die Ungenauigkeit von Positionsschätzungen nicht berücksichtigt und deshalb eine Darstellung als Punkt anstelle einer WDF gewählt. Diese Ansätze modellieren autorisierte Zonen ebenfalls durchgehend als Polygone. Die Verfügbarkeit von RBAC-Elementen wird in diesen Ansätzen abgeleitet, indem ein Punkt–in–Polygon–Test der Nutzerposition auf dem definierten Polygon durchgeführt wird. Das Möglichkeit einer Falschentscheidung aufgrund von Positionsfehlern wird nicht berücksichtigt und die Ungewissheit über das Vorhandensein der geforderten Eigenschaft an einzelnen Orten wird ignoriert.

Wie die obige Evaluation gezeigt hat, kann der risikobasierte Ansatz erheblich zur Reduktion des Opportunitätsverlusts beitragen. Dabei konnte selbst im schlechtesten Fall noch eine Reduktion des Opportunitätsverlusts von ca. 10% beobachtet werden. Die Analyse der Laufzeit hat gezeigt, dass die Anwendung des vorgestellten Ansatzes nur praktikable Antwortzeiten erlaubt, sofern die Anzahl der Ortsbeschränkungen pro Autorisierungspfad auf einen Wert von $2 - 4$ begrenzt grenzt wird.

Zusammenfassend kann gesagt werden, dass der vorgestellte Ansatz zur standortbasierten Erweiterung von RBAC durch die verwendeten Eigenschaftsmodelle eine größere Ausdrucksstärke für Ortsbeschränkungen erlaubt, als die bisher verwendeten Polygone. Ebenfalls werden Positionsfehler berücksichtigt, was ein wichtiger Aspekt ist, wenn diese ein nicht-vernachlässigbares Ausmaß haben, wie dies in vielen realistischen Anwendungs-

szenarien der Fall ist. Der vorgestellte Ansatz bietet also eine rationale und verlässlichere Grundlage zur Integration mobiler Endgeräte in moderne Arbeitsumgebungen, beispielsweise in zunehmend digitalisierte Fertigungsprozesse. Ein wichtiger Schritt für zukünftige Arbeiten ist jedoch die Entwicklung von Verfahren zur vertrauenswürdigen Positionsschätzung. Ebenfalls muss zwischen zwei eintreffenden Positionsschätzungen der Nutzerstandort risikobasiert interpoliert werden, so dass ein mögliches Verletzen der Bedingung nicht unerkannt bleibt. Eine alternative Möglichkeit mit diesem Problem umzugehen, wird im nächsten Abschnitt vorgestellt.

4.3 Filterbasierte kontinuierliche Auswertung von Ortsbeschränkungen

Ein wichtiger Aspekt ist in vielen Szenarien, dass selbst nach der Autorisierung noch kontinuierlich überprüft wird, ob der Nutzer die Ortsbeschränkungen erfüllt. Die Autorisierung erfordert somit eine anschließende Nutzungskontrolle, welche darauf basiert, mittels iterativer Überprüfungen der Ortsbeschränkungen die Nutzung eines Zugriffsrechts kontinuierlich zu regeln [37,109]. Ortsbeschränkungen, welche auf dieses Modell angewandt werden, beschränken daher nicht mehr nur den möglichen Ort des Nutzers sondern seine Trajektorie, also den zurückgelegten Pfad des Nutzers in der räumlich–zeitlichen Domäne [134,139]. Typischerweise werden Trajektorien als Polylinien definiert und mittels Interpolation aus den einzelnen Positionsschätzungen des Nutzers, die z.B. mittels GPS erfasst werden, abgeschätzt. Eine kontinuierlich durchgesetzte Ortsbeschränkung kann somit als Trajektorienbeschränkung aufgefasst werden. Diese erlauben es, Zugriffsrechte auf Nutzer zu begrenzen, deren zurückgelegte Trajektorie den geforderten Randbedingungen genügt. Eine Möglichkeit ist es zu fordern, dass die Trajektorie für die Dauer der Nutzung einer gewährten Zugriffsrechts vollständig innerhalb einer autorisierten Zone verläuft.

In existierenden Arbeiten zur kontinuierlichen Auswertung von Ortsbeschränkungen werden Positionsfehler nicht beachtet. Dabei wird die Trajektorie des Nutzers als eine fixe Polylinie modelliert, die aus der Aneinanderreihung der durchgeführten Positionsschätzungen konstruiert wird [35]. Mit dem Konzept des Partikelfilters existiert aber ein Verfahren, welches gerade in Kombination mit WLAN-Fingerprinting eine deutlich bessere Abschätzung der Nutzertrajektorie als eine solche Aneinanderreihung zeigen kann [65,146]. Partikelfilter sind spezielle Bayesische Filter, deren Leistungsfähigkeit darin begründet liegt, dass der negative Einfluss einzelner Positionsfehler auf die geschätzte Trajektorie reduziert wird. Ein Partikel repräsentiert hierbei eine Hypothese über den Standort des Nutzers, welche sich mit dem zeitlichen Verlauf und eintreffenden Positionsschätzungen verändern kann. Die Historie der Standorte eines Partikels ist somit eine mögliche Trajektorie des Nutzers. Anstelle einer einzelnen Polylinie erlaubt die Gesamtheit der Partikel, ein Bündel möglicher Trajektorien anzugeben. Somit kann eine probabilistische Aussagen über den Verlauf der Nutzertrajektorie getroffen werden. Hierfür genügt es zu ermitteln, wie hoch der prozentuale Anteil derjenigen Trajektorien aus dem Bündel ist, welche z.B. innerhalb

einer bestimmten Zone verlaufen.

Da keine der existierenden Arbeiten mögliche Positionsfehler in den Trajektorien berücksichtigt, sind diese in Gebäuden, wo meist WLAN-Fingerprinting zur Positionierung eingesetzt wird, direkt von Positionsfehlern betroffen. Werden die Trajektorien durch die Aneinanderreihung einzelner Positionsschätzungen erzeugt, so entstehen durch Messausreißer häufig Trajektorien, die fälschlicherweise anzeigen, dass der Nutzer die autorisierte Zone verlassen hat. Dies hat inakzeptabel viele falsche Autorisierungsentscheidungen und hohen Opportunitätsverlust zur Folge. Ebenso ist das Problem zu lösen, eine maximale Zeitspanne (Timeout) zu finden, die höchstens zwischen zwei aufeinanderfolgenden Positionsschätzungen verstreichen darf. Ein zu großer Wert kann das unbemerkte Verlassen der autorisierten Zone zwischen zwei Positionsschätzungen ermöglichen.

Im Folgenden wird daher ein Ansatz vorgestellt, der auf der Arbeit von Marcus et al. aufsetzt und eine kontinuierliche Autorisierungsstrategie für Ortsbeschränkungen erlaubt [95]. Hierbei wird die risikobasierte Autorisierungsstrategie zusammen mit Partikelfiltern auf Trajektorien angewandt. Zunächst wird in Unterabschnitt 4.3.1 die nötige Architektur beschrieben und das Angreifermodell spezifiziert. Es werden die beiden Hauptbeiträge des entwickelten Ansatzes beschrieben. Zum Einen ist dies die effiziente Anpassung der risikobasierten Autorisierungsstrategie auf ein Bündel von vermuteten Nutzertrajektorien, welches durch einen Partikelfilter hergeleitet wird. Zum Anderen wird ein Verfahren vorgestellt, welches den Timeout bis zur nächsten eintreffenden Positionsschätzung dynamisch und basierend auf der Gewissheit über den aktuellen Zustand des Nutzers bestimmt. Beide Beiträge werden anhand der Fingerprint-Datenbank aus Abb. 3.1(b) und 60 aufgezeichneten Trajektorien evaluiert.

4.3.1 Die Architektur und das Angreifermodell

Wird ein Zugriffsrecht gewährt, das über einen längeren Zeit genutzt wird, so muss kontinuierlich überprüft werden, ob der Nutzer die Bedingungen für die Nutzung noch erfüllt. Der bedeutendste allgemeine Ansatz ist UCON ABC von Sandhu et al. [123], wobei ausgehend von einem attributbasierten Zugriffskontrollmodell kontinuierlich überprüft wird, ob die Attribute des Nutzers die Bedingung noch erfüllen. Dieses Prinzip ist in Abb. 4.14 dargestellt. Die Entscheidung, ob das Recht für eine laufende Nutzung entzogen werden soll wird hier kontinuierlich wiederholt. Dieser Ansatz ist sehr allgemein gehalten, so dass für die Anwendung zur standortbasierten Autorisierung eine konkrete Realisierung der Architektur, der Autorisierungsstrategie und der Ermittlung der relevanten Attribute nötig ist.

Im Folgenden wird deshalb die entwickelte Architektur vorgestellt, welche eine kontinuierliche Auswertung von Ortsbeschränkungen mithilfe eines Partikelfilters ermöglicht. Hierzu werden probabilistische Trajektorien erfasst und bei der Auswertung verwendet. Die Wahrscheinlichkeit, mit welcher die probabilistische Trajektorie der Ortsbeschränkung genügt, kann als Attribut verstanden werden.

Die Architektur und der Nachrichtenaustausch zwischen den Komponenten sind in Abb. 4.12 dargestellt. Solche Komponenten, die zur Durchsetzung der Nutzungskontrolle neu ein-

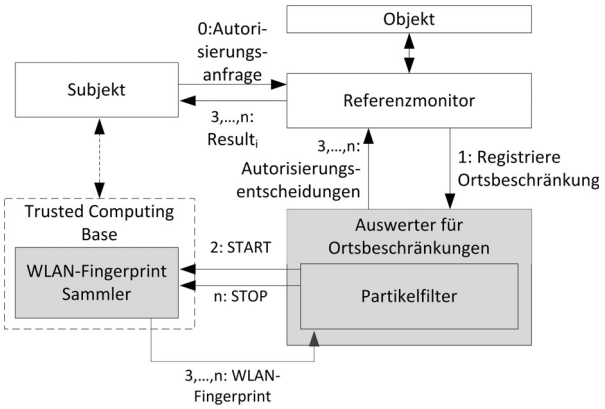


Abbildung 4.12: Neu eingeführte Komponenten (grau) arbeiten kontinuierlich zusammen, um Nutzungsentscheidungen bzgl. der registrieren Ortsbeschränkungen abzuleiten.

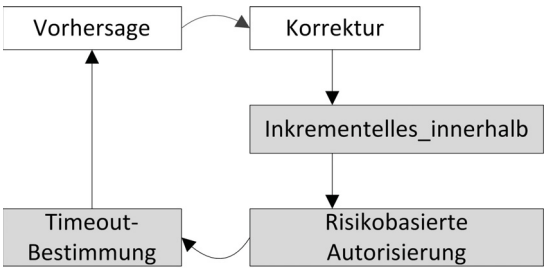


Abbildung 4.13: Ergänzung des klassischen Partikelfilters um drei Schritte.

geführt werden, sind grau hinterlegt. Zu Beginn stellt der Nutzer, also das Subjekt, eine Autorisierungsanfrage an den Referenzmonitor, um für ein Zugriffsrecht autorisiert zu werden. Der Referenzmonitor prüft, ob dem Zugriffsrecht eine Ortsbeschränkung zugeordnet ist und registriert diese im Auswerter für Ortsbeschränkungen (AfO). Der AfO umfasst den Betrieb des Partikelfilters, die Herleitung probabilistischer Trajektorien aus den Partikeln und wendet auf diese die risikobasierte Autorisierungsstrategie an. Der AfO kontaktiert die Komponente WLAN-Fingerprint-Sammler (WFS) auf dem mobilen Endgerät des Nutzers. Der WFS läuft, entsprechend des Vorschlags von Ulltveit-Moe et al. [144] in einer Trusted Computing Umgebung [50], so dass seine Funktionsweise nicht durch softwareseitige Manipulationen von Signalstärkemessungen beeinflusst werden kann. Dies ermöglicht es dem mobilen Endgerät eines Nutzers ein Attest zu erzeugen, das durch den AfO verifiziert werden kann und nachweist, dass sicherheitsrelevante Softwarekomponenten korrekt geladen und nicht kompromittiert wurden. Die relevanten Softwarekomponenten umfassen u.a. die Gerätetreiber, den Betriebssystemstack und den WFS selbst. Der WFS erfasst kontinuierlich WLAN-Fingerprints, die sequentiell zusammen mit ihrem jeweiligen Aufnahmezeitpunkt und dem erwähnten Attest digital signiert an den AfO übermittelt werden. Diese kontinuierliche Übermittlung erfolgt, bis die Zugriffsrechte durch den Referenzmonitor entzogen werden, oder durch den Nutzer manuell beendet werden.

Für die Einsetzbarkeit des Systems ist es unerlässlich, dass Nutzer daran gehindert werden, einen WFS auf einem fremden Endgerät zu spezifizieren, da sonst die ermittelten Trajektorien keine Aussage über den eigentlichen Pfad des Nutzers hätten. Daher werden die Nutzungsanfragen geschützt durch die Trusted Computing Base erzeugt und müssen zwangsweise den Dienstzugangspunkt des eigenen WFS an den Referenzmonitor übermitteln. Der entwickelte Ansatz erlaubt anschließend die probabilistische Abschätzung von Nutzertrajektorien im AfO und die darauf aufbauende risikobasierte Auswertung der be-

schriebenen Ortsbeschränkungen.

Die beschriebene Architektur ist konform zu dem zugrundeliegenden Angreifermodell. Hierbei wird ein Angreifer als ein mobiler Nutzer definiert, der die Abschätzung seiner Trajektorie in der Hinsicht manipuliert, dass Zugriffsrechte durch den Referenzmonitor gewährt werden, obwohl seine eigentliche Trajektorie nicht der zugrundeliegenden Ortsbeschränkung genügt. Insbesondere wird angenommen, dass ein Angreifer folgende Möglichkeiten besitzt:

- Manipulation von Sensordaten auf seinem mobilen Endgerät
- Verzögerung der Übermittlung von aufgezeichneten WLAN-Fingerprints an den AfO
- Bewegungsfreiheit in der autorisierten Zone und ihrer Umgebung, die durch die Ortsbeschränkung festgelegt ist

Ferner ist die Annahme, dass ein Angreifer nicht in der Lage ist, folgende Aktionen durchzuführen:

- Manipulation von gemessenen WLAN-Signalstärken
- Manipulation der Uhr seines mobilen Endgeräts
- Wiedereinspielen von veralteten WLAN-Fingerprints
- Manipulation von WLAN-Access-Points und der Infrastruktur

Um diesen Möglichkeiten eines potentiellen Angreifers gerecht zu werden, müssen für den eingesetzten Partikelfilter einige Randbedingungen beachtet werden.

4.3.2 Realisierung eines Partikelfilters zur standortbasierten Autorisierung

Im folgenden Unterabschnitt wird behandelt, wie der Korrektur- und Vorhersageschritt eines Partikelfilters umgesetzt werden kann, so dass dabei das definierte Angreifermodell berücksichtigt wird.

Der Vorhersageschritt: Ableiten von Trajektorienhypothesen

Für einen Zeitpunkt t sei die Menge der Partikel als $\mathcal{X}_t$ gegeben. Wird die Historie eines einzelnen Partikels betrachtet, so erhält man eine Hypothese über die vom Nutzer zurückgelegte Trajektorie. Im Schritt der Vorhersage wird für ein jedes Partikel seine bisherige Trajektorie verlängert, indem ein zusätzliches Segment angefügt wird. Dieses Segment besteht selbst aus Teilsegmenten, denn die Zeitspanne der Vorhersage, also genau die Zeit zwischen zwei eintreffenden Positionsschätzungen, wird in Teilintervalle von maximal 550 ms partitioniert, was der Zeit entspricht, die ein Mensch typischerweise für einen Schritt benötigt [103]. Nachdem ein solches Teilintervall verstrichen ist, wird für jedes Partikel das anzufügende Segment um ein weiteres Teilsegment erweitert. Solche Teilsegmente stellen für jedes Partikel eine mögliche Fortführung seiner bisherigen Trajektorie um einen

weiteren Schritt dar und werden als gerade Linien konstruiert. Hierbei wird eine lineare Bewegung des Partikels von seiner letzten Position l mit einer Geschwindigkeit v in die Richtung α während der Dauer des Teilintervalls angenommen. Ist zu Beginn des Vorhersageschritts ein Partikel $x_t^{[i]}$ gegeben, so wird das durch die Vorhersage konstruierte Segment als $\tau(x_t^{[i]}) = \langle (l_{t_0}, \alpha_{t_0}, v_{t_0}, t_{t_0}), \ldots, (l_{t_m}, \alpha_{t_m}, v_{t_m}, t_{t_m}) \rangle$ notiert, das sich aus den erwähnten m Teilsegmenten zusammensetzt. Die Zusammensetzung von Segmenten aus solchen Teilsegmenten ist in Abb. 4.15 veranschaulicht.

Angenommen, die autorisierte Zone, die von der Ortsbeschränkung gefordert wird, ist durch ein Polygon $\mathcal{Z}$ gegeben. Sei $t = 0$ der Zeitpunkt, zu dem das Zugriffsrecht erteilt und der Partikelfilter initialisiert wird, so ergibt sich die vollständige Trajektorie des Nutzers zu einem Zeitpunkt $t = j$ aus der Konkatenation $\tau(x_0^{[i]}) \circ \tau(x_1^{[i]}) \circ \ldots \circ \tau(x_j^{[i]})$ der Segmente aus den einzelnen Vorhersageschritten bis zum Zeitpunkt j. Diese Konkatenation der Segmente wird schließlich als die Grundlage zur risikobasierten Auswertung von Ortsbeschränkungen herangezogen. Im Folgenden soll $\tau(x_k^{[i]})$ *innerhalb* $\mathcal{Z}$ ein Prädikat darstellen, welches prüft, ob die Teilsegmente von $\tau(x_t^{[i]})$ vollständig innerhalb von $\mathcal{Z}$ verlaufen.

Ein wichtiger Aspekt bei der Konstruktion der Teilsegmente von $\tau(x_t^{[i]})$ ist, dass hierbei keine Messungen von inertialen Sensoren verwendet werden, um z.B. die realen Schritte besser durch die Teilsegmente abzubilden. Ansonsten könnte ein Angreifer nämlich durch Schütteln oder Bewegen seines mobilen Endgeräts den Partikelfilter manipulieren und das System wäre dem Angreifermodell nicht mehr angemessen. Dies ist ein Nachteil, da durch Beschleunigungssensoren und Kompass eine bessere Abbildung der Realität im Schritt der Vorhersage von Partikelfiltern möglich ist [73]. Dazu wird die Koppelnavigation zur Konstruktion der Teilsegmente eingesetzt. Im typischen Einsatzgebiet solcher Systeme zur Navigation innerhalb von Gebäuden, ist es unkritisch, dass ein Nutzer, z.B. durch das Schütteln seines mobilen Endgeräts, die Vorhersage irreführt. Hieraus würde lediglich eine schlechtere Navigation folgen, was einem solchen Nutzer nur Nachteile verschafft. Im Falle der Nutzungskontrolle könnte durch absolutes Stillhalten des mobilen Endgeräts das Verharren auf einer Stelle vorgetäuscht werden, so dass kein Segment ein mögliches Verlassen der autorisierten Zone abbilden würde. Neben dem Verzicht auf Kompassdaten bei der Positionsbestimmung mit WLAN-Fingerprinting, muss somit auch in der Vorhersage auf Genauigkeit zugunsten verringerter Angriffsmöglichkeiten verzichtet werden.

Um für das beschriebene Anwendungsszenario der Nutzungskontrolle solche Angriffe auszuschließen, basiert der vorliegende Ansatz auf einem Bewegungsmodell basierend auf zufälligen Wegpunkten (Random Waypoint Model). Hierbei werden für jedes Partikel $x_t^{[i]}$ die einzelnen Teilsegmente, die $\tau(x_t^{[i]})$ angehängt werden, ausschließlich basierend auf einem statistischem Modell der menschlichen Bewegung und somit ohne Sensormessungen erstellt. Ein solches Modell wurde von Widyawan et al. vorgestellt, das in dem vorliegenden Ansatz angewandt wird [146]. Die neue Position eines Partikels berechnet sich gemäß dieses Modells als:

$$l_j = \begin{bmatrix} l_{j_x} \\ l_{j_y} \end{bmatrix} = \begin{bmatrix} l_{j-1_x} + v_{j-1}\cos(\alpha_{j-1})\Delta t + n_{j-1} \\ l_{j-1_y} + v_{j-1}\sin(\alpha_{j-1})\Delta t + n_{j-1} \end{bmatrix} \tag{4.43}$$

Im ersten Schritt der iterativen Berechnung von $\tau(x_t^i)$ für ein Partikel x_t^i gemäß (4.43)

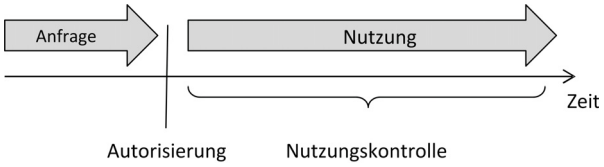


Abbildung 4.14: Zeitliche Einordnung der Autorisierung und Nutzungskontrolle.

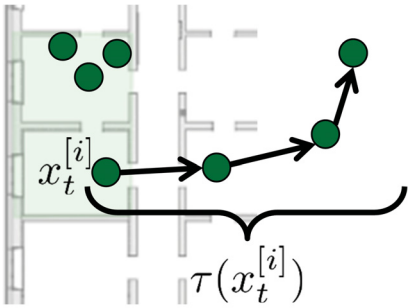


Abbildung 4.15: Für ein Partikel i besteht sein Segment $\tau(x_t^{[i]})$ aus einer Reihe von Teilsegmenten.

werden die Werte für l_{j-1}, α_{j-1} und v_{j-1} entsprechend des letzten Elements in $\tau(x_{t-1}^i)$ initialisiert. Der Winkel α ergibt sich dann zu:

$$\alpha_0 \in [0, 2\pi]\,; \alpha_t = (\alpha_{t-1}, 2\pi - \arctan\left(\frac{\sqrt{v_t}}{2}\Delta t\right) \tag{4.44}$$

Die Geschwindigkeit v berechnet sich als:

$$v_0 \in [0, 10\ \mathrm{ms}^{-1}]; v_t = \left|\mathcal{N}(v_{t-1}, 1\ ms^{-2}\Delta t)\right| \tag{4.45}$$

Dabei steht $\mathcal{N}(\mu, \sigma^2)$ für das zufällige Ziehen aus einer Normalverteilung.

In dem entwickelten Ansatz wird zusätzlich ein Kartenabgleich (Map Matching) durchgeführt, um realistische Trajektorien zu erhalten, welche die Gegebenheiten des zugrundeliegenden Gebäudeplans beachten [146]. Somit wird es möglich, beim Anhängen eines weiteren Teilsegments $\tau(x_t^{[i]})$ an die Trajektorie eines Partikels $x_t^{[i]}$ zu beachten, dass das Teilsegment keine Wände kreuzt. Bei der Konstruktion von $\tau(x_t^{[i]})$ wird dies realisiert, indem sukzessive probiert wird, ein weiteres Teilsegment anzuhängen, bis ein zuvor festgelegter Schwellwert an maximalen Versuchen erreicht ist. Da aufgrund dieser Konstruktion kein Teilsegment eine Wand schneidet, gilt dies auch für alle Segmente.

Ist die maximale Anzahl an Versuchen erreicht und konnten über das Bewegungsmodell nur Teilsegmente gefunden werden, die eine Wand schneiden, so wird das Gewicht $w_t^{[i]}$ des Partikels auf 0 gesetzt. Das Messmodells und die letzte Messung z_t werden in solchen Fällen also ignoriert. Somit werden die Gewichtungen der Partikel auch durch den Vorhersageschritt beeinflusst:

$$w_t^{[i]} = \begin{cases} 0, & \text{kein gültiges } \tau(x_t^{[i]}) \text{ gefunden} \\ p(z_t|x_t^{[i]}), & \text{sonst} \end{cases} \tag{4.46}$$

Eine Visualisierung der sich fortbewegenden Partikelwolke ist in Abb. 4.16(c) gegeben. Die resultierenden Trajektorien sind also aufgrund der Nichtbeachtung von Sensormessungen robust gegen Angriffe durch Sensormanipulation und können zur standortbasierten Autorisierung angewendet werden.

Der Korrekturschritt: Selektion realistischer Hypothesen

Der Korrekturschritt muss ebenfalls dem Angreifermodell genügen. In dem entwickelten System werden einzelne Positionsschätzungen (μ, Σ) mittels WLAN-Fingerprinting ermittelt und die WDF $wdf^{laplace}_{\mathbf{F}|\mu,\sigma}(f_x, f_y)$ vom Laplace-Fehlerschätzer verwendet. Es gilt somit $z_t = \mu$ und für das Messmodell $p(z_t|x_t^{[i]})$ dieser fixen Messung z_t folgt direkt aus der WDF:

$$p(z_t|x_t^{[i]}) = wdf^{laplace}_{\mathbf{F}|\mu,\sigma}(l) \tag{4.47}$$

wobei l die räumliche Position des Partikels darstellt. Wie bereits in Abschnitt 3.1 besprochen, darf in der Positionierung mittels WLAN-Fingerprinting der Kompass nicht verwendet werden, um die Manipulationsmöglichkeiten von Angreifern einzuschränken.

4.3.3 Die risikobasierte Autorisierungsstrategie für Trajektorien

Im Folgenden wird die Anpassung der risikobasierten Autorisierungsstrategie für probabilistische Trajektorien, die über einen Partikelfilter bestimmt werden, vorgestellt.

Probabilistische Trajektorien

Die einfachste, konventionelle Möglichkeit zur Konstruktion der Trajektorie des Nutzer ist die chronologische Konkatenation von einzelnen Positionsschätzungen. Dabei werden keine Filter eingesetzt, weshalb der Effekt von Positionsfehlern bzw. einzelnen Messausreißern ungehindert zum Tragen kommt. In der Literatur werden deshalb Partikelfilter zur Verfolgung von Nutzern eingesetzt, wobei der Effekt von Messausreißern bei der Abschätzung ihrer Trajektorie reduziert werden kann [65,73,146]. Dies erfolgt, indem nach Ausführung des Korrekturschritts der Mittelwert der einzelnen Partikelpositionen gebildet wird. Die so erstellten Mittelwerte werden chronologisch aneinandergereiht, was schließlich die Hypothese über die Nutzertrajektorie darstellt. Auf diese Art und Weise geht jedoch Information über einzelne Hypothesen verloren. Somit kann es vorkommen, dass eine so hergeleitete Trajektorie z.B. komplett innerhalb eines bestimmten Raumes verläuft, obwohl alle einzelnen Trajektorien der Partikel außerhalb verlaufen.

Um die Informationen aus den Trajektorien der einzelnen Partikel vollständig auszuwerten, verwendet der nachfolgend vorgestellte Ansatz das Bündel der Trajektorien, das sich aus der Historie der Partikel ergibt. Dieses Bündel an Trajektorien wird die Grundlage zur Anpassung der risikobasierten Autorisierungsstrategie.

Wird eine einzelne Trajektorie aus der chronologischen Konkatenation von einzelnen Punkten konstruiert, so besteht jeder Abtastpunkt aus einem fixen Ort und einem Zeitstempel [134]. Hierbei gibt es zunächst keine Beschreibung der Ungewissheit des tatsächlichen Pfades des Nutzers für die Zeit zwischen zwei Abstastpunkten. Im Bereich der Datenbanken bewegter Objekte wird deshalb der Begriff des Beads (engl. von Perlenschnur) definiert. Dies sind ellipsoide Strukturen, die alle Punkte umfassen, an denen eine Person unter Annahme einer maximalen Geschwindigkeit in der Zwischenzeit zweier Abtastpunkte gewesen

sein könnte [139]. Aufgrund der Ungewissheit zwischen den Abtastpunkten werden Trajektorien als Sequenz von Beads definiert. Die tatsächliche Trajektorie der Person verläuft vollständig innerhalb der Beads. Mit jedem neuen Abtastpunkt, wird die aktuelle Sequenz an Beads um einen weiteren Bead verlängert.

In solchen Fällen kann über spezielle räumlich–zeitliche Abfragen an die Datenbank ermittelt werden, mit welcher Wahrscheinlichkeit die Sequenz von Beads z.B. innerhalb eines bestimmten Raumes verläuft. Dies ist eine Voraussetzung zur späteren Anwendung der risikobasierten Strategie. Wird jedoch ein Partikelfilter zur Abschätzung verwendet, so entsteht durch die Betrachtung der zurückgelegten Trajektorien der einzelnen Partikel eine diskrete Menge von einzelnen Hypothesen über die reale Trajektorie des Nutzers. Diese formen keine Beads. Deshalb ergeben sich insgesamt die folgenden Gründe, warum die klassischen Verfahren zur Auswertung von räumlich–zeitlichen Abfragen nicht in Kombination mit dem vorgestellten Partikelfilter angewandt werden:

- Mögliche Bewegungsbahnen werden durch die diskreten Trajektorien der Partikel abgeschätzt.
- Beim Einsatz eines Partikelfilters kann sich die Trajektorie mit jedem weiteren Abtastpunkt verändern, z.B. wenn Partikel sterben.
- Einzelne Positionsschätzungen werden über eine WDF gemäß Abschnitt 3.1 beschrieben, anstelle punktueller Orte.

Auf Basis dieser probabilistischen Trajektorien wird im Folgenden die entsprechende Anpassung der risikobasierten Strategie zur kontinuierlichen Auswertung von Ortsbeschränkungen vorgestellt.

Risikobasierte Autorisierung für Trajektorien

Damit die risikobasierte Autorisierungsstrategie auf Basis eines Trajektorienbündels arbeitet, muss ihre Definition entsprechend angepasst werden. Dabei sei vorausgesetzt, dass die Trajektorien des Bündels mithilfe des beschriebenen Partikelfilters und den eingegangenen Positionsschätzungen $\langle(\mu,\Sigma)_0,\ldots,(\mu,\Sigma)_t\rangle$ für die Zeitspanne $[0;t]$ bestimmt werden. Das Trajektorienbündel kann für einen Zeitpunkt t aus der Menge der Partikel $\mathcal{X}_t$ extrahiert werden. Hierzu werden für jedes Partikel i dessen Segmente $\tau(x_0^{[i]}),\ldots,\tau(x_t^{[i]})$ konkateniert.

Die risikobasierte Strategie nach (4.25) wird so modifiziert, dass anstelle von $p_{\mathcal{Z}}$ für einen Zeitpunkt t nun der Prozentsatz der Trajektorien des Bündels verwendet wird, der vollständig innerhalb von $\mathcal{Z}$ verläuft. Dieser Prozentsatz wird im Folgenden als $p_{\mathcal{Z}}^{Traj}(\mathcal{X}_t)$ bezeichnet und berechnet sich als:

$$p_{\mathcal{Z}}^{Traj}(\mathcal{X}_t) = |\mathcal{X}_t|^{-1} \cdot \left|\left\{x_t^{[i]} \in \mathcal{X}_t | \forall k \in \{0,\ldots,t\} : \tau(x_k^{[i]})\ \textit{innerhalb}\ \mathcal{Z}\right\}\right| \tag{4.48}$$

Im Folgenden soll $p_{\mathcal{Z}}^{Traj}(\mathcal{X}_t)$ als $p_{\mathcal{Z}}^{Traj}$ abgekürzt werden. Für die risikobasierte Autorisie-

rung auf probabilistischen Trajektorien ergibt sich schließlich aus (4.25) folgende Definition:

$$\text{aut}^{Traj}\left(p_{\mathcal{Z}}^{Traj}\right) \Leftrightarrow p_{\mathcal{Z}}^{Traj}\,\mathrm{U}\,(RP) + \left(1 - p_{\mathcal{Z}}^{Traj}\right)\mathrm{U}\,(FP) > p_{\mathcal{Z}}^{Traj}\,\mathrm{U}\,(FN) + \left(1 - p_{\mathcal{Z}}^{Traj}\right)\mathrm{U}\,(RN) \quad (4.49)$$

Trifft eine neue Positionsschätzung mit Zeitstempel t am AfO ein, so wird nach der Durchführung des Korrekturschritts über die Fortführung der Zugriffsberechtigung mittels dieser angepassten risikobasierten Strategie entschieden. Nur wenn die Bedingung wahr ist, darf der Nutzer das gewährte Zugriffsrecht weiterhin nutzen. Die Entscheidung über Zugriffsrechte in der Zeitspanne zwischen zwei Korrekturschritten wird in Unterabschnitt 4.3.4 vorgestellt.

Grundsätzlich entsteht bei der Auswertung von (4.48) ein hoher Berechnungsaufwand durch die Ermittlung von $p_{\mathcal{Z}}^{Traj}$. Insbesondere muss für jedes Partikel i für alle Zeitpunkte $k \in \{0, \ldots, t\}$ überprüft werden, ob $\tau(x_k^{[i]})$ *innerhalb* $\mathcal{Z}$ gilt. Im Folgenden wird eine Erweiterung vorgestellt, die eine effizientere Bestimmung von $p_{\mathcal{Z}}^{Traj}$ erlaubt und (4.48) ersetzt.

Dazu wird die Datenstruktur für Partikel so erweitert, dass diesen jeweils ein Boolescher Wert `ist_gültig` zugewiesen und dynamisch aktualisiert werden kann. Die Anzahl der nötigen Überprüfungen von $\tau(x_k^{[i]})$ *innerhalb* $\mathcal{Z}$ kann somit stark reduziert werden. Dieser Boolesche Wert beschreibt für jedes Partikel i zum Zeitpunkt t, ob alle seine bisherigen Segmente vollständig innerhalb von $\mathcal{Z}$ liegen:

$$x_t^{[i]}.\texttt{ist\_gültig} = \texttt{wahr} \;\Leftrightarrow\; \forall k \in \{0, \ldots, t\} : \tau(x_k^{[i]})\ \textit{innerhalb}\ \mathcal{Z} \quad (4.50)$$

Wird ein weiteres Segments $\tau(x_{t+1}^{[i]})$ angefügt, so kann dieses natürlich aus $\mathcal{Z}$ herausragen. Somit wird nach einem durchgeführten Korrekturschritt zunächst für jedes Partikel die Bedingung `ist_gültig` aktualisiert, bevor (4.49) ausgewertet wird. Der Laufzeit-Vorteil ergibt sich aus zwei Aspekten. Zum Einen muss diese Eigenschaft nur für Partikel aktualisiert werden, für die zuvor noch `ist_gültig` = `wahr` gilt. Wurde die Bedingung bereits durch ein früheres Segment verletzt, so bleibt diese auch durch Anfügen eines weiteren Segments verletzt. Zum Anderen muss für diese Partikel jeweils nur für das letzte Segment überprüft werden, ob dieses vollständig in $\mathcal{Z}$ liegt, anstatt jedes mal die komplette Historie prüfen zu müssen. Konkret wird $p_{\mathcal{Z}}^{Traj}$ als Prozentsatz der Partikel bestimmt, für die `ist_gültig` = `wahr` gilt. Diese Bestimmung erfolgt für eine neue Positionsschätzung mit Zeitstempel $t+1$ direkt nach dem Korrekturschritt und unmittelbar vor der Auswertung von aut^{Traj}. Das Verfahren ist in Algorithmus 5 dargestellt. Offensichtlich entspricht dessen Anwendung der direkten Anwendung von (4.48), da $x_0^{[i]}.ist\_gültig = \tau(x_0^{[i]})\ innerhalb\ \mathcal{Z}$ und:

$$x_{t+1}^{[i]}.ist\_gültig\ = x_t^{[i]}.ist\_gültig \wedge \tau(x_{t+1}^{[i]})\ innerhalb\ \mathcal{Z} \quad (4.51)$$

gilt. Durch diese angepasste risikobasierte Autorisierung steht ein effizientes Mittel zur Verfügung, um mithilfe von Partikelfiltern die Durchsetzung einer Nutzungskontrolle zu realisieren. Um diese auch in der Zeit zwischen zwei eintreffenden Positionsschätzungen zu

Algorithmus 5 Ein Algorithmus zur inkrementellen Bestimmung von $p_{\mathcal{Z}}^{Traj}$.

Eingabe: Partikelwolke $\mathcal{X}_{t+1}$, Autorisierte Zone $\mathcal{Z}$
Vorbedingung: Ausführung direkt nach Korrekturschritt

```
1: function INKREMENTELLES_INNERHALB( X_{t+1}, Z )
2:     for each x_{t+1}^[i] ∈ X_{t+1} do
3:         if x_t^[i].ist_gültig ∧ ¬ τ(x_{t+1}^[i]) innerhalb Z then
4:             x_{t+1}.ist_gültig ← falsch            ▷ Letztes Segment verletzt Bed.
5:         else
6:             x_{t+1}.ist_gültig ← x_t.ist_gültig    ▷ Bed. bleibt verletzt
7:         end if
8:     end for
9:     return |X_{t+1}|^{-1} · |{ x_{t+1}^[i] ∈ X_{t+1} | x_{t+1}.ist_gültig = wahr }|
10: end function
```

realisieren, wird im nächsten Unterabschnitt ein Konzept vorgestellt, welches dynamisch die maximal erlaubte Zeitspanne bis zur nächsten eintreffenden Positionsschätzung basierend auf $p_{\mathcal{Z}}^{Traj}$ bestimmt.

4.3.4 Dynamische Bestimmung des maximalen Positionierungsintervalls

Das Positionierungsintervall beschreibt die maximale Zeitspanne (Timeout), die zwischen dem Eintreffen von zwei Positionsschätzungen am AfO verstreichen darf. In der Zeit zwischen zwei Positionsschätzungen könnte ein autorisierter Nutzer das System angreifen, indem er die autorisierte Zone verlässt und das Zugriffsrecht weiterhin nutzt, obwohl dieses nur innerhalb von $\mathcal{Z}$ gewährt werden sollte.

Eine Möglichkeit dieses Problem zu lösen ist die Vorgabe eines fixen Timeouts. Je nach der Gewissheit über den Standort des Nutzers ist jedoch ein anderer Timeout erforderlich. Zeigen zum Zeitpunkt t die Partikel $\mathcal{X}_t$ an, dass er sich mit hoher Wahrscheinlichkeit im Randbereich der autorisierten Zone befindet, so ist intuitiv ein kleiner Timeout zu wählen, da weniger Zeit zum Verlassen von $\mathcal{Z}$ benötigt wird. Befindet sich der Nutzer jedoch genau in der Mitte von $\mathcal{Z}$, so wird er mehr Zeit benötigen um überhaupt die Grenze zu erreichen und schließlich $\mathcal{Z}$ zu verlassen. Diese Überlegung ist die Grundlage des im Folgenden vorgestellten Verfahrens zur dynamischen Bestimmung von Timeouts.

Ein Nutzer, der das System angreifen möchte, wird im Extremfall nach einer durchgeführten Positionsschätzung die autorisierte Zone $\mathcal{Z}$ schnellstmöglich verlassen. Er wählt dazu den kürzesten Weg aus $\mathcal{Z}$ heraus, den er mit seiner schnellstmöglichen Schrittgeschwindigkeit geht. Zur Bestimmung von *timeout* wird angenommen, dass jedes Partikel der Menge $\mathcal{X}_t$ einen solchen Angreifer repräsentiert. Für *timeout* ergibt sich die kürzest mögliche Zeitspanne, innerhalb der die Partikel aus $\mathcal{X}_t$ so bewegt werden können, dass eine neue Partikelwolke $\mathcal{X}'_t$ entsteht, deren Wert $p_{\mathcal{Z}}^{Traj}(\mathcal{X}'_t)$ keine Autorisierung nach (4.49)

erlaubt. Hierzu wird das Konzept des Angreifer-Bewegungsmodells eingeführt.

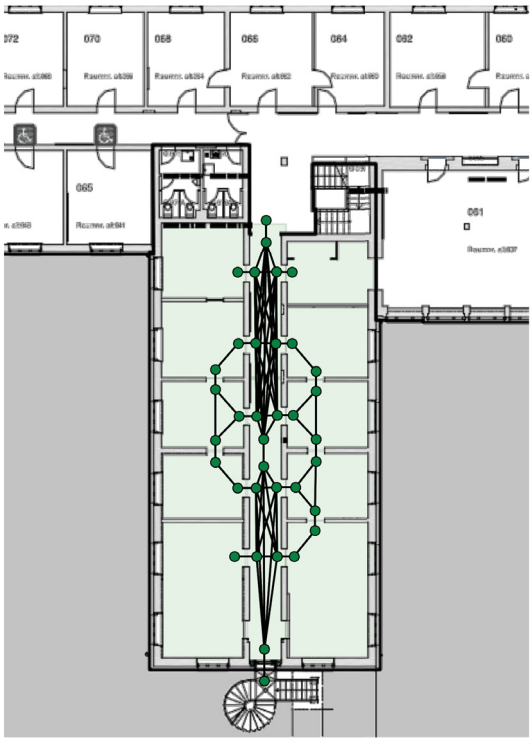
Das Angreifer-Bewegungsmodell Das Random-Waypoint-Modell, das wie oben beschrieben im Vorhersageschritt zur Bewegung der Partikel angewandt wird, ist nicht geeignet, um $\mathcal{X}'_t$ herzuleiten. Es spiegelt in der Bewegung der Partikel nicht die Bewegung eines Angreifers wider. Die zeitliche Dauer, ab welcher die Partikelwolke mit dem Random-Waypoint-Modell schließlich (4.49) verletzt, kann deutlich länger als die Zeitspanne sein, die der echte Angreifer zum Verlassen der autorisierten Zone benötigt. Es kann somit nicht zur Bestimmung von *timeout* eingesetzt werden. Insbesondere liegt dies daran, dass Türen in der Regel nur einen kleinen Teil der Wandfläche eines Raumes darstellen. Im Random-Waypoint-Modell müssten alle Partikel zufällig ihre nächstgelegene Türe treffen, um die autorisierte Zone wie ein Angreifer zu verlassen. Die Wahrscheinlichkeit, dass ein Partikel einen Angreifer abbildet, ist im Random-Waypoint-Model deshalb verschwindend gering. Das führt dazu, dass die Zeit deutlich unterschätzt wird, die ein Angreifer tatsächlich zum Verlassen der autorisierten Zone und bis zur Verletzung der Ortsbeschränkung benötigt.

Zur Bestimmung von *timeout* wird deshalb ein eigens entwickeltes Angreifer-Bewegungsmodell auf die Partikelwolke angewandt. Partikel, die außerhalb von $\mathcal{Z}$ liegen und deren Trajektorie die Ortsbeschränkung schon verletzt hat, werden dabei nicht bewegt. Die Partikel, die sich innerhalb der autorisierten Zone befinden und deren Trajektorie auch vollständig innerhalb von $\mathcal{Z}$ liegt, werden jeweils auf ihrem kürzesten Weg in Richtung des Ausgangs der autorisierten Zone bewegt. Ein schematischer Vergleich beider Bewegungsmodelle ist in Abb. 4.16(b) gegeben.

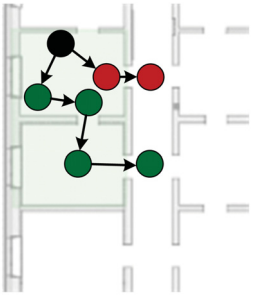
Implementierung des Angreifer-Bewegungsmodells Der erste Schritt ist das Anlegen eines Wegpunktgraphen $G = (V, E)$ für den zu unterstützenden Gebäudeplan. Die Knoten V stellen hierbei Koordinaten aus $\mathbb{R}^2$ und die Kanten E Verbindungen zwischen diesen Knoten dar. Im Folgenden wird davon ausgegangen, dass autorisierte Zonen entweder einzelne Räume oder deren Vereinigungen umfassen. Für die verwendete Testumgebung ergibt sich schließlich der in Abb. 4.16(a) dargestellte Wegpunktgraph. Kirkpatrik et al. verwenden in [77] ein ähnliches Konzept von Begehbarkeitsgraphen autorisierter Zonen, jedoch nicht im Hinblick auf die Berechnung eines geeigneten Timeouts, sondern um zu bestimmen, wie wahrscheinlich sich andere Personen in Nachbarräumen befinden.

Bei der Erstellung des Begehbarkeitsgraphen aus Abb. 4.16(a) wird über die autorisierten Zonen iteriert und für jede ihrer Türen ein Paar von Knoten eingefügt. Diese Paare von Knoten modellieren die Möglichkeit zum Übertritt in einen anderen Raum. Ein Knoten befindet sich dabei unmittelbar vor der Tür innerhalb der autorisierten Zone, der zweite Knoten liegt außerhalb davon ebenfalls unmittelbar an der Tür. Sind die Knoten V vollständig erfasst, wird hieraus die Kantenmenge E konstruiert. Dabei wird für jedes Paar von zwei Knoten, die innerhalb des gleichen Raums liegen, eine Kante angelegt.

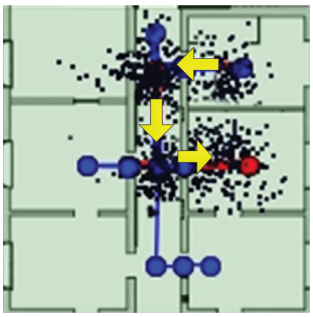
Im nächsten Schritt wird mithilfe des Dijkstra-Algorithmus eine $n \times n$ Matrix konstruiert, wobei $n = |V|$. Diese Matrix wird im Folgenden als Distanzmatrix D bezeichnet und



(a) Wegpunktgraph für das Angreifer-Bewegungsmodell.



(b) Random-Waypoint- und Angreifer-Bewegungsmodell (grün/rot) für ein Partikel (schwarz).



(c) Visualisierung des Partikelfilters.

Abbildung 4.16: Visualisierungen zur Bewegung von Partikeln. Abb. 4.16(a) zeigt den Wegpunktgraph für die Testumgebung. Abb. 4.16(b) stellt die mögliche Bewegung im Random-Waypoint- und im Angreifer-Bewegungsmodell gegenüber. Abb. 4.16(c) zeigt die Fortbewegung der Partikelwolke, die für 4 Zeitpunkte nach dem Korrektuschritt eingezeichnet ist.

enthält für alle Paare von Knoten die metrische Länge des kürzesten Pfades in G, der diese verbindet. Der kürzeste Pfad zwischen zwei Knoten *n1* und *n2* wird gemäß D als $\mathrm{D}(n1, n2)$ notiert.

Darauf basierend kann nun für jedes Partikel, das sich zum Zeitpunkt t noch in der autorisierten Zone befindet, seine minimale Austrittszeit berechnet werden. Diese beschreibt die kürzest mögliche Zeitspanne, in der sich das Partikel unter Annahme einer maximalen Geschwindigkeit v_{max} aus der autorisierten Zone bewegen kann. Auf Basis der einzelnen Austrittszeiten wird schließlich im nächsten Paragraphen der *timeout* bestimmt.

Algorithmus 6 beschreibt die Vorgehensweise zur Bestimmung der minimalen Austrittszeiten. Zuerst wird dabei der Knoten *n1* mit der kürzesten euklidische Distanz zum Partikel $x_t^{[i]}$ bestimmt, der ebenso innerhalb der autorisierten Zone liegt. Diese Distanz *d1* wird gespeichert. Im nächsten Schritt wird ausgehend von *n1* der kürzeste Pfad gesucht, der

Algorithmus 6 Ein Algorithmus zur Bestimmung der minimalen Austrittszeit.

Eingabe: Partikel $x_t^{[i]}$, Wegegraph $G = (V, E)$, Distanzmatrix D, Autorisierte Zone $\mathcal{Z}$
Vorbedingung: $x_t^{[i]}.\texttt{ist\_gültig} = \texttt{wahr}$

1: **function** MINIMALE_AUSTRITTSZEIT($x_t^{[i]}$, G, $\mathcal{Z}$)
2: $V' \leftarrow \{v' \in V \mid v' \notin \mathcal{Z}\}$ ▷ Alle Knoten außerhalb von $\mathcal{Z}$
3: $n1 \leftarrow \arg\min_{v \in V \setminus V'} \|x_t^{[i]} - v\|_2$ ▷ Nächster Knoten zum Partikel in $\mathcal{Z}$
4: $d1 \leftarrow \|x_t^{[i]} - n1\|_2$ ▷ Euklidische Distanz zu n1
5: $d2 \leftarrow \min(\{\mathrm{D}(n1, n2) \mid n2 \in V'\})$ ▷ Kürzester Austrittspfad in Distanzmatrix
6: **return** $(d1 + d2)/v_{max}$
7: **end function**

aus $\mathcal{Z}$ herausführt. Dessen Länge wird in *d2* gespeichert. Unter Annahme einer maximalen Geschwindigkeit der Angreifer von v_{max} ergibt sich über $t = \frac{s}{v}$ die minimale Austrittszeit als $\frac{d1+d2}{v_{max}}$.

Timeout-Bestimmung mittels Angreifer-Bewegungsmodell Wurde der Korrekturschritt für eine Positionsschätzung mit Zeitstempel t durchgeführt, so kann ausgehend von der Partikelwolke $\mathcal{X}_t$ für jeden späteren Zeitpunkt t' der Prozentsatz an Partikeln bestimmt werden, die unter dem Angreifer-Bewegungsmodell noch eine Trajektorie besitzen, die komplett innerhalb von $\mathcal{Z}$ verläuft:

$$p_{\mathcal{Z}}^{Traj}(\mathcal{X}_t, t') = p_{\mathcal{Z}}^{Traj}(\mathcal{X}_t) - \left|\{\, x_t^{[i]} \in \mathcal{X}_t \mid x_t^{[i]}.\texttt{ist\_gültig} \wedge \texttt{minimale\_Austrittszeit}\left(x_t^{[i]}, G, \mathcal{Z}\right) \leq t' \right\}\Big| \cdot |\mathcal{X}_t|^{-1} \tag{4.52}$$

Der gesuchte Timeout ist schließlich die kleinste Zeitspanne $t' - t$, nach der die Trajektorien so vieler Partikel die Ortsbeschränkung verletzen, dass die risikobasierte Autorisierung nach (4.49) zu einer Ablehnung führt:

$$timeout = \min\left(\left\{t' \in \mathbb{R} \mid t < t' \wedge \mathrm{aut}^{Traj}\left(p_{\mathcal{Z}}^{Traj}(\mathcal{X}_t, t')\right) = \texttt{falsch}\right\}\right) - t \tag{4.53}$$

Ausgehend von einer Zustandsschätzung $\mathcal{X}_t$ des Nutzers, liefert dies also die kleinste Zeitspanne, nach der die Zugriffsrechte entzogen werden müssen, sofern keine neue Positionsschätzung am AfO eintrifft.

4.3.5 Evaluation

Im Folgenden wird eine Evaluation des entwickelten Ansatzes vorgestellt.

Testumgebung und Hardware Voraussetzung für die Evaluation ist die Bereitstellung von autorisierten Zonen und Trajektorien. Insgesamt werden 5 autorisierte Zonen verwendet, die jeweils aus der Vereinigung von benannten Räumen bzw. Bereichen aus Abb. 3.1(a)

bestehen. Sie setzen sich folgendermaßen zusammen: $\langle 01 \rangle$, $\langle 06; 08 \rangle$, $\langle 05; 07 \rangle$, $\langle 07; 09 \rangle$ und $\langle 01 - 06; \mathit{f1} \rangle$. Für jede dieser Zonen werden 12 aufgezeichnete Nutzertrajektorien verwendet, die zuvor durch Ablaufen eines Pfads für jeweils ca. 60 s mittels eines HTC Desire aufgezeichnet wurden. Die Aufzeichnung enthält spätestens alle 1,5 s eine Messung des WLAN-Fingerprints. Ferner liegt die manuell ergänzte Grundwahrheit zu jeder Trajektorie vor. Für jede der modellierten autorisierten Zonen können die zugehörigen Trajektorien bzgl. ihrer Grundwahrheit folgendermaßen klassifiziert werden: Drei der abgelaufenen Trajektorien verlaufen vollständig innerhalb der autorisierten Zone, wobei bei einer Trajektorie stationär auf einem Punkt gestanden wurde. Drei Trajektorien verlaufen außerhalb, aber in direkter Nähe zur autorisierten Zone und liegen innerhalb des Gebäudes. Darunter ist wieder eine stationäre Trajektorie. Jeweils zwei Trajektorien wurden aufgenommen, welche zunächst innerhalb der autorisierten Zone verlaufen, diese verlassen und dann wieder betreten. Zuletzt wurden jeweils noch drei Trajektorien aufgenommen, welche außerhalb des Gebäudes aber in direkter Nähe zur autorisierten Zone verlaufen. Diese aufgezeichneten Trajektorien werden bzgl. ihrer abgelaufenen Grundwahrheit in drei Klassen eingeordnet: Jederzeit gültige Trajektorien (*c1*), die stets innerhalb der autorisierten Zone verlaufen, zunächst gültige Trajektorien (*c2*), die nach einer gewissen Zeit außerhalb verlaufen und ungültige Trajektorien (*c3*), die von Beginn an nicht innerhalb der autorisierten Zone verlaufen.

Evaluationsergebnisse Zunächst wird für die Trajektorien jeder Klasse der minimale Wert $p_{\mathcal{Z}}^{Traj}$ ermittelt, der während der Anwendung des Partikelfilters auftritt. Um anhand dieses Wertes auf die Klasse rückzuschließen, muss das minimale $p_{\mathcal{Z}}^{Traj}$ für Trajektorien der Klasse *c1* möglichst groß sein. Für die Trajektorien der Klassen *c2* und *c3* sollte dieser Wert hingegen möglichst klein sein. Für jede dieser Klassen ist die kumulative Verteilung der minimal beobachteten Werte $p_{\mathcal{Z}}^{Traj}$ ihrer Trajektorien in Abb. 4.17 dargestellt. Es zeigt sich, dass in der Klasse *c1* in über 75% der Fälle, der minimale Wert von $p_{\mathcal{Z}}^{Traj}$ größer als 20% ist. Die Klassen *c2* und *c3* hingegen zeigen in ca. 90% der Fälle einen minimalen Wert $p_{\mathcal{Z}}^{Traj}$ von 0%.

Der entwickelte Ansatz muss mit einer Adaption der naiven Strategie verglichen werden. Diese konkateniert alle abgeleiteten Positionsschätzungen und formt eine Trajektorie $\langle \mu_1, \ldots, \mu_n \rangle$. Ziel des Partikelfilters ist es, im Mittel einen geringeren Opportunitätsverlust zu erreichen, als die naive Strategie.

Wie beim Ansatz zur Erweiterung von RBAC, soll das Verhalten untersucht werden, für solche Ortsbeschränkungen mit $\mathrm{U}(RP) = \mathrm{U}(RN) = 1$, $\mathrm{U}(FP) = 0$ und $\mathrm{U}(FN) \in [0; 1]$ (Fall 1), sowie Ortsbeschränkungen mit $\mathrm{U}(RP) = \mathrm{U}(RN) = 1$, $\mathrm{U}(FN) = 0$ und $\mathrm{U}(FP) \in [0; 1]$ (Fall 2). In diesen Abbildungen U ist der Nutzen von *FP* und *FN* stets kleiner, als der Nutzen der richtigen Entscheidungen *RP* und *RN*. Im Folgenden sei wieder $u := [\mathrm{U}(RP) - \mathrm{U}(FN)]$ und $t := [\mathrm{U}(RN) - \mathrm{U}(FP)]$. Die Ortsbeschränkungen, für deren U der erste Fall gilt, besitzen ein Verhältnis $u/t \in [0; 1]$, was sich leicht durch Einsetzen nachprüfen lässt. Für den zweiten Fall gilt $u/t \in [1; \infty]$.

Die prozentuale Reduktion des Opportunitätsverlusts beim Einsatz der risikobasierten

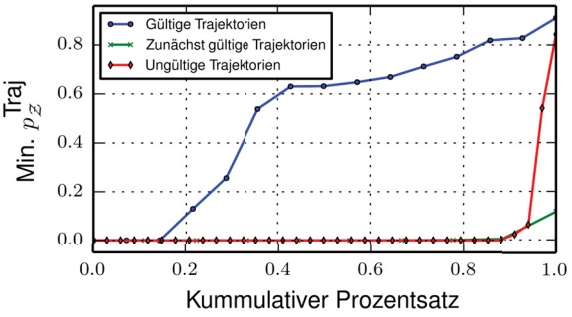


Abbildung 4.17: Die kumulative Verteilung der minimalen Werte von $p_{\mathcal{Z}}^{Traj}$ der Trajektorien einer Klasse.

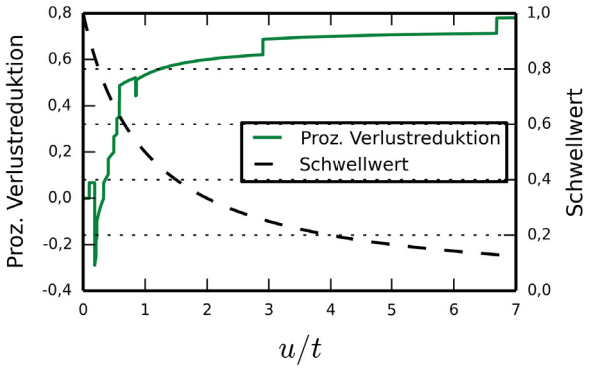


Abbildung 4.18: Prozentuale Reduktion des Opportunitätsverlusts beim Einsatz der risikobasierten Strategie basierend auf dem Partikelfilter.

Strategie gegenüber dem Einsatz der adaptierten naiven Strategie ist in Abb. 4.18 dargestellt. Je größer die Werte auf der Ordinatenachse, umso stärker kann für eine entsprechende Ortsbeschränkung vom Einsatz des vorgestellten Systems profitiert werden. Es zeigt sich, dass der vorgestellte Ansatz für gewisse Werte u/t einen größeren Opportunitätsverlust verursacht, als die adaptierte naive Strategie. Dies lässt sich erklären, indem in Abhängigkeit von u/t der Schwellwert betrachtet wird, den $p_{\mathcal{Z}}^{Traj}$ übersteigen muss, um durch die risikobasierte Strategie autorisiert zu werden. Dieser Schwellwert ist in Abb. 4.18 als gestrichelte Linie dargestellt und gemäß Satz 4.1.2 berechnet. Dabei zeigt sich, dass für Werte von u/t nahe 0, ein minimaler Wert $p_{\mathcal{Z}}^{Traj}$ von annähernd $80 - 100\%$ gefordert ist. Nur wenige der Trajektorien aus der Klasse *c1* erfüllen dieses Kriterium und können zu einer richtigen Entscheidung führen. Die naive Strategie ist mit ihren wenig korrekt autorisierten Trajektorien aus *c1* im Vorteil. Es ist erkennbar, dass mit größer werdenden Werten von u/t auch der nötige Schwellwert für $p_{\mathcal{Z}}^{Traj}$ sinkt und mit jeder weiteren Trajektorie der Klasse *c1*, die nun dem Schwellwert genügt, eine Stufe im Verlauf der prozentualen Verlustreduktion entsteht. Das lokale Minimum des Verlaufs bei ca. $u/t = 1$ ergibt sich aus der Trajektorie der Klasse *c3*, deren minimaler Wert $p_{\mathcal{Z}}^{Traj}$ mit 55% sehr hoch ist.

Aus dieser Analyse kann die Schlussfolgerung getroffen werden, dass für eine Ortsbeschränkung mit Verhältnis u/t die Einsetzbarkeit des vorgestellten Systems stark davon abhängt, wie die minimalen Werte von $p_{\mathcal{Z}}^{Traj}$ verteilt sind. Insbesondere gilt für Trajektorien der Klasse *c1*, dass ihr minimaler Wert von $p_{\mathcal{Z}}^{Traj}$ möglichst hoch sein muss, damit über die Aufnahmedauer hinweg eine Autorisierung durch die risikobasierte Strategie erfolgt. Ist die prozentuale Verlustreduktion für eine zu unterstützende Ortsbeschränkung mit u/t negativ, so kann der minimale Wert von $p_{\mathcal{Z}}^{Traj}$ z.B. durch Ausbringung eines präziseren Positionierungssystems oder durch Erhöhung der Partikelanzahl erreicht werden. Für Ortsbeschränkungen mit einer beliebigen Abbildung U für den Nutzen kann diese Analyse ebenso durchgeführt werden, wobei dann im Allgemeinen kein Zurückgreifen mehr auf den

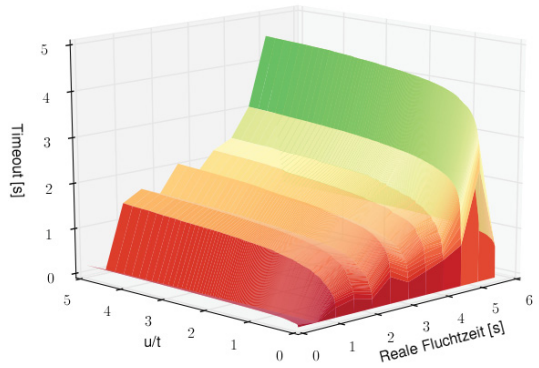


Abbildung 4.19: Die gelieferten Timeouts in Abhängigkeit von u/t und der realen minimalen Austrittszeit.

Klasse der Trajektorie	**Ignorierbare Partikel**
Gültige Trajektorie	30%
Zunächst gültige Trajektorie	72%
Ungültige Trajektorie	92%

Tabelle 4.3: Einsparung durch inkrementelle Berechnung von $p_{\mathcal{Z}}^{Traj}$.

Vergleich mit dem minimal benötigten Schwellwert möglich ist (siehe Satz 4.1.2).

Im nächsten Schritt wird untersucht, welche Einsparung der Einsatz von Algorithmus 5, also der Funktion `inkrementelles_innerhalb` bringt. Je kleiner die Menge der Partikel ist, für die bestimmt werden muss ob ihr letztes Pfadsegment innerhalb von $\mathcal{Z}$ verläuft, desto größer die Performanzsteigerung. Für die Trajektorien der unterschiedlichen Klassen ist der Prozentsatz der Partikel, für die im Mittel dank Algorithmus 5 diese Überprüfung entfällt, in Tab. 4.3 abgebildet. Natürlich hängt der Wert stark von der jeweiligen Klasse von Trajektorien ab. Für die ungültigen Trajektorien der Klasse *c3* können im Mittel 92% der Partikel ignoriert werden. In der Klasse *c1* ist das natürlich nicht der Fall, da die Trajektorien der Partikel im Optimalfall alle innerhalb von $\mathcal{Z}$ verlaufen sollen. Die hier erreichten 30% beruhen also nur auf der Ungenauigkeit des eingesetzten Partikelfilters.

Zuletzt soll gezeigt werden, dass die dynamisch hergeleiteten Timeouts mit den realen minimalen Austrittszeiten korrelieren, die der Nutzer von seiner realen Position bis zum Verlassen der autorisierten Zone benötigen würde. Die hergeleiteten Timeouts sind in Abb. 4.19 auf der Z-Achse dargestellt, in Abhängigkeit von der jeweiligen realen Austrittszeit und dem Wert u/t der zugrundeliegenden Ortsbeschränkung. Es zeigt sich, dass die Werte gut mit der realen Austrittszeit korrelieren, sofern $u/t > 1$ gilt. Die Gründe sind ähnlich, wie bei der obigen Diskussion zur prozentualen Verlustreduktion. Für die Werte $u/t < 1$ ist der minimale Schwellwert so hoch, dass dieser bereits unterschritten wird, nachdem nur wenige, türnahe Partikel die autorisierte Zone verlassen haben. Für die übrigen Fälle unterschätzen die hergeleiteten Timeouts tendenziell die reale Austrittszeit. Dennoch ist diese Lösung deutlich flexibler, als der Einsatz eines starren Timeouts. Zu dessen Herleitung existiert keine formale Methodik, weshalb er von Experten abgeschätzt werden muss.

4.3.6 Diskussion

In diesem Abschnitt wurde ein Ansatz für den Einsatz innerhalb von Gebäuden vorgestellt, der die kontinuierliche Überprüfung von Ortsbeschränkungen auf Basis der Trajektorien von Nutzern erlaubt. Nach der Autorisierung kann eine Nutzungskontrolle bzgl. des gewährten Zugriffsrechts durchgeführt werden. Durch den Einsatz eines Partikelfilters wird der Einfluss von Messausreißern stark reduziert. Ferner werden probabilistische Trajektorien hergeleitet, auf welche die risikobasierte Autorisierungsstrategie angewandt wird. Für das Szenario der standortbasierten Autorisierung wurden nötige Anforderungen an dem Korrektur- und Vorhersageschritt des Partikelfilters diskutiert, um Angriffe zu erschweren. Es wurde ein Algorithmus angegeben, um die Effizienz der risikobasierten Strategie zu verbessern, indem ignorierbare Partikel nicht beachtet werden. Ferner wurde ein Verfahren eingeführt, wie auf Basis der Partikelwolke dynamisch ein Timeout bestimmt werden kann, der angibt, wann spätestens die nächste Positionsschätzung eintreffen muss bis das Zugriffsrecht automatisch entzogen wird. In verwandten Arbeiten wird die Autorisierung auf Trajektorien durchgeführt, die durch Aneinanderreihung von einzelnen Positionsschätzungen entstehen. Einzelne Messausreißer können somit die Trajektorie stark verfälschen. Die Ungewissheit über den tatsächlichen Pfad des Nutzers wird daher nicht berücksichtigt und die Autorisierungsentscheidung entsprechend der naiven Strategie getroffen. Dabei wird lediglich überprüft, ob die erstellte Trajektorie vollständig innerhalb der autorisierten Zone verläuft. Derzeit existiert auch kein Ansatz, der es erlaubt, einen dynamischen Timeout für das späteste Eintreffen der nächsten Positionsschätzung abzuleiten. Stattdessen wird in der Literatur mit fixen Timeouts gearbeitet, die schwer begründet werden können. Der Hauptbeitrag des vorgestellten Ansatzes ist also ein Verfahren zur kontinuierlichen Auswertung von Ortsbeschränkungen basierend auf der risikobasierten Strategie und probabilistischen Trajektorien, die von einem Partikelfilter hergeleitet werden. Der Ansatz wurde gegen eine umfangreiche Testumgebung evaluiert. Dabei hat sich gezeigt, dass die Einsetzbarkeit stark von der Abbildung U der jeweiligen Ortsbeschränkung abhängt. Für die untersuchten Fälle konnte der Opportunitätsverlust gegenüber der naiven Strategie im besten Fall um bis zu 80% reduziert werden. Ferner konnte gezeigt werden, dass die hergeleiteten Timeouts gut mit der tatsächlichen minimal benötigten Austrittszeit eines möglichen Angreifers korrelieren. Der vorgestellte Ansatz trägt somit wesentlich zur Einsetzbarkeit von kontinuierlichen Ortsbeschränkungen in Gebäuden bei. In der Praxis kann das Problem entstehen, dass durch das Bewegungsmodell die Partikelwolke der wahren Trajektorie des Nutzers nicht folgen kann und innerhalb eines Raumes gefangen ist, weil kein Partikel die Tür verlässt. Der Autorisierungsstrategie wird somit ein falsches Bild vermittelt, was zu Falschentscheidungen führen kann. In zukünftigen Arbeiten sollte deshalb untersucht werden, wie ein Neustart des Partikelfilters in solchen Situationen mit der standortbasierten Autorisierung verbunden werden kann.

Kapitel 5

Analyse der Durchsetzung von Ortsbeschränkungen

In der Praxis erfolgt die Durchsetzung einer Ortsbeschränkung $(\mathcal{Z}, \mathrm{U})$ durch Einsatz einer standortbasierten Autorisierungsstrategie und eines Positionierungssystems. Derzeit existieren jedoch keine Analyseverfahren zur Erfassung und Beurteilung des Systemverhaltens, das sich unter diesen Randbedingungen ergibt. Somit wird erst durch empirische Untersuchungen zur Laufzeit erkennbar, in wie vielen Fällen die Entscheidungen der standortbasierten Autorisierung aufgrund von Positionsfehlern von der Spezifikation der Ortsbeschränkung abweichen und Falschentscheidungen entstehen.

Eine Beurteilung, ob diese Abweichung den Einsatz eines Positionierungssystems mit höherer Präzision und Richtigkeit oder eine alternative Autorisierungsstrategie erforderlich macht, ist bisher nur durch die persönliche Einschätzung eines Experten möglich. Eine solche Einschätzung ist wenig transparent und nicht vergleichbar, weshalb formale Analyseverfahren benötigt werden. Ein weiterer Vorteil solcher formaler Verfahren ist zusätzlich, dass bereits vor der Inbetriebnahme der standortbasierten Autorisierung eine Beurteilung möglich wird. Zunächst muss dabei ein Verfahren geschaffen werden, das die quantitative Bewertung einer Konfiguration aus Positionierungssystem und Autorisierungsstrategie zur Durchsetzung einer Ortsbeschränkung erlaubt. Dieses Verfahren muss für jede Gruppe von möglichen Nutzern der standortbasierten Autorisierung quantifizieren, inwiefern die Ortsbeschränkung unter der gegebenen Konfiguration entsprechend den Anforderungen der jeweiligen Nutzergruppe durchgesetzt wird. Beispiele für solche Nutzergruppen sind gutartige Nutzer, Angreifer und unbeteiligte Passanten. Ferner ist es nötig ein Verfahren bereitzustellen, das eine Ordnung auf Konfigurationen aus Positionierungssystem und Autorisierungsstrategie bzgl. des Opportunitätsverlusts erlaubt, der im Betrieb nach einer Autorisierungsentscheidung erwartet wird. Denn je geringer der Erwartungswert des Opportunitätsverlusts, desto mehr Nutzen aus Autorisierungsentscheidungen ist im Betrieb zu erwarten. Somit lässt sich insgesamt die nützlichste Konfiguration auswählen, also die Konfiguration, die insgesamt den größten erwarteten Nutzen für eine Autorisierungsentscheidung liefert. Zusätzlich wird ein Kriterium benötigt, das eine Aussage darüber trifft, ob eine Konfiguration aus Positionierungssystem und Autorisierungsstrategie prinzipiell für

die Durchsetzung einer gegebenen Ortsbeschränkung geeignet ist. Nur so lässt sich bereits vor der Inbetriebnahme entscheiden, ob ein Positionierungssystem mit höherer Präzision und Richtigkeit benötigt wird, oder ob eine alternative Autorisierungsstrategie zu wählen ist.

Das folgende Kapitel stellt formale Analyseverfahren vor, die eine quantitative und qualitative Bewertung der Durchsetzung von Ortsbeschränkungen ermöglichen. Dazu werden in Abschnitt 5.1 Qualitätsparameter für Ortsbeschränkungen definiert. Diese erlauben die Beurteilung des Autorisierungsverhaltens für eine Ortsbeschränkung unter einer gegebenen Autorisierungsstrategie und einem Positionierungssystem aus Sicht von drei Nutzergruppen. In Abschnitt 5.2 folgt eine Analysemethode zur Untersuchung des erwarteten Opportunitätsverlusts von Autorisierungsstrategien unter gegebenen Randbedingungen und ein Kriterium, um die Eignung von Positionierungssystemen qualitativ zu beurteilen. Abschließend wird in Abschnitt 5.3 eine Vorgehensweise zur Auswahl einer Konfiguration basierend auf den entwickelten Verfahren angegeben.

5.1 Analyse der Durchsetzung von Ortsbeschränkungen aus Nutzersicht

Die Nutzer eines Zugriffsrechts, dem eine Ortsbeschränkung $(\mathcal{Z}, \mathrm{U})$ zugewiesen ist und das durch die standortbasierte Autorisierung geschützt ist, lassen sich in drei Gruppen unterteilen. Diese Gruppen umfassen die gutartigen Nutzer, die Angreifer und unbeteiligte Passanten. Dabei befinden sich gutartige Nutzer innerhalb der autorisierten Zone und beabsichtigen das Zugriffsrecht ohne schadhafte Absichten zu nutzen. Ein Angreifer hingegen ist eine Person, die sich außerhalb der autorisierten Zone befindet und versucht dort eine Positionsschätzung zu erhalten, die zur Erfüllung der Ortsbeschränkung führt. Dabei verfolgt ein Angreifer das Ziel, das Zugriffsrecht entgegen der Ortsbeschränkung zu missbrauchen und Schaden zu verursachen. Für gutartige Nutzer sowie für Angreifer erfolgt die Autorisierung reaktiv und wird vom Nutzer selbst initiiert. Die dritte Nutzergruppe ist die Gruppe der unbeteiligten Passanten. Diese Nutzer befinden sich außerhalb der autorisierten Zone und werden durch eine proaktive Autorisierung des Zugriffsrechts gestört. Dabei wird das Zugriffsrecht automatisch erteilt, sobald die Position des Nutzers die Ortsbeschränkung erfüllt. Treten nun Positionsfehler auf, so weichen die Autorisierungsentscheidungen von der definierten Semantik der Ortsbeschränkung ab. So wird ein gutartiger Nutzer im schlechtesten Fall aufgrund eines Positionsfehlers nicht autorisiert, obwohl er sich innerhalb der autorisierten Zone befindet. Ein Angreifer kann das Zugriffsrecht von außerhalb der autorisierten Zone nutzen, wenn ein Positionsfehler auftritt, der suggeriert, dass sich der Angreifer innerhalb der autorisierten Zone befindet. Ebenso besteht die Möglichkeit, dass unbeteiligte Passanten aufgrund eines Positionsfehlers innerhalb der autorisierten Zone verortet werden und durch eine proaktive Autorisierung belästigt werden.

Die Problematik soll verdeutlicht werden, indem das Szenario eines Museums aus Beispiel 4.1.2 aufgegriffen wird. Dort wird Besuchern über eine spezielle Applikation auf ihren

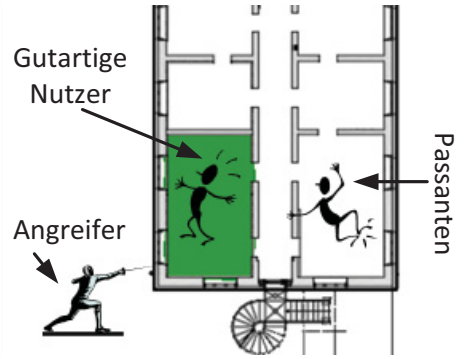


Abbildung 5.1: Innerhalb der autorisierten Zone $\mathcal{Z}$ (grün), sollen gutartige Nutzer die Audioführung nutzen dürfen. Außerhalb davon soll Angreifern die Nutzung verwehrt und Passanten nicht fälschlicherweise proaktiv angeboten werden.

mobilen Endgeräten eine Audioführung mit Erklärungen bereitgestellt. In einem einzelnen Raum findet eine Sonderausstellung statt, für die separate Tickets gelöst werden müssen. Die Erklärungen für diese Sonderausstellung dürfen nur darin abgehört werden. Zur Realisierung der Funktionalität wird eine Ortsbeschränkung für das Zugriffsrecht erstellt, welches Nutzer zum Abhören der Erklärungen berechtigt. Zur Durchsetzung der Ortsbeschränkung kommt eine Konfiguration aus standortbasierter Autorisierungsstrategie und eines Positionierungssystems zum Einsatz. Gutartige Nutzer befinden sich mit einem gültigen Ticket in der Sonderausstellung und sollen zuverlässig die Erklärungen abhören können. Angreifer sollen keine Möglichkeit haben, den Kauf des Sondertickets zu umgehen und die Erklärungen außerhalb abzuhören, da hierdurch Umsatzeinbußen entstehen. Außerdem sollen ehrliche Nutzer, die sich außerhalb befinden, nicht durch das proaktive Abspielen von Erklärungen zur Sonderausstellung belästigt werden. Dieser Fall tritt ein, wenn sie zufällig eine Positionsschätzung erhalten, die anzeigt, dass sie sich in der Sonderausstellung befinden. Ein solches Verhalten der Applikation wird natürlich als unpassend und störend empfunden und führt in diesem Beispiel zu Umsatzeinbußen, da der Audioführer von solchen Nutzern künftig nicht mehr akzeptiert und genutzt wird. Die Problematik wird durch Abb. 5.1 verdeutlicht.

Jede Nutzergruppen erzeugt individuelle Anforderungen. Für gutartige Nutzer soll das Zugriffsrecht innerhalb der autorisierten Zone verfügbar sein. Es soll daher möglichst selten der Fall eintreten, dass ihre Positionsschätzung die Ortsbeschränkung nicht erfüllt. Angreifer sollen möglichst geringe Erfolgschancen auf eine Positionsschätzung haben, die zur Autorisierung führt. Unbeteiligte Passanten sollen mit zunehmender Distanz zur autorisierten Zone immer unwahrscheinlicher durch eine proaktive Autorisierung gestört werden. Benötigt wird ein Verfahren, das für jede der drei Nutzergruppen quantifiziert, inwiefern die individuelle Anforderung erfüllt ist.

Zur Lösung dieses Problems wird in diesem Abschnitt basierend auf der Vorarbeit von Marcus et al. [99] das Konzept der Autorisierungsmodelle eingeführt. Für eine gegebene Ortsbeschränkung $(\mathcal{Z}, \mathrm{U})$ modellieren diese für jeden geographischen Punkt, wie

wahrscheinlich dort eine Positionsschätzung erhalten wird, die unter dem eingesetzten Positionierungssystem und der verwendeten Autorisierungsstrategie zur Erfüllung der Ortsbeschränkung führt. Basierend auf solchen Autorisierungsmodellen werden Qualitätsparameter für die Nutzergruppen definiert. Durch die Analyse dieser Qualitätsparameter kann schließlich vor der Inbetriebnahme der Ortsbeschränkung bereits analysiert werden, welche Auswirkung die gewählte Konfiguration aus Positionierungssystem und Autorisierungsstrategie auf die Nutzergruppen hat. Somit kann das Problem vermieden werden, dass erst während des Betriebs klar wird, dass die standortbasierte Autorisierung zu fehlerhaftem und ungewolltem Verhalten führt.

Die entwickelte Methodik wird im Folgenden vorgestellt. In Unterabschnitt 5.1.1 wird das Konzept der Autorisierungsmodelle eingeführt. Darauf basierend werden die entwickelten Qualitätsparameter definiert. In Unterabschnitt 5.1.2 wird die Effektivität des Ansatzes untersucht. Hierbei wird anhand von zwei Fallstudien die Relevanz einer solchen Analyse vor der Ausbringung von Ortsbeschränkungen gezeigt. Die erreichten Ergebnisse werden in Unterabschnitt 5.1.3 zusammengefasst und diskutiert.

5.1.1 Die Qualität durchgesetzter Ortsbeschränkungen

Unabhängig von der verwendeten Autorisierungsstrategie führt das Auftreten von Positionsfehlern zur Problematik, dass für einen gegebenen Punkt nicht exakt bestimmt werden kann, ob ein Nutzer dort eine Positionsschätzung erhält, welche die Ortsbeschränkung erfüllt. Der Grund ist, dass sich die Fehler von Positionierungssystemen, wie in Abschnitt 3.1 gezeigt, nichtdeterministisch verhalten. Um dieses Verhalten zu formalisieren wird im Folgenden das Konzept von Autorisierungsmodellen für Ortsbeschränkungen hergeleitet, die in Abhängigkeit von einer bestimmten Autorisierungsstrategie und einem Positionierungssystem berechnet werden. Formal ist ein Autorisierungsmodell eine bedingte WDF, welche jedem geographischen Punkt die Wahrscheinlichkeit zuordnet, dort eine Autorisierung zu erhalten. Hierzu wird die kontinuierliche Zufallsvariable GTP zur Modellierung des wahren Orts des Nutzers (von engl. Ground Truth Position) und die diskrete Zufallsvariable Aut für die Autorisierung eingeführt. Das Autorisierungsmodell wird schließlich als $\mathrm{P}\left(Aut|GTP\right)$ notiert. Liegt das Autorisierungsmodell einer Ortsbeschränkung für eine Konfiguration aus Autorisierungsstrategie und Positionierungssystem vor, lassen sich daraus Qualitätsparameter bestimmen.

Autorisierungsmodelle für Ortsbeschränkungen

Für eine gegebene Ortsbeschränkung $(\mathcal{Z}, \mathrm{U})$, hängt das Autorisierungsmodell von der Autorisierungsstrategie i und dem Positionierungssystem j ab. Durch die später vorgestellten Qualitätsparameter wird deshalb immer eine Konfiguration (i, j) bewertet, für die das Autorisierungsmodell zuvor separat berechnet werden muss. Hierfür wird neben der Autorisierungsstrategie i zusätzlich die, in Unterabschnitt 3.1.5 bereits eingeführte, Fehlerverteilung F_{fehler} zur Modellierung des Positionierungssystems j benötigt.

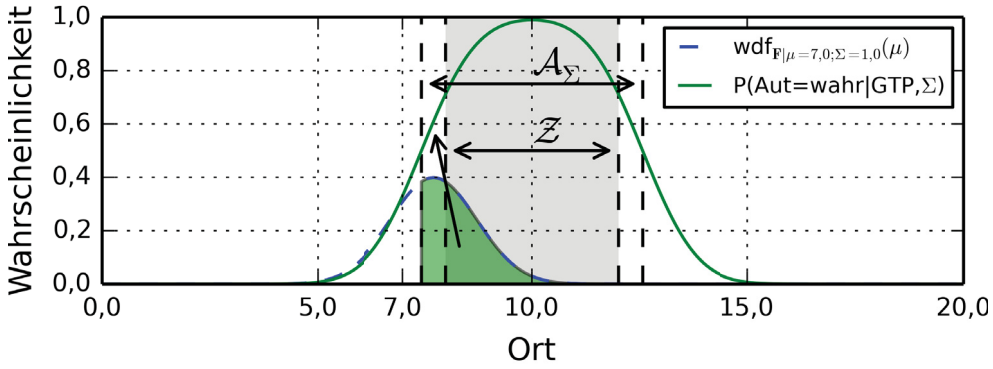


Abbildung 5.2: Ein Beispiel im Eindimensionalen mit einer autorisierten Zone $\mathcal{Z}$ (grau), einer effektiven autorisierten Zone $\mathcal{A}_\Sigma$ für ein festes Σ und die zugehörige Verteilung $\mathrm{P}\left(Aut|\mathrm{GTP}, \Sigma\right)$. Die grüne Fläche unter der beispielhaft dargestellten Normalverteilung $f_{\mu=7,\Sigma=1}$ entspricht ihrem Integral über die effektive autorisierte Zone $\mathcal{A}_\Sigma$. Dies entspricht somit ebenfalls $\mathrm{P}\left(aut|7, 1\right)$.

Zur Herleitung des Autorisierungsmodells wird das Konzept der effektiven autorisierten Zone $\mathcal{A}_\Sigma$ eingeführt. Für Positionsschätzungen, die eine Fehlerschätzung mit Formparameter $\Sigma = \left(\begin{smallmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{smallmatrix}\right)$ besitzen, beschreibt $\mathcal{A}_\Sigma$ die Fläche, auf welcher ein zugehöriger Mittelwert μ liegen muss, damit die Positionsschätzung (μ, Σ) autorisiert wird. Formal berechnet sich die Fläche $\mathcal{A}_\Sigma$ als:

$$\mathcal{A}_\Sigma = \left\{\mu \in \mathbb{R}^2 \,|\, \mathrm{aut}^i(\mu, \Sigma)\right\} \tag{5.1}$$

Hierbei beschreibt $\mathrm{aut}^i(\mu, \Sigma)$ die Anwendung einer der in Abschnitt 4.1 eingeführten Autorisierungsstrategien. Darunter fällt auch die erweiterte risikobasierte Strategie, falls anstelle der Ortsbeschränkung eine erweiterte Ortsbeschränkung $(\mathrm{P}(E|X), \mathrm{U})$ gegeben ist.

Beispiel 5.1.1 (Effektive autorisierte Zone)**.** *Das Konzept der effektiven autorisierten Zone wird in Abb. 5.2 anhand eines eindimensionalen Beispiels verdeutlicht. Hier sei eine Ortsbeschränkung mit autorisierter Zone $\mathcal{Z}$ unter der risikobasierten Autorisierungsstrategie gegeben. Für den Nutzen gilt* $\mathrm{U}(FP) = 0{,}6$*;* $U(FN) = 0{,}0$ *und* $\mathrm{U}(RP) = \mathrm{U}(RN) = 1$*. Die gelieferten Fehlerschätzungen sind in diesem Beispiel Normalverteilungen mit einer Standardabweichung Σ und einem Mittelwert μ. Die Fläche der effektiven autorisierten Zone für $\Sigma = 1$ überragt hier die autorisierte Zone $\mathcal{Z}$. Dies folgt unmittelbar aus dem Verhalten der risikobasierten Autorisierungsstrategie und des Prädikats* $\mathrm{aut}^{risikobasiert}$*. Entsprechend der Abbildung* U *für den Nutzen reicht nämlich gemäß Satz 4.1.2 eine Aufenthaltswahrscheinlichkeit von $p_\mathcal{Z} = 28{,}5\%$, um eine Autorisierung zu erhalten. Mögliche Punkte für μ, die diese Bedingung unter $\Sigma = 1$ erfüllen, liegen hier auch außerhalb von $\mathcal{Z}$.*

Zurück im Zweidimensionalen, sei nun eine fixe WDF zur Fehlerschätzung mit Formparameter $\Sigma = \left(\begin{smallmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{smallmatrix}\right)$ angenommen. Die Wahrscheinlichkeit, dass ein Nutzer an seinem realen Standort *gtp* eine Positionsschätzung erhält, deren Mittelwert innerhalb einer bestimmten Zone ist, lässt sich mittels $wdf_{\mathbf{F}|gtp,\sigma}(\mu)$ bestimmen.

Wie oben gezeigt, werden die Positionsschätzungen (μ, Σ) autorisiert, welche der Bedingung $\mu \in \mathcal{A}_\Sigma$ genügen. Für einen gegebenen Punkt *gtp* entspricht also die Wahrscheinlichkeit, mit der man eine Positionsschätzung mit $\mu \in \mathcal{A}_\Sigma$ erhält, genau der Autorisierungswahrscheinlichkeit in Abhängigkeit von Σ:

$$\mathrm{P}\left(Aut = \texttt{wahr} | GTP = gtp, \Sigma\right) = \int_{\mathcal{A}_\Sigma} wdf_{\mathbf{F}|gtp,\sigma}(\mu)\,\mathrm{d}\mu \tag{5.2}$$

Diese Verteilung gibt zwar für jeden Ort *gtp* die Autorisierungswahrscheinlichkeit an, allerdings ist sie noch abhängig vom Formparameter $\Sigma = \left(\begin{smallmatrix}\sigma^2 & 0\\ 0 & \sigma^2\end{smallmatrix}\right)$ der Fehlerschätzung und kann somit keine allgemeine Aussage treffen. Reale Fehlerschätzungen können natürlich mit verschiedenen Formparametern Σ auftreten und sind somit auch nicht auf fixe Werte beschränkt. Vielmehr folgen sie der Verteilung F_{fehler} des Positionierungssystems. Bei der Herleitung des endgültigen Autorisierungsmodells muss dies berücksichtigt werden. Die Abhängigkeit der Verteilung aus (5.2) vom Parameter Σ wird beseitigt, indem über F_{fehler} integriert wird:

$$\mathrm{P}\left(Aut = \texttt{wahr} | GTP = gtp\right) = \int_0^\infty \mathrm{P}\left(Aut = \texttt{wahr} | GTP = gtp, \Sigma = \left(\begin{smallmatrix}\sigma^2 & 0\\ 0 & \sigma^2\end{smallmatrix}\right)\right) \cdot \mathrm{F}_{fehler}(\sigma)\,\mathrm{d}\sigma \tag{5.3}$$

Das endgültige Autorisierungsmodell $\mathrm{P}\left(Aut|GTP\right)$ ergibt sich aus der Anwendung von (5.3). Es beschreibt die Autorisierungswahrscheinlichkeit jedoch nur für eine einzige Positionsschätzung. Werden n Positionsschätzungen an einem Ort *gtp* durchgeführt, beträgt die Wahrscheinlichkeit, dass davon mindestens eine zur Autorisierung führt:

$$\mathrm{P}_n\left(Aut = \texttt{wahr} | GTP = gtp\right) := 1 - \left(1 - \mathrm{P}\left(Aut = \texttt{wahr} | GTP = gtp\right)\right)^n \tag{5.4}$$

Dies ist die Gegenwahrscheinlichkeit zu dem Fall, dass während der n Versuche keine einzige Autorisierung erfolgt. Ist die Positionierungsfrequenz ϑ bekannt, also die Anzahl an Positionsschätzungen, die pro Sekunde mit einem Positionierungssystem erhalten werden, lässt sich die Autorisierungswahrscheinlichkeit in Abhängigkeit von der Zeit t bestimmen. Dazu wird $n = \lfloor \vartheta \cdot t \rfloor$ gesetzt. Die Wahrscheinlichkeit, dass von n Positionsschätzungen alle zur Autorisierung führen, berechnet sich als:

$$\mathrm{P}_n\left(Aut = \texttt{wahr} | GTP = gtp\right) := \mathrm{P}\left(Aut = \texttt{wahr} | GTP = gtp\right)^n \tag{5.5}$$

Die nachfolgenden Qualitätsparameter sind somit für jedes benötigte Zeitintervall berechenbar.

Qualitätsparameter für Ortsbeschränkungen

Gegeben sei eine Konfiguration (i, j), bestehend aus einer Autorisierungsstrategie i und einem Positionierungssystems j, die zur Durchsetzung einer Ortsbeschränkung $(\mathcal{Z}, \mathrm{U})$ eingesetzt wird. Dabei werden im Folgenden die erweiterte risikobasierte Strategie und erweiterte

Ortsbeschränkungen ausgeschlossen, da die Qualitätsparameter abhängig von der autorisierten Zone $\mathcal{Z}$ sind. Anhand des Autorisierungsmodells $\mathrm{P}\left(Aut|GTP\right)$ kann die Qualität, mit welcher die Ortsbeschränkung durchgesetzt wird, aus verschiedenen Blickwinkeln abgeschätzt werden. Für Ortsbeschränkungen mit $\min\left(\mathrm{U}(RP);\mathrm{U}(RN)\right) > \max\left(\mathrm{U}(FP);\mathrm{U}(FN)\right)$ ist das Idealverhalten, dass keine Falschentscheidungen bei der Durchsetzung auftreten. In diesem Fall werden ausschließlich Nutzer autorisiert, die sich innerhalb von $\mathcal{Z}$ befinden. Außerhalb von $\mathcal{Z}$ wird niemals autorisiert. Ein solches Idealverhalten ist jedoch nur mit einem theoretischen Positionierungssystem möglich, womit keine Positionsfehler auftreten und stets der exakte wahre Standort des Nutzers als Positionsschätzung geliefert wird. Für den theoretischen Fall eines solchen fehlerfreien Positionierungssystems *opt* ergibt sich das Autorisierungsmodell:

$$\mathrm{P}\left(Aut = \texttt{wahr}|\,GTP = \texttt{gtp}\right) = \begin{cases} 1, & \text{falls } gtp \in \mathcal{Z} \\ 0, & \text{sonst} \end{cases} \tag{5.6}$$

Der Vergleich des Autorisierungsmodells einer Konfiguration (i, j) mit diesem optimalen Modell ist die Grundlage zur Herleitung der Qualitätsparameter für (i, j). Im Folgenden werden drei Qualitätsparameter zur Bewertung der Durchsetzung von Ortsbeschränkungen vorgestellt, welche deren Qualität jeweils aus Sicht einer dedizierten Nutzergruppe beschreiben. Jede dieser Gruppen erzeugt Anfragen mit bestimmten Charakteristika:

- Gutartige Nutzer stellen Anfragen innerhalb von $\mathcal{Z}$ und halten sich dort gemäß einer Gleichverteilung auf. Sie beabsichtigen das Zugriffsrecht ohne negative Absichten zu nutzen.
- Angreifer stellen gezielt Anfragen von dem Punkt außerhalb von $\mathcal{Z}$, der die höchste Autorisierungswahrscheinlichkeit aufweist und richten durch die Falschautorisierung Schaden an.
- Passanten befinden sich außerhalb von $\mathcal{Z}$ und werden durch eine proaktive Autorisierung gestört. Sie haben allerdings keine Nutzungs- oder Missbrauchsabsichten.

Weicht nun das reale Autorisierungsmodell für eine Konfiguration (i, j) vom Idealverhalten ab, so sind die einzelnen Nutzergruppen hierdurch auf unterschiedliche Art betroffen. Gutartige Nutzer, die sich gleich verteilt innerhalb der autorisierten Zone aufhalten, haben eine geringere Chance autorisiert zu werden, falls Positionsfehler möglich sind. Die Verfügbarkeit des zu gewährenden Zugriffsrechts wird ungewollt eingeschränkt. Angreifern wird somit auch eine Chance geboten, außerhalb von $\mathcal{Z}$ autorisiert zu werden und durch Missbrauch Schaden anzurichten. Die Angreifbarkeit der Ortsbeschränkung erhöht sich also durch eine solche Abweichung. Wird proaktiv autorisiert, sobald sich ein Nutzer innerhalb von $\mathcal{Z}$ befindet, so sind auch Passanten durch eine solche Abweichung betroffen. Da sich Passanten außerhalb von $\mathcal{Z}$ aufhalten, nimmt die fälschliche Autorisierung mit größer werdenden Positionsfehlern für diese Nutzer zu. Diese Abweichung vom Idealverhalten führt zu einer gesteigerten Aufdringlichkeit.

Die Verfügbarkeit eines Zugriffsrechts, das durch eine Ortsbeschränkung geschützt ist, beschreibt die Qualität aus Sicht der gutartigen Nutzer. Ihr Wert ergibt sich aus der mittleren Wahrscheinlichkeit, mit welcher diese Nutzergruppe für das Zugriffsrecht autorisiert wird.

Definition 5.1.1 (Verfügbarkeit)**.** *Gegeben sei eine Autorisierungsstrategie i und ein Positionierungssystem j zur Durchsetzung einer Ortsbeschränkung $(\mathcal{Z}, \mathrm{U})$. Der Qualitätsparameter $verfügbarkeit_{i,j}$ ist definiert als die erwartete Autorisierungswahrscheinlichkeit für gutartige Nutzer, die sich gleich verteilt innerhalb von $\mathcal{Z}$ aufhalten:*

$$verfügbarkeit_{i,j} = \frac{1}{|\mathcal{Z}|} \int_{\mathcal{Z}} P(Aut = \texttt{wahr} | GTP = gtp) \;\; d\, gtp \tag{5.7}$$

Hierbei bezeichne $P(Aut|GTP)$ das zugehörige Autorisierungsmodell und $|\mathcal{Z}|$ die Fläche der autorisierten Zone.

Für eine verlässliche Bereitstellung des zugrundeliegenden Zugriffsrechts ist es unerlässlich, dass der Wert von $verfügbarkeit_{i,j}$ maximiert wird. Je nach Definition von U können zu kleine Werte darauf hinweisen, dass im Betrieb mit dem Positionierungssystem j in weiten Teilen von $\mathcal{Z}$ sehr wahrscheinlich Falsch-Negativ-Entscheidungen auftreten werden und somit nicht autorisiert wird. Im Falle des optimalen Autorisierungsmodells gilt stets $verfügbarkeit_{i,opt} = 1$, was dazu führt, dass alle Anfragen autorisiert werden, die von Personen innerhalb der autorisierten Zone stammen. Jedes reale Positionierungssystem j weist hingegen nur Werte auf mit $0 \leq verfügbarkeit_{i,j} \leq 1$.

Ein böswilliger Nutzer bzw. Angreifer einer Ortsbeschränkung $(\mathcal{Z}, \mathrm{U})$ befindet sich an den Orten außerhalb von $\mathcal{Z}$, an denen er die größten Erfolgschancen für einen erfolgreichen Angriff besitzt. Die Verwundbarkeit eines Zugriffsrechts, das durch eine Ortsbeschränkung geschützt ist, bezeichnet daher die größte Wahrscheinlich, mit der ein Angreifer außerhalb von $\mathcal{Z}$ autorisiert wird. Wie oben beschrieben, versucht ein solcher Nutzer das zu unrecht gewährte Zugriffsrecht derart auszunutzen, dass hierdurch monetärer Schaden entsteht.

Definition 5.1.2 (Verwundbarkeit)**.** *Gegeben sei eine Autorisierungsstrategie i und ein Positionierungssystem j zur Durchsetzung einer Ortsbeschränkung $(\mathcal{Z}, \mathrm{U})$. Der Qualitätsparameter $verwundbarkeit_{i,j}$ ist definiert als die maximale Autorisierungswahrscheinlichkeit, die außerhalb von Z auftritt:*

$$verwundbarkeit_{i,j} = \max\left(\{P(Aut = \texttt{wahr} | GTP = gtp) \mid gtp \notin \mathcal{Z}\}\right) \tag{5.8}$$

Hierbei bezeichne $P(Aut|GTP)$ das zugehörige Autorisierungsmodell.

Je niedriger die Verwundbarkeit einer Konfiguration (i, j), umso schwieriger ist es für Angreifer eine Falsch-Positiv-Autorisierung zu erhalten. Liegt die autorisierte Zone innerhalb eines Gebäudes, kann Def. 5.1.2 so angepasst werden, dass nur solche $gtp \notin \mathcal{Z}$ berücksichtigt werden, die in begehbaren Teilen des Gebäudes und nicht auf Wänden liegen. Im Betrieb mit einem optimalen Positionierungssystem sind Falsch-Positiv-Autorisierungen

ausgeschlossen, so dass ein Angreifer niemals fälschlicherweise autorisiert wird. Für reale Positionierungssysteme gilt hingegen $0 \leq \mathit{verwundbarkeit}_{i,j} \leq 1$.

Da im Allgemeinen keine näheren Informationen vorliegen, wird für Passanten vereinfachend angenommen, dass sich diese gleich verteilt außerhalb von $\mathcal{Z}$ bewegen. Eine wünschenswerte Eigenschaft ist, dass mit zunehmender Entfernung zu $\mathcal{Z}$ die Wahrscheinlichkeit abnimmt, mit der ein Nutzer fälschlicherweise proaktiv autorisiert wird. Die Ausdehnung des Gebiets um $\mathcal{Z}$ herum, in dem eine fälschliche Autorisierung wahrscheinlicher als ein Schwellwert α eintritt, wird dazu als Maß verwendet.

Definition 5.1.3 (α–Aufdringlichkeit)**.** *Gegeben sei eine Autorisierungsstrategie i und ein Positionierungssystem j zur Durchsetzung einer Ortsbeschränkung* $(\mathcal{Z}, \mathrm{U})$*. Der Qualitätsparameter* α*–aufdringlichkeit*$_{i,j}$ *ist definiert als die größte geographische Distanz zu* $\mathcal{Z}$*, an der noch wahrscheinlicher als* α *autorisiert wird:*

$$\alpha\text{–}\mathit{aufdringlichkeit}_{i,j} = \max\left(\{d\left(\mathcal{Z}, \mathit{gtp}\right) \mid \mathit{gtp} \notin \mathcal{Z} \wedge P\left(\mathit{Aut} = \texttt{wahr} \mid \mathit{GTP} = \mathit{gtp}\right) \geq \alpha\} \cup \{0\}\right) \quad (5.9)$$

Die Funktion $d\left(\mathcal{Z}, \mathit{gtp}\right)$ *bezeichnet die kleinste geographische Distanz eines Punkts gtp zu der autorisierten Zone* $\mathcal{Z}$*. Ferner ist* $P\left(\mathit{Aut}|\mathit{GTP}\right)$ *das zugehörige Autorisierungsmodell.*

Genügt kein Punkt *gtp* der geforderten Eigenschaft, so wird für diesen Qualitätsparameter der Wert 0 gesetzt. Liegt $\mathcal{Z}$ innerhalb eines Gebäudes, so kann (wie auch oben beschrieben) die Berechnung dahingehend verfeinert werden, dass nur $\mathit{gtp} \notin \mathcal{Z}$ berücksichtigt werden, die in begehbaren Flächen des Gebäudes liegen. Eine weitere Verfeinerung ist möglich, sofern nähere Informationen über das Bewegungsverhalten der Passanten bekannt sind. Dann kann ihr Aufenthaltsort realistischer modelliert werden, als durch die verwendete Gleichverteilung. Für das Idealverhalten mit einem optimalen Positionierungssystem ergibt sich stets $\mathit{aufdringlichkeit}_{i,opt} = 0$ m für alle Werte von α. Generell gilt, dass die empfundene Qualität der Ortsbeschränkung im Betrieb für die Nutzergruppe der Passanten steigt, je niedriger der Wert der Aufdringlichkeit ist.

Im realen Einsatz einer Ortsbeschränkung ergibt sich entsprechend der Sequenz der Autorisierungsanfragen eine Sequenz aus zugehörigen wahren Nutzerpositionen $\langle \mathit{gtp}_0, \ldots, \mathit{gtp}_n \rangle$ mit $\mathit{gtp}_i \in \mathbb{R}^2$. Liegt ein Präfix dieser Sequenz vor, so kann zwar für jedes gtp_i der zugehörige Typ der drei vorgestellten Nutzergruppen bestimmt werden. Ein Problem ergibt sich aber, wenn vorhergesagt werden soll, welcher prozentuale Anteil an allen Anfragen von einer einzelnen Nutzergruppe ausgeht. Die Kenntnis darüber würde es erlauben, die einzelnen Qualitätsparameter untereinander zu gewichten und mittels einer gewichteten Summe einen Wert für die Beurteilung der Qualität einer Konfiguration (i, j) herzuleiten. Weil Information über die prozentualen Anteile nicht vorliegt, werden die Qualitätsparameter für jede Nutzergruppe einzeln angegeben.

Ausgehend von einem Zugriffsrecht, das durch eine Ortsbeschränkung geschützt ist, wird die Beurteilung der wahrnehmbaren Abweichung für die drei Nutzergruppen gegenüber dem Betrieb mit einem fehlerfreien Positionierungssystem möglich. Diese drei Qualitätsparameter sind hilfreich, um für eine gegebene Ortsbeschränkung bereits vor der Inbe-

triebnahme zu beurteilen, ob die Konfiguration aus Autorisierungsstrategie und Positionierungssystem den Anforderungen aus Nutzersicht genügt. Im nächsten Unterabschnitt wird die Relevanz einer solchen Analyse anhand einer Fallstudie verdeutlicht.

5.1.2 Fallstudie: Ein ortsbezogener Dienst für Gebäude

In Folgenden wird die Berechnung der entwickelten Qualitätsparameter am Beispiel von zwei standortbasierten Diensten vorgestellt, die Nutzern innerhalb einer autorisierten Zone bereitgestellt werden sollen. Zur Umsetzung dieser funktionalen Anforderung wird die standortbasierte Autorisierung eingesetzt, weshalb für beide Dienste eine Ortsbeschränkung $(\mathcal{Z}, \mathrm{U})$ definiert wird. In beiden Fällen sind die autorisierten Zonen identisch und liegen innerhalb der bereits in Abschnitt 3.1 eingeführten Testumgebung. Hierbei wird das Büro mit Bezeichner *03*, das eine Fläche von 16,2 m^2 hat, als autorisierte Zone $\mathcal{Z}$ gewählt. Dieses Büro ist in Abb. 5.3 und 5.4 als grüne Fläche zu sehen. Als Positionierungssystem dient WLAN-Fingerprinting, basierend auf der vorgestellten Fingerprint-Datenbank und dem Normal-Fehlerschätzer. Als Modellierung für dieses Positionierungssystem wird folglich auch die in Unterabschnitt 3.1.5 eingeführte Verteilung für $\mathrm{F}_{fehler}^{Normal}$ verwendet. Natürlich lässt sich die Analyse auch für den Laplace-Fehlerschätzer durchführen, indem stattdessen die Verteilung $\mathrm{F}_{fehler}^{Laplace}$ verwendet wird.

Im nächsten Schritt wird für die Ortsbeschränkungen der zwei Beispieldienste D_1 und D_2 jeweils die Abbildung U für den Nutzen definiert. Die zugeordneten Werte sind in Tab. 5.1 dargestellt. In diesem Beispiel ist für Dienst D_1 der Nutzen von *FP* größer als der Nutzen von *FN*. Für den Dienst D_2 gilt genau die inverse Situation, so dass hier der Nutzen von *FN* größer als der Nutzen von *FP* ist. Intuitiv wird erwartet, dass D_1 auch mit geringeren Werten von $p_{\mathcal{Z}}$ autorisiert und D_2 hohe Werte benötigt. Das Verhalten beider Dienste wird also sehr unterschiedlich ausfallen, weshalb ein starker Unterschied bzgl. der Autorisierungsmodelle zu erwarten ist.

Die Autorisierungsmodelle basieren auf einer numerischen Approximation von (5.3). In beiden Fällen ist es das Ziel herauszufinden, wie sich die Qualitätsparameter des Dienstes im Betrieb verhalten. Dies ist nötig um zu entscheiden, ob die Konfiguration aus Autorisierungsstrategie und Positionierungssystem für eine der Nutzergruppen zu ungenügenden Qualitätsparametern führt.

Die zugehörigen Autorisierungsmodelle sind in Abb. 5.3 und 5.4 durch ihre Konturlinien dargestellt. Hier zeigt sich in beiden Fällen eine deutliche Abweichung vom optimalen Autorisierungsmodell. Das folgt direkt aus der jeweiligen Definition von U. So ist für den Dienst D_1 zu beobachten, dass die Autorisierungswahrscheinlichkeit selbst in einiger Entfernung zu $\mathcal{Z}$ noch größer 0 ist. Innerhalb von $\mathcal{Z}$ ergibt sich für beinahe die ganze Fläche sogar ein Wert von über 90%. Im Vergleich dazu zeigt der Dienst D_2 ein deutlich restriktiveres Verhalten, was aus dem vergleichsweise geringen Nutzen von Falsch-Positiv-Entscheidungen folgt. Die Autorisierungswahrscheinlichkeit ist selbst innerhalb von $\mathcal{Z}$ größtenteils deutlich unter 1.

Im nächsten Schritt werden für D_1 und D_2 die entwickelten Qualitätsparameter der Verfügbarkeit, Verwundbarkeit und der 0,05–Aufdringlichkeit betrachtet. Der Schwellwert

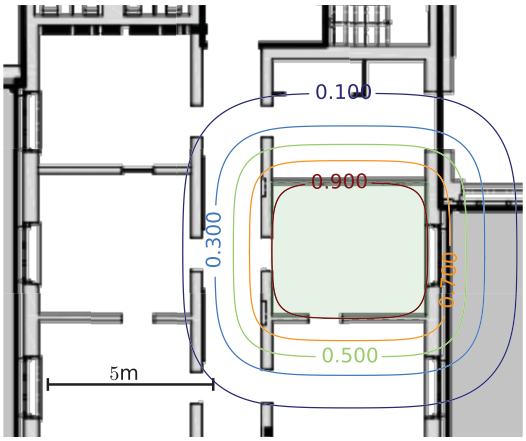


Abbildung 5.3: Autorisierungsmodell für Dienst D_1.

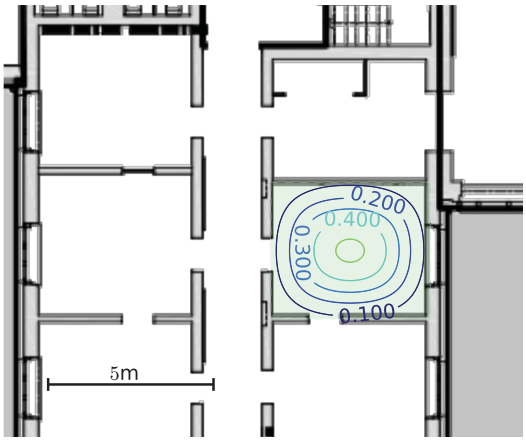


Abbildung 5.4: Autorisierungsmodell für Dienst D_2.

$\alpha = 0{,}05$ wurde hier deshalb gewählt, um genau die Umgebung der autorisierten Zone abzubilden, innerhalb der ein Passant mit einer größeren Wahrscheinlichkeit als 5% durch eine proaktive Dienstbereitstellung belästigt wird. Die Ergebnisse sind in Tab. 5.1 dargestellt. Sowohl für D_1, als auch für D_2 bestätigt sich die obige Vermutung, dass die Qualitätspara-

Dienst	U(RP)	U(RN)	U(FP)	U(FN)	**Verfügbarkeit**	**Verwundbarkeit**	0,05–**Aufdringlichkeit**
D_1	1	1	0,84	0	0,92	0,75	2,89 m
D_2	1	1	0	0,84	0,28	0,03	0 m

Tabelle 5.1: Der Nutzen und die berechneten Qualitätsparameter für D_1 und D_2.

meter stark mit den Autorisierungsmodellen korrelieren, die in Abb. 5.3 und 5.4 dargestellt sind. Hierbei zeigt D_1 größere Werte für alle drei Qualitätsparameter. Bis auf den hohen Wert der Verfügbarkeit ist dies jedoch gegenüber D_2 ein Nachteil, da eine höhere Verwundbarkeit und Aufdringlichkeit des Dienstes entsteht. Da aber für den Dienst D_1 der Opportunitätsverlust aus einem FP im Vergleich zum Opportunitätsverlust aus einem FN klein ist, ist die Anforderung bzgl. der Verwundbarkeit und Aufdringlichkeit gegenüber der Verfügbarkeit als weniger wichtig einzustufen. Im Vergleich dazu zeigt der Dienst D_2 eine sehr geringe Verfügbarkeit für gutartige Nutzer. Vorteilhaft ist jedoch die geringe Verwundbarkeit des Dienstes. Im Falle der Aufdringlichkeit ergibt sich bzgl. des Schwellwerts $\alpha = 0{,}05$ ein Sonderfall. Außerhalb von $\mathcal{Z}$ erreicht kein Punkt eine größere Wahrscheinlichkeit als 5%, mit der eine Positionsschätzung erhalten wird, die zur Autorisierung führt. Die Aufdringlichkeit gegenüber Passanten kann somit als sehr gering eingestuft werden.

Abschließend soll die Qualität des Dienstes für einzelne Nutzergruppen im Betrieb bewertet werden. Im Falle des Diensts D_1, wo ein FP deutlich weniger Opportunitätsverlust erzeugt als ein FN, kann die erreichte Qualität mit dem eingesetzten Positionierungssystem als ausreichend betrachtet werden. Im Falle von D_2 hingegen zeigt sich, wie die Qualität

aufgrund des eingesetzten Positionierungssystems leidet. Dies führt dazu, dass der Dienst D_2 im dargestellten Szenario kaum verfügbar bzw. einsetzbar ist. In solchen Fällen ist es zwingend notwendig zu untersuchen, wie sich die Qualitätsparameter für weitere zur Verfügung stehende Positionierungssysteme und Autorisierungsstrategien verhalten, um schließlich eine geeignete Konfiguration auszuwählen.

5.1.3 Diskussion und Zusammenfassung

In diesem Abschnitt wurde ein Ansatz zur Berechnung von Qualitätsparametern von durchgesetzten Ortsbeschränkungen eingeführt. Die Berechnungen erfolgten ausgehend von einer gegebenen Ortsbeschränkung, definiert durch $\mathcal{Z}$ und U, einer Autorisierungsstrategie und einem gegebenen Positionierungssystem. Es wurden drei Nutzergruppen identifiziert und für jede Nutzergruppe separat ein Qualitätsparameter definiert. Diese Parameter quantifizierten die Abweichungen im Autorisierungsverhalten aus Sicht der jeweiligen Nutzergruppe, die sich unter dem eingesetzten Positionierungssystem im Vergleich zu einem fiktiven, fehlerfreiem Positionierungssystem ergaben.

Als Grundlage für die Berechnung der Qualitätsparameter wurde das Konzept des Autorisierungsmodells eingeführt. Das Autorisierungsmodell einer Ortsbeschränkung wurde dabei abhängig von der Autorisierungsstrategie und dem Positionierungssystem berechnet. Formal betrachtet, drückt dieses Modell für jeden Punkt x die bedingte Wahrscheinlichkeit aus, dass am Punkt x eine Positionsschätzung erhalten wird, die zur Autorisierung führt.

Als Nutzergruppen wurden gutartige Nutzer, Angreifer und unbeteiligte Passanten identifiziert. Für gutartige Nutzer, die sich gleich verteilt innerhalb von $\mathcal{Z}$ befinden, wurde der Qualitätsparameter als mittlere Autorisierungswahrscheinlichkeit innerhalb von $\mathcal{Z}$ definiert. Als Angreifer wurden Personen definiert, die versuchen, außerhalb von $\mathcal{Z}$ eine Falsch-Positiv-Autorisierung zu erlangen und Schaden durch Missbrauch des eingeräumten Zugriffsrechts zu verursachen. Der Qualitätsparameter für Angreifer wurde deshalb als die maximale Autorisierungswahrscheinlichkeit unter den Punkten außerhalb von $\mathcal{Z}$ definiert. Die Nutzergruppe der unbeteiligten Passanten wurde als Gruppe von Personen definiert, die sich außerhalb von $\mathcal{Z}$ befinden und nicht durch eine proaktive Autorisierung gestört werden sollen. Der zugehörige Qualitätsparameter wurde ausgehend von einem Schwellwert α definiert. Unter allen Punkten außerhalb von $\mathcal{Z}$, für welche das Autorisierungsmodell eine höhere Wahrscheinlichkeit als α angibt, wurde der am weitesten von $\mathcal{Z}$ entfernte Punkt ausgewählt. Dessen Distanz zu $\mathcal{Z}$ wurde als Qualitätsparameter für Passanten definiert.

Die Einsetzbarkeit und Notwendigkeit der entwickelten Qualitätsparameter wurde anhand einer konkreten Fallstudie gezeigt. Dabei wurden zwei Ortsbeschränkungen definiert, die sich stark im Opportunitätsverlust eines *FN* und eines *FP* unterschieden haben. Es hat sich gezeigt, dass die zugehörigen Autorisierungsmodelle stark voneinander abweichen. Die zugehörigen Qualitätsparameter wurden berechnet und diskutiert. Dabei wurde gezeigt, dass für den Fall, in dem der Opportunitätsverlust nach einem *FN* geringer ist, als der Opportunitätsverlust nach einem *FP*, die Verfügbarkeit für gutartige Nutzer gegeben ist, jedoch auf Kosten der Qualitätsparameter für Angreifer und Passanten. Im umgekehrten Fall wurde eine sehr geringe Verwundbarkeit gegenüber Angreifern und eine vernachlässig-

bare Aufdringlichkeit gegenüber Passanten erreicht. Entsprechend war die Verfügbarkeit für gutartige Nutzer nicht mehr gegeben.

Durch das vorgestellte Verfahren konnte bereits vor der Inbetriebnahme untersucht werden, ob ein Positionierungssystem unter einer gegebenen Autorisierungsstrategie den Anforderungen zur Durchsetzung einer Ortsbeschränkung aus Nutzersicht genügt. Gegenüber verwandten Arbeiten ergab sich der Vorteil, dass das Verhalten im Betrieb prognostiziert werden kann und zur Auswahl eines Positionierungssystems einsetzbar ist. Bisher erfolgte die Auswahl des Positionierungssystems lediglich anhand dessen technischer Eckdaten, anstatt das einhergehende Verhalten der standortbasierten Autorisierung zu untersuchen. In zukünftigen Arbeiten sollten ausgehend von erweiterten Ortsbeschränkungen und deren Autorisierungsmodellen ebenso geeignete Qualitätsparameter zur Bewertung aus Nutzersicht entwickelt werden. Die drei vorgestellten Qualitätsparameter sind nämlich abhängig von $\mathcal{Z}$ und können daher nicht auf erweiterte Ortsbeschränkungen angewendet werden können.

5.2 Analyse des erwarteten Opportunitätsverlusts von Autorisierungsstrategien

Um für eine Ortsbeschränkung zu entscheiden, welche Autorisierungsstrategie für ein fixes Positionierungssystem eingesetzt werden soll, muss ermittelt werden, welche Autorisierungsstrategie im Mittel den geringsten Opportunitätsverlust bereitet. Anhand dieses Opportunitätsverlusts kann nicht nur die nützlichste Autorisierungsstrategie ausgewählt werden. Es kann auch entschieden werden, ob ein Positionierungssystem für die Auswertung einer Ortsbeschränkung geeignet ist.

5.2.1 Der Opportunitätsverlust von Autorisierungsstrategien

Gegeben sei eine Ortsbeschränkung bestehend aus einer autorisierten Zone $\mathcal{Z}$ und einer Abbildung U. Der Opportunitätsverlust für eine konkrete Positionsschätzung (μ, Σ) berechnet sich, wie in (4.11) und (4.12) gezeigt, basierend auf der Autorisierungsentscheidung und der wahren Position des Nutzers. Liegt die wahre Position nicht vor, ist die Berechnung nicht möglich. Bekannt ist aber, dass die wahre Position des Nutzers mit Wahrscheinlichkeit $p_{\mathcal{Z}}$ innerhalb von $\mathcal{Z}$ liegt. Im Falle einer Autorisierung von (μ, Σ) tritt daher mit Wahrscheinlichkeit $p_{\mathcal{Z}}$ ein *RP* bzw. mit Wahrscheinlichkeit $(1 - p_{\mathcal{Z}})$ ein *RN* und jeweils der damit verbundene Opportunitätsverlust auf. Analog gilt im Falle einer Ablehnung, dass mit Wahrscheinlichkeit $p_{\mathcal{Z}}$ ein *FN* bzw. mit Wahrscheinlichkeit $(1 - p_{\mathcal{Z}})$ ein *RN* und der jeweils zugehörige Opportunitätsverlust auftritt. Somit ergibt sich folgende Definition für den erwarteten Opportunitätsverlust:

Definition 5.2.1 (Erwarteter Opportunitätsverlust)**.** *Gegeben sei eine Ortsbeschränkung* $(\mathcal{Z}, \mathrm{U})$*, eine Positionsschätzung* (μ, Σ) *und eine Autorisierungsstrategie* aut^i *mit* $i \in \{$*positiv, negativ, naiv, schwellwertbasiert, risikobasiert*$\}$ *zur Durchsetzung der Ortsbeschrän-*

kung. Der erwartete Opportunitätsverlust ist basierend auf der Vorarbeit in Marcus et al. [98] definiert als:

$$\text{opp.-verlust}_i\,(\mu,\Sigma) = \begin{cases} p_{\mathcal{Z}} \cdot [\max(\mathrm{U}(RP);\mathrm{U}(FN)) - \mathrm{U}(RP)] \\ \quad + (1-p_{\mathcal{Z}}) \cdot [\max(\mathrm{U}(RN);\mathrm{U}(FP)) - \mathrm{U}(FP)]\,, \textit{ falls } \mathrm{aut}^i(\mu,\Sigma) \\ p_{\mathcal{Z}} \cdot [\max(\mathrm{U}(RP);\mathrm{U}(FN)) - \mathrm{U}(FN)] \\ \quad + (1-p_{\mathcal{Z}}) \cdot [\max(\mathrm{U}(RN);\mathrm{U}(FP)) - \mathrm{U}(RN)]\,, \textit{ sonst} \end{cases} \tag{5.10}$$

Hierbei bezeichnet $p_{\mathcal{Z}}$ wieder die Aufenthaltswahrscheinlichkeit in $\mathcal{Z}$, die sich basierend auf der WDF von (μ,Σ) ergibt.

Für erweiterte Ortsbeschränkungen basierend auf Eigenschaftsmodellen und der erweiterten risikobasierten Strategie muss zur Berechnung des erwarteten Opportunitätsverlusts der Wert $p_{\mathcal{Z}}$ durch $P(e)$ ersetzt werden. Dessen Berechnungsvorschrift ist oben in (4.33) angegeben. Im Folgenden wird jedoch von der Anwendung auf Ortsbeschränkungen basierend auf Definition 4.1.2 ausgegangen.

Der erwartete Opportunitätsverlust $\text{opp.-verlust}_i\,(\mu,\Sigma)$ gilt nur für eine konkrete Positionsschätzung (μ,Σ). Davon unabhängig ergibt sich der insgesamt erwartete Opportunitätsverlust $\mathrm{E}(\textit{opp.-verlust}_i)$. Zu seiner Berechnung wird angenommen, dass die Werte μ gleich verteilt aus einer Fläche $\mathcal{R} \subseteq \mathbb{R}^2$ stammen. Im Falle von WLAN-Fingerprinting ist dieser Bereich auf die Fläche begrenzt, welche durch die Fingerprint-Datenbank abgedeckt wird. Für die Kovarianzmatrizen $\Sigma = \left(\begin{smallmatrix} \sigma^2 & 0 \\ 0 & \sigma^2 \end{smallmatrix}\right)$ gilt wieder die Annahme, dass diese symmetrisch sind und die Werte σ der Verteilung $\mathrm{F}_{\textit{fehler}}$ folgen.

Definition 5.2.2 (Insgesamt erwarteter Opportunitätsverlust)**.** *Gegeben sei eine Ortsbeschränkung $(\mathcal{Z},\mathrm{U})$. Ferner sei eine Fläche $\mathcal{R}$ und Verteilung $F_{\textit{fehler}}$ gegeben, so dass die Mittelwerte der Positionsschätzungen einer Gleichverteilung auf $\mathcal{R}$ folgen und die auftretenden Fehlerschätzungen σ durch $F_{\textit{fehler}}$ beschrieben werden. Für diese Parameter ist der insgesamt erwartete Opportunitätsverlust basierend auf der Vorarbeit von Marcus et al. [98] definiert als:*

$$\mathrm{E}(\textit{opp.-verlust}_i) = \int_0^\infty \mathrm{F}_{\textit{fehler}}(\sigma) \cdot \int_{\mu\in\mathcal{R}} \frac{1}{|\mathcal{R}|} \cdot \text{opp.-verlust}_i\,(\mu,\Sigma)\; d\mu\; d\sigma \tag{5.11}$$

Hierbei bezeichnet $|\mathcal{R}|$ den Inhalt der Fläche $\mathcal{R}$.

Im Allgemeinen folgen die Positionsschätzungen μ in der Realität nicht exakt einer Gleichverteilung auf $\mathcal{R}$. Sind keine näheren Informationen über die reale Verteilung der Anfragen bekannt, ist der insgesamt erwartete Opportunitätsverlust eine Approximation seines realen Werts. Daher ist (5.11) entsprechend anzupassen, sofern für ein konkretes Szenario die Information über die Verteilung der Werte μ vorliegt. Alternativ ist die Ermittlung von $\mathrm{E}(\textit{opp.-verlust}_i)$ anhand von diskreten Testdaten möglich, wie z.B. den Daten aus

Abb. 3.1(c). Dabei wird die Verteilung der Positionsschätzungen μ durch die Monte-Carlo-Methode angenähert. Sei M die Menge der Testdaten, die aus Trippeln $(gtp_k, \mu_k, (\sigma_{mls})_k)$ besteht. Dann ergibt sich aus Anpassung von (5.11):

$$\mathrm{E}(\textit{opp.-verlust}_i) = \int_0^\infty \mathrm{F}_{\textit{fehler}}(\sigma) \cdot \sum_{\mu \in M} \frac{1}{|M|} \cdot \textit{opp.-verlust}_i(\mu, \Sigma)\, \mathrm{d}\sigma \tag{5.12}$$

Im Folgenden wird der insgesamt erwartete Opportunitätsverlust der risikobasierten und der naiven Strategie, sowie der Positiv- und Negativ-Strategie anhand eines Beispielszenarios evaluiert.

Evaluation

Zur Evaluation werden insgesamt 35 autorisierte Zonen auf den benannten Bereichen aus Abb. 3.1(a) gebildet. Diese Menge besteht aus den abgebildeten, benannten Bereichen zuzüglich aller autorisierter Zonen, die sich durch Vereinigung von zwei benachbarten benannten Bereichen bilden lassen. Ferner werden zwei Klassen von Ortsbeschränkungen für die Evaluation definiert:

- Klasse 1 enthält Ortsbeschränkungen mit $\mathrm{U}(RP) = \mathrm{U}(RN) = 1$, $\mathrm{U}(FP) = 0$ und $\mathrm{U}(FN) \in [0;1]$. Sei $u := [\mathrm{U}(RP) - \mathrm{U}(FN)]$ und $t := [\mathrm{U}(RN) - \mathrm{U}(FP)]$, dann gilt für Ortsbeschränkungen dieser Klasse $u/t \in [0;1]$.
- Klasse 2 enthält Ortsbeschränkungen mit $\mathrm{U}(RP) = \mathrm{U}(RN) = 1$, $\mathrm{U}(FN) = 0$ und $\mathrm{U}(FP) \in [0;1]$. Für solche Ortsbeschränkungen gilt $u/t \in [1;\infty]$.

Für beide Klassen gilt, dass FP und FN stets einen kleineren Nutzen erzeugen, als die richtigen Entscheidungen RP und RN. Als theoretisches Modell für das eingesetzte Positionierungssystem dient die Verteilung $\mathrm{F}_{\textit{fehler}}^{\textit{Laplace}}$ basierend auf dem Laplace-Fehlerschätzer aus Unterabschnitt 3.1.5. Für jede der autorisierten Zonen wird abhängig von u/t der insgesamt erwartete Opportunitätsverlust für jede der vier Autorisierungsstrategien berechnet. Die Berechnung erfolgt basierend auf (5.12) mittels der Monte-Carlo-Methode. Dabei werden die Testdaten aus Abb. 3.1(c) als Menge M verwendet.

Die Mittelwerte der Ergebnisse sind in Abb. 5.5 dargestellt. Unter der Positiv-Strategie können nur die Fälle RP und FP auftreten. Da Ortsbeschränkungen innerhalb der Klasse 1 konstante Werte $\mathrm{U}(RP) = 1$ und $\mathrm{U}(FP) = 0$ besitzen, ist der insgesamt erwartete Opportunitätsverlust für die Positiv-Strategie innerhalb dieser Klasse auch konstant und hat den Wert 0,85. Für Ortsbeschränkungen der Klasse 2 gilt $\mathrm{U}(RP) = 1$ und $\mathrm{U}(FP) \in [0;1]$. Dabei nimmt der Wert $\mathrm{U}(FP)$ mit steigender Abszisse u/t zu, weshalb $\mathrm{E}(\textit{opp.-verlust}_{\textit{positiv}})$ ab $u/t = 1$ stetig sinkt. Für $u/t \to \infty$ konvergiert $\mathrm{E}(\textit{opp.-verlust}_{\textit{positiv}})$ gegen 0, da der Opportunitätsverlust t eines FP gegen 0 konvergiert.

Unter der Negativ-Strategie können nur die Fälle RN und FN auftreten. Für Ortsbeschränkungen der Klasse 2 ist $\mathrm{U}(RN) = 1$ und $\mathrm{U}(FN) = 0$, weshalb in dieser Klasse unter der Negativ-Strategie der insgesamt erwartete Opportunitätsverlust konstant ist und den Wert 0,09 hat. Innerhalb der Klasse 1 gilt $\mathrm{U}(RN) = 1$ und $\mathrm{U}(FN) \in [0;1]$, wobei $\mathrm{U}(FN)$

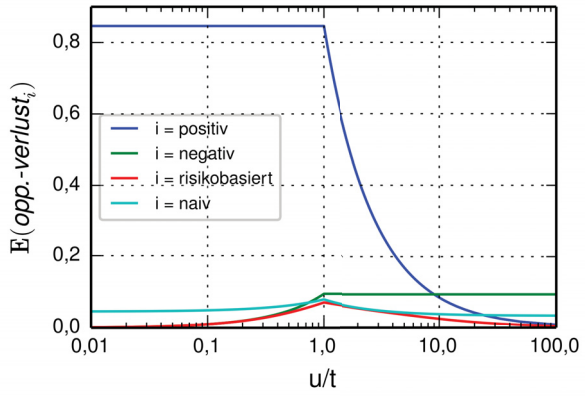


Abbildung 5.5: Der insgesamt erwartete Opportunitätsverlust in der beschriebenen Evaluationsumgebung.

mit wachsender Abszisse u/t abnimmt, bis bei $u/t = 1$ der Wert $\mathrm{U}(FN) = 0$ erreicht ist. Je kleiner $\mathrm{U}(FN)$, desto größer der Opportunitätsverlust eines *FN*. Für $u/t \to 0$ konvergiert $\mathrm{U}(FN)$ gegen 1, weshalb der Opportunitätsverlust u, der aus einem *FN* folgt, gegen 0 konvergiert. Der Kurvenverlauf für $\mathrm{E}(opp.\text{-}verlust_{negativ})$ konvergiert deshalb für $u/t \to 0$ gegen 0 und steigt auf dem Intervall $u/t \in [0; 1]$ stetig, bis sein Maximum von 0,09 erreicht ist.

Die Kurvenverläufe zeigen, dass der insgesamt erwartete Opportunitätsverlust der Positiv- und Negativ-Strategie für $u/t = 1$ nicht identisch ist, obwohl der Opportunitätsverlust u, der aus einem *FN* entsteht, und der Opportunitätsverlust t, der aus einem *FP* entsteht, identisch sind. Der Grund ist, dass im Mittel nur 11,3% der Positionsschätzungen aus der Menge M innerhalb der jeweiligen autorisierten Zone liegen. Es liegt daher ein Szenario vor, in dem Anfragen zur Nutzung eines geschützten Zugriffsrechts in 88,7% der Fälle von außerhalb der zugeordneten autorisierten Zone erfolgen. Die Wahrscheinlichkeit, dass das Autorisieren der Positiv-Strategie einen *FP* bewirkt, ist somit höher als die Wahrscheinlichkeit, dass das Ablehnen der Negativ-Strategie einen *FN* bewirkt. Mit wachsender Abszisse $u/t > 1$ wächst $\mathrm{U}(FP)$, wodurch ein *FP* unter der Positiv-Strategie stetig weniger Opportunitätsverlust erzeugt. Im Mittel ist in diesem Szenario daher erst bei $u/t = 9{,}4$ die Gleichheit des insgesamt erwarteten Opportunitätsverlusts für die Positiv- und Negativ-Strategie erreicht. Der geringere Opportunitätsverlust t eines *FP* im Vergleich zum Opportunitätsverlust u eines *FN*, wiegt dann im Mittel auf, dass die Positiv-Strategie mehr Falschentscheidungen trifft, als die Negativ-Strategie.

Unter der naiven Strategie ist die Anzahl der *FP* und *FN*, wie bei der Positiv- und Negativ-Strategie, unabhängig von u/t. Für $u/t = 1$ gilt der Sonderfall $\mathrm{U}(FP) = \mathrm{U}(FN) = 0$, weshalb sowohl ein *FP*, als auch ein *FN* den größtmöglichen Opportunitätsverlust von 1 auf der Skala des Nutzens erzeugen. Dabei entsteht das Maximum des insgesamt erwarteten Opportunitätsverlusts mit einer Ordinate von 0,08. Für $u/t \to 0$ konvergiert der Kurvenverlauf gegen eine Konstante, die aus der Anzahl der erwarteten *FP* folgt, da in diesem Extremfall aufgrund von $\mathrm{U}(FN) = 1$ kein Opportunitätsverlust für *FN* entsteht.

Entsprechend konvergiert der Kurvenverlauf für $u/t \to \infty$ gegen eine Konstante, die aus der Anzahl der erwarteten *FN* folgt, da im Extremfall $\mathrm{U}(FP) = 1$ kein Opportunitätsverlust für *FP* entsteht.

Der Kurvenverlauf der risikobasierten Strategie zeigt bei $u/t = 1$ ein Maximum, das mit dem Wert 0,07 das kleinste der vier Maxima ist. Dieses Maximum hat dieselbe Ursache, wie das Maximum der naiven Strategie. In der risikobasierten Strategie ist im Gegensatz zu den oben genannten Strategien die Anzahl der *FP* und *FN* abhängig von der Abszisse u/t. Weil stets die Autorisierungsentscheidung mit dem geringsten erwarteten Opportunitätsverlust getroffen wird, ist der insgesamt erwartete Opportunitätsverlust der risikobasierten Strategie eine theoretische untere Schranke für den insgesamt erwarteten Opportunitätsverlust der restlichen Strategien. In den Extremfällen $u/t \to 0$ und $u/t \to \infty$ konvergiert das Verhalten der risikobasierten Strategie gegen das Verhalten der Negativ- bzw. Positiv-Strategie. Für $u/t \to 0$ konvergiert der optimale Schwellwert gegen 1, weshalb im Extremum keine Autorisierung mehr erfolgt. Für $u/t \to \infty$ konvergiert der geforderte Schwellwert gegen 0, so dass im Extremum stets autorisiert wird.

5.2.2 Kriterium zur Eignung von Positionierungssystemen

Zwei Autorisierungsstrategien i und j können bzgl. ihres insgesamt erwarteten Opportunitätsverlusts verglichen werden, der für eine Ortsbeschränkung basierend auf $\mathcal{Z}$ und U, sowie ein gegebenes Positionierungssystem auftritt:

Definition 5.2.3 (Prozentuale Verlustreduktion)**.** *Sei eine Ortsbeschränkung* $(\mathcal{Z}, \mathrm{U})$ *gegeben, sowie zwei Autorisierungsstrategien* $i, j \in \{$*positiv,negativ, naiv, schwellwertbasiert, risikobasiert*$\}$*. Für beide Autorisierungsstrategien sei ferner der insgesamt erwartete Opportunitätsverlust gegeben. Unter diesen Randbedingungen ist die prozentuale Verlustreduktion der Strategie* i *gegenüber der Strategie* j *folgendermaßen definiert:*

$$\text{proz.-verlustreduktion}\,(i,j) = \frac{E\left(\textit{opp.-verlust}_j\right) - E\left(\textit{opp.-verlust}_i\right)}{E\left(\textit{opp.-verlust}_j\right)} \tag{5.13}$$

Die prozentuale Verlustreduktion ermöglicht die Definition eines Kriteriums zur qualitativen Bewertung, ob ein Positionierungssystem für die Durchsetzung einer Ortsbeschränkung mit einer konkreten standortbasierten Autorisierungsstrategie geeignet ist. Dazu muss sich gegenüber der Positiv- und der Negativstrategie eine positive prozentuale Verlustreduktion ergeben. Andernfalls würde es im Mittel mehr Nutzen bringen, die Positiv- bzw. die Negativstrategie anzuwenden, also die Ortsbeschränkung zu ignorieren, oder das Zugriffsrecht niemals zu gewähren.

Definition 5.2.4 (Eignung eines Positionierungssystems)**.** *Gegeben sei eine Autorisierungsstrategie* $i \in \{$*naiv, schwellwertbasiert, risikobasiert*$\}$*, eine Ortsbeschränkung* $(\mathcal{Z}, \mathrm{U})$*, sowie die prozentuale Verlustreduktion* proz.-verlustreduktion $(i,$ *positiv*$)$*, als auch der Wert* proz.-verlustreduktion $(i,$ *negativ*$)$*. Das eingesetzte Positionierungssystem ist geeignet genau dann wenn:*

$$\text{proz.-verlustreduktion}\,(i,\textit{positiv}) > 0 \wedge \text{proz.-verlustreduktion}\,(i,\textit{negativ}) > 0 \tag{5.14}$$

Diese Bedingung kann natürlich auch so formuliert werden, dass die minimale prozentuale Verlustreduktion gegenüber der Positiv- und Negativ-Strategie stets größer 0 sein muss:

$$\min\left(\text{proz.-verlustreduktion}\left(i, \textit{positiv}\right); \text{proz.-verlustreduktion}\left(i, \textit{negativ}\right)\right) > 0 \qquad (5.15)$$

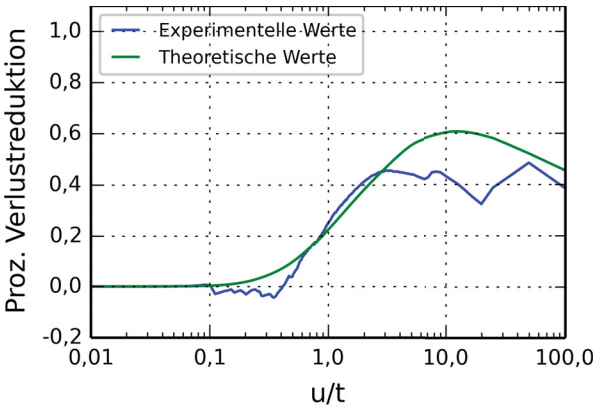
Im Folgenden wird die Anwendbarkeit des Kriteriums evaluiert, indem Aussagen über die Eignung eines Positionierungssystems theoretisch hergeleitet werden und mit empirisch ermittelten, realen Daten verglichen werden.

Evaluation des Kriteriums

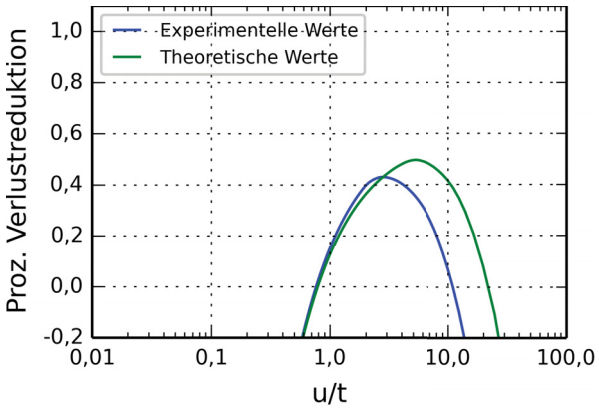
Das Kriterium zur Auswahl eines Positionierungssystems wird anhand der Testumgebung aus Unterabschnitt 5.2.1 evaluiert. Dazu werden die identischen 35 autorisierten Zonen verwendet und Ortsbeschränkungen basierend auf den beiden definierten Klassen 1 und 2 untersucht. Als theoretisches Modell für das eingesetzte Positionierungssystem dient wieder die Verteilung $\mathrm{F}_{fehler}^{Laplace}$ basierend auf dem Laplace-Fehlerschätzer aus Unterabschnitt 3.1.5.

Für jede der autorisierten Zonen wird abhängig von u/t das Minimum der prozentualen Verlustreduktion der risikobasierten Strategie gegenüber der Positiv- und der Negativ-Strategie berechnet. Der dazu benötigte insgesamt erwartete Opportunitätsverlust wird wieder basierend auf (5.12) mittels der Monte-Carlo-Methode approximiert. Dabei werden die Testdaten aus Abb. 3.1(c) als Menge M verwendet. Abb. 5.6(a) zeigt den Mittelwert der erhaltenen, theoretisch berechneten Minima über die 35 autorisierten Zonen in Abhängigkeit von u/t.

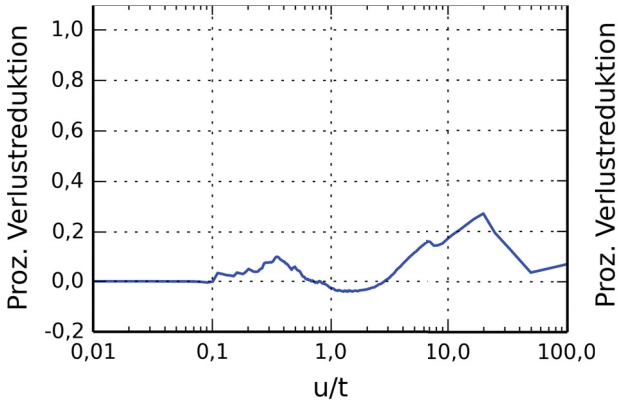
Die risikobasierte Strategie zeigt in diesem theoretischen Modell stets eine positive prozentuale Verlustreduktion. Mit steigenden Werten u/t wird bei $u/t = 11$ ein Maximum durchschritten, wonach die prozentuale Verlustreduktion wieder abnimmt. Die Lage des Maximums wird klar, wenn nochmals Abb. 5.5 für den insgesamt erwarteten Opportunitätsverlust betrachtet wird. Dabei ist erst für $u/t > 9{,}4$ gegeben, dass der insgesamt erwartete Opportunitätsverlust der Positiv-Strategie kleiner ist, als der entsprechende Wert der Negativ-Strategie. Im Intervall $[1; 9{,}4]$ verläuft der insgesamt erwartete Opportunitätsverlust der Negativ-Strategie konstant und die prozentuale Verlustreduktion hängt in diesem Intervall nur vom fallenden insgesamt erwarteten Opportunitätsverlust der risikobasierten Strategie ab. Der Wert der prozentualen Verlustreduktion nimmt deshalb innerhalb dieses Intervalls mit wachsender Abszisse stetig zu. Ab $u/t = 9{,}4$ entspricht der Kurvenverlauf der prozentualen Verlustreduktion jedoch der prozentualen Verlustreduktion gegenüber der Positiv-Strategie anstatt der Negativ-Strategie. Weil der insgesamt erwartete Opportunitätsverlust der Positiv-Strategie mit zunehmender Abszisse u/t weiterhin fällt, nimmt auch die prozentuale Verlustreduktion für $u/t > 9{,}4$ wieder ab, woraus die Existenz und Lage des Maximums des Kurvenverlaufs folgt. Die Verschiebung des Maximums zu einer größeren Abszisse folgt daraus, dass hier nicht, wie zuvor, die Mittelwerte des insgesamt erwarteten Opportunitätsverlusts verglichen werden, sondern für jedes Testdatum auf jeder autorisierten Zone direkt die prozentuale Verlustreduktion berechnet wird.



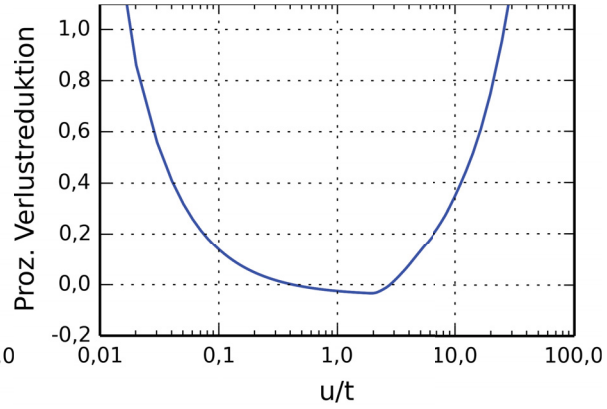
(a) Min. proz. Verlustreduktion der risikobasierten Strategie gegenüber Positiv- und Negativ-Strategie.



(b) Min. proz. Verlustreduktion der naiven Strategie gegenüber Positiv- und Negativ-Strategie.



(c) Vorhersagefehler zur risikobasierten Strategie.



(d) Vorhersagefehler zur naiven Strategie.

Abbildung 5.6: Theoretische und experimentelle Untersuchung des Minimums der prozentualen Verlustreduktion entsprechend (5.15) für die risikobasierte bzw. die naive Strategie gegenüber der Positiv- und Negativ-Strategie. Die unteren Graphen zeigen den jeweiligen Vorhersagefehler der theoretischen Untersuchung.

Die theoretische Evaluation des Kriteriums wird mit der prozentualen Verlustreduktion verglichen, die sich anhand der Testdaten aus Abb. 3.1(c) ergibt. Dazu wird für jede der 35 definierten autorisierten Zonen die Menge der Testdaten als reale Stichprobe von Anfragen betrachtet und mittels jeder der vier Autorisierungsstrategien ausgewertet, sowie der real auftretende Opportunitätsverlust bestimmt. Anhand der Ergebnisse wird die prozentuale Verlustreduktion berechnet, die sich für die naive bzw. risikobasierte Strategie gegenüber der Positiv- und Negativ-Strategie ergibt. Der Mittelwert aus den Werten für die 35 autorisierten Zonen ist in Abhängigkeit von u/t in Abb. 5.6(a) angetragen.

Die Differenz des experimentellen Werts zur theoretisch ermittelten prozentualen Verlustreduktion ist in Abb. 5.6(c) angetragen. Es zeigt sich, dass die prozentuale Verlustreduk-

tion der risikobasierten Strategie sowohl gegenüber der Positiv-Strategie, als auch gegenüber der Negativ-Strategie im Intervall $[0{,}1; 0{,}4]$ negativ ist. In der Praxis ist die Eignung eines Positionierungssystems unter der risikobasierten Strategie deshalb nicht stets gegeben, obwohl dies aus entscheidungstheoretischer Sicht zu erwarten ist. Der Grund ist, dass die abgeleiteten WDF des Fehlerschätzers nur eine Approximation der realen Verteilung der wahren Position des Nutzers um die Positionsschätzung darstellen. Aufgrund dieser Tatsache werden einzelne Werte $p_{\mathcal{Z}}$ über- bzw. unterschätzt. Die Autorisierungsentscheidung der risikobasierten Strategie wird getroffen, indem der erwartete Nutzen einer Autorisierung und einer Ablehnung berechnet wird. Aufgrund der über- bzw. unterschätzten Werte von $p_{\mathcal{Z}}$ kommt es auf den Testdaten zu suboptimalen Entscheidungen, die aufgrund der suboptimalen Fehlerschätzung nicht vermeidbar sind. Die maximale Abweichung beträgt 0,27, so dass zur Prüfung des Kriteriums aus Definition 5.2.4 in vergleichbaren Szenarien eine experimentelle Ermittlung der prozentualen Verlustreduktion empfohlen wird, sofern die theoretisch ermittelte prozentuale Verlustreduktion unterhalb dieser Grenze liegt.

Die Mittelwerte der Minima, die sich für die theoretisch berechnete, prozentuale Verlustreduktion der naiven Strategie gegenüber der Positiv- und Negativ-Strategie ergeben, sind in Abhängigkeit von u/t in Abb. 5.6(b) dargestellt. Auch hier lässt sich der Kurvenverlauf erklären, indem anhand von Abb. 5.5 der insgesamt erwartete Opportunitätsverlust der naiven Strategie, sowie der Positiv- und der Negativ-Strategie verglichen wird. Im Bereich $u/t \in [0; 0{,}78[$ ist der insgesamt erwartete Opportunitätsverlust der naiven Strategie größer, als der entsprechende Wert für die Negativ-Strategie. Die prozentuale Verlustreduktion ist deshalb in diesem Bereich negativ. Im Intervall $[0{,}78; 24{,}75]$ ist der insgesamt erwartete Opportunitätsverlust der naiven Strategie kleiner als die entsprechenden Werte der Positiv- und Negativ-Strategie. Daher ist die prozentuale Verlustreduktion ist in diesem Intervall positiv, wodurch entsprechend des Kriteriums aus Definition 5.2.4 das verwendete Positionierungssystem unter der naiven Strategie im Mittel für die autorisierten Zonen geeignet ist. Das Maximum wird bei $u/t = 4{,}95$ erreicht. Für $u/t > 24{,}75$ unterschreitet der insgesamt erwartete Opportunitätsverlust der Positiv-Strategie den entsprechenden Wert der naiven Strategie. Die Eignung des Positionierungssystems ist deshalb im Intervall $]24{,}75; \infty]$ nicht mehr gegeben.

Die experimentellen Werte für die prozentuale Verlustreduktion werden wieder basierend auf den Testdaten aus Abb. 5.6(a) bestimmt. Dazu wird die prozentuale Verlustreduktion der naiven Strategie gegenüber der Positiv- und Negativ-Strategie berechnet, die sich auf den Testdaten ergibt. Die Ergebnisse sind ebenfalls in Abb. 5.6(b) angetragen. Die Abweichung der experimentell ermittelten Werte zu den theoretisch ermittelten Werten zeigt Abb. 5.6(d). Auf den experimentellen Testdaten ist das Kriterium aus Definition 5.2.4 für das Intervall $u/t \in [0{,}75; 11{,}0]$ erfüllt. Das Maximum liegt bei $u/t = 2{,}68$. Auf den experimentellen Daten werden insgesamt weniger RP und RN erzeugt, als durch das Modell des Positionierungssystems erwartet wird, das als Grundlage zur theoretischen Berechnung der prozentualen Verlustreduktion dient. Folglich erhöht sich die Zahl der FN und FP gegenüber dem Wert, der theoretisch erwartet wird. Dies führt dazu, dass das Intervall von geeigneten Werte u/t auf den realen Testdaten kleiner ist, als durch die theoretische Berechnung erwartet. In den Extremfällen $u/t \to 0$ und $u/t \to \infty$ führt dies zu

einer stark zunehmenden Abweichung zwischen dem real beobachteten Wert und dem zuvor theoretisch ermittelten Wert.

Implikationen für verwandte Arbeiten

In diesem Abschnitt wurde ein Kriterium zur Bewertung der Eignung von Positionierungssystemen eingeführt. Die Annahme dabei ist, dass ein Positionierungssystem unter der verwendeten Autorisierungsstrategie geeignet ist, falls ihr Einsatz gegenüber der Positiv- und der Negativstrategie einen geringeren insgesamt erwarteten Opportunitätsverlust zeigt. Liegt eine Ortsbeschränkung vor, für die dies unter gegebenem Positionierungssystem und gegebener Autorisierungsstrategie nicht der Fall ist, so wird das Positionierungssystem als ungeeignet eingestuft. Mithilfe dieser Vorgehensweise kann für alle existierenden Arbeiten aus der Literatur zu standortbasierter Autorisierung, Geo-Fencing oder zonenbasierten Diensten ermittelt werden, ob deren Annahme von punktgenauen Positionsschätzungen und somit deren Anwendung der naiven Strategie gerechtfertigt ist. Die Voraussetzung dafür ist, dass die Abbildung U bekannt ist. Wird ein Positionierungssystem als ungeeignet bzgl. des entwickelten Kriteriums eingestuft, kann ein solches Positionierungssystem ermittelt werden, das dem jeweiligen Szenario genügt und einen sinnvollen Betrieb der Ortsbeschränkung zulässt.

5.3 Die Inbetriebnahme von Ortsbeschränkungen

In diesem Kapitel wurde zunächst ein Ansatz zur Bestimmung von Qualitätsparametern von Ortsbeschränkungen vorgestellt, die sich ergeben, wenn ein bestimmtes Positionierungssystem und eine der Autorisierungsstrategien eingesetzt wird. Diese Qualitätsparameter erlauben es, für die drei identifizierten Nutzergruppen eine Aussage zu treffen, ob der Betrieb der Ortsbeschränkung den Anforderungen genügt. Ergänzend wurde eine Methodik vorgestellt, mit der die prozentuale Verlustreduktion der risikobasierten gegenüber der naiven Strategie ermittelt werden kann. Es wurde ein binäres Entscheidungskriterium vorgestellt, das die Eignung von Positionierungssystemen bewertet.

Mithilfe dieser Werkzeuge lässt sich bereits vor der Inbetriebnahme einer Ortsbeschränkung ein geeignetes Positionierungssystem und eine passende Autorisierungsstrategie auswählen. Die Methodik ist in Abb. 5.7 zusammenfassend veranschaulicht.

Zunächst wird die Ortsbeschränkung als Tupel $(\mathcal{Z}, \mathrm{U})$ definiert und eine Autorisierungsstrategie ausgewählt. Dann wird die Menge der geeigneten Positionierungssysteme mithilfe von (5.14) ermittelt. Gibt es keinen Kandidaten, muss eine alternative Autorisierungsstrategie ausgewählt werden. Aus der Menge geeigneter Positionierungssysteme wird das ausgewählt, welches gemäß der Analyse in Unterabschnitt 5.2.1 den geringsten Opportunitätsverlust und somit den größten Nutzen generiert. Für dieses werden dann die drei Qualitätsparameter bestimmt und dahingehend untersucht, ob sie für alle drei Nutzergruppen den fallspezifischen Anforderungen genügen. Ist dies nicht der Fall, wird eine alternative Autorisierungsstrategie ausgewählt. Ansonsten kann die Ortsbeschränkung schließlich in

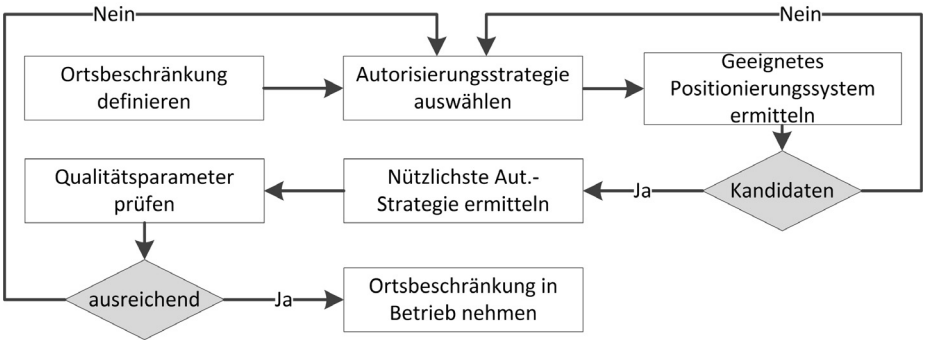


Abbildung 5.7: Vorgehensweise zur Inbetriebnahme von Ortsbeschränkungen.

Betrieb genommen werden.

Ein weiterer Vorteil der entwickelten Ansätze ist, dass die Verfahren aus verwandten Arbeiten damit ebenso analysiert werden können, sofern eine klare Autorisierungsstrategie existiert und eine Abbildung U für den Nutzen bereitsteht.

Kapitel 6

Zusammenfassung und Ausblick

6.1 Zusammenfassung

In modernen mobilen Endgeräten, wie Tablet-Computern und Smartphones, steht inzwischen ausreichend Rechenleistung bereit, um sehr flexibel einsetzbare IT-Systeme zu realisieren und das mobile Arbeiten zu ermöglichen. Ebenso sind immer leistungsfähigere Sensoren verbaut, die eine Bestimmung der Position des Nutzers erlauben. Dadurch ist die Grundlage geschaffen, Zugriffsrechte in diesen IT-Systemen auf Basis des Standorts des Nutzers zu vergeben. Zur Durchsetzung dieser Semantik wird die standortbasierte Autorisierung eingesetzt, die klassische Zugriffskontrollmodelle durch Ortsbeschränkungen erweitert. Um ein Zugriffsrecht zu erlangen, muss der Nutzer vom klassischen Zugriffskontrollmodell autorisiert werden und die zugeordnete Ortsbeschränkung muss für die Position des Nutzers erfüllt sein. Zum Einen wird so die Stärkung der Informationssicherheit in mobilen Systemen möglich, indem die Möglichkeiten unberechtigter Dritter beschränkt werden, die in Besitz des mobilen Endgeräts gelangen. Dazu wird eine Ortsbeschränkung auf Basis einer autorisierten Zone definiert, zu der nur berechtigte Nutzer der mobilen Anwendung physisch Zutritt haben. Unberechtigte Dritte müssen somit zusätzlich zum mobilen Endgerät das Zutrittsrecht zur zugeordneten, autorisierten Zone erlangen. Ein weiteres Anwendungsfeld sind mobile soziotechnische Systeme im Industrieumfeld, in denen der Nutzer mittels seines mobilen Endgeräts an der Steuerung und Überwachung von Maschinen beteiligt ist. Ohne Berücksichtigung des Standorts kann sich der Nutzer während der Bedienung an beliebigen Orten befinden und im Notfall zur Schadensbegrenzung nicht mehr zeitnah manuell eingreifen. Aus Gründen der Betriebssicherheit ist es deshalb nötig, die Bedienung auf ausreichend nahe Orte zu begrenzen. Ebenso ist die standortbasierte Autorisierung ein geeignetes Werkzeug zur Umsetzung standortbezogener Dienste und wird dabei zur Implementierung funktionaler Anforderungen eingesetzt.

Bisher wird die Realisierung der standortbasierten Autorisierung durch auftretende Positionsfehler erschwert, weil die Ungewissheit von Positionsschätzungen nicht erfasst und berücksichtigt wird. Dadurch treten, abhängig vom Szenario, häufig Falschentscheidungen während der Autorisierung auf, wodurch die Semantik verletzt wird und Schaden entsteht.

Es existieren keine Methoden zur Analyse, ob ein Positionierungssystem aufgrund der Größe seiner Positionsfehler als Grundlage für die standortbasierte Autorisierung in einem gegebenen Szenario geeignet ist. Der Fokus der vorliegenden Arbeit ist deshalb zunächst die Entwicklung von Qualitätsparametern, unter denen sich das Verhalten der standortbasierten Autorisierung in Abhängigkeit vom eingesetzten Positionierungssystem und dem Verfahren zur Ableitung von Autorisierungsentscheidungen bewerten und vergleichen lässt. Anschließend wird die Fragestellung untersucht, die Ungewissheit von Positionsschätzungen am Beispiel von WLAN-Fingerprinting, einem der wichtigsten Positionierungssysteme innerhalb von Gebäuden, statistisch zu erfassen. Ausgehend davon werden Verfahren entwickelt, diese Ungewissheit bei der Ableitung von Autorisierungsentscheidungen zu berücksichtigen. Es wird ein Kriterium definiert, welches die Eignung eines Positionierungssystems festlegt.

Die Positionsbestimmung ist Grundvoraussetzung für die Anwendung standortbasierter Autorisierung. In Gebäuden wird dabei überwiegend WLAN-Fingerprinting eingesetzt, was, wie jedes andere Positionierungssystem auch, inhärenten Positionsfehlern unterliegt. Die Positionsfehler übersteigen dabei oftmals die Größe von autorisierten Zonen. Damit die Ungewissheit über die aktuelle Position bei der standortbasierten Autorisierung berücksichtigt werden kann, wird in Kapitel 3 ein Verfahren vorgestellt, das eine statistische Modellierung der Positionsfehler von WLAN-Fingerprinting erlaubt. Dabei wird ausgehend von den kNN zu einer durchgeführten Messung eine WDF basierend auf der Laplace-Verteilung hergeleitet, welche die Position des Nutzers beschreibt. Es wird eine Evaluationsmethodik basierend auf QQ-Plots eingeführt und gezeigt, dass der entwickelte Fehlerschätzer die Positionsfehler weniger stark über- bzw. unterschätzt, als bisher existierende Ansätze. Ein Nachteil von WLAN-Fingerprinting ist aktuell, dass zur Positionsbestimmung basierend auf den kNN zunächst ein optimaler Wert für k empirisch zu ermitteln ist. Mit SMART-kNN wird eine Erweiterung von WLAN-Fingerprinting vorgestellt, die nicht auf diesen Wert angewiesen ist. Stattdessen wird die Anzahl der nächsten Nachbarn, die zur Positionsbestimmung berücksichtigt werden, dynamisch und basierend auf einer Messung des Nutzers bestimmt. Es wird gezeigt, dass damit keine größeren Positionsfehler auftreten, als bei der Verwendung eines fixen k, aber die vorhergehende Ermittlung dieses Parameters entfällt. Ausgehend von der WDF einer Positionsschätzung ist es zur Behandlung von Positionsfehlern erforderlich, die Ungewissheit zu erfassen, die bzgl. der Erfüllung einer Ortsbeschränkung herrscht. Dazu wird die WDF über die autorisierte Zone numerisch integriert, wodurch sich die Aufenthaltswahrscheinlichkeit als Maß für die Ungewissheit ergibt. Es wird ein Verfahren vorgestellt, das diese rechenintensive Operation in eine Phase der Vorberechnung von Matrizen verlagert. Während der Anwendung der standortbasierten Autorisierung ist zur Ermittlung der Aufenthaltswahrscheinlichkeit lediglich eine Sequenz von Lesezugriffen auf den vorberechneten Matrizen nötig. Es wird gezeigt, dass für Fehlerschätzungen zwischen 1 m und 7 m, die Aufenthaltswahrscheinlichkeit dadurch höchstens um 7% über- bzw. unterschätzt wird. Die Laufzeit wird dabei um den Faktor 150–300 gegenüber der direkten Berechnung verringert. Zuletzt wird die unberechtigte Weitergabe des mobilen Endgeräts als weitere Ursache von Positionsfehlern betrachtet. In diesem Fall stimmt die wahre Position des eingeloggten Nutzers nicht mehr mit der ermittelten Positi-

on des mobilen Endgeräts überein. Um den Nutzer an sein mobiles Endgerät zu koppeln, wird der Einsatz von kontinuierlicher, biometrischer Authentifizierung vorgeschlagen. Es wird ein Anforderungskatalog an entsprechende Verfahren vorgestellt, der für den Einsatz zusammen mit der standortbasierten Autorisierung zu beachten ist. Darunter fallen die Aspekte der Anwendbarkeit, Energieeffizienz, Reaktionsgeschwindigkeit und der Transparenz. Existierende Verfahren werden auf die Erfüllung dieser Aspekte hin untersucht. Es wird gezeigt, dass aktuell kein Verfahren allen Anforderungen genügt und eine Fusion mehrerer Verfahren nötig ist. Die Auswahl zu fusionierender Verfahren wird anhand von zwei Fallstudien diskutiert.

Ist die Positionsschätzung eines Nutzers gegeben, erfolgt darauf basierend die Auswertung von Ortsbeschränkungen. In Kapitel 4 wird mit der risikobasierten Autorisierungsstrategie eine Methodik zur Auswertung von Ortsbeschränkungen eingeführt, die aus entscheidungstheoretischer Sicht optimal ist. Dabei werden den vier Ausgängen RP, RN, FP und FN einer Autorisierungsentscheidung mittels der Methodik nach von Neumann und Morgenstern symbolische Werte für deren Nutzen zugeordnet. Eine suboptimale Autorisierungsentscheidung erzeugt dabei weniger Nutzen, als im besten Fall möglich ist, wodurch Opportunitätsverlust entsteht. Davon ausgehend autorisiert die risikobasierte Strategie genau dann, wenn der erwartete Opportunitätsverlust einer Autorisierung geringer ist, als der erwartete Opportunitätsverlust einer Ablehnung. Die risikobasierte Strategie wird erweitert, indem anstelle von Polygonen zur Modellierung autorisierter Zonen das Konzept von Eigenschaftsmodellen verwendet wird. Formal ist ein Eigenschaftsmodell als bedingte Wahrscheinlichkeit definiert, mit der an einem Punkt x eine Eigenschaft vorhanden ist, die zur Autorisierung vorausgesetzt wird. Es wird gezeigt, dass Eigenschaftsmodelle bzgl. ihrer Ausdrucksstärke eine Generalisierung des bisherigen Konzepts der autorisierten Zonen darstellen. Sie erlauben gegenüber autorisierten Zonen eine flexiblere Modellierung von Ortsbeschränkungen, falls die Punkte mit geforderter Eigenschaft nicht exakt durch ein Polygon umschrieben werden können. Ferner wird gezeigt, wie ausgehend vom Konzept der risikobasierten Strategie ein optimaler Schwellwert zum Betrieb der existierenden, schwellwertbasierten Strategie herzuleiten ist. Ausgehend von der erweiterten risikobasierten Strategie wird eine Erweiterung von RBAC vorgestellt, die Positionsfehler beachtet. Ortsbeschränkungen werden einzelnen Elementen der RBAC-Richtlinie zugewiesen. Es wird durch Evaluation gezeigt, dass der Opportunitätsverlust gegenüber der bisherigen Verfahrensweise ohne Beachtung von Positionsfehlern um mindestens 10% sinkt. Dabei steigt die Komplexität der Auswertung gegenüber der bisherigen Modelle mit zunehmender Zahl an Ortsbeschränkungen exponentiell, so dass empfohlen wird, innerhalb eines Autorisierungspfads der RBAC-Richtlinie maximal $2-4$ Ortsbeschränkungen zuzuordnen. Ergänzend wird ein Ansatz vorgestellt, der die kontinuierliche Auswertung von Ortsbeschränkungen unter der risikobasierten Strategie unterstützt. Dazu werden Partikelfilter einsetzt, um den Einfluss von Messausreißern zu reduzieren. Bisherige Ansätze konkatenieren hingegen die Sequenz aus punktuellen Positionsschätzungen, um eine Trajektorie zu konstruieren und interpolieren deren Verlauf zwischen den Punkten. In bisherigen Verfahren wird überprüft, ob diese Trajektorie innerhalb der autorisierten Zone der Ortsbeschränkung enthalten ist. In der Evaluation zeigt sich, dass der Vorteil gegenüber dem bisherigen Verfahren stark vom Nut-

zen der einzelnen Fälle *RP*, *RN*, *FP* und *FN* abhängt. Im besten Fall wird dadurch eine Verringerung des Opportunitätsverlusts um 80% erreicht. Ferner wird in den existierenden Ansätzen ein statischer Timeout für die erlaubte Zeitspanne zwischen zwei Positionsschätzungen verwendet, der durch einen Experten festgelegt wird. Derzeit existiert keine Methodik zur systematischen Herleitung dieses Timeouts. Ausgehend von der aktuellen Ungewissheit über die Position des Nutzers wird deshalb ein Verfahren zur dynamischen Bestimmung dieses Timeouts angegeben. Die Timeouts werden in einer Evaluation gegen die tatsächlich benötigte Austrittszeit aus der autorisierten Zone verglichen. Dabei zeigt sich, dass die Timeouts eine sehr gute Approximation der wahren Austrittszeit darstellen.

In Kapitel 5 werden drei Nutzergruppen der standortbasierten Autorisierung identifiziert. Gutartige Nutzer befinden sich innerhalb der autorisierten Zone und erfüllen die Ortsbeschränkung des benötigten Zugriffsrechts. Angreifer befinden sich außerhalb davon und beabsichtigen eine Positionsschätzung zu erhalten, die zur unberechtigten Autorisierung führt, um das Zugriffsrecht anschließend zu missbrauchen und Schaden zu verursachen. Unbeteiligte Passanten befinden sich ebenfalls außerhalb der autorisierten Zone und werden im Falle einer irrtümlichen, proaktiven Autorisierung gestört. Es wird eine Methodik eingeführt, die eine quantitative Bewertung der standortbasierten Autorisierung aus Sicht der jeweiligen Nutzergruppe erlaubt, indem jeweils ein Qualitätsparameter berechnet wird. Diese Parameter quantifizierten die Abweichungen im Autorisierungsverhalten aus Sicht der jeweiligen Nutzergruppe, die sich unter dem eingesetzten Positionierungssystem im Vergleich zu einem fiktiven, fehlerfreien Positionierungssystem ergibt. Zu deren Berechnung werden Autorisierungsmodelle eingeführt, die formal die bedingte Wahrscheinlichkeit für jeden Punkt x beschreiben, dort eine Positionsschätzung zu erhalten, die zur Autorisierung führt. An einer Fallstudie wird gezeigt, dass die Autorisierungsmodelle und somit die Qualitätsparameter stark vom Nutzen der vier Ausgänge *RP*, *RN*, *FP* und *FN* abhängen. Ist der Opportunitätsverlust eines *FP* im Vergleich zum Opportunitätsverlust eines *FN* hoch, zeigt das Autorisierungsmodell unter der risikobasierten Strategie ein restriktives Verhalten. Dabei verschlechtert sich der Wert des Qualitätsparameters für gutartige Nutzer. Die Werte der Qualitätsparameter für Angreifer und unbeteiligte Passanten profitieren in diesem Fall vom restriktiven Verhalten. Entsprechend wird im umgekehrten Fall, in dem der Opportunitätsverlust eines *FN* größer als der eines *FP* ist, tendenziell die Erfolgswahrscheinlichkeit eines Angreifers erhöht und ein unbeteiligter Passant mit einer höheren Wahrscheinlichkeit fälschlicherweise proaktiv autorisiert. Ferner ist zu entscheiden, ob das eingesetzte Positionierungssystem aufgrund der Größe seiner Positionsfehler prinzipiell geeignet ist. Bisher existiert dazu kein Kriterium. Es wird ein Kriterium vorgestellt, das die qualitative Bewertung erlaubt, ob ein Positionierungssystem zur Durchsetzung der definierten Ortsbeschränkung unter der zugrundeliegenden Autorisierungsstrategie geeignet ist. Dabei wird das Konzept des insgesamt erwarteten Opportunitätsverlusts eingeführt. Dessen Berechnung erfolgt in Abhängigkeit von einer Ortsbeschränkung, bestehend aus autorisierter Zone und Werten für den Nutzen der vier Ausgänge, einer Autorisierungsstrategie und einem gegebenen Positionierungssystem. Durch diesen Wert wird der Opportunitätsverlust beschrieben, der unter den genannten Randbedingungen während des Betriebs der standortbasierten Autorisierung als Konsequenz einer Autorisierungsentscheidung er-

wartet wird. Die Bedingung des definierten Kriteriums ist, dass der insgesamt erwartete Opportunitätsverlust der eingesetzten Autorisierungsstrategie geringer ist, als der insgesamt erwartete Opportunitätsverlust der Positiv- und Negativ-Strategie, die alle Anfragen unabhängig vom Standort autorisiert bzw. ablehnt. In der Evaluation wird gezeigt, dass die Eignung der risikobasierten Strategie in der Praxis nicht unabhängig vom eingesetzten Positionierungssystem ist und von den zugeordneten Werten für den Nutzen der vier Ausgänge abhängt. Der Grund ist, dass einzelne Fehlerschätzungen die Aufenthaltswahrscheinlichkeit über- bzw. unterschätzen. Mittels des insgesamt erwarteten Opportunitätsverlusts ist es ferner möglich unter zwei Konfigurationen aus Positionierungssystem und Autorisierungsstrategie diejenige auszuwählen, die insgesamt weniger Opportunitätsverlust erzeugt. Basierend auf den vorgestellten Analysemethoden wird abschließend eine Methodik vorgestellt, die bereits vor der Inbetriebnahme der standortbasierten Autorisierung die systematische Auswahl des Positionierungssystems und der Autorisierungsstrategie erlaubt.

Durch die vorgestellten Ergebnisse wird ein wesentlicher Beitrag zur Einsetzbarkeit der standortbasierten Autorisierung, insbesondere in Gebäuden, geleistet. Erstmals ist es dadurch auf rationale Weise möglich, eine Autorisierungsentscheidung herzuleiten, wenn Ungewissheit über die wahre Position des Nutzers besteht. Durch die vorgestellte erweiterte risikobasierte Autorisierungsstrategie wird das bisherige Konzept der Polygone als Grundlage der standortbasierten Autorisierung generalisiert. Dies erlaubt eine deutlich ausdrucksstärkere und nachvollziehbare Modellierung von Ortsbeschränkungen. Durch die entwickelten Analyseverfahren stehen erstmals Werkzeuge bereit, um die Eignung eines Positionierungssystems für die standortbasierte Autorisierung bereits vor deren Inbetriebnahme zu bewerten. Hierdurch wird erreicht, dass nicht erst im Produktiveinsatz klar wird, ob die Positionsfehler des Positionierungssystems für ein gegebenes Szenario zu groß sind. Dieser Beitrag ist besonders im Hinblick auf das immer wichtigere Internet der Dinge relevant. Dort sind Szenarien denkbar, in denen z.B. ein Küchenherd aus Sicherheitsgründen automatisch abgeschaltet wird, wenn sich das Smartphone des Nutzers nicht in der Nähe von 2–3 m befindet. Denkbar ist auch, dass eine Kaffeemaschine automatisch startet, wenn das Smartphone daneben gelegt wird. All diesen Szenarien liegt eine Aktion zugrunde, die nur ausgelöst werden soll, wenn sich das Smartphone innerhalb einer autorisierten Zone befindet. Durch das entwickelte Kriterium kann hier schon vorab ermittelt werden, wie groß die Zone sein muss, damit ein zufriedenstellender Betrieb ermöglicht wird. Ein weiterer Vorteil ergibt sich bei der Übertragung der Analyseverfahren auf verwandte Arbeiten zur standortbasierten Autorisierung. Bis auf wenige Ausnahmen wird in diesen Arbeiten die naive Strategie angewandt, die auf einem Punkt-in-Polygon-Test basiert. Dort wird nicht berücksichtigt, ob das Ignorieren von Positionsfehlern eine legitime Annahme ist. Durch das vorgestellte Kriterium kann für diese verwandten Arbeiten abhängig vom Szenario bestimmt werden, ob diese Annahme gerechtfertigt ist. Unabhängig davon ist es mit dem Konzept der prozentualen Verlustreduktion möglich, für eine Ortsbeschränkung die Konfiguration aus Positionierungssystem und Autorisierungsstrategie zu wählen, für die aus entscheidungstheoretischer Sicht im Betrieb der größte Nutzen erwartet wird. Zusätzlich leistet das Konzept der Autorisierungsmodelle den Beitrag, dass erstmals eine Analyse und quantitative Bewertung des Verhaltens der standortbasierten Autorisierung in Abhängig-

keit von den gewählten Parametern aus Sicht der drei Nutzergruppen ermöglicht wird.

6.2 Ausblick

In zukünftigen Arbeiten ist es wichtig, die entwickelten Modelle in den Entwurfsprozess von Ortsbeschränkungen effektiv einzubinden. Dazu werden Entwicklungswerkzeuge benötigt, die eine interaktive Oberfläche zur Modellierung von Ortsbeschränkungen bieten und die Erzeugung von Eigenschaftsmodellen unterstützen.

Ebenso ist es wichtig, die entwickelten Analyseverfahren für das Testen von standortbezogenen Diensten bereits während der Entwicklungszeit nutzbar zu machen. Ausgehend davon, dass der standortbezogene Dienst innerhalb einer autorisierten Zone bereitzustellen ist, können klassische Unit-Tests in der Hinsicht erweitert werden, so dass „Soft-Unit-Tests“ entstehen. Denkbar ist, dass dabei anstelle eines binären Kriteriums quantitativ bewertet wird, inwiefern die Qualitätsparameter der drei Nutzergruppen von der Spezifikation des Diensts abweichen. Bisher ist eine solche Analyse nur empirisch zur Laufzeit mit einem echten Positionierungssystem möglich. Interessant ist auch die Fragestellung, wie sich das Konzept des Nutzens auf Bereichsabfragen für Datenbanken bewegter Objekte übertragen lässt. Anstelle der Autorisierung steht hier die Frage im Vordergrund, ob ein Element in die Ergebnismenge aufzunehmen ist. Auch hier ist das Konzept des Nutzens einsetzbar, um die bisher verwendeten Schwellwerte systematisch herzuleiten.

Wichtig ist in zukünftigen Arbeiten vor allem die Übertragung der Fehlerschätzung auf mehrere Stockwerke, indem z.B. eine dreidimensionale Verteilung angegeben wird. Zur sog. Stockwerkserkennung gibt es bereits erste Arbeiten, die dazu z.B. das Barometer des Smartphones einsetzen. Andere Arbeiten befassen sich mit der Auswertung des Beschleunigungssensors, um das Treppensteigen zu erkennen.

Ein weiterer offener Punkt ist die Frage der Privatsphäre des Nutzers beim Einsatz der standortbasierten Autorisierung. Ungeklärt ist hier, wie groß z.B. gezielt eingeführte Positionsfehler sein dürften, mit denen der wahre Standort verschleiert werden kann. Es ist bisher nicht untersucht, wie davon die Qualitätsparameter, der insgesamt erwartete Opportunitätsverlust und die Eignung des Positionierungssystems betroffen sind. Ein starker Einflussfaktor ist sicherlich die Größe der autorisierten Zone, so dass innerhalb von Gebäuden durchdachte Methoden nötig sind, um die Privatsphäre zu schützen.

Ebenso sollte in zukünftigen Arbeiten die Beachtung von Positionsfehlern auf Verfahren zur standortbasierten Autorisierung übertragen werden, die nicht auf einer autorisierten Zone basieren, sondern z.B. die Nähe eines anderen Nutzers zur Autorisierung verlangen. Das entspricht in gewisser Weise solchen Eigenschaftsmodellen, in denen sich der spezifische Punkt (z.B. der Notausschalter) dynamisch über die Zeit fortbewegt, wodurch sich diese Modelle zeitlich ändern. Ein anderes Szenario kann erfordern, dass z.B. mindestens x Personen im selben Raum anwesend sind. Die Anpassung der entwickelten Konzepte für solche Ortsbeschränkungen ist daher noch ein wichtiger Punkt für künftige Arbeiten.

Literaturverzeichnis

[1] R. Abdunabi, I. Ray und R. France: *Specification and Analysis of Access Control Policies for Mobile Applications*. In *Proceedings of the 18th ACM Symposium on Access Control Models and Technologies*, SACMAT '13. ACM (2013), Seiten 173–184.

[2] S. Aich, S. Mondal, S. Sural und A. Majumdar: *Role Based Access Control with Spatiotemporal Context for Mobile Applications*. In *Transactions on Computational Science IV*, herausgegeben von M. Gavrilova, C. Tan und E. Moreno, Band 5430 von *Lecture Notes in Computer Science*. Springer (2009), Seiten 177–199.

[3] S. Aich, S. Sural und A. Majumdar: *STARBAC: Spatiotemporal Role Based Access Control*. In *On the Move to Meaningful Internet Systems 2007: CoopIS, DOA, ODBASE, GADA, and IS*, herausgegeben von R. Meersman und Z. Tari, Band 4804 von *Lecture Notes in Computer Science*. Springer (2007), Seiten 1567–1582.

[4] B. Altintas und T. Serif: *Improving RSS-Based Indoor Positioning Algorithm via K-Means Clustering*. In *11th European Wireless Conference 2011 - Sustainable Wireless Technologies*, European Wireless '11. VDE-Verlag (2011), Seiten 1–5.

[5] *Android*. URL: `www.android.com`, zuletzt besucht am 20.03.2015.

[6] A. Anjos und S. Marcel: *Counter-Measures to Photo Attacks in Face Recognition: A Public Database and a Baseline*. In *Proceedings of the 2011 IEEE International Joint Conference on Biometrics*, IJCB '11. IEEE (2011), Seiten 1–7.

[7] C.A. Ardagna, M. Cremonini, E. Damiani, S. De Vimercati und P. Samarati: *A Middleware Architecture for Integrating Privacy Preferences and Location Accuracy*. In *New Approaches for Security, Privacy and Trust in Complex Environments*, herausgegeben von H. Venter, M. Eloff, L. Labuschagne, J. Eloff und R. von Solms, Band 232 von *IFIP International Federation for Information Processing*. Springer (2007), Seiten 313–324.

[8] C.A. Ardagna, M. Cremonini, E. Damiani, S.D.C. di Vimercati und P. Samarati: *Supporting Location-based Conditions in Access Control Policies*. In *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, ASIACCS '06. ACM (2006), Seiten 212–222.

[9] C.A. Ardagna, M. Cremonini, S. De Capitani di Vimercati und P. Samarati: *Access Control in Location-Based Services*. In *Privacy in Location-Based Applications*, herausgegeben von C. Bettini, S. Jajodia, P. Samarati und X. Wang, Band 5599 von *Lecture Notes in Computer Science*. Springer (2009), Seiten 106–126.

[10] V. Atluri und W. Huang: *An Authorization Model for Workflows*. In *Computer Security - ESORICS 96*, herausgegeben von E. Bertino, H. Kurth, G. Martella und E. Montolivo, Band 1146 von *Lecture Notes in Computer Science*. Springer (1996), Seiten 44–64.

[11] P. Bahl und V. Padmanabhan: *RADAR: An In-Building RF-based User Location and Tracking System*. In *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies*, INFOCOM '00. IEEE (2000), Seiten 775–784.

[12] C. Beder, A. McGibney und M. Klepal: *Predicting the Expected Accuracy for Fingerprinting Based WiFi Localisation Systems*. In *Proceedings of the 2011 International Conference on Indoor Positioning and Indoor Navigation*, IPIN '11. IEEE (2011), Seiten 1–6.

[13] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved und S. Möller: *On the Need For Different Security Methods on Mobile Phones*. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, MobileHCI '11. ACM (2011), Seiten 465–473.

[14] T. Benesch: *Schlüsselkonzepte zur Statistik*. Springer, 2013.

[15] E. Bertino, B. Catania, M.L. Damiani und P. Perlasca: *GEO-RBAC: A Spatially Aware RBAC*. In *Proceedings of the 10th ACM Symposium on Access Control Models and Technologies*, SACMAT '05. ACM (2005), Seiten 29–37.

[16] E. Bertino und M.S. Kirkpatrick: *Location-based Access Control Systems for Mobile Users: Concepts and Research Directions*. In *Proceedings of the 4th ACM SIGSPATIAL International Workshop on Security and Privacy in GIS and LBS*, SPRINGL '11. ACM (2011), Seiten 49–52.

[17] R. Bhatti, M. Damiani, D. Bettis und E. Bertino: *Policy Mapper: Administering Location-Based Access-Control Policies*. In *Internet Computing*, Jahrgang 12, Nummer 2. IEEE (2008), Seiten 38–45.

[18] R. Bhatti, A. Ghafoor, E. Bertino und J.B.D. Joshi: *X-GTRBAC: An XML-based Policy Specification Framework and Architecture for Enterprise-wide Access Control*. In *ACM Transactions on Information and System Security*, Jahrgang 8, Nummer 2. ACM (2005), Seiten 187–227.

[19] G. Bordogna, M. Pagani, G. Pasi und G. Psaila: *Evaluating Uncertain Location-based Spatial Queries*. In *Proceedings of the 2008 ACM Symposium on Applied Computing*, SAC '08. ACM (2008), Seiten 1095–1100.

[20] L. Cai und H. Chen: *TouchLogger: Inferring Keystrokes on Touch Screen from Smartphone Motion*. In *Proceedings of the 6th USENIX Conference on Hot Topics in Security*, HotSec '11. USENIX Association (2011), Seiten 1–6.

[21] S.M. Chandran und J.B.D. Joshi: *LoT-RBAC: A Location and Time-Based RBAC Model*. In *Web Information Systems Engineering - WISE 2005*, herausgegeben von A. H. Ngu, M. Kitsuregawa, E. J. Neuhold, J.-Y. Chung und Q. Z. Sheng, Band 3806 von *Lecture Notes in Computer Science*. Springer (2005), Seiten 361–375.

[22] J. Chen und R. Cheng: *Efficient Evaluation of Imprecise Location-Dependent Queries*. In *Proceedings of the IEEE 23rd International Conference on Data Engineering*, ICDE '07 (2007), Seiten 586–595.

[23] L. Chen und J. Crampton: *On Spatio-temporal Constraints and Inheritance in Role-based Access Control*. In *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, ASIACCS '08. ACM (2008), Seiten 205–216.

[24] P.C. Cheng, P. Rohatgi, C. Keser, P. Karger, G. Wagner und A. Reninger: *Fuzzy Multi-Level Security: An Experiment on Quantified Risk-Adaptive Access Control*. In *Proceedings of the 2007 IEEE Symposium on Security and Privacy*, SP '07. IEEE (2007), Seiten 222–230.

[25] R. Cheng, L. Chen, J. Chen und X. Xie: *Evaluating Probability Threshold k-Nearest-Neighbor Queries Over Uncertain Data*. In *Proceedings of the 12th International Conference on Extending Database Technology: Advances in Database Technology*, EDBT '09. ACM (2009), Seiten 672–683.

[26] R. Cheng, Y. Xia, S. Prabhakar, R. Shah und J.S. Vitter: *Efficient Indexing Methods for Probabilistic Threshold Queries over Uncertain Data*. In *Proceedings of the 30th International Conference on Very Large Data Bases*, VLDB '04. VLDB Endowment (2004), Seiten 876–887.

[27] L. Cirio, I. Cruz und R. Tamassia: *A Role and Attribute Based Access Control System Using Semantic Web Technologies*. In *On the Move to Meaningful Internet Systems 2007: OTM 2007 Workshops*, herausgegeben von R. Meersman, Z. Tari und P. Herrero, Band 4806 von *Lecture Notes in Computer Science*. Springer (2007), Seiten 1256–1266.

[28] A.v. Cleeff, W. Pieters und R. Wieringa: *Benefits of Location-Based Access Control: A Literature Study*. In *Proceedings of the 2010 IEEE/ACM International Conference on Green Computing and Communications & International Conference on Cyber,*

Physical and Social Computing, GREENCOM-CPSCOM '10. IEEE (2010), Seiten 739–746.

[29] M. Conti, I. Zachia-Zlatea und B. Crispo: *Mind How You Answer Me!: Transparently Authenticating the User of a Smartphone When Answering or Placing a Call*. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11. ACM (2011), Seiten 249–259.

[30] M.J. Covington, W. Long, S. Srinivasan, A.K. Dev, M. Ahamad und G.D. Abowd: *Securing Context-aware Applications Using Environment Roles*. In *Proceedings of the 6th ACM Symposium on Access Control Models and Technologies*, SACMAT '01. ACM (2001), Seiten 10–20.

[31] M.J. Covington, M.J. Moyer und M. Ahamad: *Generalized Role-Based Access Control for Securing Future Applications*. Technischer Bericht GIT-CC-00-02. Georgia Institute of Technology (2002). URL: `http://hdl.handle.net/1853/6580`, zuletzt besucht am 12.03.2015.

[32] F.C. Crow: *Summed-area Tables for Texture Mapping*. In *Proceedings of the 11th Annual Conference on Computer Graphics and Interactive Techniques*, SIGGRAPH '84. ACM (1984), Seiten 207–212.

[33] I.F. Cruz, R. Gjomemo, B. Lin und M. Orsini: *A Location Aware Role and Attribute Based Access Control System*. In *Proceedings of the 16th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, GIS '08. ACM (2008), Seiten 1–2.

[34] M. Damiani und E. Bertino: *Access Control and Privacy in Location-Aware Services for Mobile Organizations*. In *Proceedings of the 7th International Conference on Mobile Data Management*, MDM '06. IEEE (2006), Seiten 1–11.

[35] M. Damiani, E. Bertino und C. Silvestri: *Approach to Supporting Continuity of Usage in Location-Based Access Control*. In *Proceedings of the 12th IEEE International Workshop on Future Trends of Distributed Computing Systems*, FTDCS '08. IEEE (2008), Seiten 199–205.

[36] M.L. Damiani, H. Martin, Y. Saygin, M.R. Spada und C. Ulmer: *Spatio-temporal Access Control: Challenges and Applications*. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*, SACMAT '09. ACM (2009), Seiten 175–176.

[37] M.L. Damiani und C. Silvestri: *Towards Movement-aware Access Control*. In *Proceedings of the SIGSPATIAL ACM GIS 2008 International Workshop on Security and Privacy in GIS and LBS*, SPRINGL '08. ACM (2008), Seiten 39–45.

[38] A. De Luca, A. Hang, F. Brudy, C. Lindner und H. Hussmann: *Touch Me Once and I Know It's You!: Implicit Authentication Based on Touch Screen Patterns*. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '12. ACM (2012), Seiten 987–996.

[39] M. De Marsico, C. Galdi, M. Nappi und D. Riccio: *FIRME: Face and Iris Recognition for Mobile Engagement*. In *Image and Vision Computing*, Jahrgang 32, Nummer 12. Elsevier (2014), Seiten 1161–1172.

[40] M. Decker: *Requirements for a Location-based Access Control Model*. In *Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia*, MoMM '08. ACM (2008), Seiten 346–349.

[41] M. Decker: *A Location-Aware Access Control Model for Mobile Workflow Systems*. In *International Journal of Information Technology and Web Engineering*, Jahrgang 4, Nummer 1. IGI Global (2009), Seiten 50–66.

[42] M. Decker: *Modelling Location-Aware Access Control Constraints for Mobile Workflows with UML Activity Diagrams*. In *Proceedings of the 3rd International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, UBICOMM '09. IEEE (2009), Seiten 263–268.

[43] M. Decker, A. Oberweis und P. Stürzel: *Ortsabhängiger Dokumentenzugriff mit Discretionary Access Control*. In *Mobile und Ubiquitäre Informationssysteme*, herausgegeben von M. Bick, S. Eulgem, E. Fleisch, J. F. Hampe, B. König-Ries, F. Lehner, K. Pousttchi und K. Rannenberg, Band 163 von *Lecture Notes in Informatics*. Gesellschaft für Informatik (2010), Seiten 153–166.

[44] M. Decker, P. Stürzel, S. Klink und A. Oberweis: *Location Constraints for Mobile Workflows*. In *Proceedings of the 2009 Conference on Techniques and Applications for Mobile Commerce*, TAMoCo '09. IOS Press (2009), Seiten 93–102.

[45] D.E. Denning und P.F. MacDoran: *Location-based Authentication: Grounding Cyberspace for Better Security*. In *Computer Fraud & Security*, Jahrgang 1996, Nummer 2. Elsevier (1996), Seiten 12–16.

[46] M.O. Derawi, C. Nickel, P. Bours und C. Busch: *Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition*. In *Proceedings of the 2010 6th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IIH-MSP '06. IEEE (2010), Seiten 306–311.

[47] A.K. Dey: *Understanding and Using Context*. In *Personal and Ubiquitous Computing*, Jahrgang 5, Nummer 1. Springer (2001), Seiten 4–7.

[48] S. Dhar und U. Varshney: *Challenges and Business Models for Mobile Location-based Services and Advertising*. In *Communications of the ACM*, Jahrgang 54, Nummer 5. ACM (2011), Seiten 121–128.

[49] C. Eckert: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*. 9. Auflage. De Gruyter Oldenbourg, 2014.

[50] J.E. Ekberg und M. Kylänpää: *Mobile Trusted Module (MTM) - An Introduction*. Technischer Bericht NRC-TR-2007-015. Nokia Research Center (2007). URL: `http://research.nokia.com/sites/default/files/tr/NRC-TR-2007-015.pdf`, zuletzt besucht am 28.02.2015.

[51] E. Elnahrawy, X. Li und R. Martin: *The Limits of Localization Using Signal Strength: A Comparative Study*. In *Proceedings of the First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks*, SECON '04. IEEE (2004), Seiten 406–414.

[52] *Estimote Beacons*. URL: `http://estimote.com/`, zuletzt besucht am 20.03.2015.

[53] F. Evennou und F. Marx: *Advanced Integration of WIFI and Inertial Navigation Systems for Indoor Mobile Positioning*. In *EURASIP Journal on Advances in Signal Processing*, Jahrgang 2006, Nummer 1. Springer (2006), Seiten 164–164.

[54] N. Fallah, I. Apostolopoulos, K. Bekris und E. Folmer: *Indoor Human Navigation Systems: A Survey*. In *Interacting with Computers*, Jahrgang 25, Nummer 1. Oxford University Press (2013), Seiten 21–33.

[55] R. Filjar, L. Bušić und P. Pikija: *Improving the LBS QoS Through Implementation of QoS Negotiation Algorithm*. In *31st International Convention Proceedings: Microelectronics, Electronics and Electronic Technology, MEET and Grid and Visualizations Systems, GV*, MIPRO '08 (2008), Seiten 1–4. URL: `http://www.ericsson.com/hr/etk/dogadjanja/mipro_2008/1174.pdf`, zuletzt besucht am 27.03.2015.

[56] J. Finnis, N. Saigal, A. Iamnitchi und J. Ligatti: *A Location-based Policy-specification Language for Mobile Devices*. In *Pervasive and Mobile Computing*, Jahrgang 8, Nummer 3. Elsevier (2012), Seiten 402–414.

[57] S. Fu und C.Z. Xu: *A Coordinated Spatio-Temporal Access Control Model for Mobile Computing in Coalition Environments*. In *Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium*, IPDPS '05. IEEE (2005), Seiten 1–8.

[58] C. Gao, Z. Yu, Y. Wei, S. Russell und Y. Guan: *A Statistical Indoor Localization Method for Supporting Location-based Access Control*. In *Mobile Networks and Applications*, Jahrgang 14, Nummer 2. Kluwer Academic Publishers (2009), Seiten 253–263.

[59] P. Gilbert, L.P. Cox, J. Jung und D. Wetherall: *Toward Trustworthy Mobile Sensing*. In *Proceedings of the 11th Workshop on Mobile Computing Systems and Applications*, HotMobile '10. ACM (2010), Seiten 31–36.

[60] P. Gilbert, J. Jung, K. Lee, H. Qin, D. Sharkey, A. Sheth und L.P. Cox: *YouProve: Authenticity and Fidelity in Mobile Sensing.* In *Proceedings of the 9th ACM Conference on Embedded Networked Sensor Systems*, SenSys '11. ACM (2011), Seiten 176–189.

[61] C. Gomez, J. Oller und J. Paradells: *Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-power Wireless Technology.* In *Sensors*, Jahrgang 12, Nummer 9. Molecular Diversity Preservation International (2012), Seiten 11 734–11 753.

[62] *Global Positioning System Standard Positioning Service Performance Standard.* Standard 4. Auflage. U.S. Department of Defense (2008). URL: `http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf`, zuletzt besucht am 20.03.2015.

[63] F. Hansen und V. Oleshchuk: *SRBAC: A Spatial Role-based Access Control Model For Mobile Systems.* In *Proceedings of the 7th Nordic Workshop on Secure IT Systems*, NORDSEC '03. Norwegian University of Science and Technology (2003), Seiten 129–141.

[64] W. He, X. Liu und M. Ren: *Location Cheating: A Security Challenge to Location-Based Social Network Services.* In *Proceedings of the 31st International Conference on Distributed Computing Systems*, ICDCS '11. IEEE (2011), Seiten 740–749.

[65] J. Hightower und G. Borriello: *Particle Filters for Location Estimation in Ubiquitous Computing: A Case Study.* In *UbiComp 2004: Ubiquitous Computing*, herausgegeben von N. Davies, E. Mynatt und I. Siio, Band 3205 von *Lecture Notes in Computer Science*. Springer (2004), Seiten 88–106.

[66] V. Honkavirta, T. Perala, S. Ali-Loytty und R. Piche: *A Comparative Survey of WLAN Location Fingerprinting Methods.* In *Proceedings of the 6th Workshop on Positioning, Navigation and Communication*, WPNC '09. IEEE (2009), Seiten 243–251.

[67] S. Ilarri, E. Mena und A. Illarramendi: *Location-dependent Query Processing: Where We Are and Where We Are Heading.* In *ACM Computing Surveys (CSUR)*, Jahrgang 42, Nummer 3. ACM (2010), Seiten 1–73.

[68] *Safety of Machinery - Emergency Stop - Principles For Design, ISO 13850.* ISO, Genf, Schweiz2006.

[69] *Accuracy (Trueness and Precision) of Measurement Methods and Results – Part 1: General Principles and Definitions, ISO 5725-1.* ISO, Genf, Schweiz1994.

[70] K. Kaemarungsi und P. Krishnamurthy: *Properties of Indoor Received Signal Strength For WLAN Location Fingerprinting.* In *Proceedings of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services*, MOBIQUITOUS '04. IEEE (2004), Seiten 14–23.

[71] M. Kessel: *Bereitstellung von Umgebungsinformationen und Positionsdaten für ortsbezogene Dienste in Gebäuden.* `http://nbn-resolving.de/urn:nbn:de:bvb:19-159785`, Ludwig-Maximilians-Universität München, Dissertation, Juli 2013.

[72] M. Kessel und M. Werner: *SMARTPOS: Accurate and Precise Indoor Positioning on Mobile Phones.* In *Proceedings of the 1st International Conference on Mobile Services, Resources, and Users*, MOBILITY '11. ThinkMind (2011), Seiten 158–163.

[73] M. Kessel und M. Werner: *Automated WLAN Calibration With a Backtracking Particle Filter.* In *Proceedings of the 2012 International Conference on Indoor Positioning and Indoor Navigation*, IPIN '12. IEEE (2012), Seiten 1–10.

[74] *Key Lemon – Face Recognition Technology.* URL: `www.keylemon.com`, zuletzt besucht am 20.03.2015.

[75] D.J. Kim, K.W. Chung und K.S. Hong: *Person Authentication Using Face, Teeth and Voice Modalities For Mobile Device Security.* In *IEEE Transactions on Consumer Electronics*, Jahrgang 56, Nummer 4. IEEE (2010), Seiten 2678–2685.

[76] M.S. Kirkpatrick und E. Bertino: *Enforcing Spatial Constraints for Mobile RBAC Systems.* In *Proceedings of the 15th ACM Symposium on Access Control Models and Technologies*, SACMAT '10. ACM (2010), Seiten 99–108.

[77] M.S. Kirkpatrick, M.L. Damiani und E. Bertino: *Prox-RBAC: A Proximity-based Spatially Aware RBAC.* In *Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, GIS '11. ACM (2011), Seiten 339–348.

[78] M. Kjærgaard: *A Taxonomy for Radio Location Fingerprinting.* In *Location- and Context-Awareness*, herausgegeben von J. Hightower, B. Schiele und T. Strang, Band 4718 von *Lecture Notes in Computer Science*. Springer (2007), Seiten 139–156.

[79] S.G. Kong, J. Heo, B.R. Abidi, J. Paik und Mongi A. Abidi: *Recent Advances in Visual and Infrared Face Recognition - a Review.* In *Computer Vision and Image Understanding*, Jahrgang 97, Nummer 1. Elsevier (2005), Seiten 103–135.

[80] S. Kotz, T. Kozubowski und K. Podgorski: *The Laplace Distribution and Generalizations: A Revisit With Applications to Communications, Exonomics, Engineering, and Finance.* Birkäuser Boston, 2001.

[81] L. Krautsevich, A. Lazouski, F. Martinelli und A. Yautsiukhin: *Influence of Attribute Freshness on Decision Making in Usage Control.* In *Security and Trust Management*, herausgegeben von J. Cuellar, J. Lopez, G. Barthe und A. Pretschner, Band 6710 von *Lecture Notes in Computer Science*. Springer (2011), Seiten 35–50.

[82] L. Krautsevich, A. Lazouski, F. Martinelli und A. Yautsiukhin: *Cost-Effective Enforcement of Access and Usage Control Policies Under Uncertainties*. In *IEEE Systems Journal*, Jahrgang 7, Nummer 2. IEEE (2013), Seiten 223–235.

[83] D. Kulkarni und A. Tripathi: *Context-aware Role-based Access Control in Pervasive Computing Systems*. In *Proceedings of the 13th ACM Symposium on Access Control Models and Technologies*, SACMAT '08. ACM (2008), Seiten 113–122.

[84] A. Kumar, N. Karnik und G. Chafle: *Context Sensitivity in Role-based Access Control*. In *ACM SIGOPS Operating Systems Review*, Jahrgang 36, Nummer 3. ACM (2002), Seiten 53–66.

[85] A. Küpper: *Location-Based Services: Fundamentals and Operation*. Wiley, 2005.

[86] N.D. Lane, E. Miluzzo, H. Lu, D. Peebles, T. Choudhury und A.T. Campbell: *A Survey of Mobile Phone Sensing*. In *IEEE Communications Magazine*, Jahrgang 48, Nummer 9. IEEE (2010), Seiten 140–150.

[87] H. Lemelson, M.B. Kjærgaard, R. Hansen und T. King: *Error Estimation for Indoor 802.11 Location Fingerprinting*. In *Location and Context Awareness*, herausgegeben von T. Choudhury, A. Quigley, T. Strang und K. Suginuma, Band 5561 von *Lecture Notes in Computer Science*. Springer (2009), Seiten 138–155.

[88] L. Li, X. Zhao und G. Xue: *Unobservable Re-authentication for Smartphones*. In *Proceedings of the 20th Annual Network and Distributed System Security Symposium*, NDSS '13. The Internet Society (2013), Seiten 1–16.

[89] H. Liu, H. Darabi, P.P. Banerjee und J. Liu: *Survey of Wireless Indoor Positioning Techniques and Systems*. In *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, Jahrgang 37, Nummer 6. IEEE (2007), Seiten 1067–1080.

[90] H. Liu und M. Schneider: *Querying Moving Objects with Uncertainty in Spatio-Temporal Databases*. In *Database Systems for Advanced Applications*, herausgegeben von J. Yu, M. Kim und R. Unland, Band 6587 von *Lecture Notes in Computer Science*. Springer (2011), Seiten 357–371.

[91] J. Machaj, P. Brida und N. Majer: *Novel Criterion to Evaluate QoS of Localization Based Services*. In *Intelligent Information and Database Systems*, herausgegeben von J.-S. Pan, S.-M. Chen und N. Nguyen, Band 7197 von *Lecture Notes in Computer Science*. Springer (2012), Seiten 381–390.

[92] J. Mäntyjärvi, M. Lindholm, E. Vildjiounaite, S. Mäkelä und H. Ailisto: *Identifying Users of Portable Devices From Gait Pattern With Accelerometers*. In *Proceedings of the 2005 IEEE International Conference on Acoustics, Speech, and Signal Processing*, ICASSP '05. IEEE (2005), Seiten 973–976.

[93] P. Marcus, M. Kessel und M. Dürr: *Regelgesteuerte Auswertungsrichtlinien für LBAC–Systeme.* In *8. Gi/KuVS–Fachgespräch, Ortsbezogene Anwendungen und Dienste*, herausgegeben von M. Werner und J. Roth. Logos (September 2011), Seiten 75–86.

[94] P. Marcus, M. Kessel und C. Linnhoff-Popien: *Securing Mobile Device-Based Machine Interactions with User Location Histories.* In *Security and Privacy in Mobile Information and Communication Systems*, herausgegeben von A. Schmidt, G. Russello, I. Krontiris und S. Lian, Band 107 von *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering.* Springer (2012), Seiten 81–92.

[95] P. Marcus, M. Kessel und C. Linnhoff-Popien: *Enabling Trajectory Constraints for Usage Control Policies With Backtracking Particle Filters.* In *Proceedings of the 3rd International Conference on Mobile Services, Resources, and Users*, MOBILITY '13. ThinkMind (2013), Seiten 52–58.

[96] P. Marcus, M. Kessel und M. Werner: *Dynamic Nearest Neighbors and Online Error Estimation for SMARTPOS.* In *International Journal On Advances in Internet Technology*, Jahrgang 6, Nummer 1 und 2. ThinkMind (2013), Seiten 1–11.

[97] P. Marcus und C. Linnhoff-Popien: *Efficient Evaluation of Location Predicates for Access Control Systems.* In *Proceedings of the 2012 6th UKSim/AMSS European Symposium on Computer Modeling and Simulation*, EMS '12. IEEE (2012), Seiten 385–390.

[98] P. Marcus und C. Linnhoff-Popien: *Handling Positioning Errors in Location-based Services.* In *Proceedings of the 8th International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies*, UBICOMM '14. Thinkmind (2014), Seiten 1–6.

[99] P. Marcus und C. Linnhoff-Popien: *Quality Estimation for Zone-based LBS under Realistic Positioning Systems.* In *Proceedings of the 3rd International Conference on Context-Aware Systems and Applications*, ICCASA '14. ICST (2014), Seiten 42–47.

[100] P. Marcus, L. Schauer und C. Linnhoff-Popien: *Location-Aware RBAC Based on Spatial Feature Models and Realistic Positioning.* In *Risks and Security of Internet and Systems - 9th International Conference, CRiSIS 2014, Trento, Italy, August 27-29, 2014, Revised Selected Papers*, herausgegeben von J. Lopez, I. Ray und B. Crispo, Band 8924 von *Lecture Notes in Computer Science.* Springer (2014), Seiten 131–147.

[101] I. Martín-Escalona und F. Barceló-Arroyo: *QoS-driven Middleware For Optimum Provisioning of Location Based Services.* In *Proceedings of the 2nd International Conference on Communication System Software and Middleware*, COMSWARE 2007. IEEE (2007), Seiten 1–6.

[102] A. Matheus und J. Herrmann: *Geospatial eXtensible Access Control Markup Language (GeoXACML)*. OGC Implementation Standard 07-026r2. Open Geospatial Consortium Inc. (2008). URL: `http://portal.opengeospatial.org/files/?artifact_id=25218`, zuletzt besucht am 16.03.2015.

[103] H.B. Menz, S.R. Lord und R.C. Fitzpatrick: *Acceleration Patterns of the Gead and Pelvis When Walking on Level and Irregular Surfaces*. In *Gait & Posture*, Jahrgang 18, Nummer 1. Elsevier (2003), Seiten 35–46.

[104] A. Mishra, M. Shin und W. Arbaugh: *An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process*. In *ACM SIGCOMM Computer Communication Review*, Jahrgang 33, Nummer 2. ACM (2003), Seiten 93–102.

[105] V. Moghtadaiee, A. Dempster und B. Li: *Accuracy Indicator For Fingerprinting Localization Systems*. In *Proceedings of the 2012 IEEE/ION Position Location and Navigation Symposium*, PLANS '12. IEEE (April 2012), Seiten 1204–1208.

[106] F.W. Olver, D.W. Lozier, R.F. Boisvert und C.W. Clark: *NIST Handbook of Mathematical Functions*. 1. Auflage. Cambridge University Press, 2010.

[107] S. Osborn, R. Sandhu und Q. Munawer: *Configuring Role-based Access Control to Enforce Mandatory and Discretionary Access Control Policies*. In *ACM Transactions on Information and System Security (TISSEC)*, Jahrgang 3, Nummer 2. ACM (2000), Seiten 85–106.

[108] K. Pahlavan und A.H. Levesque: *Wireless Information Networks*. 2. Auflage. John Wiley & Sons, 2005.

[109] J. Park und R. Sandhu: *The UCONABC Usage Control Model*. In *ACM Transactions on Information and System Security*, Jahrgang 7, Nummer 1. ACM (2004), Seiten 128–174.

[110] W.R. Pestman: *Mathematical Statistics*. De Gruyter, 2009.

[111] M. Peterson: *An Introduction to Decision Theory*. Cambridge University Press, 2009.

[112] S. Ravada, M. Ali, J. Bao und M. Sarwat: *ACM SIGSPATIAL GIS Cup 2013: Geofencing*. In *Proceedings of the 21st ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, SIGSPATIAL'13. ACM (2013), Seiten 584–587.

[113] I. Ray und M. Kumar: *Towards a Location-based Mandatory Access Control Model*. In *Computers & Security*, Jahrgang 25, Nummer 1. Elsevier (2006), Seiten 36 – 44.

[114] I. Ray, M. Kumar und L. Yu: *LRBAC: A Location-Aware Role-Based Access Control Model*. In *Information Systems Security*, herausgegeben von A. Bagchi und V. Atluri, Band 4332 von *Lecture Notes in Computer Science*. Springer (2006), Seiten 147–161.

[115] I. Ray und M. Toahchoodee: *A Spatio-temporal Role-Based Access Control Model*. In *Data and Applications Security XXI*, herausgegeben von S. Barker und G.-J. Ahn, Band 4602 von *Lecture Notes in Computer Science*. Springer (2007), Seiten 211–226.

[116] E. Rissanen: *eXtensible Access Control Markup Language (XACML) Version 3.0*. OASIS Standard xacml-3.0-core-spec-os-en. OASIS (Januar 2013). URL: `http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf`, zuletzt besucht am 16.03.2015.

[117] S. Rodriguez Garzon und B. Deva: *Geofencing 2.0: Taking Location-based Notifications to the Next Level*. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*, UbiComp '14. ACM (2014), Seiten 921–932.

[118] M. Roshanaei und M. Maleki: *Dynamic-KNN: A Novel Locating Method in WLAN Based on Angle of Arrival*. In *Proceedings of the IEEE Symposium on Industrial Electronics and Applications*, Band 2 von *ISIEA '09*. IEEE (2009), Seiten 722–726.

[119] S.J. Russell und P. Norvig: *Artificial Intelligence: A Modern Approach*. 3. Auflage. Prentice Hall, 2010.

[120] J. Ryoo, H. Kim und S.R. Das: *Geo-fencing: Geographical-fencing Based Energy-aware Proactive Framework for Mobile Devices*. In *Proceedings of the 2012 IEEE 20th International Workshop on Quality of Service*, IWQoS '12. IEEE (2012), Seiten 1–9.

[121] R. Sandhu, E.J. Coyne, H.L. Feinstein und C.E. Youman: *Role-Based Access Control Models*. In *Computer*, Jahrgang 29, Nummer 2. IEEE (1996), Seiten 38–47.

[122] R. Sandhu, D. Ferraiolo und R. Kuhn: *The NIST Model for Role-based Access Control: Towards a Unified Standard*. In *Proceedings of the 5th ACM Workshop on Role-based Access Control*, RBAC '00. ACM (2000), Seiten 47–63.

[123] R. Sandhu und J. Park: *Usage Control: A Vision for Next Generation Access Control*. In *Computer Network Security*, herausgegeben von V. Gorodetsky, L. Popyack und V. Skormin, Band 2776 von *Lecture Notes in Computer Science*. Springer Berlin Heidelberg (2003), Seiten 17–31.

[124] N. Sastry, U. Shankar und D. Wagner: *Secure Verification of Location Claims*. In *Proceedings of the 2nd ACM Workshop on Wireless Security*, WiSe '03. ACM (2003), Seiten 1–10.

[125] L. Schauer, F. Dorfmeister und M. Maier: *Potentials and Limitations of WIFI-Positioning Using Time-of-Flight*. In *Proceedings of the 2013 International Conference on Indoor Positioning and Indoor Navigation*, IPIN '13. IEEE (2013), Seiten 1–9.

[126] T. Scheidat, M. Biermann, J. Dittmann, C. Vielhauer und K. Kümmel: *Multibiometric Fusion for Driver Authentication on the Example of Speech and Face.* In *Biometric ID Management and Multimodal Communication*, herausgegeben von J. Fierrez, J. Ortega-Garcia, A. Esposito, A. Drygajlo und M. Faundez-Zanuy, Band 5707 von *Lecture Notes in Computer Science*. Springer (2009), Seiten 220–227.

[127] F. Seco, A. Jimenez, C. Prieto, J. Roa und K. Koutsou: *A Survey of Mathematical Methods for Indoor Localization.* In *Proceedings of the 2009 IEEE International Symposium on Intelligent Signal Processing*, WISP '09. IEEE (Aug 2009), Seiten 9–14.

[128] W. Shi, J. Yang, Y. Jiang, F. Yang und Y. Xiong: *Senguard: Passive User Identification on Smartphones Using Multiple Sensors.* In *Proceedings of the 2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications*, WiMob '11. IEEE (2011), Seiten 141–148.

[129] B. Shin, J.H. Lee, T. Lee und H.S. Kim: *Enhanced Weighted k-Nearest Neighbor Algorithm for Indoor Wi-Fi Positioning Systems.* In *Proceedings of the 8th International Conference on Computing Technology and Information Management*, Band 2 von *ICCM '12*. IEEE (April 2012), Seiten 574–577.

[130] H. Shin und V. Atluri: *Spatiotemporal Access Control Enforcement under Uncertain Location Estimates.* In *Data and Applications Security XXIII*, herausgegeben von E. Gudes und J. Vaidya, Band 5645 von *Lecture Notes in Computer Science*. Springer (2009), Seiten 159–174.

[131] H. Shin, V. Atluri und J. Cho: *Efficiently Enforcing Spatiotemporal Access Control Under Uncertain Location Information.* In *Journal of Computer Security*, Jahrgang 19, Nummer 3. IOS Press (2011), Seiten 607–637.

[132] I. Sommerville: *Software Engineering.* 8. Auflage. Pearson Studium, 2006.

[133] S. Sonkamble, R. Thool und B. Sonkamble: *Survey of Biometric Recognition Systems and Their Applications.* In *Journal of Theoretical & Applied Information Technology*, Jahrgang 11, Nummer 1 und 2. EBSCO Industries (2010), Seiten 45–71.

[134] S. Spaccapietra, C. Parent, M.L. Damiani, J.A. de Macedo, F. Porto und C. Vangenot: *A Conceptual View on Trajectories.* In *Data & Knowledge Engineering*, Jahrgang 65, Nummer 1. Elsevier (2008), Seiten 126–146.

[135] M. Strembeck und G. Neumann: *An Integrated Approach to Engineer and Enforce Context Constraints in RBAC Environments.* In *ACM Transactions on Information and System Security*, Jahrgang 7, Nummer 3. ACM (2004), Seiten 392–427.

[136] S. Thrun, W. Burgard und D. Fox: *Probabilistic Robotics.* The MIT Press, 2005.

[137] M. Toahchoodee und I. Ray: *On the Formalization and Analysis of a Spatio-temporal Role-based Access Control Model*. In *Journal of Computer Security*, Jahrgang 19, Nummer 3. IOS Press (2011), Seiten 399–452.

[138] D.T. Toledano, R.F. Pozo, Á.H. Trapote und L.H. Gómez: *Usability Evaluation of Multi-modal Biometric Verification Systems*. In *Interacting with Computers*, Jahrgang 18, Nummer 5. Oxford University Press (2006), Seiten 1101–1122.

[139] G. Trajcevski: *Uncertainty in Spatial Trajectories*. In *Computing with Spatial Trajectories*, herausgegeben von Y. Zheng und X. Zhou. Springer (2011), Seiten 63–107.

[140] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh und S. Ben-David: *Biometric Authentication on a Mobile Device: A Study of User Effort, Error and Task Disruption*. In *Proceedings of the 28th Annual Computer Security Applications Conference*, ACSAC '12. ACM (2012), Seiten 159–168.

[141] M. Trojahn und P. Marcus: *Towards Coupling User and Device Locations Using Biometrical Authentication on Smartphones*. In *Proceedings of the 7th International Conference for Internet Technology and Secured Transactions*, ICITST '12. IEEE (2012), Seiten 736–741.

[142] M. Trojahn und F. Ortmeier: *Biometric authentication Through a Virtual Keyboard For Smartphones*. In *International Journal of Computer Science & Information Technology*, Jahrgang 4, Nummer 5. AIRCC (2012), Seiten 1–12.

[143] D. Tse und P. Viswanath: *Fundamentals of Wireless Communication*. Cambridge University Press, 2005.

[144] N. Ulltveit-Moe und V. Oleshchuk: *Mobile Security with Location-Aware Role-Based Access Control*. In *Security and Privacy in Mobile Information and Communication Systems*, herausgegeben von R. Prasad, K. Farkas, A. Schmidt, A. Lioy, G. Russello und F. Luccio, Band 94 von *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*. Springer (2012), Seiten 172–183.

[145] *unwiredlabs LocationAPI*. URL: `http://unwiredlabs.com/`, zuletzt besucht am 20.03.2015.

[146] Widyawan, M. Klepal und S. Beauregard: *A Novel Backtracking Particle Filter for Pattern Matching Indoor Localization*. In *Proceedings of the 1st ACM International Workshop on Mobile Entity Localization and Tracking in GPS-less Environments*, MELT '08. ACM (2008), Seiten 79–84.

[147] M. Youssef und A. Agrawala: *The Horus WLAN Location Determination System*. In *Proceedings of the 3rd International Conference on Mobile Systems, Applications, and Services*, MobiSys '05. ACM (2005), Seiten 205–218.

[148] M. Youssef, V. Atluri und N.R. Adam: *Preserving Mobile Customer Privacy: An Access Control System for Moving Objects and Customer Profiles*. In *Proceedings of the 6th International Conference on Mobile Data Management*, MDM '05. ACM (2005), Seiten 67–76.

[149] S. Zahid, M. Shahzad, S. Khayam und M. Farooq: *Keystroke-Based User Identification on Smart Phones*. In *Recent Advances in Intrusion Detection*, herausgegeben von E. Kirda, S. Jha und D. Balzarotti, Band 5758 von *Lecture Notes in Computer Science*. Springer (2009), Seiten 224–243.

[150] P.A. Zandbergen: *Positional Accuracy of Spatial Data: Non-Normal Distributions and a Critique of the National Standard for Spatial Data Accuracy*. In *Transactions in GIS*, Jahrgang 12, Nummer 1. John Wiley & Sons (2008), Seiten 103–130.

[151] P.A. Zandbergen: *Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning*. In *Transactions in GIS*, Jahrgang 13, Nummer S1. John Wiley & Son (2009), Seiten 5–25.