Probabilistic Motion and Intention Prediction for Autonomous Vehicles

Probabilistische Bewegungs- und Intentionsvorausssge fÃijr autonome Fahrzeuge
Master-Thesis von Lina Jukonyte aus Utena, Litauen
Juni 2019

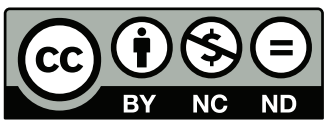
TECHNISCHE
UNIVERSITÄT
DARMSTADT

Probabilistic Motion and Intention Prediction for Autonomous Vehicles
Probabilistische Bewegungs- und Intentionsvorausssge fÃijr autonome Fahrzeuge

Vorgelegte Master-Thesis von Lina Jukonyte aus Utena, Litauen

1. Gutachten: Prof. Jan Peters, Ph.D., Prof. Matthias Hollick, Ph.D.
2. Gutachten: Dorothea Koert, M.Sc., Joni Pajarinen, D.Sc. (Tech.)
3. Gutachten: Dominik PÃijllen, M.Sc.

Tag der Einreichung:



Erklärung zur Master-Thesis

Hiermit versichere ich, die vorliegende Master-Thesis ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die aus Quellen entnommen wurden, sind als solche kenntlich gemacht. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.
In der abgegebenen Thesis stimmen die schriftliche und elektronische Fassung überein.

Darmstadt, den 20. Juni 2019

(Lina Jukonyte)

Thesis Statement

I herewith formally declare that I have written the submitted thesis independently. I did not use any outside support except for the quoted literature and other sources mentioned in the paper. I clearly marked and separately listed all of the literature and all of the other sources which I employed when producing this academic work, either literally or in content. This thesis has not been handed in or published before in the same or similar form.
In the submitted thesis the written copies and the electronic version are identical in content.

Darmstadt, June 20, 2019

(Lina Jukonyte)

Abstract

Decision-making task is one of the most determinant bonds for constructing an autonomous system. Making solid decisions by foreseeing and estimating future consequences on its own, it what makes autonomous systems intelligent. Decision making on its own is already complex task, but for vehicles, it makes more complex because of the uncertainty of the real world and continues vehicles' interaction with other vehicles and obstacles. Sensors which are using for real-world understanding and features as speed, position, other objects of traffic, etc. are noisy and very dependables from external conditions. But again, it is very hard to measure others road users' intentions due to its randomness, additionally, completely or partially visible obstacles of the road can make any received measurements and information useless. The unit responsible for decision making has to be sensible for these issues and be able to foresee the future conditions that could develop in an endless number of ways to achieve the final goal with the maximum reward or, in other words, with a minimum cost of the process.

TODO: add part about what was done in the thesis (at the very end).
Removing a driver from behind the wheel takes away more than just the physical responses. It also eliminates the complex decision-making that goes into even routine journeys – choosing whether to swerve into a neighboring lane to avoid a possible obstacle or navigating ambiguous intersections.

Zusammenfassung

Hier können Sie Ihre deutsche Zusammenfassung schreiben.

Acknowledgments

Contents

Figures and Tables

List of Figures

List of Tables

Abbreviations, Symbols and Operators

1 Introduction

People nowadays can hardly imagine their life without driving. And it is natural since traveling brings independence and freedom to human life. For example, an average American person makes 2.2 driving trips per day and spends 50.6 minutes on the road, which makes over 300 hours every year people spend in their cars [8]. Despite the joy driving brings to people, traffic safety is a major aspect which cannot be ignored. With increasing time which people spend on the cars, a number of a vehicle-related accident is far away from being perfect. The World Health Organization (WHO) annually announce a report which includes a total number of people lives which were taken away due to car accidents. The latest report was published in December of 2018 and stated that during this year there was more than 1.35 million death worldwide [9].
Recent years were full of massive developments towards autonomous driving in autonomous industry. Achievements in one area can be helpful in developing other areas, i.e. great success in image recognition and perception can allow computers to achieve super-human performance [10], etc. Unfortunately, image recognition and environmental perception alone are not enough to solve all the problems of autonomous cars. In ideal circumstances achieving full autonomy of the cars would help not only to save the environment, as well it would benefit traffic participants with more smoothly traffic and more safety on the roads. Industrial innovation experts from ARK Invest strongly believe that with fully autonomous cars accidents on the road would drop to 80% [11].
Although autonomous cars are something that engaging a wide range of engineers for some time already, this area not fully developed yet and will continue engage engineers even more in the future. At the moment big achievement which is equipped into the majority of new cars is Automotive Driver Assistance Systems (ADAS), which for the fact does not enable yet full autonomy of the cars, but it successfully assists driver while driving a car.
It is not a secret that all drivers need to interact with each other non-stop in one way or another while they are driving. This communication together with the individual behaviour of a driver is the main key to traffic safety. The behaviour of the driver can be considered as a combination of current traffic observations, short future forecast, decision making and completing actions. The driver should make decisions and actions with full safety concept for himself and other traffic participants. The same is with fully autonomous vehicles: algorithm which is running while a car is driving should ensure all passengers in the car and other traffic participants safety while making decisions and maneuvering through traffic. It is not hard to understand that one of the biggest problem with both the ADAS systems and the full autonomous cars is the human factor. To improve ADAS systems and achieve safety in fully autonomous cars, prediction methods are essential. Requirements for prediction are precision preciseness (with some time in advance), efficiency and reliability. This thesis will focus on the movement and intention prediction of humans in other cars.

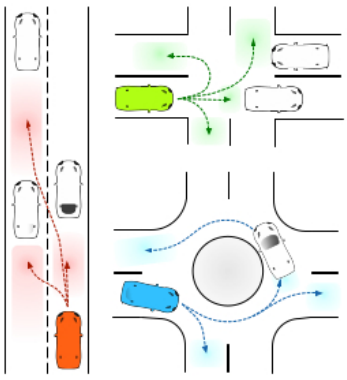


Figure 1.1.: Insertion Areas (Colored Regions) Under Different Driving Scenarios [1]

1.1 Background

Beyond trendy names like Tesla, Google, Aptiv, etc., chasing driverless cars, beyond a large number of automobile brands and other tech engineers, University of Darmstadt (TuD) has its own Autonomous Driving Darmstadt for Students (aDDa) working group [12]. aDDa initiative started on October 2017. A group of students and their supervisors from eight different departments at TuD are working for one purpose to develop fully autonomous car by themselves, here, at University.

All participants of the working group closely cooperate bringing together interdisciplinary know-how experience to jointly set up and operate an autonomous vehicle. One special feature of aDDa is that the main work is done in the context of student projects (final thesis, semester work, permanent work at the team, etc.). By working together on the complex tasks of autonomous driving, participants are solving problems for tomorrow.
In not so long period of glsaDDa existing, it is made a lot of developments and improvement of existing systems. Some works to mention: "Development and Implementation of a Long-Term Dynamics Control for Automated Driving", "Collision Avoidance in Uncertain Environments for Autonomous Vehicles using POMDPs", "Conception and Design of a Camera Mounting and Calibration for Test Vehicle", "Development of an IT Security Concept for an Automated Vehicle, Pedestrian Detection", "Tracking and Intention Prediction in the Context of Autonomous Driving" and much more [12]. This thesis is also a part of aDDa project.

1.2 Purpose

Humans are very irrational and unpredictable and because of that, it is very hard to model them. Moreover, there are no two exact same people, what makes the task to model human behavior almost impossible, since every possible scenario as an endless possible outcome. When an individual is driving it is nearly always necessary to take into account surrounding cars and other traffic participants due to ensure safe, fast and energy optimized journey.
Due to the irrationality of humans and recent success and a still big interest in autonomous cars, the purpose of this thesis is to provide an initial step in a probabilistic collision prediction and decision-making system which aims at producing a risk field for the vehicle that predicts upcoming risks. This step will include creating an algorithm which will use a probabilistic approach and tries to predict future movement and intention of surrounding cars in urban areas.change pictures and maybe explain more about thesis approach in general.
The overall research question is defined as:

- How can probabilistic movement prediction using future estimations be applied for an autonomous vehicle?

This research question is then subdivided into smaller questions and task to achieve during in this research work. Three of these tasks, which are the focus of this thesis, are defined as

- Find/create a probabilistic model that learns from various demonstrations. And use this model for trajectory and intention prediction of the car in front of ego vehicle.
- Investigate if prior information about environment can improve quality of predictions.
- Investigate, how feasible is a probabilistic future movement estimation system, in terms of accuracy and computational time, for real-time applications?

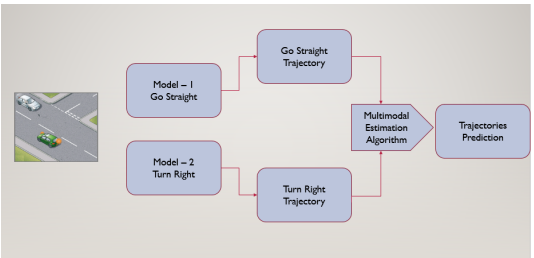


Figure 1.2.: Scheme of Simple Model Based Approach [2]

The most important thing in driving independent of the car is driverless or need a driver is safety. Safety is not possible without security, and considering this, this thesis will provide an overview of the main security and privacy issues on autonomous driving considering movement prediction. Which leads us to the forth and the final research question for this thesis:

- FINALLY DECIDE

1.2.1 Scope of the Thesis

Autonomous systems are very complex by its' nature and it is natural to make substantial limitations to obtain a reasonable scope for a master's thesis. This thesis has been decided to use Robot Operating System (ROS) environment

system, RViz as its' simulation visualization tool, programming part is done in Python and C++ programming languages. Additionally, the evaluated scenarios have been chosen to be T-intersections and crossroads (four-way intersection) with a known environment, limited to only include a single vehicle in addition to the ego vehicle. This choice has been made due to the system complexity, concerning interactions, that multiple cars would introduce. The vehicles in these scenarios are considered to be cars.
Furthermore, some research areas which include image processing, object tracking, mapping and trajectory planning will not be addressed since these areas constitute research areas single-handedly. Incorporating any of these areas would make this thesis even more complex and remove attention from what should be the main focus of the thesis: the probabilistic future movement estimation.

1.3 Thesis Outline

This study focuses on developing and evaluating probabilistic based movement and intention prediction algorithm. This the algorithm uses external cues to predict surrounding vehicles movement in urban situation.
The thesis is organized as follows:

- Chapter 2. **Fundamentals and Related works** focuses foundation of the work and presents a theory behind the scope of the thesis.
- Chapter 3. **Approach** describes approaches of the thesis.
- Chapter 4. **Simulation Setup** defines how and why simulation was set in the way in was. Defines inputs for the system and experiments.
- Chapter 5. **Experiments and Results** describes experiments done during the thesis writing period and evaluate results which were received by performing various experiments.
- Chapter 6. **Security Aspects** is based on the fact that "there is no safety without security" and tries to explain the main security and privacy issues of autonomous cars related to movement predictions.
- Chapter 7. **Conclusion and Future Works** wind up this thesis with conclusions and future works based on the findings of previous chapters.

2 Fundamentals and Related Work

2.1 State of the Art

The most studies related to movement prediction on vehicles focus on lane change predictions. And there are various different methods are proposed to solve this task, the most popular are: Dynamic Bayesian Networks (DBN), Bayesian Networks (BN), Support Vector Machine (SVM), Hidden Markov Model (HMM), Mind-tracing and Fuzzy Logic (FL).
BN could be considered as a graphical representation of probability distribution. In [13, 14] DBN and BN are used to recognize actions which driver is intend to perform. Lateral movement of a vehicle is expressed using BN, having several various nodes for probability. The probability distribution for every node is determined by doing an analysis of driver behaviour in the past while driving. And ultimately, the final prediction is obtained by calculating the probability of a certain movement with respect to the possibility for every node.
In [15, 16] process of driving is described as a set of various different states while driving. When some particular actions appear in particular defined sequence, it is possible to calculate the probability that the state will change to a particular state. In these works likelihood of states shifting is designed using HMM. Authors of [17, 18] expanded their past work using even more realistic test case - they equipped a vehicle with sensors and used received graphical data to get more accurate results. Graphical models together with HMMs and its extensions were trained using the data from experimental driving, seven different driver models were created: passing, changing lanes (to the right or to the left), turning right or left, starting and stopping. The result authors received and presented was "on average, the predictive power of our models is of 1 second before the maneuver starts taking place" [18].
Author of [19] proposed new method for prediction making, which was named Mind-tracing. It is a computational framework which is able to predict possible drivers' intentions. This method is different from others because here different cognitive model versions which include a flood of a possible intention and action is used. Each action and possible intention are compared with a driver's behaviour at the same time. And the closet to the human behaviours is used for the further intentions expression.
[20] introduces FL as an alternative method for modelling behaviour of the driver. The research paper is mainly focused on the process of decision making on lanes of a highway. For getting results a triangular membership function was used, fuzzy rules were defined by observing training procedure and learning from obtained results. The model was developed using actual traffic data. The used model combines the speed and speed difference of the vehicle, the lead and lag gap distances and the remaining distance to the end of the merge lane as input variables. The precision of prediction using the model was higher than using the binary Logit model. The high prediction accuracy received using this model results in prediction accuracy made using this model overall.
[21] tested the validity and accuracy of SVM in movement prediction. After choosing proper hints for movement changing, data recorded by doing test were divided into different groups which were used for training classifier. Predictions were made using current information of the vehicle and classification hints at the current time.
Even though all methods have the same purpose, it is very hard to compare them directly. Results received having measurements in different situations and in different time steps, e.g. one research paper gives prediction two seconds in advance before a lateral position of vehicle's overlaps with the lane border, while other paper gives prediction only one second before crossing the lane. Furthermore, there is no exact definition of *lane crossing* moment, usually, it is the moment when vehicle cross edge of a lane, but in some paper, it is not clear enough.
Since it is not possible to make a clear comparison between methods due to essential differences in testing environments and different data sets, the Table 2.1 lists the best timing accuracy for each method.

As it is possible from the results shown in the table the best methods for predicting movement changes is received by using BN and SVM. These two methods are able to predict quite accurate and with a relatively short period of time, what will lead in having more time in advance to decide which action to make.
For further work, any Bayesian filter/classifier could be an acceptable method for examining behaviour of the driver for various reasons:

- Bayesian-based methods can perform well while working with a very big amount of data;
- It gives results with high accuracy from a problem, containing many features. It is needful to include different physical data while modeling and examining drivers' behaviour. Traditional statistical classifiers most likely to be insufficient while processing high dimensional data.

Table 2.1.: Different Methods Performance Comparison

Method	References	Accuracy	Time
(Dynamic) Bayesian Network	[13]	80%	1.5s before changing movement
	[14]	89%	0.5s after changing movement
Support Vector Machine	[21]	87%	0.3s after changing movement
Hidden Markov Model	[15]	89.4%	2s after changing movement
	[16]	95.2%	2s after changing movement
	[17, 18]	Unknown	0.4s before any sign of changing movement appears
Mind-tracing	[19]	82%	1.1s before changing movement
Fuzzy Logic	[20]	86.8%	Unknown

- Bayesian filter/classifier are robust to over-fitting problem and rely on margin maximization instead of finding an edge for prediction directly from the training data.

2.2 Probabilistic Estimation Methods

Reasonable prediction and following decision-making process require considering uncertainty and objectives for the current situation. In this section, uncertainty will be represented as a probability distribution.
Uncertainty can be a result of partial information about the state of the world. In a real world trying to fulfil any given task, it is possible to meet various reasons which do not allow to finish a task without any difficulties. What means, that with information we have at hand, it is hardly possible to make a task evaluation with being completely certain.
Uncertainty can appear from practical and theoretical limitations while trying to predict future events, e.g., trying to exactly predict how a human would react in one situation or another, a decision support system would need to consider a model of the human brain. Even if the operation is known very well, it is still difficult to predict the end state and next actions which will be taken, due to spontaneous failures or other agent actions.
A robust prediction (and later decision) making system need to take into account sources of uncertainty, which exist in the current state and consider it when computing the future outcomes for events. In order to describe uncertainty computationally, it needs to have a formal representation.

2.2.1 Belief State and Probability

Solving tasks which involve uncertainty, it is very important to be able to compare the credibility of different statements. For example, if belief for action E is stronger than our belief for action T, then E $\succ$ T. If E and T have the same degree of belief, then E $\sim$ T.
It is also beneficial to be able to compare beliefs about statements considering some given information, e.g., we can say that likelihood for action C may happen while E condition is happening is bigger than having T, then this expression would be written (E | C) $\succ$ (T | C).
In order to make particular assumptions about the relationships of the operators $\succ$, $\prec$ and $\sim$. The assumption of *universal comparability* and *transitivity* assumptions requires to hold the same mathematical rules. Both assumptions allow representing degrees of belief by a real-valued function [22], i.e. probability function P can be expressed like that:

$$P(A|C) > P(B|C) \iff (A|C) \succ (B|C)$$

$$P(A|C) = P(B|C) \iff (A|C) \sim (B|C).$$

If new assumptions about the probability P form, then P need to satisfy the main axioms of probability: $0 \leqslant$ P (A | B) $\leqslant$ 1. If we are sure that A action will happen when B action is given then P (A | B) = 1. If A action will not happen when B action is given, then P (A | B) = 0.
Deep review about probability theory won't be provided in here, but this work relies on important probabilities properties. The first of them is a definition of *contidion probability*:

$$P(A|B) = \frac{P(A,B)}{P(B)}, \tag{2.1}$$

where P(A, B) shows the probability of A and B both being true.
Another property which is important is the *law of total probability*, which states that if β is a set of "mutually exclusive and exhaustive propositions" [22], then

$$P(A|C) = \sum_{B \epsilon \beta} P(A|B,C)P(B|C) \tag{2.2}$$

Finally, the most important rule for further work comes from the definition of *conditional probability*:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}. \tag{2.3}$$

This equation is known as ***Bayes' rule***, and as mentioned earlier, it will be very important for the following work.
But still, after this short introduction, question what exactly belied state is, still exists. One option to answer this would be the most believable next state for an examined object, considering experience in the past, which is given. This idea can be sound and save the basis for predictions in some cases, but in general, this idea is not sufficient. Being able to operate efficiently the degree of uncertainty must be taken into account, e.g. if the main agent is confused what future state could be, it could be proper to ask directions, take a look into the map, search for reference point, etc.
Other options for belief computation would be using probability distributions over states of the world, which we have. In this case, distributions encode the subjective probability for the main agent and include information about the state of the world and give a basis for taking action under uncertainty we have. Moreover, sufficient statistical information of action made in the past and initial belief state of the agent is comprised, i.e. computed belief state for the current agent's state and additional information about its past observations and/or action made, would provide any further information about the current state of the world [23].
Computing belief states[23]:
A belief b is a probability distribution over state space $\mathcal{S}$, *b(s)* is the probability set to world state s by belief state b. The axioms for belief state is the same as for probabilities: $0 \leqslant$ b(s) $\leqslant 1$, for all s ϵ $\mathcal{S}$ and $\sum_{s \epsilon \mathcal{S}} b(s) = 1$. At every new step, new belief *b'* must be computed given old belief b, an action a and an observation o. The new belief of an new state *b'(s')* can be calculated using formula:

$$\begin{aligned} b'(s') =& Pr(s'|o,a,b) \\ &= \frac{Pr(o|s',a,b)Pr(s'|a,b)}{Pr(o|a,b)} \\ &= \frac{Pr(o|s',a)\sum_{s \epsilon \mathcal{S}} Pr(s'|a,b,s)Pr(s|a,b)}{Pr(o|a,b)} \\ &= \frac{O(s',a,o)\sum_{s \epsilon \mathcal{S}} T(s,a,s')b(s)}{Pr(o|a,b)} \end{aligned} \tag{2.4}$$

The denominator of equation (2.4), Pr(o | a, b), can be interpreted as a normalizing factor, which is independent of next state s', which causes the sum of belief of all possible next states to 1. The state estimator function SE(b, a, o), which task is to update the belief state based on the *a, o* and the previous b, as its output gives new belief for new state *b'*.
Please note, that this subsection and the computation of belief states description is taken directly from Partially observable Markov decision process (POMDP) steps description. In later work, belief update will act an important role, but it will be computed using different components. Detail description of belief computation related to this work will be provided in next chapters.
To have particular classifier is not enough for making accurate trajectory and movement predictions. Next chapter introduce with the most popular model for movement predictions.

2.3 Movement Prediction

Foresee future moments and trajectories for dynamical objects in traffic scenarios is vital in order to obviate risks which occur on the roads. Prediction despite of short or long term they are, must have sufficient time in advance to avoid traffic situations we, as traffic participants, don't want. In this section, relevant researches for trajectory and movement predictions are introduced.
There is numerous research made on a trajectory and movement predictions with a vehicle as interest on traffic scenarios. [3] suggesting a one way of classifying methods for motion prediction. The main three categories with an increased rate of flexibility were defined: ***physical-based, maneuver-based*** and ***interaction aware***.

- **Physics-based** motion models are the most simple of all categories. It is considered that the movement of vehicles depends only on the laws of physics. A wider description is in subsection 2.3.1.
- **Maneuver-based** motion models are more advanced than physics-based because maneuver-based motion models also consider future movements of a car which also depends on the maneuver which is intended to perform by a driver. A wider description is in subsection 2.3.2.
- **Interaction-aware** motion models take into account consideration connections between maneuvers of the car, as well as rules of the traffic. This method as not so popular as previous ones due its complicity to adapt to the real life scenarios. A wider description is in subsection 2.3.3.

Figure 2.1 summarizes motion models defined in [3].

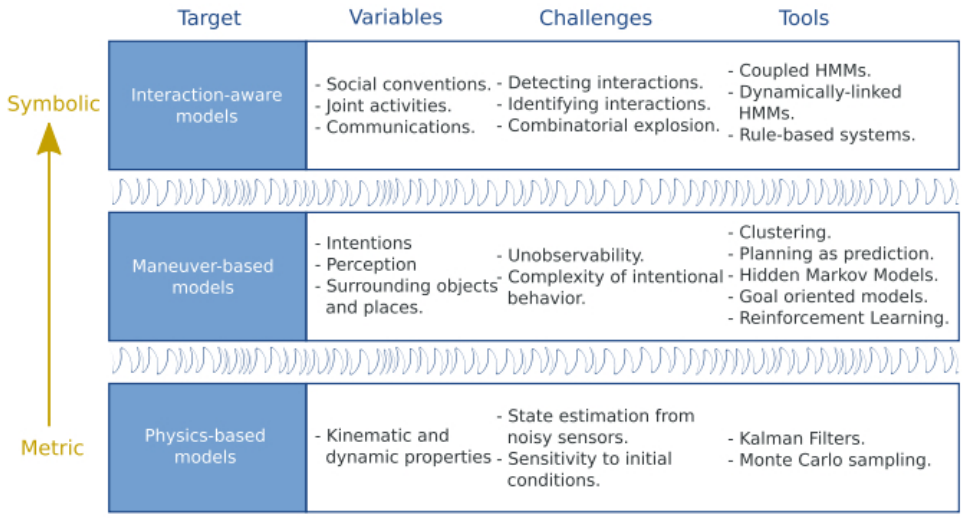


Figure 2.1.: Motion Modeling Overview [3]

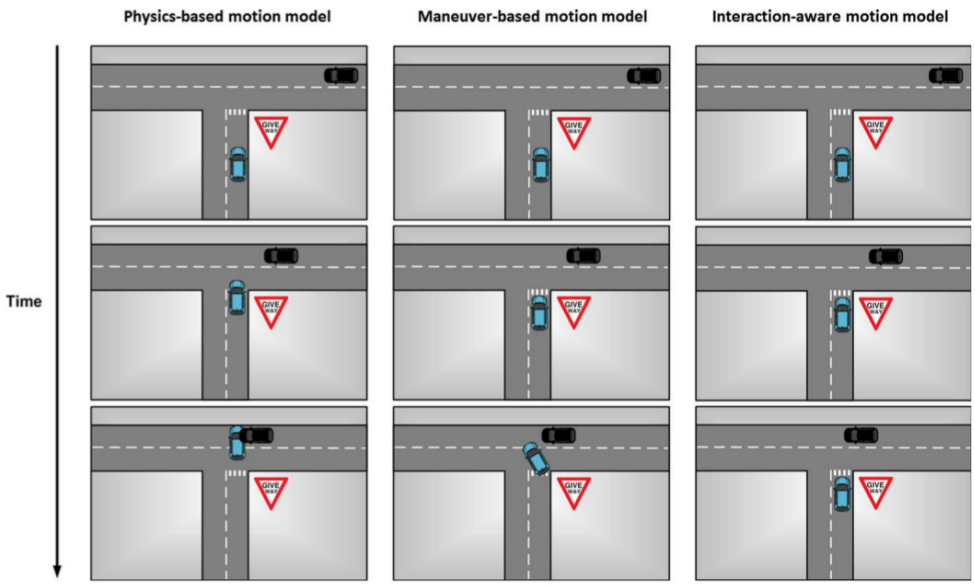


Figure 2.2.: Examples of motion prediction with the different types of motion models [3]

Together with above-mentioned categories, authors of [24] introduced one more category to predict movements - ***data-driven based***.

- **Data-driven** based motion and trajectory prediction can be classified into clustering-based and probabilistic approaches. A wider description is in subsection 2.3.4.

2.3.1 Movement Prediction Using Physics-Based Models

Physics-based movement prediction models imply vehicles as a dynamic item, controlled by the physics' laws. Movements are predicted using dynamic and kinematic models with control inputs (e.g. acceleration, deceleration, steering), properties of the car (e.g. length, weight) and some external conditions (e.g. the friction coefficient of the road surface) to the process state of the vehicle (e.g. position, speed, direction). Great work has been done using *physics-based* motion models and it still remains the most commonly used motion models for motion prediction in the context of road safety. The complexity of the models depends on a representation of the dynamics and kinematics of a vehicle, as well as, how uncertainties are handled, whether or not the road geometry is taken into account, etc.
Dynamic and kinematic models can be used for movement prediction in a lot of different ways, the main difference is how uncertainties are handled. Three main approaches will be described as follow: ***single trajectory simulation, Gaussian noise simulation*** and ***Monte Carlo simulation*** [3].

- **Single Trajectory Simulation.** The simplest method to predict future movements and trajectory of a car is to apply simple dynamic or/and kinematic models for the current state of a car while assuming that the current state of the car is determined with absolutely highest confidence and applied model (dynamic, kinematic or both) is the perfect representation for the movement of the car. This simple approach was used in [25] using dynamic and [26, 27] kinematic models. The main benefit of this straightforward approach is computational efficiency, that allows this method to be used in real time. On the other hand, predictions made by this method do not consider uncertainties of the current state and as a result, predicted movements and trajectories are not trustworthy for use in a long term ($>$ 1 sec.) predictions.

- **Gaussian Noise Simulation.** The uncertainty of the current state of a vehicle and its evolution during the time is a very important factor in movement or trajectory prediction and it can't be avoided. In [28, 29, 27] this is modelled using a normal distribution. Gaussian Noise function is very popular because of its uncertainty representation in Kalman Filter (KF), which is still a conventional method for vehicle state estimation having noisy sensors measurements in account. There are some cases where dynamic, kinematic and sensor models are linear and uncertainty is modelled using a normal distribution instead of KF Bayesian filter is used. Filtering mainly contains of two steps: prediction and update steps. In the first time step at time step t, a current state of the vehicle is is given to the dynamic or kinematic model, which gives predicted state for the next time step which has a Gaussian distribution shape. In the following step, predicted state of the next time step is combined with sensor measurements of the same time step, which is Gaussian distribution as well. Filtering is a looping of these two steps every time when new measurements are available.

  By looping the first step, it is possible to get a mean and covariance matrix for every future timestep for the vehicle state. This can be modified into a trajectory mean with linked uncertainty (i.e. normal distribution in each timestep), as showed in [30, 28]. As compared to the approached of *single trajectory simulation*, Gaussian Noise simulation techniques have the benefit of uncertainty representation on the predicted trajectory or movements. However, there are some limitaitons as well: modelling uncertainties employing normal distribution is not quite enough to show the different possible maneuvers. A possible solution for this could be uncertainty representation using Variational Gaussian Mixture Model (VGMM). Author of [31] used Switching Kalman Filter (SKF) for this exact purpose. [29] depends on mass of KF to show possible models for movement evolution for vehicle and be able to freely change between them. [27] introduced an alternative approach: to use heuristics and change different kinematic model depending on the current situation.

- **Monte Carlo Simulation.** In generic case when no assumptions in advance are made about models linearity or uncertainty model, distribution expresion on predicted vehicle states are not clear. Monte Carlo method is the right tool for this kind of situation. The idea under the Monte Carlo method is to randomly sample the input of the dynamic or kinematic model and to generate potential future trajectories. If the road topology is taken into account, various mass can be added to the generated trajectories and movements to penalize the ones which do not respect the restriction of the road design. Kinematic and dynamic models can be used for Monte Carlo method by categorizing inputs instead of considering them as a constant. Typical inputs are categorized to acceleration, steering angle or lateral deviation. To be able to take into account eligibility of the movement, generated trajectory samples, which has a bigger acceleration than physically is allowed can be removed, as it was done in [32] or consider limitations which vehicle has (weight, length, etc.) and distribute dynamic and kinematic models in a more realistic manner and remove all impracticable trajectories from predefined trajectories list as it was done in [33]. Monte Carlo method can be used to foresee trajectory or movements for a vehicle with a very well known current state or for vehicle which has uncertainty in the current state, which was estimated by one of the filtering algorithms.

2.3.2 Movement Prediction Using Maneuver-Based Models

Maneuver-based motion models show vehicles as independent moving entities, i.e. it is assumed that the movement of a vehicle on the road match to a series of independently executed movements from the other vehicles on the same road. Oxford dictionary [34] a movement/maneuver as “a physical movement or series of moves requiring skill and care”. Term behaviour in literature often is used meaning the same meaning, e.g. in [35, 36, 37], for the sake of simplicity word "movement" or "maneuver" will be used in this work with defined meaning. Movement and trajectory prediction using maneuver-based motion models work with in advance recognized movements which driver possibly intend to perform. If an algorithm can recognize intended movement, the algorithm can assume that future actions of the driver will match the recognized movement. Due to this a *priori* information, trajectories received with this method are more relevant and reliable than the ones received using physics-based motion models. Maneuver-based motion models rely on prototype trajectories or on movement intention estimation.
Vehicle motion classification into maneuver/movement classes has been extremely widely applied not only in driver assistance systems but into natural driving studies [38, 39, 40, 41, 42, 43, 44, 45, 46, 47]. Authors of the majority of approaches are using heuristinc [41] or training classifiers like SVMs in [42], HMMs [38, 43, 44]. Long Short Term Memorys (LSTMs) in [45], Bayesian networks [46], etc., as movement-based features using speed, deceleration, acceleration, yaw rate, lane position, turn signals, distance from other vehicle and other road context information. Authors of [41] classified vehicle’s movement into class "keep lane" or "change lane" grounded on how far the closest car is and predicted future trajectory by applying quintic polynomial of the current car movement state and pre-defined ultimate movement state for each movement class, defined before.Authors of [46] used six different movement classes, which were defined before and using DBN based on multiple movements and context based features selected the potentially right future movement. Authors of [47] defined an individual Gaussian process for three movement classes and established a multi-modal distribution for possible future trajectories using each model. However, in the study, only one case-based prediction has been introduced. Authors of [38] also determined separate Gaussian processes, this time for four different movement classes, which were classified using a hierarchical HMM. This method was tested on real highway data. Authors of another study [39] used a random forest classifier for movements classification into pre-defined movement classes: left or right lane changes or keep lane. Authors used a separate Gaussian Mixture Regression (GMR) model for predicting lateral movement for vehicles using each class. Method was tested on real highway data. Similar method, but without predifined movements classes for prediction longitudinal motion for vehicles were used in [40].

2.3.3 Movement Prediction Using Intention Aware Models

Interaction-aware motion models introduce cars as manoeuvring items which co-operate with each other, i.e. a movement of a vehicle is considered to be affected by a movement of the other moving object in the traffic scene. Keeping into account the dependencies between the separate moving objects leads to a much better explanation of their movement compared with **maneuver-based** motion models described in the previous subsection. As a result, it gives a better perception of the current situation.
Despite this, a relatively small amount of researches is done considering inter-moving-objects interaction in movement prediction. Authors of [48] assigned two movement classes for vehicles approaching an intersection together, applying a polynomial classifier which "punishes" cases that potentially would lead to near-collisions situations. Authors of [49] worked with a much complex scenario and assigned movement classes to multiple together interacting vehicles in a highway scenario. However, foreseen movements, trajectories of a vehicle are assumed to be given in advance. Results reported using a simulated environment. [24] in their work considered multiple interacting vehicles together with the difficulty of estimating their future motion. Authors of [39] not directly used inter-moving-objects interaction by including comparative positions and velocities of vehicles close by as features for movement and trajectory prediction.

2.3.4 Movement Prediction Using Data-Driven Model

As mentioned earlier *data-driven* movement prediction can be generally classified into clustering-based and probabilistic approaches. **Clustering-based** approaches group the training data in order to provide a set of possible prototype trajectories [50, 51]. Partially observed trajectories are checked and compared with a prototype trajectory using various distance measurements, as Dynamic Time Warping (DTW), Longest Common Subsequence (LCSS), Hausdorff distance, etc. and after matching movement trajectory with prototype trajectory, later one is used as a model for future movement. Clustering approach is quite easy, but the main disadvantage of this method is the deterministic nature of the predictions. **Probabilistic** approach contrary learn probability distribution of every movement trajectory class and gives the conditional distribution for future movements, given current trajectory. This lets us avoid some degree of natural uncertainty of predicting the future.

Authors of [52, 38] for modelling trajectories and for motion prediction use Gaussian Processes which are the most popular approaches solving prediction problems so far. [39] uses GMR for prediction longitudinal movement of a vehicle, while [40] uses the same method for lateral movement prediction. [53] uses VGMMs for conditional distribution within snippets of future having snippets of movement history models. The latest approach is much easier and computationally more effective when compared to Gaussian Process Regression. Authors proved the efficiency of method predicting non-linear movements in turns at the intersection scenarios.

2.3.5 Limitations of Methods for Movement Prediction

Subsections 2.3.1, 2.3.2, 2.3.3 and 2.3.4 described movement prediction with different feature based model. This subsection will introduce limitations of all these methods.

- **Physics-based approach.** Predictions using physics-based motion models are restricted to very short-term (< 1 sec.) motion prediction due to low-level motion (dynamic and kinematic) properties this method relies on. Usually using this method it is unable to foresee any change in the vehicle movement which happens due to an execution of a particular maneuver (e.g. speed up, slow down, make a turn, etc.), or changes caused by external factors (e.g. slowing down due to traffic lights, signs, other vehicles, etc).

- **Maneuver-based approach.** For a very long time, the biggest limitation of prototype trajectories was time representation. When the movement models are showed using a finite set of trajectories it takes a very large number of prototypes to represent the large variation in the implementation of an every possible movement pattern. Handling subtle situation in traffic, as movements with waiting time at a stop line, not constant velocity caused by traffic is a very big issue for such models. For a certain extent, Gaussian Processes (GP) were introduced. They solved this kind of problem by introducing time-independent movement patterns [52]. On the other hand, GPs have some other limitations as well. First of all to be able to take into account all possible traffic scenarios, has very heavy computational time, despite that they are not considering the physical limitations of a vehicle and due to that may generate or predict unrealistic trajectories and movements. To solve these problems the best solution so far was proposed in [54]. Authors used Rapidly-exploring Random Tree (RRT) to be abe to "randomly sample points toward dynamically feasible trajectories, using as inputs the current state of the vehicle and the sample trajectories generated by the GPs" [54]. Another issue with using predefined prototype trajectories is an adaptation to a different road, i.e. for different intersections. Each movement model is defined for a specific road/intersection geometry and topology, what means that prototype models only can be used with the same or very similar topology.

  Maneuver-based approach contains similar limitations which described under limitations of data-driven approach.

- **Interaction-aware approach.** Prediction using interaction-aware motion models are the most exhaustive method suggested in the literature so far. Using it, is possible to predict for a longer-term as compared to physics-based motion prediction models, and predictions are more trustworthy than using maneuver-based motion models in predictions due to taking dependencies between the surrounding cars into consideration. However this completeness has some disadvantages as well: calculation of all possible trajectories with all possible models take a lot of time and because of that, it is not very compatible with using in real-time situations. For this reason, using interaction-aware motion predictions are not so popular.

- **Data-driven approach.** The assumption that movement of vehicles do not depend on each other and other traffic participants is not accurate. All vehicles without any exceptions use a road together with other traffic participants and movement performed by one vehicle directly or indirectly effects others. Dependencies with each other are quite strong at intersection, where road rules, not only movement of other cars must be taken into account. Ignoring these reliances can lead to wrong interpretations of the situations, and affects the evaluation of the risk. A data-driven approach is quite easy, but not always it pays attention to these critical dependabilities and it is quite difficult to pre-define all possible action of other traffic participants, i.e. the main disadvantage of this method is the deterministic nature of the predictions.

3 TBD

Probably I need to restructure content, but not sure exactly where to put what

4 Setup and Implementation

ROS simulation environment was used for testing approaches. ROS is a framework where testing cases can be easily developed and tested. In a current simulator, there are few small environments imitated consisting of a static map (T and X intersection) and the car itself.
In order to visualize simulation RViz which is s a 3D visualizer for showing data and state information from ROS was used. A snapshot of the simulation environment is in Figure 4.1. The code was written in Python and C++ programming languages.

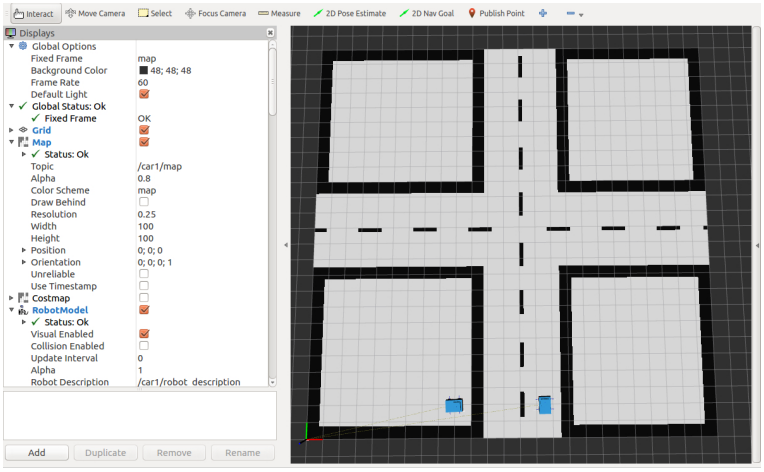


Figure 4.1.: The RViz environment that runs the simulation, having X-Intersection in mind

For this project, several testing cases were developed. Methods tested offline (with having all trajectory for testing) and online (having only current and last position). Data from every run is stored in order to analyze it and see how each method effect performance of the system. Parameters and results for each trajectory are independent and tested several times in a specific environment to be able to draw conclusions from the results we received during the testing.

4.1 Data Collection

To be able to test our approach database of various trajectories need to be used. To make our own database for possible trajectories and not to use already existing data was taken at the beginning stage of this project. Due to that data collection was one of the first steps after all simulation environment was set.
To be able to control car in ROS environment and record data joy package was used. Joy package is a ROS driver for a "generic Linux joystick".The package consists of joy_node, a node which allows communication between a generic joystick and ROS. Joy message, which contains information about the current state of each button on joystick is published by node [55], having this information command start to move, turn to any direction, stop is sent to the object we want to control in ROS environment. When an object, the car in our car is able to move in ROS using a joystick we recorded and stored a car's position every few milliseconds.
For each map type, slightly different types of trajectories were recorded. For X-intersection a various number of trajectories for movement to the right, straight and left were recorded, while for T-intersection only movement t the right and left was recorded.

4.2 Brief Algorithm Explanation

In this section a brief overview of the main code algorithm for getting test results will be explained.

4.2.1 Map Recognition

In this project, two (so far) maps, imitating X and T intersection, were used. Map recognition is necessary because the further calculation is a bit different on T and X intersection maps.

The map is recognized using .... Not exactly sure if I will leave current map recognition algorithm, where I am using simple contour recognition or will go to a more complicated one. That's why here I left this section empty.

4.2.2 Trajectories' Unification

The problem with our current database is that there are a lot of trajectories which have a different number of time steps. This happened because of different trajectory length (e.g. to go straight takes less time and it is a less distance than going to left or right), the velocity of the car may differ in each or even in the same trajectory (velocity depends on control of the joystick), etc. Having different time steps in trajectories makes some problems in further calculations, comparison of results, the calculation over thousands of steps also has a longer computation time, etc. Because of that trajectories, unification is a necessary step.
Unification made using interpolation when all trajectories transformed to have an equal number of time steps, in spite of the original number of time steps. This is achieved by interpolation, in mathematics interpolation is a method of building new data points inside the range of a discrete set of known/given data points.

The pseudo code below (Figure 4.2) shows the way of interpolation in this project.

```
1  begin
       x, y        # coordinates of trajectory which needs to be interpolated

       # Calculate the n-th discrete difference along the given x and y axis
2      xd[n] = a[n+1] - a[n]
3      yd[n] = a[n+1] - a[n]

       # Calculate Euclidean distance between xd[n] and yd[n]
4      dist = np.sqrt(xd[n] ** 2 + yd[n] ** 2)

       # Calculate cumulative sum of the elements along dist
5      u = np.cumsum(dist)

       # Stack array u in sequence column wise (horizontally)
6      u = np.hstack([[0], u])

       # Calculate evenly spaced numbers over a specified interval [start, stop]
7      t = np.linspace(0, u.max(), len_des)

       # Calculate the one-dimensional linear interpolation with given discrete data points
8      xn = np.interp(t, u, x)
9      yn = np.interp(t, u, y)
10 end
11 return xn, yn # interpolated coordinated of given trajectory
```

Figure 4.2.: Pseudo code for interpolation (need to rewrite it to make it pseudo)

Figure 4.3 shows 3 original trajectories and interpolated version of the same trajectories. Original trajectory, which goes to the right has 7,581 time steps, while straight trajectory has 13,666 and the left trajectory has 10,929 time steps after interpolation all trajectories contain 10 steps (number of time steps can be changed according to preference or test case). As can be seen, interpolation does not ruin trajectories and can be used in further calculations.

4.3 Modeling Belief for Prediction Making

A Bayesian version of a Gaussian mixture model is used for calculating the belief for each trajectory class and this section gives definitions for beliefs representing for a car over trajectory classes (going right, going straight, going left). Since we can only observe the current position of the car, which means that trajectory class is partially observable, due to that our belief is represented as a probability distribution over all trajectory classes.
For maintaining correct belief, belief update must be done every time step. Updating belief constantly is important because of sudden position change can show drivers' intentions and what his next steps could be. To be able to predict

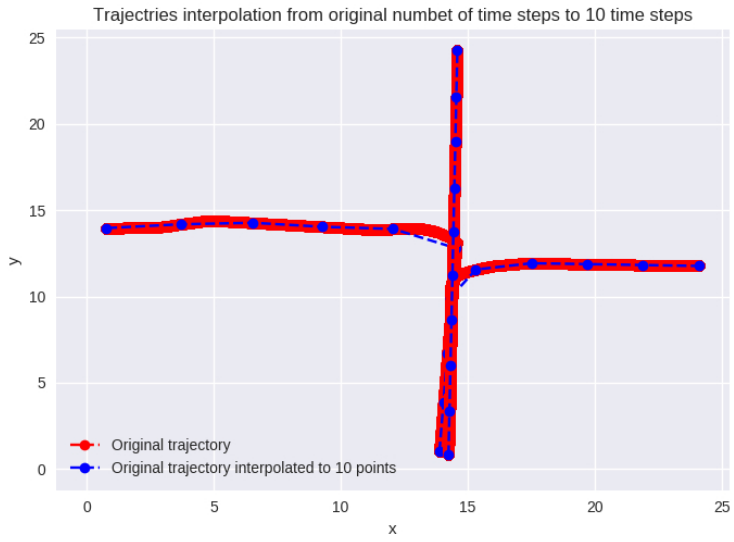


Figure 4.3.: Original and Interpolated Trajectories

possible future movement current position information need to consider every time when belief update is calculated. The belief update is calculated using Bayes rule formula 4.1 below:

$$\begin{aligned} b_{t+1}(k) &= Pr(k|o_t, b) \\ &= \frac{Pr(o_t|k,b)Pr(k|b)}{Pr(o_t|b)} \\ &= \frac{Pr(o_t|k,b)Pr(k|b)}{\sum_k Pr(o_t|b)Pr(k|b)} \\ &= \frac{Pr(o_t|k,b)b_t(k)}{\sum_k Pr(o_t|b)Pr(k|b)} \end{aligned} \tag{4.1}$$

With given formula belief for future step $b_{t+1}(k)$ for a predefined class is calculated. $Pr(o_t|k,b)$ is the car position observation model, which returns the probability (or likelihood) of going to any direction from the current position, observed with o_t. This likelihood can be calculated using multivariable Gaussian probability distribution function f(x,μ,Σ). This probability distribution function looks the following:

$$f(x,\mu,\Sigma) = \frac{1}{\sqrt{(2\pi)^n det(\Sigma)}} exp(-\frac{1}{2}(x-\mu)^T \Sigma^{-1}(x-\mu)), \tag{4.2}$$

where dimensionality n = 2 and x is a currently observed position of the car $x = (o_t^x, o_t^y)^T$, μ is a mean from all predefined trajectories in data base for the same class $\mu_k = (\mu_{t,k}^x, \mu_{t,k}^y)^T$ and Σ is a covariance matrix of all predefined trajectories in data base for the same class $\Sigma_k = (\Sigma_{t,k}^x, \Sigma_{t,k}^y)^T$.Mean for x and for y coordinates can be found using formula 4.3 and formula 4.4 respectively:

$$f(\mu_x) = \frac{\sum_{i=1}^n x_i}{n} \tag{4.3}$$

$$f(\mu_y) = \frac{\sum_{i=1}^n y_i}{n} \tag{4.4}$$

Covariance value can be calculated using formula 4.5

$$f(\Sigma_{x.y}) = \frac{\sum_{i=1}^n (x_i - \mu_x)(y_i - \mu_y)}{n-1} \tag{4.5}$$

The denominator of formula 4.1 is the so-called normalization factor, which sums all likelihoods of the car over all movement classes at the current time step. The final result of formula will return updated belief that car is moving towards any of classes.
Figure 4.4 shows pseudo-code how belief updates are made over time, as an input having current belief b_t at time step t, current car position x_t, y_t from the last made observation, as well we have before calculated mean and covariance values at that time, $\mu^x_{t,k}, \mu^y_{t,k}$ and $\Sigma^x_{t,k}, \Sigma^y_{t,k}$ respectively.

```
1  begin
     b_t          #current belief
     x_t, y_t     #observed current car position
     Σ_t          #mean (x and y values) of predefined trajectories in current time step
     μ_t          #covariance matrix (2x2 size) of predefined trajectories in current time step
     b_t+1 ← Ø    #updated belief (empty set)
     η ← Ø        #normalization factor (empty set)

   #normalization factor calculation for each observation probability
2    for k∈K do
3      p_k = f((x_t, y_t), μ_t, Σ_t) from N((x_t, y_t) | μ_t, Σ_t)
4      η = η + p_k
5    end

   #new goal distribution over classes calculation
6    for k∈K do
7    b_t+1(k) ← p_k b_t(k) / η
8    end
9  end
10 return b_t+1
```

update.jpg

Figure 4.4.: Pseudo Code for Updating belief

4.4 Trajectory Scaling

Computation time for prediction is one of the main things which needs to be fast. Even though more belief updates give more precise results, more computations take more time. In this project, we took various numbers of time steps and compared results to get them as precise as possible and have fewer time steps (e.g. we aimed to keep precision of trajectory of 100-time steps but have only 10-time steps trajectory).
There were a lot of various trajectories with various numbers of points, but with an original approach result still was that with more time steps prediction results were more precise. Later on, Toy Problem approach came into the sight. [56] defines it as "In scientific disciplines, a toy problem is a problem that is not of immediate scientific interest, yet is used as an expository device to illustrate a trait that may be shared by other, more complicated, instances of the problem, or as a way to explain a particular, more general, problem-solving technique".
After unsuccessfully trying different methods, the idea of raising a likelihood (formula 4.2) of the trajectory with a bigger number of time steps at every time step by $\frac{1}{\frac{biggernumberoftimestepsintrajectory}{smallernumberoftimestepsintrajectory}}$ and then compare results of matching points in each trajectories.
To simplify all this, let's have an example: let's imagine we have the trajectory interpolated to 100-time steps and we want to see how results differ when we do belief updates all 100 times with doing belief at every 10th step (10th, 20th, ..., 90th, 100th). Without doing any changes in the original code, these results are not matching, in fact, they differ quite a lot. But if we raise likelihood (formula 4.2) of the trajectory where belief is updating 100 times by $\frac{1}{\frac{100}{10}} = \frac{1}{10}$ at every time step and then do belief updates as normal and compare them with belief updates which are calculated every 10th step with making no changes in the original code. After comparison of these results, it was easy to see that results are matching or are close enough to each other. The pseudo code of the given example is in Figure 4.5.
Having this in mind we can make our prediction making the process faster and more precise.

```
1  begin
     N          #number of time steps (e.g. 100)
     n          #number of time steps for scaling (e.g. 10)
     b_t        #current belief
     x_t, y_t   #observed current car position
     Σ_t        #mean (x and y values) of predefined trajectories in current time step
     μ_t        #covariance matrix (2x2 size) of predefined trajectories in current time step
     b_t+1 ← Ø  #updated belief (empty set)
     η ← Ø      #normalization factor (empty set)

     #belief  update calculation for N time steps
2    for i in range (1, N+1) do
       #normalization factor calculation for each observation probability

3      for k∈K do
4        p_k = f((x_t, y_t), μ_t, Σ_t)^1/(N/n) from N((x_t, y_t) | μ_t, Σ_t)^1/(N/n)
5        η = η + p_k
6      end

       #new goal distribution over classes calculation
7      for k∈K do
8      b_t+1(N)(k) ← p_k b_t(k) / η
9      end

       #take the every nth step from trajectory with N steps
10     if i % n == 0 do

11 - 17  #Belief update calculated exactly the same as in Figure 4.4

18     end
19 end
20 return b_t+1(N), b_t+1(n)
```

Figure 4.5.: Pseudo Code for Scaling Trajectory for Belief Update

4.5 Online Method for Prediction Making

The online method uses the same, previously described techniques and principles for calculation. The predefined database with trajectories exists, calculations and all preparation for a future working with them are made as well. The one difference between online and offline methods is that all testing and its results visualizations are happening in ROS and RViz. And the main difference from an offline method, the online method does not have a whole testing trajectory at the beginning, during testing only past and current steps are known. which makes all interpolation kinda complicated, and I need to discuss that with you on a meeting, maybe I am just don't know something and I am raising a problem when it doesn't exist. Results of prediction are also highlighted in real time in RViz environment.

5 Experiments and Results

In this chapter experiments, made by using different simulation setups, are described. The number of experiments for each trajectory class and for each map is done. Results were analyzed separately and then compared.

5.1 Vehicle is Moving Through X-Intersection

Every time we start belief update calculation we have to initialize the value of belief at the very first time step. When the testing map is X-intersection (Figure 5.1), from its' starting position, which is $x_0, y_0 = (14.5, 2.0)$ car can go to any direction it wants: right, straight or left. There are equal chances that car will go to any direction, so initial belief set to be equal for each direction $b_0 = (0.333, 0.333, 0.333)$

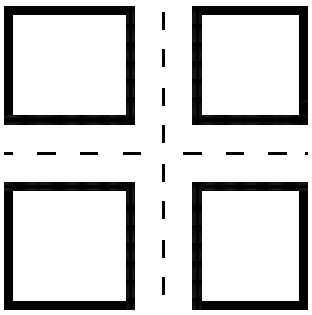


Figure 5.1.: X-intersection map

5.1.1 Moving to the Right Direction

The testing trajectory of going to right looks as it is shown as a red line in Figure 5.2.

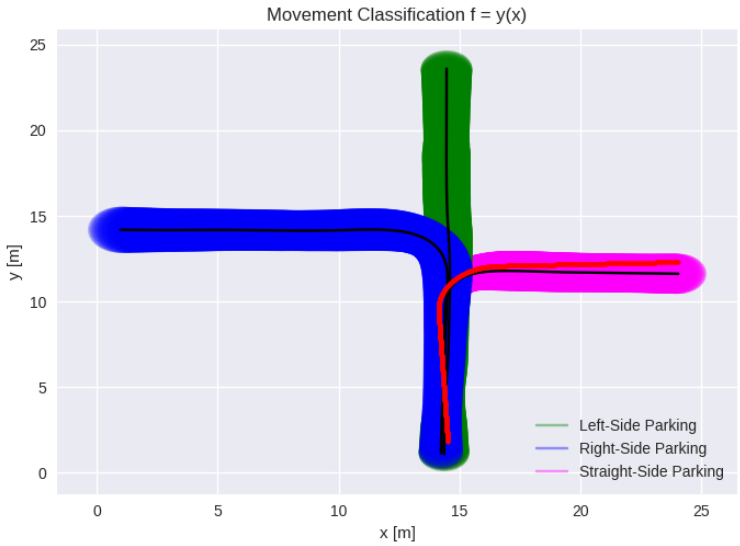


Figure 5.2.: Testing Trajectory (red) of going to the right

At first, the prediction making was checked for all trajectory, when it has 10-time steps. Results are in Figure 5.3.

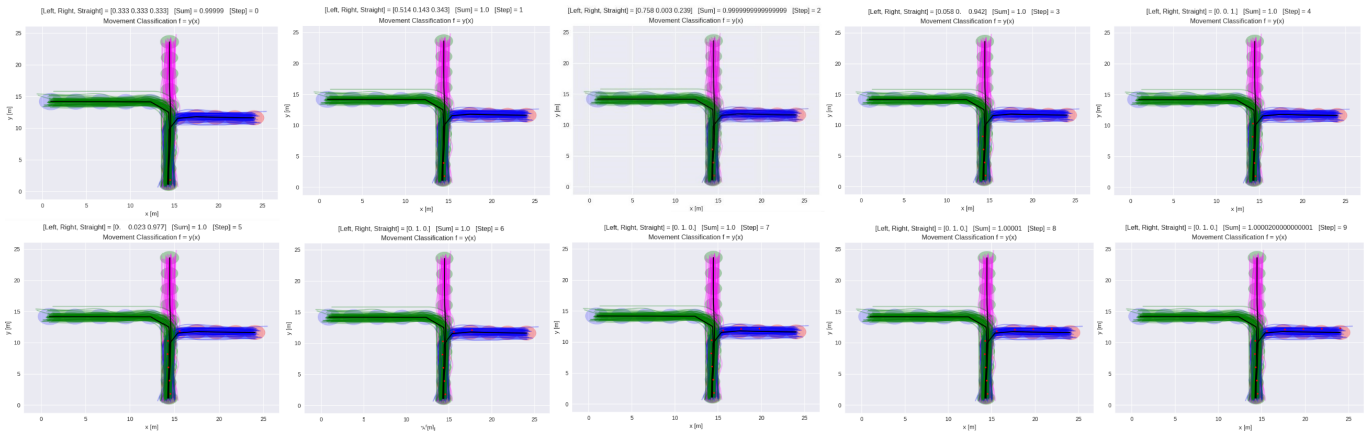


Figure 5.3.: Prediction making for trajectory which goes to the right. Trajectory has 10-time steps

From the series of plots, we can see that in the 7th step belief that direction is right equals to 1. In Figure 5.4 is shown how beliefs are changing over time. Left graph of the Figure 5.4 shows belief changes when trajectory has 10 points and for better visibility, there was added one more graph on the right, where is the same trajectory, just it was interpolated 100 times instead of 10.

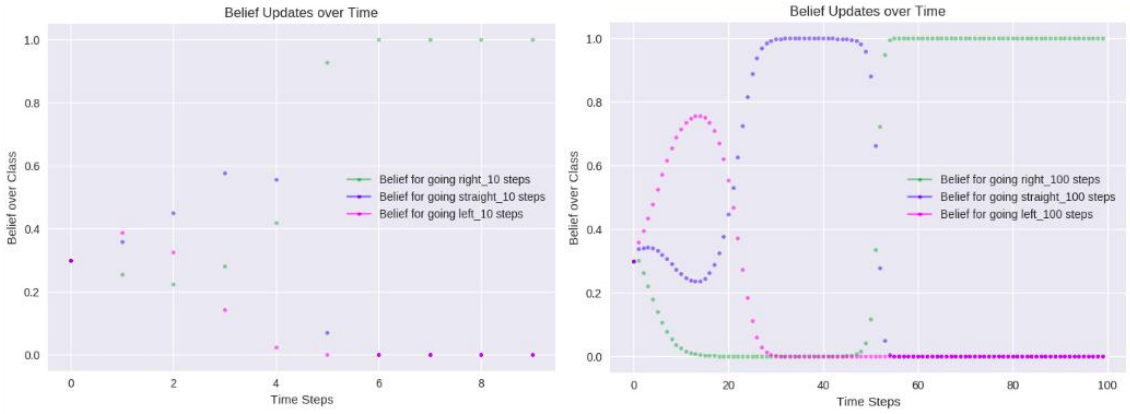


Figure 5.4.: Belief changes over time. For trajectory with 10 steps on the left, for trajectory with 100 steps on the right. Trajectory direction is right

To be able to see how belief is changing over time withing different trajectories and compare if there are the same results at the same steps in the same movement class, we plotted 10 random trajectories going to the right. Results are shown in Figure 5.5.

Figure 5.5.: Belief changes over time for different trajectories which belong to the same movement class. Trajectories have 100 time steps. Trajectory direction is right

From the Figure 5.5 it is possible to see that some trajectories have a better time for being sure to which direction car is moving and some of them have a worse time than others. Next two figures will show trajectories which have "the best" (Figure 5.7) and "the worst" (Figure 5.6) times in the movement prediction.

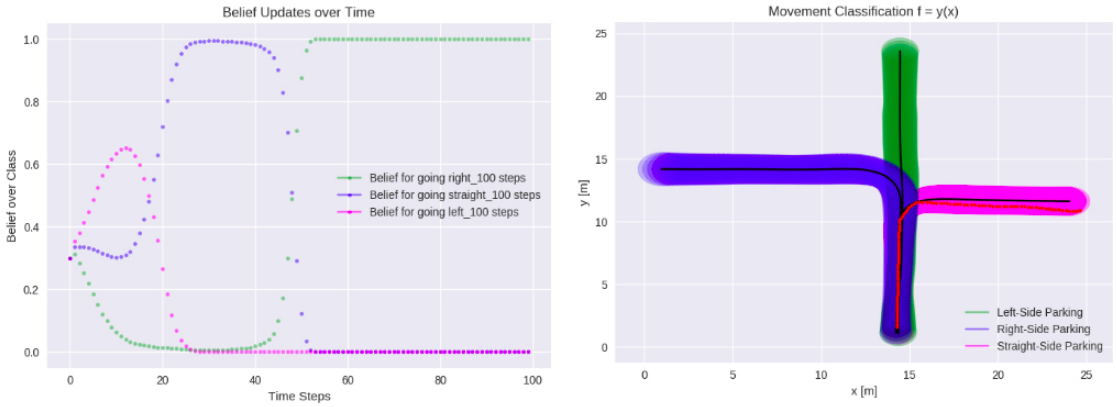


Figure 5.6.: Belief over time changing (left image) and image of testing trajectory (right image). Trajectories have 100 time steps. Trajectory direction is right

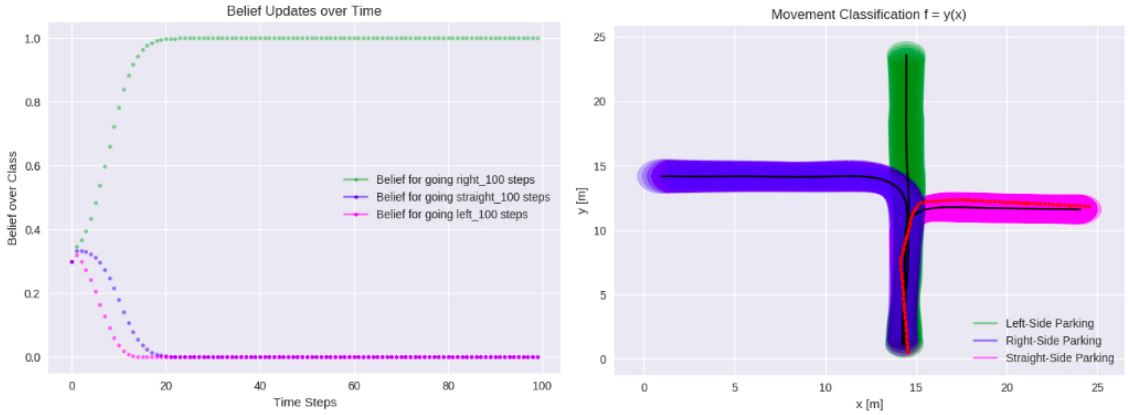


Figure 5.7.: Belief over time changing (left image) and image of testing trajectory (right image). Trajectories have 100 time steps. Trajectory direction is right

By looking at Figure 5.6, "the worst" results can be explained by the position of the trajectory: it is close to all means, so it is natural that precise of prediction making can be disturbed in this case.
By looking at Figure 5.7 and "good" results we can also make an assumption that trajectory is not on the means of classes and due to that precise of prediction making is better in this case.

5.1.2 Moving Straight

The testing trajectory of going straight looks as it is shown as a red line in Figure 5.8.

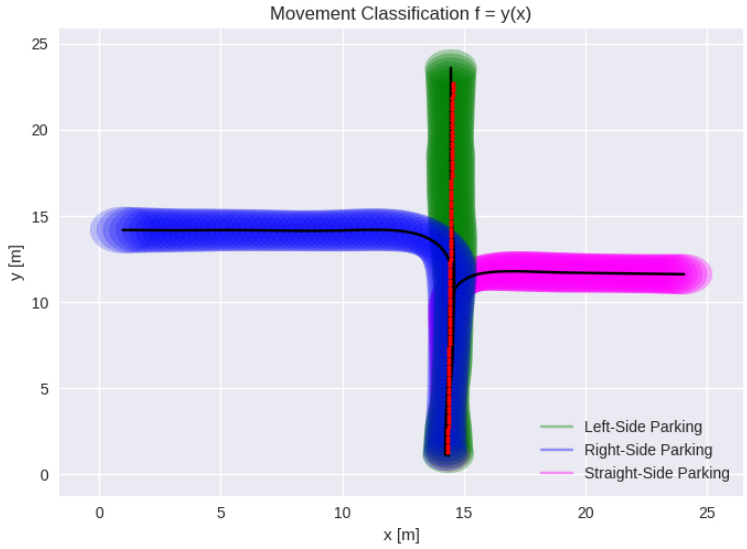


Figure 5.8.: Testing Trajectory (red) of going straight

At first, the prediction making was checked for all trajectory, when it has 10-time steps. Results are in Figure 5.9.

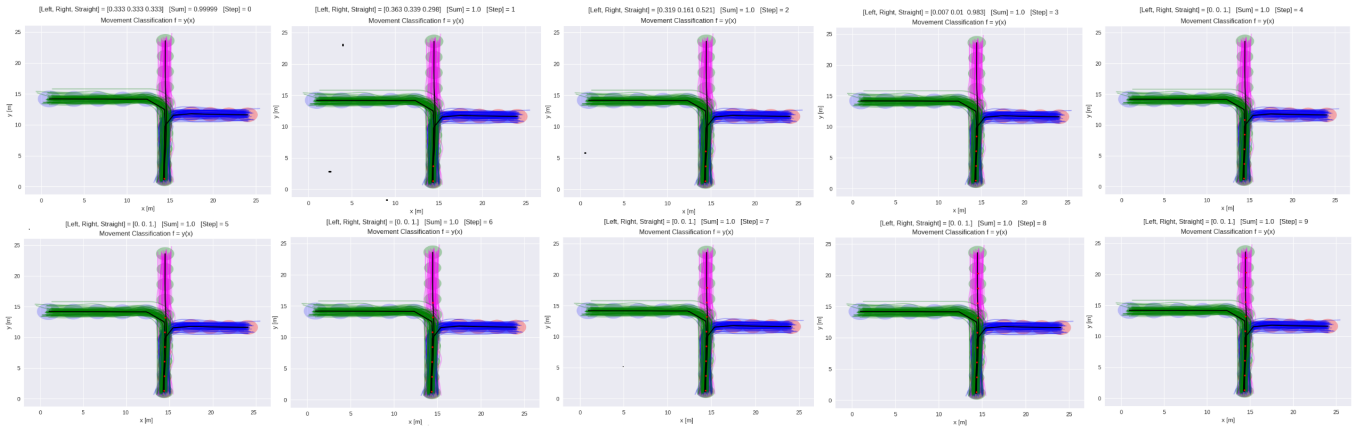


Figure 5.9.: Prediction making for trajectory which goes straight. Trajectory has 10-time steps

From the series of plots, we can see that in the 4th step belief that direction is straight is equal to 0.983. In Figure 5.10 is shown how beliefs are changing over time. Left graph of the Figure 5.10 shows belief changes when trajectory has 10 points and for better visibility, there was added one more graph on the right, where is the same trajectory, just it was interpolated 100 times instead of 10.

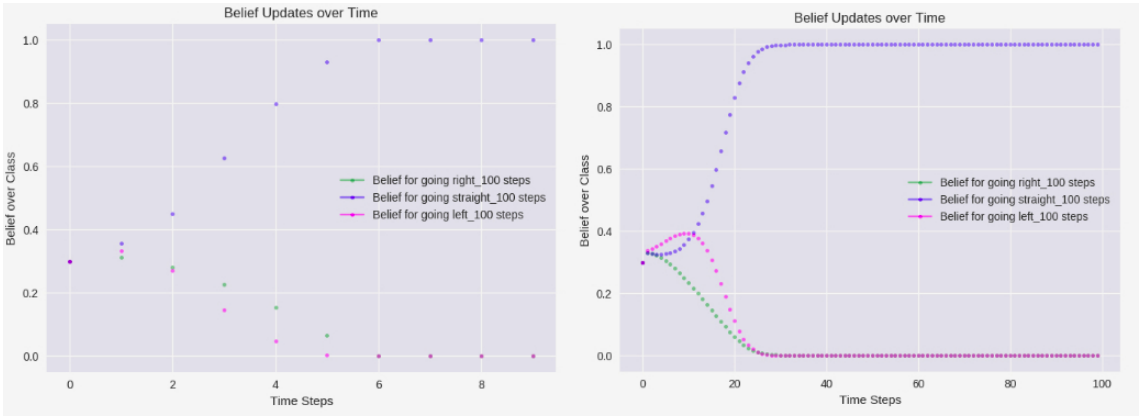


Figure 5.10.: Belief changes over time. For trajectory with 10 steps on the left, for trajectory with 100 steps on the right. Trajectory direction is straight

To be able to see how belief is changing over time withing different trajectories and compare if there are the same results at the same steps in the same movement class, we plotted 10 random trajectories going straight. Results are shown in Figure 5.11.

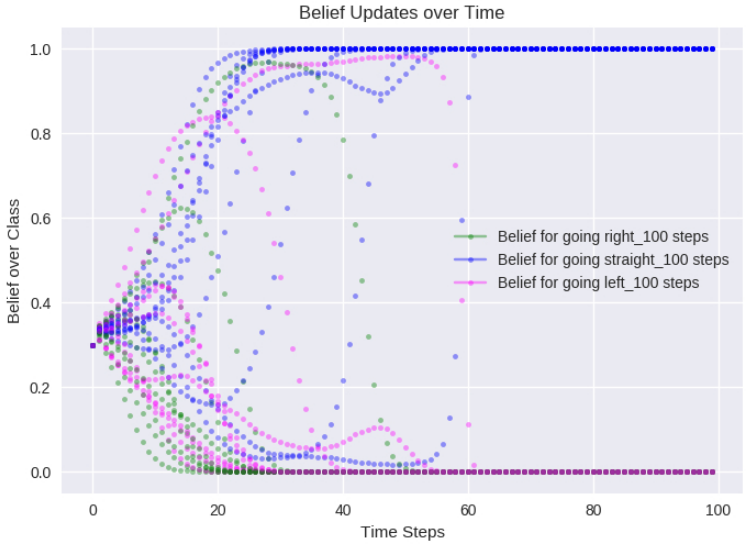


Figure 5.11.: Belief changes over time for different trajectories which belong to the same movement class. Trajectories have 100 time steps. Trajectory direction is straight

From the Figure 5.11 it is possible to see that some trajectories have a better time for being sure to which direction car is moving and some of them have a worse time than others. Next two figures will show trajectories which have "the best" (Figure 5.13) and "the worst" (Figure 5.12) times in the movement prediction.

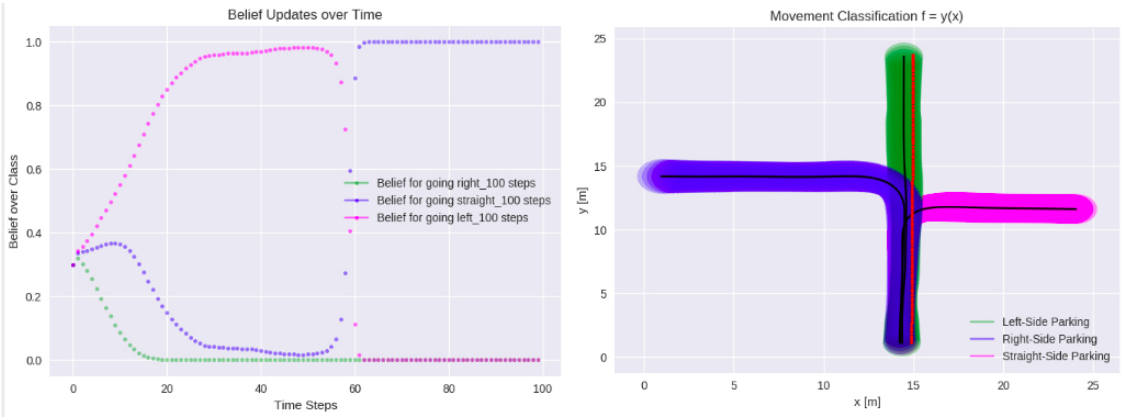


Figure 5.12.: Belief over time changing (left image) and image of testing trajectory (right image). Trajectories have 100 time steps. Trajectory direction is straight

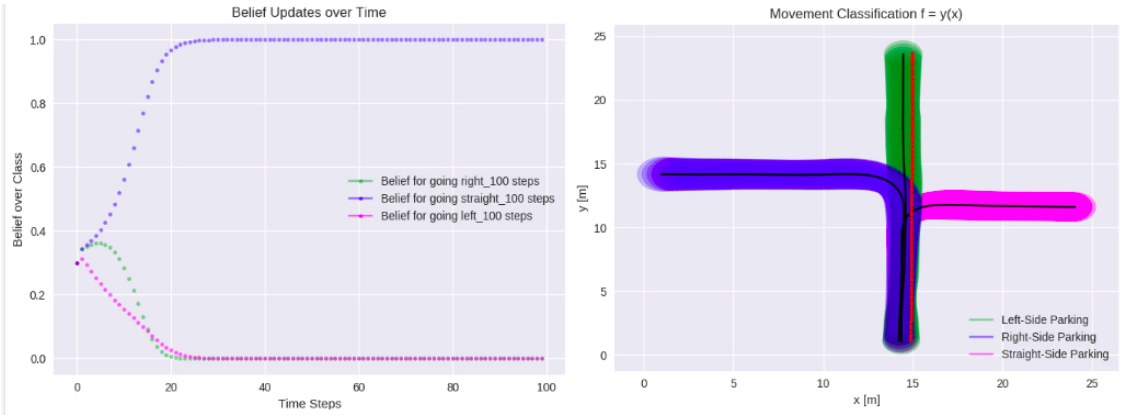


Figure 5.13.: Belief over time changing (left image) and image of testing trajectory (right image). Trajectories have 100 time steps. Trajectory direction is straight

By looking at Figure 5.12, "the worst" results can be explained by the position of the trajectory: it is closer to standard deviation values of left class mean, this could be the case, why prediction is that car is going to the left, until it is sure that it is not going to the left.
By looking at Figure 5.13 and "good" results we can also make an assumption that trajectory and coordinates at each time step is closer to mean and it is in the range of standard deviation of straight mean.

By looking into separate results of class straight one more very interesting case was noticed. Here (Figure 5.14) prediction is correct from the very first steps, but the changing of dynamics of prediction is interesting. This dynamics might be explained by car movement trajectory (it is not moving exactly straight, it is making some turning, which can be the reason of this result).

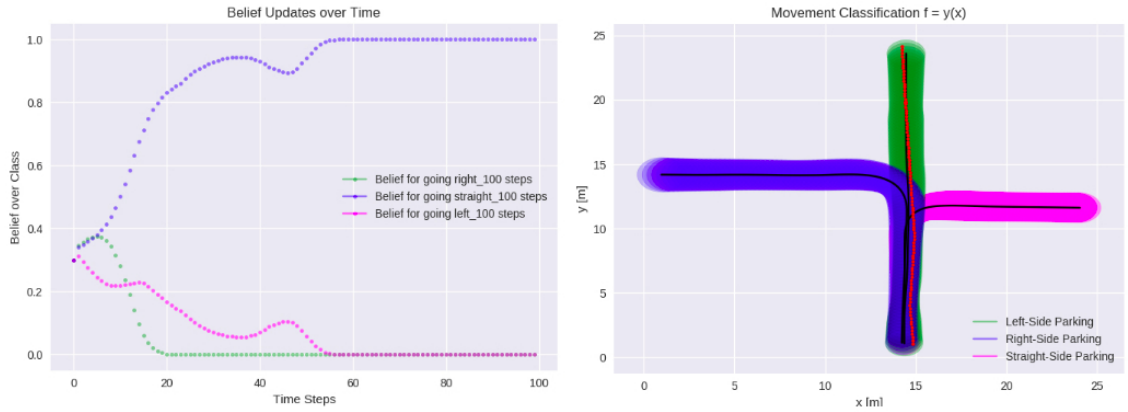


Figure 5.14.: Belief over time changing (left image) and image of testing trajectory (right image). Trajectories have 100 time steps. Trajectory direction is straight

5.1.3 Moving to the Left Direction

The testing trajectory of going to the left looks as it is shown as a red line in Figure 5.15.

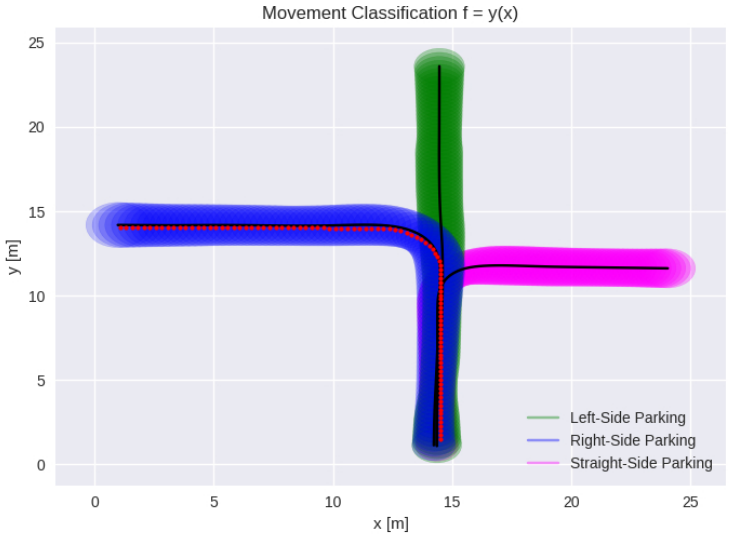


Figure 5.15.: Testing Trajectory (red) of going to the left

At first, the prediction making was checked for all trajectory, when it has 10-time steps. Results are in Figure 5.16.

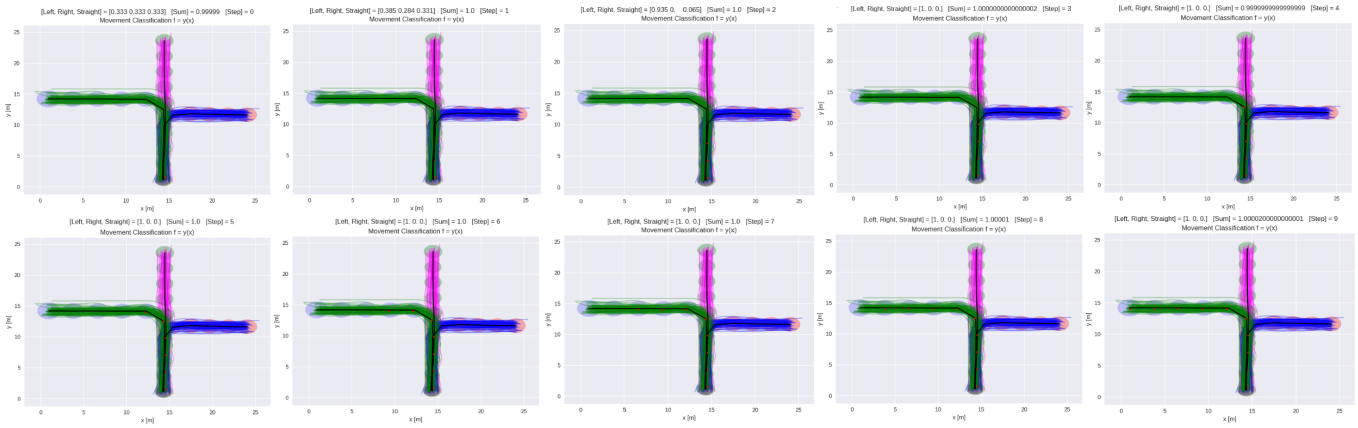


Figure 5.16.: Prediction making for trajectory which goes left. Trajectory has 10-time steps

From the series of plots, we can see that in the 3rd step belief that direction is left is equal to 0.935. In Figure 5.17 is shown how beliefs are changing over time. Left graph of the Figure 5.17 shows belief changes when trajectory has 10 points and for better visibility, there was added one more graph on the right, where is the same trajectory, just it was interpolated 100 times instead of 10.

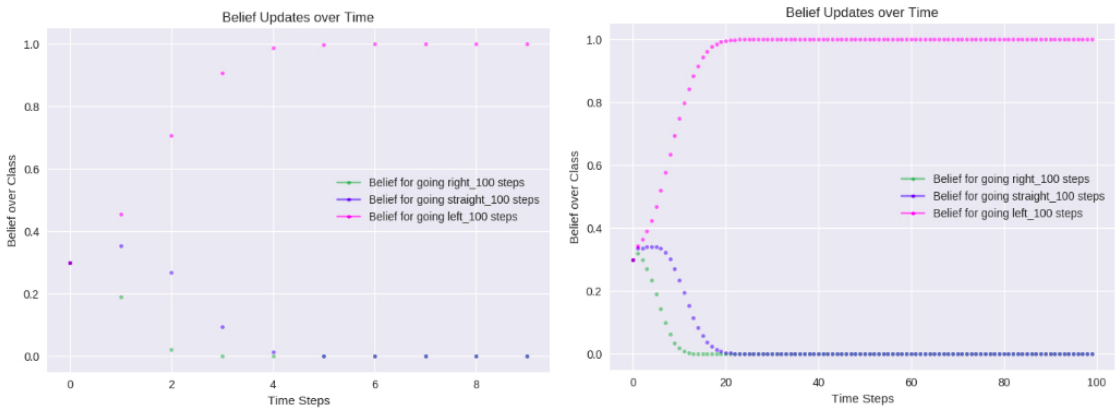


Figure 5.17.: Belief changes over time. For trajectory with 10 steps on the left, for trajectory with 100 steps on the right. Trajectory direction is left

To be able to see how belief is changing over time withing different trajectories and compare if there are the same results at the same steps in the same movement class, we plotted 10 random trajectories going straight. Results are shown in Figure 5.18.

Figure 5.18.: Belief changes over time for different trajectories which belong to the same movement class. Trajectories have 100 time steps. Trajectory direction is left

From the Figure 5.18 it is possible to see that some trajectories have a better time for being sure to which direction car is moving and some of them have a worse time than others. Next two figures will show trajectories which have "the best" (Figure 5.20) and "the worst" (Figure 5.19) times in the movement prediction.

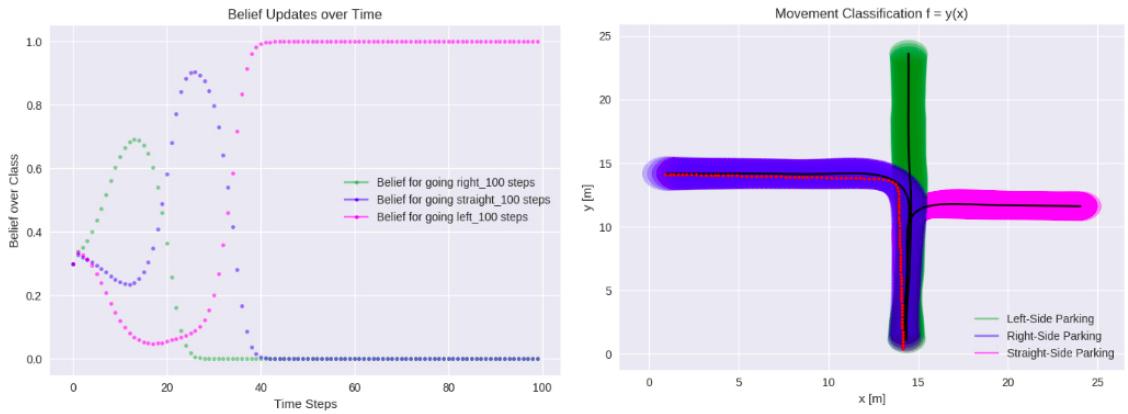


Figure 5.19.: Belief over time changing (left image) and image of testing trajectory (right image). Trajectories have 100 time steps. Trajectory direction is left

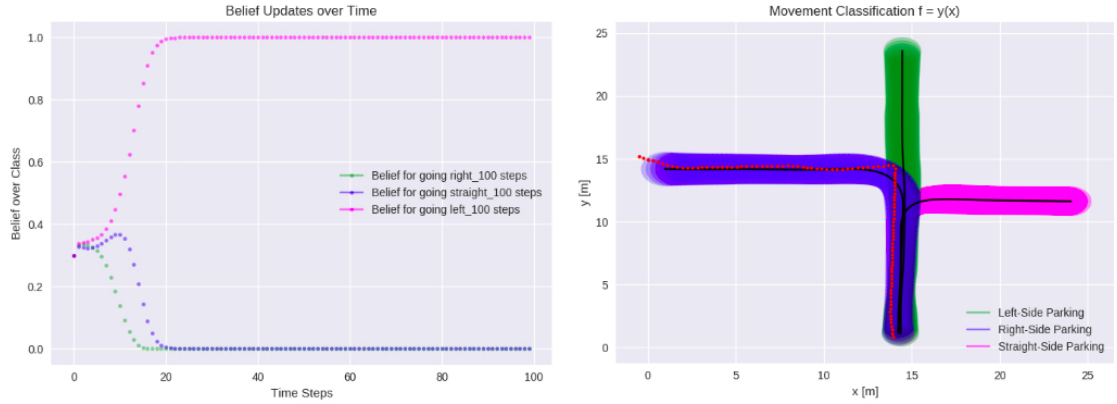


Figure 5.20.: Belief over time changing (left image) and image of testing trajectory (right image). Trajectories have 100 time steps. Trajectory direction is left

TO THINK WHY IT IS DIFFER

5.2 Vehicle is Moving Through T-Intersection

In this section results of simulation setup for T-Intersection (map looks like it is shown in Figure 5.21) will be described. As in the case of the map with X-Intersection, starting position of the car is $x_0, y_0 = (14.5, 2.0)$, but in this setup, the car can go only to the left or right, straight direction does not exist in this case. As in the previous case, at the very beginning, initial belief must be set. Since we already know that there is no way that car is going straight (there is no straight from car starting position), we have so-called some prior information. Initial belief for going right and left is calculated by formula $\frac{\#of\,trajectories going to the right in our database}{\#of\,trajectories going to the right in our database + \#of\,trajectories going to the left in our database}$ and $\frac{\#of\,trajectories going to the left in our database}{\#of\,trajectories going to the right in our database + \#of\,trajectories going to the left in our database}$ respectively. After calculation initial belief set to be $b_0[left, right, straight] = (0.533, 0.467, 0.000)$

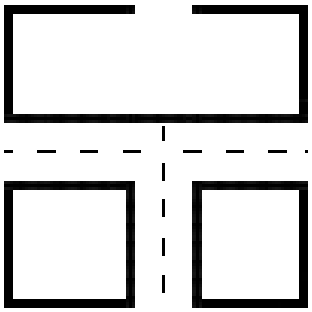


Figure 5.21.: T-intersection map

5.2.1 Moving to the Right Direction

The testing trajectory of going to right looks as it is shown as a red line in Figure 5.22.

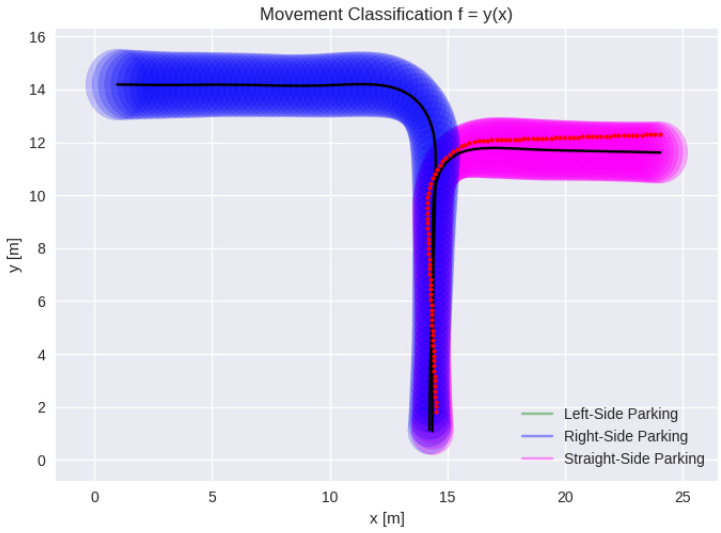


Figure 5.22.: Testing Trajectory (red) of going to right

In Figure 5.23 is shown how beliefs are changing over time. Left graph of the Figure 5.23 shows belief changes when trajectory has 10 points and for better visibility, there was added one more graph on the right, where is the same trajectory, just it was interpolated 100 times instead of 10.

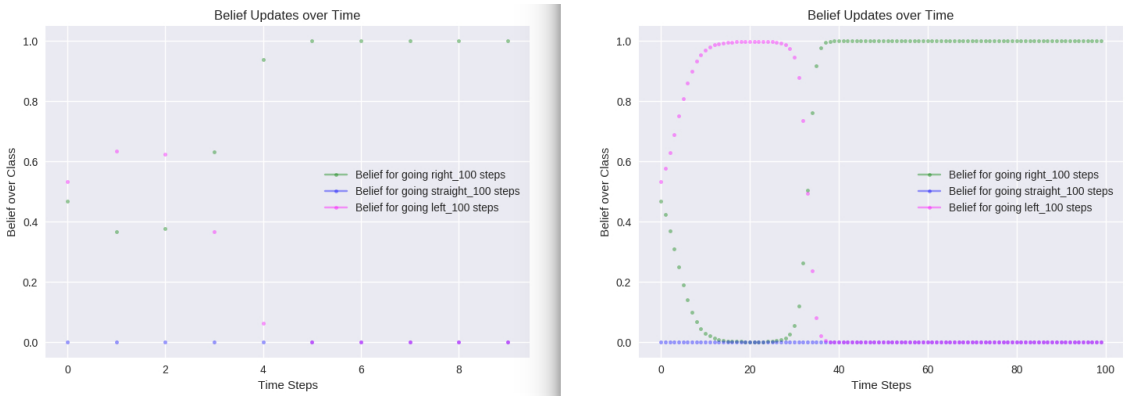


Figure 5.23.: Belief changes over time. For trajectory with 10 steps on the left, for trajectory with 100 steps on the right. Trajectory direction is right

To be able to see how belief is changing over time withing different trajectories and compare if there are the same results at the same steps in the same movement class, we plotted 10 random trajectories going to the right. Results are shown in Figure 5.24.

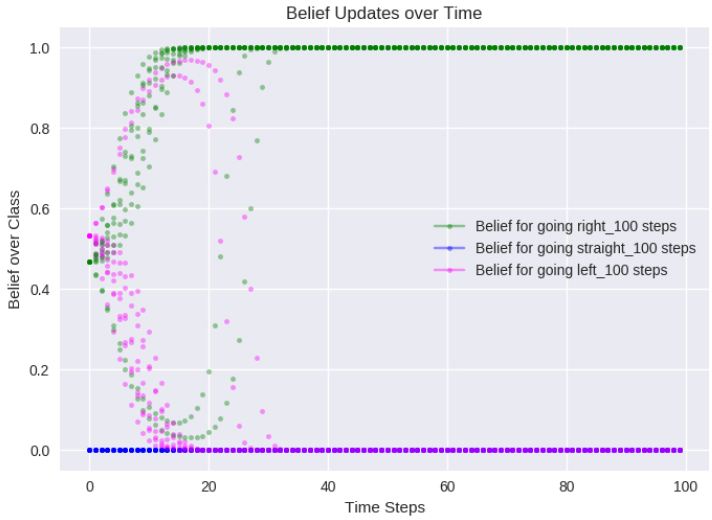


Figure 5.24.: Belief changes over time for different trajectories which belong to the same movement class. Trajectories have 100 time steps. Trajectory direction is right

From the Figure 5.24 it is possible to see that correct prediction is made much faster than in case of map with X-Intersection (Figure 5.5).

5.2.2 Moving to the Left Direction

The testing trajectory of going to right looks as it is shown as a red line in Figure 5.25.

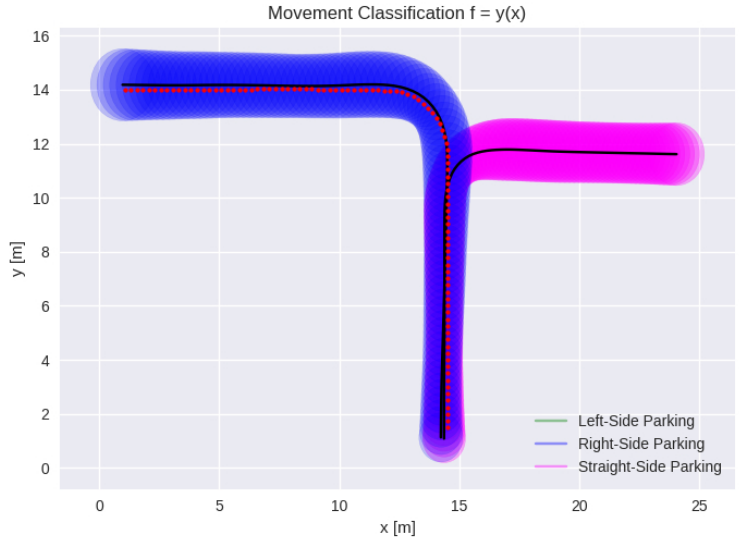


Figure 5.25.: Testing Trajectory (red) of going to the left

In Figure 5.26 is shown how beliefs are changing over time. Left graph of the Figure 5.26 shows belief changes when trajectory has 10 points and for better visibility, there was added one more graph on the right, where is the same trajectory, just it was interpolated 100 times instead of 10.

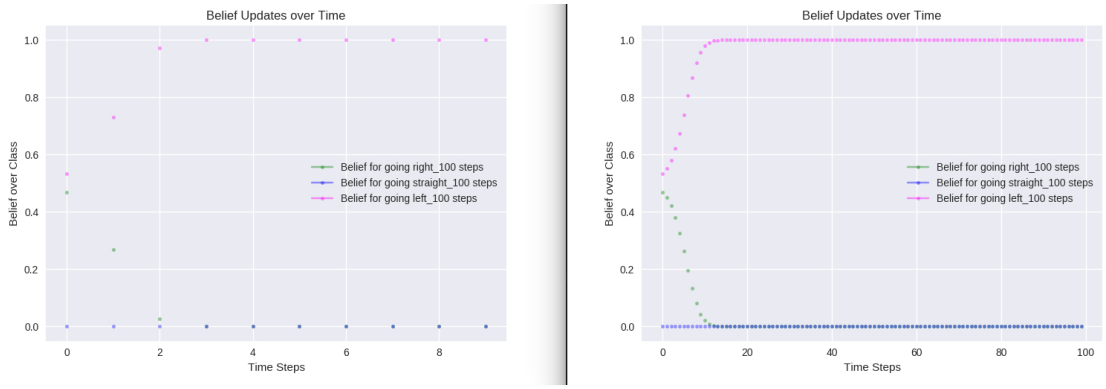


Figure 5.26.: Belief changes over time. For trajectory with 10 steps on the left, for trajectory with 100 steps on the right. Trajectory direction is left

To be able to see how belief is changing over time withing different trajectories and compare if there are the same results at the same steps in the same movement class, we plotted 10 random trajectories going to the right. Results are shown in Figure 5.27.

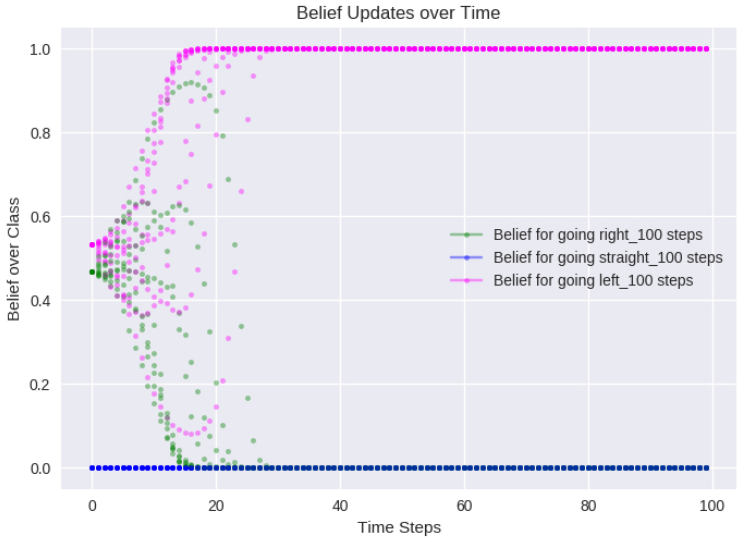


Figure 5.27.: Belief changes over time for different trajectories which belong to the same movement class. Trajectories have 100 time steps. Trajectory direction is left

As we could see from the Figure 5.24, the same results we can see from Figure 5.27: the correct prediction is made much faster than in case of map with X-Intersection. This happened because of prior knowledge.

5.3 Results Comparison Before and After Scaling

As mentioned before trajectory scaling while updating belief can allow not to make calculations so frequently, but still, keep the same precision of results as having a lot of belief updates.

One test on scaling was done having one trajectory interpolated 100 times, at every step in 100-time step trajectory likelihood (formula 4.2) was powered by 0.1 and results were compared with taking every 10th step from the same trajectory, but with calculation as normal. The scaling algorithm is described in Figure 4.5. To show the difference between scaled results and not scaled results two different graphs will be shown for one test.

5.3.1 X-Intersection

X-Intersection has three directions and scaling within all three of them will be shown.

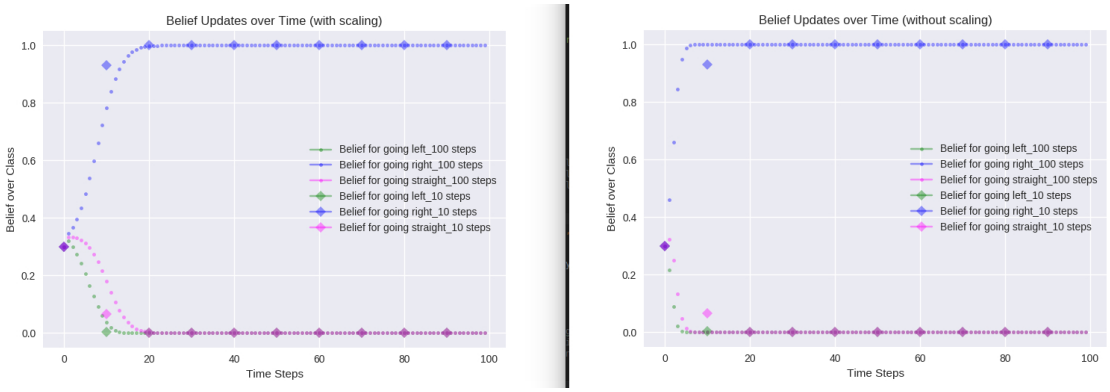


Figure 5.28.: Belief updates using scaling. Direction of the testing trajectory is right

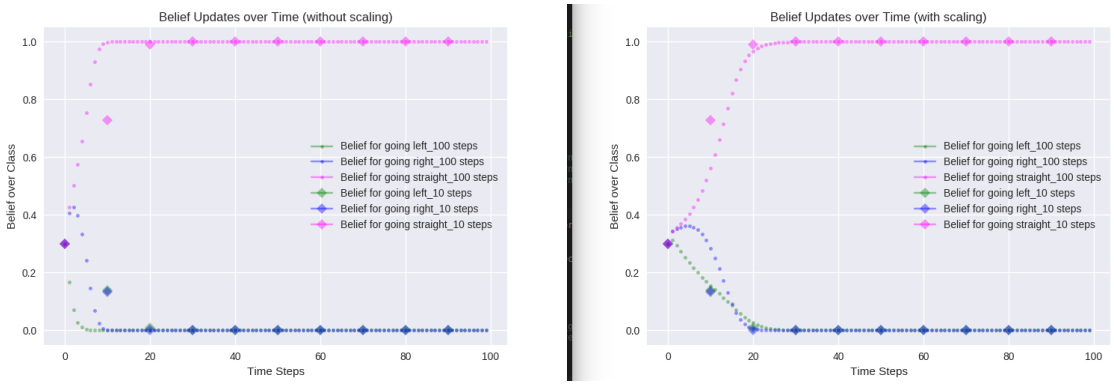


Figure 5.29.: Belief updates using scaling. Direction of the testing trajectory is straight

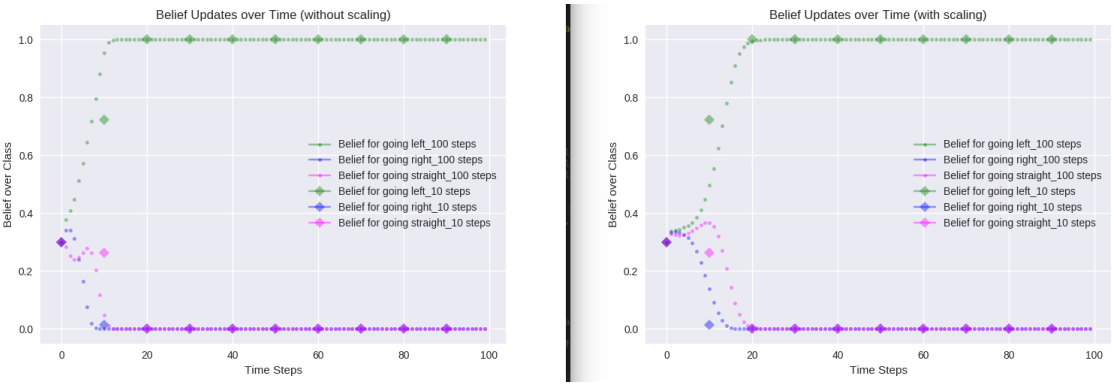


Figure 5.30.: Belief updates using scaling. Direction of the testing trajectory is left

5.3.2 T-Intersection

X-Intersection has two directions and scaling within right and left directions will be shown.

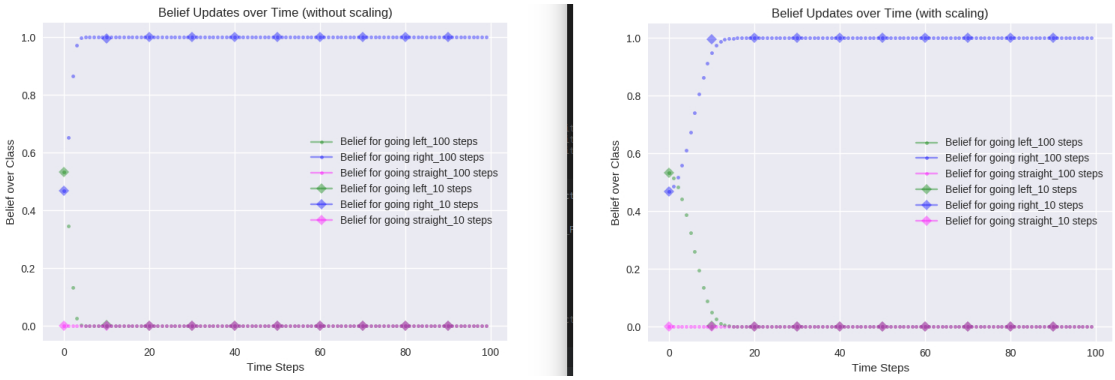


Figure 5.31.: Belief updates using scaling. Direction of the testing trajectory is right

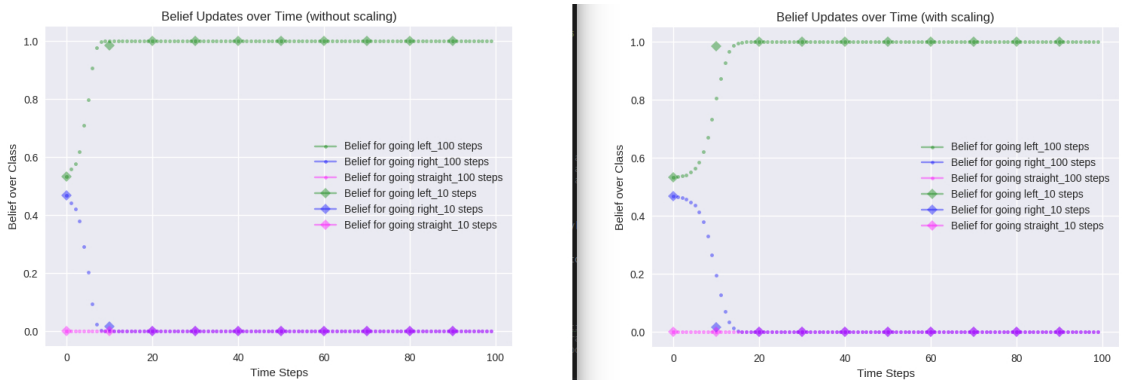


Figure 5.32.: Belief updates using scaling. Direction of the testing trajectory is left

5.4 Prediction Making in Online Method

in process

6 Security Aspects

Fully autonomous cars are not quite ready to go into the roads yet, but they are getting closer to reality more than ever before. More than 60 cities in the world have testing programs for autonomous cars (and possible cyber vulnerabilities). Around 80$ billion is already invested in the technology, and almost every modern vehicle manufacturer has dedicated some resources for more and more automation in the newly launched car [??]. According to statistics [??] around 130k cars with partial automation are sold yearly and with current predictions until 2020 around 98k fully automated vehicles will be sold. Until 2040 this number is expected to be more than 96 million, which represents 95% of all vehicles sold. Without a big novelty in technology, autonomous cars are promising enhanced safety and improved convenience, however, it still has a darker side. Autonomous cars essentially can be called Internet cars and being high-tech vehicles they have vulnerabilities and a lot of security issues. This chapter aim is to get to the bottom of potential security risks and defense strategies.

6.1 General Overview. Background

As autonomous vehicles are getting closer to reality as private and public transit vehicles, it is natural to be interested in safety and security which these new technologies are promising. One report made by FBI brought out a number of security vulnerabilities and concerns related to autonomous vehicles, stating that autonomous technologies can become a potentially deadly weapon in the future [??]. But greater concern than terrorism attacks on autonomous vehicles are the risk of controls systems being hacked in and taking control of a driving or other essential systems and in this way to put into a dangerous situation driver or passengers of the car. Overtaking a control of the car can be used to consciously cause an accident or to drive a car into all new unplanned location and potentially steal a car using technologies. It also can allow lock passengers inside against their will. Or to track the car user and make a profile of the person, who is driving/using a car. In fact, autonomous cars technology are still quite new and it is still hard to see the full scope for security risks of autonomous vehicles.
This can sound too non-realistic, but white hat hackers for years already have been showing security issues related to connected cars, demonstrating how easy is to take control and do harm over a lot of various systems even in non-automated vehicles. All these vulnerabilities connected to the Internet are open to various kind of attacks. Even advanced autopilot system, designed by Tesla can be tricked quite easily. One of Chinese security company demonstrated that it is very easy to spoof sensors of a vehicle, causing them to sense "ghost" objects or fail to detect a real object at all [??]. Here natural question can arise, so what makes autonomous vehicles so vulnerable against malicious attacks as compared with non- or only partial autonomous cars? Authors of [4] suggesting two main reasons:

1. **The increased interaction between autonomous cars and environment.** At the moment the most communications between vehicles on the road occurs via Vehicular Ad Hoc Networks (VANETs). This type of communication allows sharing fast changing surrounding information with vehicles which are nearby communicating vehicle. This allows for other cars/drivers in the cars to be aware of what is the road situation nearby them [57]. Since technologies are improving and fully autonomous cars will be on the roads in the very near future, Vehicle to Infrastructure (V2I) and Vehicle to Internet of Things (V2IoT) communication will be more common on the roads. Due to connectivity in one network, only one "infected" vehicle can compromise the entire network if the network is not properly secured.

2. **The increased interaction between components of the system inside, so-called intra vehicular communication.** Autonomous cars have a lot of different Electronic Control Unitss (ECUs) which are connected with each other using Controller Area Network (CAN) bus. One of the biggest advantages of using CAN bus is that it is like a central unit into which a lot of different modules can be added or removed without changing the wiring architecture in the car. CAN has three main parts: **Data link layer**, which is responsible for data transferring. **High speed** physical layer and **Low speed** physical layer which is also responsible for fault toleration. In most cases, the most important control units (which has a direct impact on safety, e.g. brake or engine control module) are connected to high speed layer and others, not so security sensitive are connected to low speed layer. Not so common situation, but it is possible to have a "gateway bridge" which opens the route for selected packages from low to high (or vice versa) layers. So it is a possibility that that malicious packets are connected to the CAN bus using low speed layer and without any further checking or suspicion it can be transferred into high speed layer causing to serious consequences. Control architecture in autonomous vehicles is working in this way what all nodes get packages from

CAN. Any malicious component which is connected to the internal vehicle network can snoop all communications or it can infect all other elements. In order to protect the network, every path for package moving should be protected to ensure the vehicle security. Unfortunately, it is impossible to predict all possible attacks and to foresee all vulnerable places, because there always be new strategies which will threaten the security of autonomous cars. "The development and improvement of one will always counteract and necessitate the development of another" [4].
Another cause of CAN vulnerabilities is that all CAN packages are not authenticated before using them for communication within the system. Any element of a network can send infected element further if former did not do any validation of the package before accepting it [58]. One way to protect network infrastructure is to use packet-level authentication method. This method allows authenticating a package without having trust association of the package sender [59].

6.2 General Overview. Attack Taxonomy

This section will introduce the potential threats, vulnerabilities and attacks of autonomous vehicles can face. For categorization of attacks, we use way proposed in [4]. Each attack is classified based on: **Type** (or source) of the attacker, **Attack vector** (path and method which was taken to get access to the vulnerable place), **Target**, **Reason/objective/motive** of the attack and **Potential outcome**.

6.2.1 Attacker

It is a source of the attack. Usually, when system face an attack it tries to mitigate that immediately. One of the steps of mitigation should be an identification of attack source. Having this information it is possible not only to prevent future attacks, but also understand why the attack was implemented in the first place.

6.2.2 Attack Vector

It is a way how the attacker got access to the system he is targeting. It is also an enabler for an adversary to exploit the targeted system. Attack vectors can briefly be categorized to *physical* and *remote* access.

Physical Access

These attacks are classified into invasive and non-invasive attacks.

1. **Non-invasive Attacks**: these attacks have no physical contact with the car, usually, embedded devices are used for attack implementation. However, being relatively close to the targeted vehicle is necessary in order attack to work.
    a) *Side-channel attacks*: this attack usually ends with leakage of useful information about transmitted data within the system or internal working paths are mixed to work in alternative ways. An attack can leak information such as power consumption, timing information, signal analysis, etc. The most common defense against this attack is employing asynchronous information processing units or/and "shielding" mechanisms.

2. **Invasive Attacks**: the main difference as compared to non-invasive attacks is that invasive attacks include a physical connection to the targeted system. The result of this attack can be the network security and ECUs can be compromised. Potential way how adversaries can connect to the car and gain access to its ECUs is On-Board Diagnostics-II (OBD-II) port which is usually used for car diagnostic. Another way to reach a car is wireless remote access, this is possible when an autonomous car is connected to the critical infrastructure, e.g. someone in the car connects a smartphone for entertainment reasons, and in this way, all internal system can be exposed to external people or networks. There are different types of invasive attacks which are discussed below.
    a) *Code Modification*:this attack may happen when attacker change the code with malicious modifications in order to compromise the system. This may be achieved by connecting OBD-II scanner to the car. As mentioned before this is a tool for vehicle diagnostic, meaning that it is widely available for anyone who wants to buy it. Advanced models of OBD-II has integrated feature for chip tunning which is used for extraction (and modification) of ECUs codes. This attack can be avoided by ensuring that all connection to the car is password protected, which enable only certified people to connect and modify codes of the car.

b) *Code Injection*: this is a very similar attack to the previous one. In this case, after connecting to the car, the attacker can inject new (most likely malicious) code instead of modifying the old one. Code injections can be made not only by an attacker, the owner of the vehicle or person who is checking a car can also inject a new code, hoping to improve the performance of a vehicle. When injected codes are non-compliant with car's components or when new codes are not proved by authorities, problems can appear. One of the ways to avoid code injections is a usage of the intrusion detection system or/and usage of privileged access, which allows only authorized people to connect to the car, owner excluded.

c) *Packet Sniffing*: also known as package analyzing. For this attack computer program or hardware, called sniffer (or analyzer) is used. A packet sniffer can see details between any communication node. Again, the tool is very useful when network related problems need to be diagnosed. But the tool can be used for malicious purposes as well: an attacker can use sniffers for collecting unprotected information, for eavesdropping or capturing packages for following replay attack. Defenses for this attack can be various encryption techniques for confidentiality in packages protection, as well as usage of real-time packages send/received update messages.

d) *Packet Fuzzing*: this technique usually is used during security testing procedures, when invalid data is sent to the system/element, expecting to get receive some error or fault conditions, which allows exploiting weak places in the system and security loopholes. While testing the system, fuzzing helps to detect problems and utilize them in a further stage. When this technique is used by adversaries, the received information is used to get into the system and do any possible harm. Protection against fuzzing is to fix all errors and security loopholes immediately after its exposure. And system updates need to be verified and authenticated before presenting it to the public and uploading to the car.

e) *In-Vehicle Spoofing*: is a situation in which an attacker, using some software tools, pretending to be another person by falsifying data. In this way, adversary gains an illegitimate advantage. In order to attack be successful adversary need to overcome security mechanisms (if exists) to replace original elements with spoofing devices. Usual defenses for this is into autonomous car network include reply attack resistance techniques and fingerprinting module to be able to differentiate between original and current module in the vehicle system [60].

Remote Access

Since wireless connection to external sensors, such as cameras, Light Detection and Ranging (LiDAR), Radio Detection and Ranging (RaDAR), Global Positioning System (GPS) are getting more and more popular, attackers can also use remote access as method to attack systems of autonomous vehicles.

1. **External Signal Spoofing**: one example for this type of attack is GPS spoofing. This attack is possible because GPS using a wireless connection. During the attack GPS receiver is deceived by sending the wrong signal to GPS from another device. The incorrect signal may be similar to real GPS signal or can be captured before and replayed at a certain time. An attacker can trick GPS receiver to accept and recognize only fake signal by gradually increasing power strength of the wrong signal until it eventually replaces the original signal. As soon as the attacker gains control of GPS device in an autonomous car, he can send false GPS information and lead car in the wrong direction and destination. This attack was not tested on autonomous cars, but it was successfully tested on GPS devices in Unmanned Aerial Vehicle (UAV) and yachts [??, ??]. GPS devices are not the only target in autonomous cars. Vehicles contain numerous sensors, which can be attacked with spoofing. One of these devices could be visual sensors like cameras, LiDARs. Similar to the previously described attack was made on LiDAR sensor in [??]. Sending fake signals to the device in a range between 20 and 250 meters from a car (sensor) a lot of non-existing obstacles can be detected as well as existing obstacles on the road can be missed. The way to protect the system against spoofing attacks is to ensure more security, not to accept any signals and information without checking the authenticity and integrity of a signal sending device. To ensure that correct information is coming to LiDAR additional information sources can be used and perform information checking between two different devices. If this cross-checks matches and succeeds information is more likely to be correct than in a case when information is not matching between different sources.

2. **Jamming**: these attacks are against wireless or external sensors for vision and due to that, the authorized communication might be destroyed. The most sensitive devices for jamming attacks are LiDAR, RaDAR, various cameras. Jamming devices can block sensors for receiving correct data. Authors of [??] used jamming to blind cameras of autonomous vehicles to hide objects on the road and make map "cleaner" as it is. There are ways to protect sensors against this attack using removable near infrared-cut filter to the camera, however, this method is working only in the day time. Another measure is photo-chromic cameras' lenses, which can filter out specific types of light.

6.2.3 Attack Target

The target component of the car is usually depends on motive/object of attack and attacker's intention. If the attacker wants to track a path which car is moving, the target element can very likely be camera and/or RaDAR or LiDAR , since they are vision elements of the car and having information from these sensors it is easy to see and follow the path, car took. If attacker targeting traffic optimization and/or passengers safety, as a target VANET can be used, ect.

6.2.4 Attack Motive

Various motives for attacks are possible, better we understand it, it is more likely to protect all control systems and ensure safe driving. One of possible reasons for attacking can be deception - this is a spreading a false information, hoping to effect behavior of other, this attack may lead to hazardous situations on the traffic/roads. One of motives can be economical - to get a financial gain. The another very serious motive, due the any reasons, can be to cause severe harm to passengers of the car, etc.

6.2.5 (Potential) Consequences

Various consensuses are possible if any of these attacks against autonomous vehicles will be successful, such as some (important) control functions might to fail or be sabotaged, data leakage (e.g. vehicle movement information) is very possible outcome [12??]. The "health" of the system is very likely will be affected after successful attacks, which can lead to passengers of the car health issues.
Figure 6.1 summaries attack taxonomy described earlier in this section.

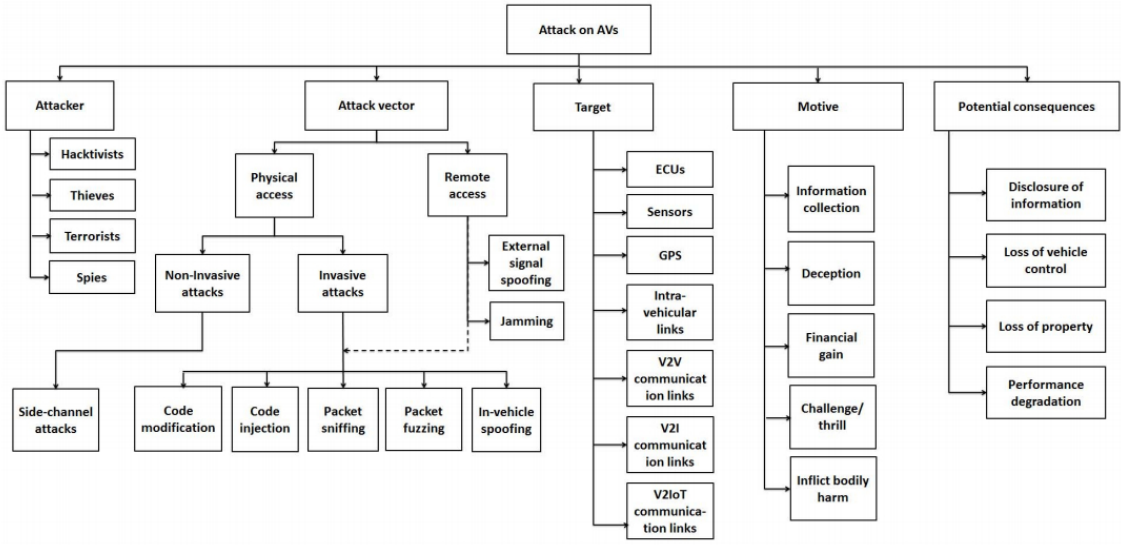


Figure 6.1.: Autonomous Vehicle Attack Taxonomy [4]

Another important problem which must to me mentioned while talking about safety and security issues on autonomous cars and is not mentioned in attack taxonomy yet is **privacy**. An attacker can arrange an attack where he follows car movement, times and makes a very detailed profile about car owner and with this information can do various things: from robbing the house of the victim while he is not at home, to selling this information to someone else, combine different attacks to do the biggest damage attacker want (or is able to) arrange.

6.3 General Overview. Defense against Attacks Taxonomy

As mentioned earlier it is very hard to predict what is going to happen to prevent yourself against attacks. However, with current knowledge about system and known potential vulnerabilities, it is possible to make some kind of predictions and develop network architectures and working protocols which are not so vulnerable. Various literature surveys propose the main 4 types of defenses for autonomous vehicles: **Preventive**, **Passive**, **Active** and **Collaborative** defenses.
This classification and different ways of protection ensure that the system is secure and resilient for different attacks.

6.3.1 Preventive Defense

This type of defense mechanisms mainly focuses on protecting a system from attack before it starts or finishes with success. Preventive defense is mainly focusing on normal working conditions and not during the attack and does not solve any issues with "after attack" scenarios.

1. **Secure Communication**: for secure communication in any case, from simple chatting to serious control commands, data encryption is basic and crucial. Using encryption content and confidentiality of messages are assured. Encryption scheme can also help with the identification of sender/received of sent data. If the encryption scheme does not include identification, integrity and identification of sender/receiver can be assured, using Message Authentication Code (MAC) algorithms. To know the integrity and authentication of another side of communication is very important for secure communication.

2. **In-Vehicle Device Authentication**: controllers used in the car can be completely trusted if they have a manufacturer certificate which gives information such us controller identifier, public key, information about authorized carryout, etc. If information, provided in certificate matches with information which car itself contains, then authentication process is successful and car safely can use all information coming from that particular controller.

3. **User Authentication**: sometimes, in order to have more protection, user authentication is used. To make sure that the right person has access to the car (e.g. doors opening, starting the car, etc.) additional biometric information can be used.

4. **Firewall**: it is an additional tool, which always can be used. Firewalls check all incoming and outgoing data traffic based on rules which user/authenticated people can define. Firewalls also can be very helpful in communication with a trusted and not-trusted environment: this is very important while communicating with different objects in vehicles' networks.

6.3.2 Passive Defense

This type of defense is similar to earlier described preventive defense. Passive defense measures are taken to minimize damage caused by an attacker without having the intention of taking initiative. A passive defense can be an additional level of protection (not the main one). As compared to active defense, the passive defense does not require any analysis from human.

1. **Attack Detection**:
    a) *Intrusion Detection*: To detect physical threats to the car is much easier than to see attacks against system operations. However, there are various models for Intrusion Detection System (IDS) which can be used for autonomous vehicles. Authors of [??, ??] proposed and tested IDS models using various computational simulation scenarios. Even though there are models which have quite good results, research and development of IDS should not stop in order to achieve higher accuracy in attack detections.
    b) *Anti-Malware*: these solutions are used in all usual computer network (or only computer) systems. Anti-malware systems need to be able to protect from harmful attempts to penetrate into the main system. Since malware for autonomous cars is a relatively new thing, it might be not possible to find numerous malware "available", but they still should be taken into account. Research communities, who specialize in autonomous cars, trying to predict possible attack models containing new malware to be prepared for these attacks.

2. **Attack Response**:
    a) *Nullification*: when an attack is recognized by system nullification can be used. This defense mechanism can neutralize an attack using cyber/electronic capabilities, e.g. GPS signal anti-jamming technologies [??]. These technologies suppressing signal from malicious jamming devices.
    b) *Isolation*: it helps vehicles to isolate themselves from other cars during an attack. Self-isolation also prevents ECUs re-programming while the car is running. Self-isolation should happen in a few levels: the autonomous vehicle network system should isolate itself from other vehicles and the affected layer should be isolated from other levels in the same networking system in order not to affect the healthy vehicle behaviour. When a car is attacked ideally it not only should isolate itself but also inform vehicles around about attack in order other cars could take some actions to defend itself against attack.

3. **Attack Recovery**:

a) *Availability*: this feature one of the most important in all types of systems. In the context of autonomous cars, availability is very important when talking about safety inside and outside of the vehicle. In order to ensure safety and have good fault toleration within the system in autonomous cars and to ensure quick recovery after attacks, availability must be ensured in the system.

6.3.3 Active Defense

This is one of the advanced and determined defense techniques. Different approached described below.

1. **Continuous Security Monitoring**: autonomous vehicles belong to critical infrastructure and it is essential that security of these systems should not be compromised. It must have (near) real-time solutions for checking and/or restoring healthy driving conditions in the car. Non-stop and continuous monitoring and "snapshots" of all running systems are required to be available for security checking at any time. It is also important to ensure that all critical devices and interfaces are not blindsided at any time while the car engine is running.

2. **Adaptive Security**: Nowadays the most critical systems are fast changing or refer to infrastructure with a fast pace, hence old and static defense mechanisms are not sufficient anymore. It is necessary to model and use defense mechanisms which are dynamic. So-called adaptive reconfigurations for target can be used for ensuring better control and balance during attack. In order to prepare it self for future attacks defense mechanisms should be able to analyze past and current attacks and use self0learning mechanisms to predict what may happen in the future and adapt defense mechanisms for new forms of attack in the future.

6.3.4 Collaborative Defense

1. **Cloud Computing**: As mentioned above, if cars in the same network over the VANET will share information about potential threats, it is possible that overall security will be improved. When all communication and communication history will be transferred to the clouds, it will become one of the main targets for attackers. Since it will be a "hot spot" for adversaries, security specialist must investigate infrastructure very well, which will give more knowledge and information about potential threats and will let to develop an adaptive defense for better protection of autonomous cars and critical infrastructure.

This section provided a brief summary of vulnerabilities, attacks and defense mechanism in term of security of autonomous vehicles. One of the most important things n security is not to stop looking for potential vulnerabilities and ways to protect the car and all network in case of attack and/or to recover as fast as possible if an attack happened. Regardless of the effectiveness of current methods, it is necessary to think about new defense mechanisms for real-time operations of the vehicle.
Figure 6.2 summaries defense against attacks taxonomy described earlier in this section.

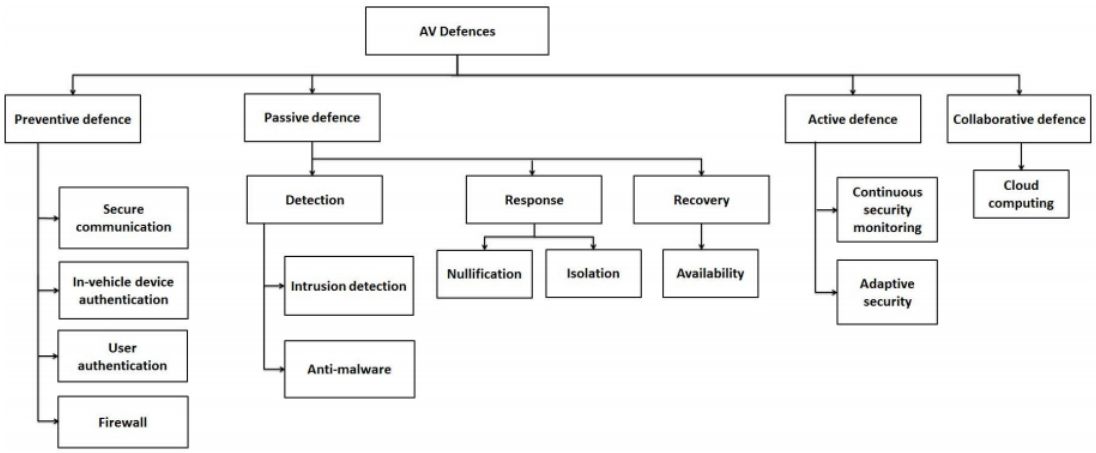


Figure 6.2.: Autonomous Vehicle Defense Taxonomy [4]

6.4 The Most Dangerous Attacks

[61] proposed the scheme from three phases which described all flow in autonomous cars: Sence, Understand and Act. The first phase contains all sensors and raw data collected from them, the raw data is proceeded and represented in the second phase and finally, having all information, in the third phase decision and action can take a place. All these phases are equally important, however, all this algorithm cannot fully functioning with poor (or fake) sensors data.
One of the most important sensors in the autonomous car is a camera and LiDAR, their proper functioning is crucial, due to their popularity in the autonomous industry - camera and LiDAR are used as the main source for information for environment perception.
Further in this section will be discussed the most common and dangerous security attacks while making movement prediction: **visual sensors (on camera and LiDAR) attacks** and common **privacy issues**.

6.4.1 Visual Sensors Attacks

For proving the concept in this thesis we are only creating simulations, i.e. we simulate everything, without using real data, for example from sensors. However, even in simulations the map and obstacles on the road is a very important aspect for prediction making. In reality, autonomous cars are equipped with various sensors which measure different physical properties (sound, light, distance, radio frequency, etc.), GPS, LiDAR, RaDAR systems and of course maps. And to ensure sensors' resilience against various attacks is one of the main challenges. And yes, any of possible attacks against sensors can cause a decision, which can end up as an accident and in the worst case can lead to fatalities. E.g. attacks on camera can cause misunderstanding of traffic signs, leading to unsafe driving conditions with additional danger to passengers in the car and/or other road participants. LiDAR can be fooled and observe non-existing obstacle on the road and start braking, or LiDAR can be triggered to not notice real obstacle and go directly to it. These are only a few scenarios, but all of them can make a huge impact on traffic and its' participants [62].

Attacks on LiDAR

For proper car guidance, which ensures safety on the road proper visualisation on an object on and around the road is necessary. To have good quality data with image-based sensors good weather conditions is required (typically they cannot give proper geometry information under poor weather conditions, e.g. when is raining or when it is not enough light). Laser technologies here had a lot of advantages and LiDAR was introduced. LiDAR working principle is based on laser scanning, and it can accurately capture all types of geometry on the road and to detect a very wide range of objects. However, a very detailed grouping of objects is still a hard task for LiDAR. Recognition of traffic signs or lanes on the road is still cameras' task.
The brief working principal of LiDAR is to notice objects which are giving a reflection of a signal sent by LiDAR. If a sent signal does not come back to the device (it can happen because of transparency of the object, absorption, range limit, when in short range there is no object, etc.), LiDAR thinks that there is no obstacle on the road. As LiDAR performs a very important role in environment perception for autonomous cars and uses simple methods for object noticing, such as light pulses, it is one of the most obvious targets on the autonomous cars. The easiest way to attack LiDAR is to create "noise" and generate (or hide) objects. This section will provide a description on already existing and tested replay and spoofing [61] attacks on LiDAR

Signal Relaying Attacks
Relaying the signal is an expansion of replay attack, which goal is to relay on the signal which was sent before the attack from another position (signal sent from LiDAR is recorded and then (repeatedly) sent from a different location). This allows creating fake echoes and due to that obstacles may appear closer/further than they truly are.
To perform an attack, only two transceivers, one with a photodetector, sensitive to wavelength LiDAR is operating on and one with the laser are necessary. The output of transceiver with photodetector is a voltage signal, which corresponds to the signal intensity which was sent from LiDAR (to be able to see the signal, oscilloscope needs to be connected to the transceiver, but it is not necessary for performing an attack). The output of the first transceiver is sent to another one transceiver (which has a laser in it) to emit a pulse in as its output.
In [61] experiments made when transceivers were in the one-meter distance from each other and in front of LiDAR. But this position is not only one which must be used for making this attack work: it can work very well when transmitters are behind the LiDAR with a bigger distance between each other. A relay attack on LiDAR is most likely to be performed from the roadside, where an attacker can easily receive signals sent by LiDAR on a car, to record them and relay them again from the different location.

Results of an attack, which were noticed by performing it was that before an attack LiDAR only noticed objects detected in short distance (around 1 meter), during the attack range of noticing objects had grown to 20-50 meters - during the attack, it was noticed that LiDAR emits not encoded pulses, and signals can be recorded, replayed and relayed to create fake echoes. Due to this movement planning and decision making can be affected, together making an impact on people and traffic safety.
Note, that to perform the relay attack is relatively easy and cheap, due to that it is widely used for attacking cars in general, not only for attacks on LiDAR.

Signal Spoofing Attacks

While signal relay attack can create echoes, this paragraph will show that it is easy to create fake objects using signal spoofing attacks on LiDAR using the original signal released by LiDAR to "replay" objects on the road and control their location. A signal, sent from LiDAR, travels approximately 200 meters back and forth in about 1.3 μs. Meaning that LiDAR should listen at least this period for incoming sent signal reflections (depending on LiDAR type time for a signal travelling might vary a little bit). In order to make attack successfull, the fake signal must arrive to LiDAR in this small time window, if the signal will come back to LiDAR after this time, it won't be noticeable, that's why attacker needs to know when to release fake signal. Working principle of LiDAR is that longer time it takes for a signal to come back, the further object is, due to that the attacker can "control" location of obstacle by delaying the original LiDAR signal before relaying it. [61] demonstrates an attack, where LiDAR receives the fake signal after the first echo of the original signal is received. This allows tricking LiDAR to think that obstacle is further away since the signal traveled back longer. In order to make the attack work attacker needs to have a transceiver and two pulse generators (they are needed to generate a fake signal, which is sent back to LiDAR). The output of transceiver is connected with the input of one pulse generator (this generator delays its output). The output of this pulse generator is connected with the input of the second (pulse) generator. A defined number of square-wave pulses are generated when the second pulse generator is triggered. These newly generated wave pulses are sent to transceiver. All variables (time for delay in the first pulse generator, number of generated pulses and copies of it, as well as pulse width and its period that is received from the second generator) for this attack can be controlled, by doing this it is possible to "create" all kind of obstacles with all kind of distance between the new object and car. Results of the attack showed that objects which are in around 50 meters distance, usually are noticed within the second echo and by tuning delays, it is very easy to make them closer or further. The first pulse generator can be configured to send multiple pulses to the second pulse generator when it receives a signal from LiDAR. Due to that, it is possible to sent multiple fake signals in sequence back to the LiDAR. The resulting in noticing multiple objects in the desired distance between each other (the first copy will appear in the second echo, the third copy in the third echo and so on until time for LiDAR listening will finish).
The same technique can be used for hiding objects and make LiDAR not see any obstacles, just in this case the pulse generator generates a copy of the signal sent in a "clean" rode.

Countermeasures

The most of countermeasures against LiDAR attack can be implemented in software. Usually, no modification of hardware is necessary, although to make devices more secure manufacturers can improve hardware implementation schemes by adding more secure (or additional) devices. Further in this paragraph countermeasures, proposed by [61], which do not require changing of hardware, will be discussed.

1. **Redundancy**: [63] demonstrated that it is possible to arrange a successful spoofing attack using different wavelengths than proposed before (as long as wavelengths are not overlapping). However, some wavelengths have some disadvantages as compared with others, combining multiple various wavelengths on the same LiDAR operation makes it much difficult to attack them at the same attack.

2. **Random probing**: LiDAR is sending signals with fixed intervals (which depend on LiDAR scanning speed and rotation speed of mirrors inside the LiDAR) between each of them. To make an attack successful, the attacker needs to know exactly when a fake signal must be sent back, for that he needs to synchronize his system with LiDAR operating intervals. One way to avoid attack could be varying these intervals in a not predictable way, however, it can be problematic for LiDAR rotation, because they need to keep constant rotation pace to know at which angle they are operating at the current moment.
   Another way to protect the car from attacks (or more precise to be aware of them) is to randomly skip signals sent from LiDAR. When LiDAR skips sending a signal, he still can listen, if the signal is coming back then it could be an indication that the car is under attack. If the frequency of sending signals is 50 Hz, skipping a few signals won't affect the quality of the LiDAR results, especially if the object is close by, however, this method can affect the quality of LiDAR results if the operating frequency is different.

3. **Shorten the pulse period**: As mentioned before, LiDAR signal usually needs about 1.3 μs to travel back and forth of 200 meters. This time window is also available for attacker operation. If the signal period would be smaller,

it would give less time for attack as well. If this defense technology is used, it is necessary to be aware that if together with a signal period, the maximum range of going back and forth should be reduced as well: if the signal period is reduced to 0.65 μs, the signal traveling range should be decreased to 100 meters too.

Attacks on Cameras

The camera is one of the very important devices in an autonomous car, it can detect traffic signs/lights, various objects on the road, etc. However, there are various ways of how the camera can be attacked: traffic sign recognition can be tricked by adding fake traffic signals at a false location, they also can be visually hidden by surrounding them with shapes which are not considered in the recognition algorithms. As mentioned before, any object recognition using a camera has its own drawbacks due to computation power or/and quality of view, also the camera very depends on the day time (during the night object recognition is more complicated), this opens a lot of different ways to attack the device itself, like attack auto-focus or light sensitivity on camera.
Further paragraphs describe attacks whose goal is to hide objects and trick auto-controls of the car. To prove that attack is possible, an attacker only needs a laser pointer or Light Emitting Diode (LED) light. During the experiments, authors of [61] uses tonal distribution (on grayscale value), with a total of 256 bins.

Blinding the Camera

As the name of attack hints, the goal of the attack is partially or fully blind the camera. Failing to recognize various objects on the road, such as traffic lights or/and signs car really affect the safety of people in the car and other traffic users.
The camera is considered to be blinded when a camera cannot tune the auto exposure or get it down anymore. When this happened, the light cannot be shadowed and image from camera becomes overexposed. The main 3 elements exist, which can make an attack less or more effective: **environment light** - when the camera is in a bright environment, more additional light is needed to raise the light in order to reach camera blinding point; **light source, which is used for blinding** and **the distance between light source and camera**. To test multiple attack scenarios tests were made in bright and dark environments and with different distances between the camera and light source (0.5 m, 1 m, 1.5 m and 2m). The thing which must be considered: when the distance between the light source and camera is bigger, more light sources are needed. Experiment as held when the light source was in front of the camera. The results of experiments showed that laser with 650 nm diode point is the most effective in a short-range environment. When laser if off, camera obviously can see the background and all view in its visibility range, when a light source is on, the background is not visible and the camera is partially blinded: light source shifted camera's tonal distribution. In the brgiht environment, the most effective light sources are the 650 nm laser, while in the dark, the 940 nm laser has the most influence. Even though experiments were not successful in achieving the full blindness, these light sources still are good enough for attack since even with partial blindness images from camera is not readable. More detailed results can be found in [61].

Countermeasures

Some methods exist to protect cameras from being attacked. Unfortunately, most countermeasures require serious hardware changes and this increases not only price range, but the size of the device as well, which can cause some problems for space limitation in the automotive environment.

1. **Redundancy**: As usual, multiple cameras which capture the same image could make a big challenge to an attacker, since he needs to blind multiple cameras at the same time. Using multiple cameras might not protect against well-prepared attacks which are using a very strong light source but for usual size attack, it would be enough. However, to put more cameras on the car requires more space on the car nominated only for cameras, it also requires more calibration, because of images with overlapping places can misalign between each other.

2. **Optics and materials**: It is always possible to add safer hardware parts to be able to ensure more resilience to attacks. Removeable near-infrared-cut filters are already available and used on security cameras, it can filter infrared lights on request. During the day time, it gives better quality pictures and during the night filter is removed an only camera's infrared light is used for night vision. Since the filter is useful only during the day time, it can protect cameras against attacks also only during the day.
   Another way to protect cameras against attacks is to use photochromic lenses, they can be set to filter only specific types of lights. As an example for photochromic lenses could be darkening glasses, which would be useful for sunlight. Depending on the type of lenses, it identifies which type of light it can (or will) filter. The advantage of these lenses is depending on the type of materials it could be that they do not affect the quality of the image in a low-light environment.

6.4.2 Slight Object, Captured with the Camera, Modification and How Does that Affect Images Recognition

To operate safely and correctly autonomous cars, as other robot-based systems have "to see" the world. For this reason, a lot of cameras are used, without them, algorithms of autonomous cars cannot fully function. The section above described some attacks on the camera itself, this section will talk about modification on street signs which can trick visual recognition algorithms in the car. As stated before to see the world pictures from cameras are used. But usually, between the images which camera is taking are some gaps, which hide some information. To solve this so-called black box of machine learning algorithms are used, these algorithms are trying to interpret some common patterns between pictures into something algorithms are familiar to. Before using these algorithms in real life they must be trained before. Usually, in this process a lot of pictures of the same thing with some differences are showing, then the algorithm is checked if it can recognise a picture of the same thing which is not in the data set which with algorithm was trained.
This training method works quite good, but it is more complicated than it can look: algorithms do not look common feature in the manner of "look for a red sign with STOP on it" (for stop sign). They are searching for features which are not so easily recognizable to human eyes. It can look a bit not understandable for human, but this machine learning algorithm recognition model works because there is a fundamental difference between how the human brain works and how the world is interpreted with artificial intelligence. Meaning that any visible changes (does not matter how big or small they are) can be understandable by human and by the algorithm in a completely different way. Even though it does not look like slight modifications on images require complicated analysis and various image manipulations to recognize the correct object. Authors of [5] showed that it is possible to fool machine learning algorithms and image recognition by introducing very small changes on the physical road sign: a bit of paint or stickers on a sign can create a lot of troubles in recognition e.g. stop sign instead of thinking that it is speed regulation sign.
[5] showed that combining the picture with the adversarial image while processing captured photo can cause vision system to recognize something completely different, an example can be seen in Figure 6.3. This can cause a lot of damage to all traffic participants.

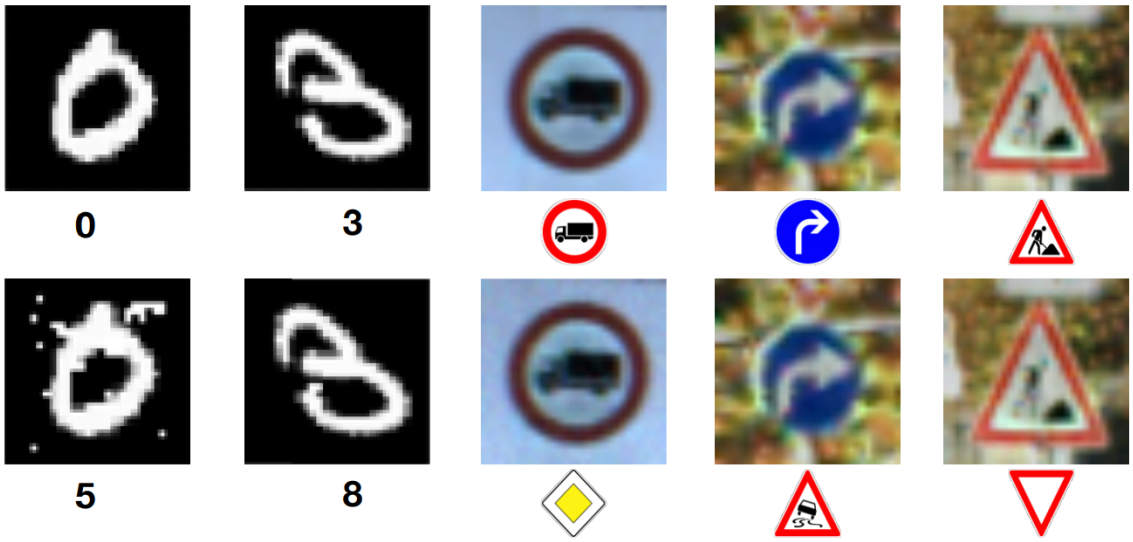


Figure 6.3.: The upper line of pictures shows the correctly recognized images (pictures had no adversarial information combined with original image). The bottom line of pictures shows captured pictures, combined with adversarial information, and what is recognized with the same algorithm [5]

Attacks, introduced in [5] are effective, but it is much harder to make it a real life rather than in the laboratory. The advertiser usually does not have direct access to control what is coming as an input to a vision recognition algorithm. As well, usually there are a bunch of other pictures of the same place in different directions and angles, so different algorithms can compare the pictures of the same place in different situations. And the last thing which does not usually work in the real world is that adversarial images contain the same features in all image not separating traffic sign or background.
The difference of method proposed in [6] is based on changing the sign physically - to alter signs in the way that visual recognition algorithms would be not able to correctly recognize the sign. For that author came with some "sign damaging" techniques: "subtle fading, camouflage graffiti, and camouflage art". Figure 6.4 shows how perturbed signs, used in experiments, look like.
There are different and easier ways to "damage" signs to mess up with visual recognition algorithms. It is possible to add some stickers or graffiti on signs as in Figure 6.5.

Figure 6.4.: Subtle perturbations on signs resulted in misclassification of stop signs and think that it is speed limit 45 sign. The sign to turn right was recognized as a stop sign [6]

Figure 6.5.: Camouflage graffiti and art stickers caused visual recognition algorithms to recognize stop sign as speed limit 45 [6]

Due to being smaller, stickers have a visibly smaller zone, their created perturbations have a more significant impact on sign recognition but less visible by the human eye, and it worked as well. According to the authors of [6]: "*The Stop sign is misclassified into our target class of Speed Limit 45 in 100% of the images taken according to our evaluation methodology. For the Right Turn sign... Our attack reports a 100% success rate for misclassification with 66.67% of the images classified as a Stop sign and 33.7% of the images classified as an Added Lane sign. [The camouflage graffiti] attack succeeds in causing 73.33% of the images to be misclassified. In [the camouflage abstract art attack], we achieve a 100% misclassification rate into our target class*".
Authors of [6] for algorithm training used publicaly available labeled data set. They assumed that the attacker won't be possible to play around with training data, but he can send images into an algorithm and see what results are coming out, to be able to see how algorithm recognize signs. And at the end authors took the "normal" image of the sign which is going to be attacked, gave it to the algorithm and received an adversarial image for result. It is probably a good assumption to make those classifiers which are used for autonomous vehicles have more sophisticated and robust than those which were used by authors. And it would be naive to think that hackers won't ever figure it out how to walk around even the most sophisticated and robust classifier ever. Probably the best defense against these attacks would be

to use a multi-modal system for road sign detection as they are using it for obstacle detections - it is not very wise to trust only one sensor for these crucial tasks [64].

6.4.3 Privacy Issues

While autonomous cars might sound very convenient and create new forms of accessibility, we do need to remember that most of this comfort comes at a very big cost of privacy. To be able to ensure safety rides and all comfortability most of the people are expecting autonomous cars has a number of various sensors, which are proceeding a lot of data. Basic sensors of the car is visualized in Figure 6.6.

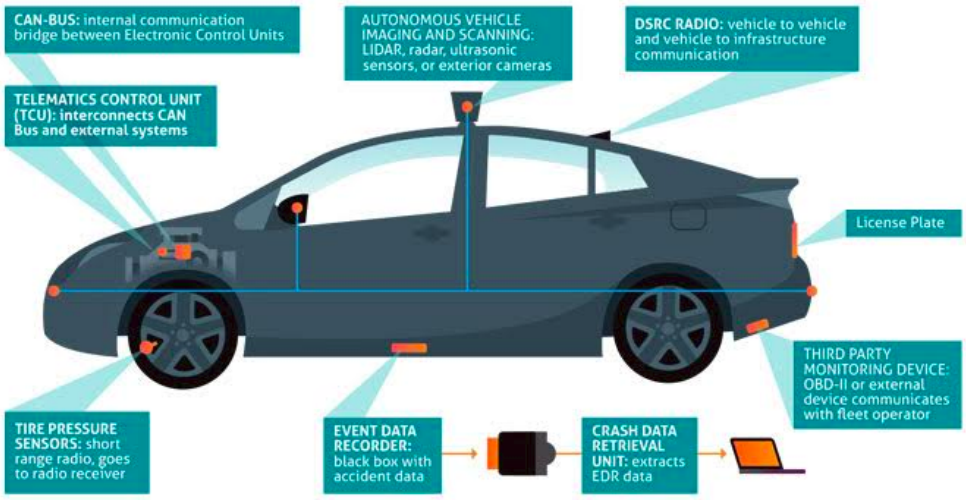


Figure 6.6.: The Basic Data-Generating Devices and Flows in Autonomous Cars [7]

Article [65] provides a very clear scenario of how "Automated vehicles will learn everything about you—and influence your behaviour in ways you might not even realize". Most of the people in the morning go at work, so considering the time of the day, when an owner of the car gets into it, an autonomous vehicle will ask (or suggest) about driving at work first. Later, during the ride to work, car's owner want to take a coffee and car can suggest the coffee store or inform about sales and other offers which are happening in the stores which are on the route to work. On first sight, it might look awesome, but on the other hand to make these suggestions car needs to have some sensitive information about car's owner life and habits, as well as potentially be influenced to announce sponsored content. When a car makes an offer to go to work, it knows that at this particular time, the car is used to go to work. When a car gives you information about sales and coffee place, the order of offers coming out is based on how much business paid to advertise this offer (more expensive advertisement is, faster it is announced). Even though a lot of people can not see any problems with it, however, it can hide two big problems. First, car for obvious reasons always retains information where the car is and this can be very valuable knowledge for attackers/hacker. By knowing the place where and when the owner of the car is working, the attacker can make an assumption about the financial status of the car owner and knowing the time he is not at home, an attacker can easily break into his house and rob it. Additionally, during the robbery, an attacker can still track the car location and whenever car starts to move from current location, it can indicate that owner os potentially coming back to home and it is about time to leave. The second problem is that accepting the first location car suggested could give the car's owner personal data to marketers for highly specific marketing purposes without him/her even knowing this.

To consider these aspects is very important while thinking about the adaptation of autonomous cars, however, all legislation on autonomous cars so far are very vague when it is related to the aspect of privacy. So far only plan to keep the car owner informed how and where his data will be used is defined [66]. This is a start, but still privacy issue not even close to being clear. A lot of people agree that it is crucial to regulate at least "minimum acceptable level of security" when it comes to data from autonomous cars, as there are minimum safety standards for the cars nowadays. We already have a very high number of issues for privacy which is related to the usage of smart technologies and it would be wise to think that the number of issues only grow with autonomous cars. Laws for privacy as always difficult to define, however, these questions are crucial for a secure transition to the safe world with autonomous cars.

Personal privacy is not the one concern which needs to be addressed. The case in 2016 when FBI was trying to force Apple to give access to personal iPhone of person who was suspected to be a shooter in San Bernardino attacks [67],

raised a legal issue: in which precedent manufacturer can (or need) to give personal user data to law enforcement. In the case, mentioned in [67], the phone was an Apple product, but the data stored in the phone was the individual property of the phone owner. Could the law enforcement/government force the manufacturer of the autonomous vehicle to decrypt the personal data and give all information where someone was and where potentially could go? Again, on the first sight, it can look very innocent for cars' manufacturer to reveal the data of "dangerous" person, but this as well could affect the general consumer. When the manufacturer create a "back doors" which can give access to data of the user, just for "in case" scenario, these "doors" can be used not only by the manufacturer, it can be used by a malicious hacker to access a data and gain an important information which could be used to harm innocent autonomous car owner. In theory, to be able to protect consumers data, a manufacturer should ensure a security level of a device/car that even they could not get access to it in any cases: yes, this can save some criminals from being caught easier, but it would protect the vast majority of the people, who has a legal right to want that their information would be protected [68].
Data and personal privacy is always a big concern when it comes to any type of technology which uses data, however, autonomous cars will have an "access" to people personal lives starting with car's location to environ them around it. With roads full of sponsored cars there will be no way that someplace and information about it will not be recorded, processed and stored. Due to that ensure safe storage for data is one of the most crucial tasks [68].

7 Conclusions and Future Works

TODO

Bibliography

[1] W. Z. Yeping Hu and M. Tomizuka, "Probabilistic Prediction of Vehicle Semantic Intention and Motion," 2018.

[2] A. Singh, "PREDICTION in Autonomous Vehicle - All You Need To Know."

[3] C. L. Stéphanie Lefèvre, Dizan Vasquez, "A survey on motion prediction and risk assessment for intelligent vehicles," *ROBOMECH Journal*, 2014.

[4] V. L. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," 2016.

[5] I. G. S. J. Z. B. C. Nicolas Papernot, Patrick McDaniel and A. Swami, "Practical Black-Box Attacks against Machine Learning," 2017.

[6] E. F. B. L. A. R. C. X. A. P. T. K. Kevin Eykholt, Ivan Evtimov and D. Song, "Robust Physical-World Attacks on Deep Learning Visual Classification," 2018.

[7] F. STAFF, "Infographic: Data and the Connected Car – Version 1.0."

[8] A. F. for Traffic Safety., "American Driving Survey, 2015 – 2016."

[9] WHO, "Global Status Report On Road Safety 2018."

[10] S. R. Kaiming He, Xiangyu Zhang and J. Sun, "Delving Deep into Rectifiers: Surpassing Human-Level Performance on ImageNet Classification," 2015.

[11] T. Keeney, "Mobility-As-A-Servive: Why Self-Driving Cars Could Change Everything," 2017.

[12] TuD, "aDDa for Students."

[13] G. B. Ismail Dagli, Michael Brost, "Action recognition and prediction for driver assistance systems using dynamic belief networks," p. 179–194, 2002.

[14] K. T. Shigeki Tezuka, Hitoshi Soma, "A study of driver behavior inference model at time of lane change using bayesian networks," p. 2308–2313, 2006.

[15] A. P. Andrew Liu, "Towards real-time recognition of driver intentions," p. 236–241, 1997.

[16] A. P. Andrew Liu, "Modeling and prediction of human behavior," p. 229–242, 1999.

[17] A. P. Nuria Oliver, "Driver behavior recognition and prediction in a smartcar,," p. 280–290, 2000.

[18] A. P. Nuria Oliver, "Graphical models for driver behavior recognition in a smartcar," p. 7–12, 2000.

[19] D. D. Salvucci, "Inferring driver intent: A case study in lane-change detection," p. 2228–2231, 2004.

[20] C. S. Yi Hou, Praveen Edara, "A genetic fuzzy system for modeling mandatory lane changing," 2012.

[21] D. D. S. Hiren M. Mandalia, "Using support vector machines for lane change detection," 2005.

[22] M. J. Kochenderfer, "Decision Making Under Uncertainty: Theory and Application," p. 11–57, 2015.

[23] A. R. C. Leslie Pack Kaelbling, Michael L. Littman, "Planning and acting in partially observable stochastic domains," p. 99–134, 1998.

[24] A. R. Nachiket Deo and M. M. Trived, "How Would Surround Vehicles Move? A Unified Framework for Maneuver Classification and Motion Prediction," 2018.

[25] J. S. Mattias Brannstrom, Erik Coelingh, "Model-Based Threat Assessment for Avoiding Arbitrary Vehicle Collisions," p. 658–669, 2010.

[26] K. K. Jrg Hillenbrand, Andreas M. Spieker, “A multilevel collision mitigation approach: situation assessment, decision making, and performance tradeoffs,” p. 528–540, 2006.

[27] A. J. A. L. A. Aris Polychronopoulos, Manolis Tsogas, “Sensor fusion for predicting vehicles’ path for collision avoidance systems,” p. 549–562, 2007.

[28] F. N. Samer Ammoun, “Real time trajectory prediction for collision risk estimation between vehicles ,” p. 417–422, 2009.

[29] M. S. Nico Kaempchen, Kilian Weiß, “IMM object tracking for high dynamic driving maneuvers,” p. 825–830, 2004.

[30] J. B. Thomas Batz, Kym Watson, “Recognition of dangerous situations within a cooperative group of vehicles,” p. 907–912, 2009.

[31] K. P. Murphy, “Dynamic Bayesian networks: representation, inference and learning,” 2009.

[32] S. B. Adrian Broadhurst and T. Kanade, “Monte Carlo road safety reasoning,” p. 319–324, 2005.

[33] A. M. Matthias Althoff, “Comparison of Markov chain abstraction and Monte Carlo simulation for the safety assessment of autonomous cars.,” p. 1237–1247, 2011.

[34] D. from Wordreference, “Definition of maneuver.”

[35] S. B. Tobias Gindele and R. Dillmann, “A probabilistic model for estimating driver behaviors and vehicle trajectories in traffic environments ,” p. 1625–1631, 2010.

[36] D. R. Ismail Dagli, “Motivation-based approach to behavior prediction,” p. 227–233, 2002.

[37] L. H. S. J. P. H. Georges S. Aoude, Vishnu R. Desaraju, “Driver behavior classification at intersections and validation on large naturalistic dataset,” p. 724–736, 2012.

[38] C. Laugier *et al.*, “Probabilistic analysis of dynamic scenes and collision risks assessment to improve driving safety,” p. 4–19, 2011.

[39] A. W. G. B. J. Schlechtriemen, F. Wirthmueller and K.-D. Kuhnert, “When will it change the lane? A probabilistic regression approach for rarely occurring events,” p. 1373–1379.

[40] G. B. J. Schlechtriemen, A. Wedel and K.-D. Kuhnert, “A probabilistic long term prediction approach for highway scenarios,” p. 732–738, 2014.

[41] V. C. Y. W. Adam Houenou, Philippe Bonnifait, “Vehicle Trajectory Prediction based on Motion Model and Maneuver Recognition,” p. 4363–4369, 2013.

[42] K. K. H. L. D. S. L. J. P. H. Georges S. Aoude, Brandon D. Luders, “Threat assessment design for driver assistance system at intersections,” p. 1855–1862, 2010.

[43] M. M. T. Brendan Tran Morris, “Trajectory learning for activity understanding: Unsupervised, multilevel, and long-term adaptive approach,” p. 2287–2301, 2011.

[44] K. D. Holger Berndt, Jorg Emmert, “Continuous driver intention recognition with hidden Markov models,” p. 1189–1194, 2008.

[45] M. M. T. Aida Khosroshahi, Eshed Ohn Bar, “Surround vehicles trajectory analysis with recurrent neural networks,” p. 2267–2272, 2016.

[46] J. A. Matthias Schreier, Volker Willert, “Bayesian, maneuver-based, longterm trajectory prediction and criticality assessment for driver assistance systems,” p. 334–341, 2014.

[47] J. F. Quan Tran, “Online maneuver recognition and multimodal trajectory prediction for intersection assistance using non-parametric regression,” p. 918–923, 2014.

[48] C. W. H. R. E. Kfer, C. Hermes and F. Kummert, “Recognition of situation classes at road intersections,” pp. 3960–3965, 2010.

[49] C. F. P. G. T. D. W. A. Lawitzky, D. Althoff and M. Buss, “Interactive scene prediction for automotive applications,” pp. 1028–1033, 2013.

[50] K. S. C. Hermes, C. Wohler and F. Kummert, “Long-term vehicle motion prediction,” p. 652–657, 2009.

[51] D. Vasquez and T. Fraichard, “Motion prediction for moving objects: a statistical approach,” p. 3931–3936, 2004.

[52] F. D.-V. J. M. Joseph and N. Roy, “A Bayesian nonparametric approach to modeling mobility patterns,” p. 1587–1593, 2010.

[53] U. K. J. Wiest, M. Hffken and K. Dietmayer, “Probabilistic trajectory prediction with Gaussian mixture models,” p. 141–146, 2012.

[54] N. R. J. P. H. Georges S. Aoude, Joshua Joseph, “Mobile agent trajectory prediction using Bayesian nonparametric reachability trees,” p. 1587–1593, 2011.

[55] ROS, “ROS joy package summary.”

[56] S. Scholar, “Toy Problem.”

[57] N. A. S. G. D. K. Swarun Kumar, Lixin Shi and D. Rus, “CarSpeak: A Content-Centric Network for Autonomous Driving,” 2012.

[58] F. R. S. P. Karl Koscher, Alexei Czeskis and T. Kohno, “Experimental Security Analysis of a Modern Automobile,” 2010.

[59] D. Lagutin, “Packet Level Authentication Overview,” 2010.

[60] K.-T. Cho and K. G. Shin, “Fingerprinting electronic control units for vehicle intrusion detection,” 2016.

[61] F. K. Jonathan Petit, Michael Feiri, “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR,” 2015.

[62] F. K. Jonathan Petit, Michael Feiri, “Revisiting Attacker Model for Smart Vehicles,” p. 1–5, 2014.

[63] H. M. Xuesong Mao, Daisuke Inoue and M. Kagami, “Demonstration of In-Car Doppler Laser Radar for Range and Speed Measurement,” p. 599–607, 3013.

[64] E. Ackerman, “Slight Street Sign Modifications Can Completely Fool Machine Learning Algorithms.”

[65] A. LaFrance, “How Self-Driving Cars Will Threaten Privacy.”

[66] A. Marshall, “Congress Units (GASP) to Spread Self-Driving Cars Across America.”

[67] A. Kharpal, “Apple vs FBI: All you need to know.”

[68] B. Cresitello-Dittmar, “Privacy Concerns of Self Driving Cars.”

[69] A. M. Matthias Althoff, “Comparison of Markov chain abstraction and Monte Carlo simulation for the safety assessment of autonomous cars,” p. 1237–1247, 2011.

A Some Appendix

Use letters instead of numbers for the chapters.