Privacy-Preserving Localization Techniques for Autonomous Vehicle Navigation Systems

By Dr. Svetlana Bozhko

Professor of Applied Mathematics, Belarusian State University

1. Introduction

In this paper, we present several privacy-preserving techniques that can be used for vehicle localization in autonomous vehicles. These techniques use plausibly deniable encryption and randomness in initial seeds to hide the location trajectory of a vehicle while it is moving. We evaluate our techniques and demonstrate that it is possible to achieve the same level of accuracy (in terms of localization) and save power on the computing platform in the autonomous vehicle, as compared to using the basic distributed (or centralized) Monte Carlo localization algorithms. Our privacy-preserving algorithms also operate about the same amount of time as Monte Carlo localization, while the vehicle is moving on a given trajectory. We also demonstrate that an adversarial observer cannot retrieve the last known location or the true position trajectory of an autonomous vehicle that uses our privacy-preserving Monte Carlo localization algorithm while it is moving. Our work is the first published evidence that privacy-preserving vehicle localization is practical.

There has been a large amount of research on vehicle localization over the past two decades. Recently, with the development of autonomous vehicles, there has been increasing interest in developing new and more accurate localization systems for autonomy. However, to our knowledge, no published work focuses on building accurate vehicle localization systems that are also privacy-aware in their design. While we are interested primarily in privacy-preserving autonomous vehicles, the techniques we present can also be used in other domains that use other variants of the Monte Carlo localization algorithm, including robotics, server-based localization (e.g., location-based services) and simulations.

1.1. Background and Motivation

There are also infrastructure-based DSRC V2I/V2V systems, but they require additional infrastructure that increases the cost and may affect the mobility of autonomous vehicles, specifically in environments such as buildings and cities with closely and irregularly distributed structures. For increased privacy preservation of the data generated and transferred to localization services provided by other vehicles or infrastructure equipment, there is a need for privacy-preserving outsourced localization services. With privacy-preserving security measures in place, many drivers would feel much more comfortable about using navigation services that give either turn-by-turn instructions or maps.

Autonomous vehicle navigation systems are equipped with localization systems to determine the location of the vehicles with high precision. Localization is one of the key problems in driver assistance systems as well as in autonomous vehicle navigation systems. Among a number of existing localization systems that can be utilized, a GPS-based system is exploited broadly due to its low installation and running costs. However, GPS-based localization systems are highly susceptible to jamming, multipath reception, and signal loss due to structural blockage.

1.2. Research Objectives

Requirements: First, we combined the segmentation speed of the existing system with the landing synchronous method. Next, we designed the autopilot architecture of this automatic driving system, and continue to optimize the privacy protection module. We compared the advantages and disadvantages of the two protocols while also achieving V2V synchronization positioning. We assessed the efficiency and security of the new protocol. We compared the performance gains in the case where the light turns red at the traffic light compared to the conventional intersection control protocol's median time. Finally, and most importantly, we must clarify whether the performance improvement obtained is significant, and what the bounds of this improvement are. The first implementation and validation of the automatic driving system under various scenarios will be demonstrated.

Because the open sharing of location information of a vehicle traveling in the smart city is risky to users since it reveals their movements to outsiders, when users are inquiring road information, we design a privacy-preserving protocol. The vehicle itself uploads only the current location to the server, while the server takes the position information corresponding

to the position request information, instead of taking the entire path of the vehicle. The various languages exchanged between the server and the vehicle in the protocol are supported by the localization system in the autonomous vehicle. That is not the main concern of our work. We propose two schemes. One of them uses the NPC to share current location information and queries position. The other scheme has been developed to compute the position information of a vehicle on a lead that is a specific segment such as a traffic light or a V2X device. Privacy information and query times vary for the two schemes.

1.3. Scope and Limitations

Once the NDF is protected and a privacy policy is chosen, we should calculate the noise to be added to the NDF to achieve the required level of privacy. However, in a remote sensing application, this calculation should be done with respect to some set of external data and a statistical criterion, such as zero knowledge.

In order to reduce the information revealed by the NDF, in a first approach, we add inaccurate data, setting our NDF as a probabilistic frequency distribution by employing a smoothing algorithm. This way, we can enlarge the size of the protected region with no added entropy. Then, we apply a privacy policy associated with a delta. With this technique, the privacy level is constant regardless of the privacy policy or the amount of noise. However, the coherence with the other parameters may be compromised, particularly in a search and rescue mission, where the first responder would like to receive the maximum information. Furthermore, in the case of an EFC, a noise parameter is essential for the Standard Operation Scenarios (SOS) compliance, and it must be calculated based on it.

2. Autonomous Vehicle Navigation Systems

A traditional approach to aiding GNSS-denied or GNSS-challenged environments leverages simultaneous localization and mapping (SLAM) algorithms to construct a map of where the vehicle has traveled. This map, created using LiDAR or cameras, is then utilized to identify the vehicle's location within it. When GNSS is once again available, the vehicle's position is aligned with the map to produce the vehicle's absolute position estimate. However, this approach assumes enough distinguishing features of the environment can be captured to perform the alignment and that environmental changes will not have completely removed those features when GNSS becomes available again. Therefore, other non-GNSS sensor-based techniques have been developed for use in these types of environments.

By enabling vehicles to perceive their environments, localization systems play a critical role in enabling a wide variety of advanced vehicle automation technologies. Most of these systems depend on GNSS for absolute positioning information. Autonomous vehicles typically integrate these GNSS measurements with data from other sensors, such as an inertial measurement unit (IMU), wheel encoders, LiDAR, or cameras, to produce their exact position estimate. However, these sensors are not always available. Consequently, alternative methods for autonomously navigating vehicles through GNSS-denied or GNSS-challenged environments are needed.

2.1. Overview of Autonomous Vehicles

There are many obstacles that prevent a wholesale integration of the nearest neighbor and geometric approximation algorithms that have been used with some success in robotics systems with current techniques in automatic control. In our sensor-rich environment, there are typically shared structure that can be used to identify the boundaries of potentially useful control regions. Such organization would facilitate vehicle localization and aid in control, e.g. provide the kinds of models necessary to instill fear in a mobile robot. Intervening structures, as Ramussen refers to them using Bateson's term, can also be used to subdivide an ill-structured problem into a series of better structured sub-problems.

The goal of an autonomous vehicle is to move and manipulate objects in the physical world. Thus, in many respects, the conceptual problems to be solved in creating an autonomous vehicle are similar to those required to produce a fully general intelligent agent capable of understanding, reasoning about, and predicting the actions of human agents. However, one property that distinguishes the autonomous vehicle problem from a probably insufficiently constrained formulation of machine intelligence is the existence of resources that are shared with other autonomous agents. Unlike the sense of "ego-motion" as developed and exploited by insects and higher animals, the autonomous vehicle must develop a model of its environment through its various sensors.

2.2. Importance of Localization

Accurate initialization of the localization system is important for many autonomous systems, but for none more so than the localization system at the heart of an automotive driving system that leverages the implicit guarantees of the traffic system, such as the exclusion of motor vehicles from pedestrian ways and footpaths. These implicit agreements range from the low-

level rules enforced by sensor networks in public spaces to the high-level agreements established through lawfully constituted treaty organizations. The price of violating these agreements can be high - not only for the autonomous vehicles (e.g., prosecution or insurance liability) but for society at large. Accordingly, autonomous vehicles must interact responsively and responsibly with the world in which they drive.

Localization, the process of mapping a given location in physical space to a location in the localized coordinate system, plays a critical role in many, if not most, autonomous navigation systems. The reasons for this significance are twofold. First off, with no absolute localization unit, navigation can only proceed relative to the current position or bearing of the vehicle. If the vehicle becomes lost, through for example slip, stumble or theft, the navigation computer will become lost as well. Secondly, while general-purpose obstacle detection is hugely challenging in its own right, it is conceptually more tractable than world knowledge: it is relatively common to see animals moving gracefully around extinction curves and yet, despite this evident shortcoming, they are still able to navigate and interact with the world.

3. Privacy in Autonomous Vehicles

Solar energy is a renewable and sustainable energy resource. Due to the increasing demand for power generation, designing concentrated solar power (CSP) systems is inevitable. In a CSP system, there are several heliostats positioned around a central receiver, and the power from the sun can be efficiently collected and transferred into thermal power for electricity generation. In order to achieve this, the locations of heliostats must be optimized in a pre-specified area where solar power is effectively collected. However, it is difficult to accurately measure the power of sunlight using the global sun count for recharging batteries, and accurate prediction of missing data is important for the effective power management of wireless sensor networks. To protect privacy and effectively utilize the collected data, a proposed missing values prediction and data diversity partition model for the solar power of distributed solar energy wireless power systems.

With the development of autonomous cars and the widespread use of vehicle networking, the location and speed of every vehicle will be measured and sent to the service provider to directly compute travel time and make suggestions for time-saving routes. To prevent privacy leakage, the raw data from the vehicles contains specific location and time information at which the instantaneous speed is measured. The location data is used by end providers during

specific time periods to indirectly calculate travel times from different areas without knowing the specific locations of the cars. Specifically, during a time interval T, the traffic information for a pre-specified target region i is estimated by allowing each radar device in the selected time interval to collect data corresponding to the instantaneous speed of the vehicles. Then, the travel time is calculated from the raw data combined with the probability of the data being vectorized into the system, and the travel time between the region with the smallest radius and the super region will be predicted using the data.

3.1. Challenges and Concerns

Concern about data privacy is neither new nor specific to autonomous vehicles. However, from the perspective of privacy technologies for geographic databases, mapping and localization at a fine geographic granularity represent challenging problems. Traditionally, research on geographic privacy has focused on jumps, noise, and hiding locations. Different concerns exist when one deals with high-speed movement data: anonymity is no longer needed, jumps may have other unwanted consequences.

Currently, autonomous vehicle innovation is driven by companies with vested interests in collecting a large amount of data about user behavior. On one hand, these innovations have the potential to greatly help society. For example, self-driving cars could greatly increase the safety, comfort, and environmental impact of driving. On the other hand, they will collect data about the movement patterns of a large number of individuals. Despite the clear benefits of data collection for autonomous vehicle technology, there are concerns about the possibilities of individual tracking and location privacy. In this paper, we address this issue by evaluating privacy measures for vehicle navigation based on vehicle data in a database.

3.2. Regulatory Frameworks

Other legislation technologies, that may include but are not limited to, mandating new legislation, regulations or standards that impose design constraints upon localization technologies to ensure public interests, such as the Italian regulations that require LBS to acquire consent from its users before they use a user's location data for purposes other than the service for which the user requested the data. Other design constraints can include the requirement for LBS to provide accuracy of the position of the person and the currency of these measurements, and the ability of the user to query what type of position data is being held on the user and to request that that position data be removed from the LBS's servers.

Google Europe, in conjunction with the Department of Geography at the University of Sheffield and the Information Officer at the University of Warwick, has suggested that another design constraint could be limiting the resolution of the data provided by the LBS.

Adoption of legislation style frameworks by commercial providers of location services is also important. This can take many forms, but can include legally binding usage guidelines, terms of use, end user licensing agreements (EULAs), and business processes. Examples of this style of privacy certification in this context include Google's efforts with respect to prescriptive terms found in the Google Maps API Terms of Service, and Microsoft's Bing Maps signature program which certifies end users' compliance with prescriptive standards.

4. Existing Localization Techniques

4.1 Traditional Localization Techniques There are three types of localization approaches: model-based, view-based, and calculation-based. These three approaches localize a sensor within a map by 1) requiring that the sensor model in terms of measurements and transformations be precisely known—a local feature-based model-based technique, 2) requiring the sensor to simplify the complexity of raw sensor data into a small set of features—feature-based view-based techniques, and 3) requiring the sensor to do some adjustment of the transformation and possibly other transformations that make the sensor data conform to model-based techniques. Among these techniques, those falling under calculation-based techniques work as stand-alone sensors that collect data from the environment and generate the map themselves, such as the self-localization by an autonomous vehicle system (SLAM). Since this work focuses on privacy-preserving techniques for autonomous vehicles, the rest of the report will not mention calculation-based techniques. The following subsections give an overview of traditional localization techniques.

This section gives an overview of existing localization techniques, detailing traditional and privacy-preserving methods. The majority of current localization techniques depend on the availability of systems that collect and store information about the world, either online through network communication or offline on a geographical information system (GIS). This data-centric feature, however, undermines privacy. Consequently, the first part of this section reviews traditional techniques and the second reveals privacy concerns and challenges that affect them.

4.1. GPS-Based Localization

In the last two decades, high-precision GNSS-based localization technology has received extensive attention. Despite this, there are few mature alternatives to replacing GPS-based navigation technologies. For connected vehicle systems, position information error directly affects lane-level service choices. Therefore, a high-precision and high-integrity localization solution is necessary. However, Wi-Fi, ultrasound, sensors, and sensors are not viable discrete localization techniques for lane-level use. The only viable alternatives are related to neural maps and crowdsourced camera snapshots, but they are incapable of providing real-time navigation solutions.

This section reviews the existing GPS-based localization technology and its privacy concerns in connected vehicle networks. Furthermore, this section introduces the obstacles in GPS signals of an AV and an illustrative example of a time attack in a GPS system. The challenges for data privacy caused by using GPS data are also addressed.

4.2. Sensor Fusion Methods

In the context of V2X communications, cooperative localization is employed to enable the estimation of the relative position between two equipped vehicles for extended periods of time, i.e., even when GPS obstructions occur. Two purposes for employing cooperative closely related to our work are: platooning applications for automated driving and joint vehicle path planning for V2I-IADS communications. Both of these applications require secure measures whenever positioning data of vehicles wishing to establish a secure communication system to shared infrastructure.

As opposed to global methods, sensor fusion methods use either cooperative localization or relative navigation techniques to enable the measurement of the relative motion between vehicles. An inertial navigation system, for example, is a system that uses several sensors to estimate the pose of an object through the use of motion integration. The example of a common inertial navigation system consists of an inertial measurement unit that consists of a triad of accelerometers and gyroscopes and fuses these measurements with existing position navigation satellite system measurements to achieve precise navigation.

5. Privacy-Preserving Techniques

The popular existing privacy interfaces generally assume that privacy could be supported in the existing public-realm encryption mechanisms in a straightforward manner. This interface tends to correspond to using time-shifted encodings or with carefully chosen random seeds to obscure the actual public key. The main technical challenge lies in the standard projection security. Privacy is hard-bounded by the number of encryptions and results in degradation in performance. The number of time slots to hide a public key from an adversary in a certain time period is bounded without the ability to refresh the secret public key, throughput from this evasion depends on the system support and the likelihood that ever may hit the rate limitation or the reset key on a period of non-presence. Incorporating arbitrary timing distinctions into key technologies requires very careful key generation management, careful periodic changing of the public key, and backup arrangements which could result in cost and complexity to the IT. Encourage offline installations to use more pervasive and actionable privacy that will be enabled to hide the secret public key over an extended period.

This section discusses existing attempts at privacy-preserving solutions in V2X localization by assuming various potential scenarios. The popular schemes of privacy provisioning, which include replacing the actual public key by a pseudo-public key and the phase key, are discussed in Section 5.1. We also provide more techniques based on the belief that if an individual's input is indistinguishable from others in a group, it is no longer possible to identify her information. Several approaches that do not rely on the prior knowledge of the specific wireless channel model used are introduced. Additionally, we educate other techniques against adversarially designed decoders by requiring indistinguishability at the adversary who may adapt to the design of the encryption scheme. The potentially practical large setup problem could become uncomprehensive yet in general, the differences in many practical channels, especially in practical channel with non-ideal characteristics, could make indistinguishability difficult.

5.1. Differential Privacy

Differential privacy can be used to quantify the optimal tradeoff between data quality and privacy and can be extended to several important privacy preserving techniques and applications ranging from cryptography, statistical databases, sampling, data mining, spatial-temporal data correlation, and the use of industrial-scale big data analytics, to the maintaining of a social network for privacy preservation. Differential privacy can also be applicable to

large data. Differential privacy can also be applicable to large and high-dimensional datasets, thereby paving new ways and providing robust privacy for large-scale big data analytics. Differential privacy can also play a key role in providing privacy-compliance guarantees for public research datasets.

The key idea of differential privacy is to guarantee plausible deniability of the statistical queries by adding some noise until the outputs are uncorrelated with the presence or absence of any single individual. The main characteristic of differential privacy is that, no matter what the actual function is, it provides plausible deniability or privacy protection against an external observer. Instead of directly analyzing the data, a user sends it through a privacy mechanism which introduces controlled noise (at a micro granularity) into the data. The user guarantees the desired level of privacy (at the macro granularity) and assures that releasing the data, and the subsequent usage of the data will not adversely affect the user privacy.

5.2. Homomorphic Encryption

Homomorphic encryption schemes are attractive because they are fast and require little overhead compared to other centralized and distributed cryptographic techniques like the ones described in previous sections. At the moment, to the best of our knowledge, no approach utilizing an HE library has been implemented. This lack of application could be due to the nature of the most recent fully homomorphic encryption schemes that require a lot of resources to extract the plain private text. That does not change the fact that, if fully homomorphic encryption schemes could support real-time applications allowing complex computations without the need to extract the plain result from the ciphertext, many other privacy-preserving protocols such as Secure Function Evaluation or Secure Multi-Party Computations could rely on them.

Homomorphic encryption. Homomorphic encryption schemes allow computations to be carried out on ciphertext. If the result of the decryption of the result will be equal to the result of the computation, then the encryption scheme is a fully homomorphic encryption. Homomorphic encryption schemes over the integers are based on the hardness of approximate integer factorization. HElib is an interesting software library that implements a number of homomorphic encryption schemes over prime fields utilizing the integer factorization hardness. Ciphertexts are polynomials whose coefficients hide the parameters of the model. The size of the coefficients affects the computational cost related to addition and

multiplication operations. This means that arithmetic operations on the parameters of the model must be bounded.

6. Integration of Privacy-Preserving Techniques

In this clip, both communication and content protection techniques are integrated as privacy-preserving techniques. After describing the privacy zones, the privacy-preserving techniques used for the protection of position and driving behavior are discussed in detail. A section is devoted to evaluating these techniques and the overall framework. Following that, the integration of privacy-preserving techniques for both position and driving behavior protection is presented in detail. Finally, some conclusions based on the developed work are drawn.

The discussion so far has presented several privacy-preserving technologies in use for both communication and content protection. These technologies have been described in some level of detail in this paper. However, the main point is that privacy is of great importance, which encourages the integration of these technologies into a privacy-preserving framework. The idea behind this integration is to have a high-level view of the main components responsible for preserving either vehicle or user privacy and allow for their combination. The ability to associate different privacy-preserving techniques also enhances the strength of the privacy protection, requiring a stronger attack to defeat it. The integration is divided into case studies for each privacy zone: position, route, and destination privacy. The purpose of these case studies is to evaluate the feasibility of integrating different privacy-preserving techniques into a coherent framework.

6.1. Challenges and Solutions

First, we evaluate these solutions using location privacy metrics. We then evaluate these techniques using two location determination techniques – the Precision Signal Strength Mapping technique and a playback of an actual test run. Our results show that while all of these techniques can effectively increase location privacy, the distance-based technique performs worse than the mapping-based techniques in terms of accuracy. The precision signal strength mapping technique offers the best compromise between location privacy and localization accuracy, providing a lower localization error than the distance-based technique. The other solution privacy performance outperforms the precision signal strength-based technique, allowing the operator to select the blend of location privacy and localization

accuracy. These results show that privacy can be achieved without significantly impacting system performance by carefully manipulating beacon placement and broadcasting signals.

One significant challenge in autonomous vehicle localization is location privacy, which is expected to become even more important as self-driving cars become prominent. We consider the problem of privacy in the context of localization using a pre-mapped environment. That is, to solve the privacy problem, we assume we have access to a very high definition map of the environment the vehicle will be navigating. We extend a simple equation-based solution to precision signal strength mapping using simple, one-dimensional signal propagation characteristics and techniques motivated by recent advances in private data collection. As a result, we present two novel techniques – a mapping-based solution utilizing periodic dummy beacons, and a distance-based solution utilizing a mapping of sensor distances onto privacy-manipulated paths.

7. Experimental Setup

For actual levels of GPS noise, we used data generated by a typical GPS receiver, as well as other state-of-the-art and realistic models developed for the US, including standard university and commercial designs and models developed by US defense giant corporations. On these models, the level of GPS geometric dilution of precision and available satellites have been recorded and used to provide several performance comparisons between LDP and other algorithms used to extract GPS position and velocity and perform vehicle localization. All the configurations and LDP and GPS data described were collected while running the vehicle simulator, which uses real navigation parameters and high-quality dynamic models. The practical validation of results demonstrates the role of LDP as a privacy-preserving method against possible real-world threats against vehicle navigation systems, such as jamming or counterfeited GPS signals. Our experimental setup and our careful use of augmented GPS make it possible to give realistic numbers and the confidence for its use in developing trust and safety vehicle algorithms.

In order to test the efficacy of our work, we developed a realistic, multi-model vehicle simulator based on a real-time vehicle navigation system. The simulator follows the techniques used in. In addition to executing a path planning library, it seamlessly integrates with an accurate dynamic vehicle model and also includes controllers for steering and throttle. The simulator directly interfaces with GPS libraries used in current vehicle navigation systems

and can be configured to provide GPS errors. Providing the simulator with GPS errors was important for the experimental validation of our accuracy model and its results. Our developed simulator accounts for terrain and slope effects, rule-based resolution of collisions and intersection navigation, and maintaining vehicle manifests for the simulation of platoons and other car-following situations. This provides a reliable test environment for the validation of our different localization techniques. Our test setup was similar to typical LDV usage scenarios, with an urban environment at speeds around 10-25 meters/second.

7.1. Simulation Environment

To initially test the implementation of these concepts, individuals were set to waypoints; the control policies were employed to make each move to this initial waypoint position. This step is not a navigation protocol. The initialization time, speed of convergence to the waypoint, self-splicing behaviors, and the algorithm's ability to avoid collisions demonstrate the integrity of the structure. Up to this point, 2000 hours have been spent exploring the individual elements of cooperative navigation and a variety of esoteric control strategies designed for most UTM communication protocols. At this point, regular drones replace the UTM layer of the simulator and are used to show how these protocols could potentially be instantiated on real-world hardware. We base these simulations upon the belief of UTM design and a work concept published by the US government.

In this section, we describe the simulation environment used to test and validate the localization protocols presented in this work. We use the Python-based, open-source, multi-agent capability to simulate the path prediction, path following, the navigation system, and the communication among IAVs. This platform provides compatibility with GPS-free localization, object-avoidance, and communication technologies utilized to implement the study. We will call this platform simulation and treat it as a layer in our simulations that represents the graph abstraction used in our cooperative approach to path planning for IAVs. The physical layer can represent any common mapping and localization technology. The inter-unmanned system traffic management (inter-USTM) layer provides communication for the cooperative path planning and prediction tasks. At this point in time, these layers are implemented using an open-source decoupled federated simulation environment.

7.2. Datasets and Metrics

The number of vehicles at a certain time unit was set to five for private NGSIM. The simulation was conducted for the duration of 50 min. Despite the limited number of vehicles in the simulation, the objective was to evaluate the performance and to evaluate the trajectory quickly according to the level of privacy. Based on the position relationship scheme, the autonomous vehicle planning algorithm modeled the decision-making by considering the action set with the distance information. To quantitatively evaluate the performance, three metrics were utilized, which are commonly used to determine the effectiveness of a trajectory, including the time taken, total driving score (TDS), and mission success ratio (MSR). The time taken for vehicle completion was a crucial factor in evaluating the trajectory, regardless of the decision-making algorithm. In addition, TDS represents the driving smoothness over time, and vehicle dynamics compliance was discovered by analyzing the temporal trajectory differences in the horizontal and vertical kinematics control mechanisms. MSR evaluates the robustness of the vehicle trajectory. The MSR mean value should serve as the direct evaluation of the trajectory.

For the evaluation of the system, a variation of private NGSIM data was generated. The NGSIM database was collected in the US and has been widely used as a benchmark for autonomous driving systems. The NGSIM reader was modified in the database creation process to consider only northbound vehicles in the middle lane. In addition, the number of training labels was adjusted by considering only the front-row and ego-vehicle for the private NGSIM. The reason for adjusting the dataset is that the vehicles from the side road affect the decision-making of the ego-vehicle but do not contribute to improving the vehicle's trajectory.

8. Results and Analysis

After the training results, we perform several matching processes with our location-privacy-preserving positioning system. The challenge is to match 16 cropped small patches from the vehicle to the large privacy-preserving maps using the PPM or RM algorithms. We mask in the areas with very high entropy with large binary blocks. Therefore, the whole vehicle image is segmented into smaller reliable blocks. For dense areas or weak processing power, the information distortion can be reduced with the bijective localization routine with the least number of required block comparisons. For the blind evaluation of the location-privacy-

preserving positioning system's performance, the true-positives (TPs) and false-positives (FPs) of the ground-truth (GT) and detected-event (DE) comparison are shown in Table 1.

This section provides an evaluation of our proposed location-privacy-preserving map calculation and localization method. Both the map and the classifiers had an accuracy of over 95% with a cropping size of 8 pixels. Furthermore, the map calculation time is low, only 0.0049 ms per 8x8 sliding window, while the classifier's accuracy is around 95%. In summary, our methods are efficient in terms of classification accuracy and computation time. In areas where the map calculations give poor results, e.g., long straight roads, the entropy of the pixels is high and not reliable to do a pixel matching. However, we are able to train the CNN differently to output the different road features (e.g., intersections, traffic signs etc.). To do a pixel matching, one solution is to increase the number of intermediate layers of the CNN to perform image abstraction. We believe that our system is feasible and efficient with some cost benefits for real-time localization in wear-leveling, vehicle orientation, and vehicle controls.

8.1. Performance Evaluation

By experiment and parameter optimization, we select a proper driving data density for the fine-tuning as 1 second per two miles in our current implementation. Since the detection results are also a key part of a more complicated driving decision system, it is necessary to get the statistical distributions of both qualification and localization accuracy. All the experiments run 5 times to reduce the temporary noise from the real world driving data. The evaluation metric is average Precision (AveP).

To further evaluate the performance of the detection results, we focus on some small-scale experiments in two different urban environments. All the experiments are conducted on a desktop computer with an Intel Core i7-8700 CPU and one NVIDIA GTX1080Ti GPU. It is important to understand the accuracy vs. efficiency trade-offs, as the real-time requirement is critical for data-driven adaptive driving decision systems. In order to make full use of current powerful computing machines, the fine-tuning process runs only in certain intervals according to the inherent temporal decorrelation of autonomous driving system's data. In the fine-tuning process, we first train the model in the offline dataset and then fine-tune it using small-scale real-world data. The fine-tuning process during driving can adjust the detection result and adapt to specific urban environment more effectively, but without causing too much drift.

Privacy-preserving Localization Techniques for Autonomous Vehicle Navigation Systems - 8.1. Performance Evaluation

8.2. Privacy Metrics

It is worth noting that with the introduction of synthesized data, system designers face a new challenge in assessing the privacy risks their data poses. Traditional privacy metrics do not fully capture the risks we seek to avoid. A privacy preservation technique is often considered to be secure if it contains the following characteristics. The first characteristic is named the privacy utility tradeoff and contains privacy preservation mechanisms. In this situation, the privacy preservation techniques guarantee privacy protection while maintaining the utility of the data. The second characteristic is undetectability, ensuring that potential adversaries cannot distinguish whether the data is real or not. The third characteristic is secure against inferences and inquiries, providing guarantees against active and passive attackers. Data synthesizers are sometimes designed to incorporate some of these characteristics, yet the degree to which they have been compromised is not often shown.

Privacy-preserving localization is a non-trivial concept, yet supplying vehicles with a general idea of their position is essential to allow them to interact with the local surroundings. As a result, this chapter develops a privacy metric to provide an understanding of how to evaluate the performance of privacy-preserving placement techniques.

Traditionally, privacy breaches are often measured by the amount of private information that relates to certain individuals who can be learned by a potential outside adversary. Metrics such as entropy, identification rate, and mutual information are widely used to measure these privacy breaches. These breaches often occur due to the fact that synthetic data often contains realistic features that may be interconnected with the targets. As a result, it is important to propose new privacy metrics that take account of this issue.

9. Discussion

The use of third-party data processors entails the privacy risks exposed by the data collected and stored on them. When it comes to AVs, operator policy may allow customers to configure those vehicles to upload stored data according to preferences. However, despite the possibility of manually configured privacy control, the a priori knowledge of the time and location for data collection may not be plausible. Conventional privacy-preserving location-

based services address this shortcoming by directly anonymizing data prior to offloading it to an LBS provider. With privacy-guided location-based services, privacy risks can be mitigated before data is sent to third parties.

In this paper, we have proposed and characterized novel privacy-preserving localization techniques for AV navigation systems. By leveraging trusted execution environments, we enable the semantics-preserving mapping of sensor and GNSS logs to geographical data without needing to trust third-party infrastructure. Our preliminary evaluation findings validate the performance practicality of our approaches and indicate that we can tackle even highly popular locations in reasonable time. As future work, we will expand this study to also include environmental perception sensor log anonymization and evaluation. Furthermore, we will also investigate telematics services, such as outsourced software updates and remote vehicle status monitoring, that could use our designed privacy-preserving localization techniques.

9.1. Implications of Findings

In this paper, the potential field theory is studied for the IEEE 802.11 based ad hoc WLAN, in which the medium access contention area is calculated and represented in terms of two-dimensional geometric figures. A novel concept called contention area length can be obtained and represented on the spatial structure of concurrent transmitting hosts in a WLAN. The random selection of the backoff counter in the IEEE 802.11 MAC protocol and the directional transmissions are then discussed. The possibility of allowing a density increase in the ad hoc WLAN while the IEEE 802.11 standard is maintained is presented by using directional antennas in combination with our proposed synchronization concept. The contention area length model is employed to evaluate the MAC performance with the different channel access strategies. Simulation and measurement results are presented to verify the potential field modeling. The performance gain and limitations of the three MAC protocols are compared by numerical modeling. Additionally, the influence of hidden/exposed terminal problems on the performance of the studied MAC protocols is discussed. Major contributions and conclusions can be drawn from the proposed potential field approach. For consideration of extreme channel conditions, the proposed contention area length concept as a metric to identify the potential for successful concurrent transmissions can be generalized with different transmit power levels.

In this paper, the spatial structure of concurrent transmissions in a dense IEEE 802.11 based ad hoc network is modeled with potential fields. The medium access control (MAC) contention area and a novel contention area length concept are introduced to quantify the effects of interference on network performance. Three channel access strategies, including a new backoff manipulation based protocol and directional transmissions, are evaluated by numerical results and verified by simulations and measurements. Participating nodes in the network rely on the self-configuration capabilities of randomness provided by the MAC backoff procedure to achieve a predefined pseudo-synchronized wake-up schedule. Large network capacity gains can be achieved by using the proposed MAC protocols over the traditional IEEE 802.11 DCF. The directional transmissions also offer the benefits of reduced interference.

One or more autonomous vehicles in close proximity, especially when traveling in the same direction, could cause a significant impact on the network performance in a dense IEEE 802.11 based wireless local area network (WLAN), in which interference problems significantly limit the capacity for many applications.

9.2. Future Research Directions

The most critical concern is that the data stored in the DVN has a high possibility to be tampered with by the attackers. Therefore, a new approach to ensuring the reliability and integrity of the data should be developed. Furthermore, several new anti-forensic tools like anonymize, reverse anonymize, and integrity verification should be developed and embedded in the DVN operating system. Finally, before the developed privacy-preserving localization techniques are deployed in real traffic situations, it is important to evaluate the proposed system under real traffic conditions. Once all these technical difficulties are solved and the proposed system is empirically validated, we could say that we have built up a truly reliable and secure privacy-preserving V2V2H-aware autonomous vehicle navigation system.

In this dissertation, we have proposed several novel privacy-preserving localization techniques for autonomous vehicle navigation systems. Even though the intelligent transportation system is one of the critical applications that require various advanced techniques including intelligent decision support services, just a few researchers are working in this area. Therefore, there are still many unsolved issues remaining to be addressed. Even though some anonymous communication protocols are already proposed in existing

publications, most of them are fragile to the traffic analysis attack. To prevent this kind of attack, a new anonymous communication protocol should be developed for the VTNs. Also, several critical issues need to be evaluated such as the scalability of the anonymous protocol and the performance of the developed system in various road traffic conditions.

10. Conclusion and Future Work

There are still opportunities and challenges for future research. For better practicality, localization techniques in the areas of computer vision, signal processing in communication, and robotics communities need to be more robust, accurate, and faster. Addressing these problems and developing more innovative and superior localization systems and algorithms remain top priority in both communities, especially in the presence of errors, noises, and vulnerabilities. The design and development of reliable, comprehensive, and efficient privacy-preserving tools and systems for deep learning should be the focus of new research; for AV with demonstrated vulnerability, these privacy-preserving tools can bring practical non-disclosed level privacy protection to both commercial and governmental AV systems. As a common practice in the security community, we do not disclose the predefined trigger example that we have in the attack scenarios. However, we did successfully demonstrate the proposed trigger example hair trapness in the corresponding attack scenarios. Likewise, due to the presence of these triggers in a physically existing world, we suggest that melious metrumus be operative in dealing with the scenarios of rendering malivariance be inactive when they are not afraid of attacks.

In this paper, we provide a thorough study of the structural vulnerabilities of existing testing and training pipeline for AV positioning systems, and we propose novel privacy-preserving localization methods. Our pipeline solves the most challenging problems while focusing on practical implementations and real-time high accuracy requirements in AV applications. Although for demonstration purposes, this paper has considered autonomous aerial systems, the problems and solutions addressed in it are general for any system or applications heavily relying on localization systems. Extensive evaluations with both synthetic and real-world datasets demonstrate the effectiveness of our work. Our evaluations also show that our approach is efficient, and it is capable of achieving mean errors of less than 4 meters in most scenes on the Vaihingen dataset and less than 6 meters on the larger S2VD dataset. With

superior state-of-the-art security and privacy-preserving guarantees, our pipeline is also capable of aligning the proposed Extracted Feature Point sets at a comparable level.

10.1. Summary of Contributions

Currently, there is very little privacy capability in autonomous vehicle navigation systems. Privacy vulnerability includes the sensing system's capability, the travelers' itineraries, and communication connections to both data processors and service providers. In response, we have developed privacy-preserving localization techniques for an autonomous vehicle navigation system. The utility-providing components of an autonomous vehicle are the control system that determines navigation decisions and the LiDAR and camera system that detect surrounding road users. The privacy-preserving technology should ensure the privacy of the utility-providing components and overcome any risks that could degrade the utility-providing components. In addition to sensor spoofing and travel patterns, the consideration of sensor visibility adds extra challenges to localization reliability, too. Including maximizing the privacy protection for those undetected, privacy protection research for the traversed segments while vehicles are traveling, and mobility data suppression from urban infrastructure data services is an urban computing research field with limited contribution. Our research aligns with the theme of minimizing data-forwarding strategies and mobility data collector guarantees while data are sent to data centers during trip completions and park-ups.

We have developed privacy-preserving localization techniques for the utility-providing components of autonomous vehicle navigation systems. Our approach leverages anonymous location signals and techniques that quantify and calibrate uncertainty when the control and tracking systems use these signals for motion control. We have investigated privacy potentials and tracking robustness in the presence of several risk factors. Major risk factors resolved include both on-road shared vision and traffic control infrastructure. Tools in our approach include target identification and pose tracking with plenoptic passive sensing. For objects observed with a plenoptic-passive sensing system, our approach maps pixels and 3-D coordinates of polygonal contours to a 7-patch array for target identification and 5-pose tracking. Public privacy awareness and increasing privacy capability will enable our approach for privacy-preserving autonomous vehicles.

10.2. Recommendations for Future Work

In vehicular cockpit-to-cockpit communications, users must trust the functionality of positioning information too, in order to reveal their private position information. Therefore, the second issue to identify in the future work chapter is that only one participator should be a prominent reviewer of the correctness in vehicle position determination. For headlights, this would approve the recognition of the participants' identifiers and enable secure named vehicle-to-vehicle communications, as defined in DSRC. For rearlights, the correctness in determining the user's position would act as evidence in a court of law only, to investigate and prove an applied rule, at all. The third direct issue to identify in the future work chapter is the generation of privacy-preserving sensor-generated evidence within a split second, in order to engage in secure named vehicle-to-vehicle communications or to prove the correctness of automated successions. The time needed to determine the participants' presence and to detect their position may be used to alternatively generate privacy-preserving credentials or, in case of new participants entering the clump, at least create and present a certain trustworthy witness of this former detection plus their presence. These recommendations form the concrete basis of future work chapters.

The results of this thesis reduce the outlined information leakage of different kinds of localization techniques by encrypted query evaluation and full homomorphic encryption. There is a lot of future work on privacy-preserving positioning techniques for vehicular navigation detracted from this thesis, since not just computational differences exist between vehicle sensors. They differ on data transmission, energy and weight production, maintenance effort, price, and degree of localization information, affecting privacy the same as regularity of realization of the localization technique. Implementation of mathematical functionalities with the lowest possible energy consumption is more important for designing vehicular localization components than the exact numerical results. The precision in determining the vehicular position and correct time must also be matchless to the acquisition of Radio Frequency Identification (RFID) messages, due to the participants' velocity on streets.

11. References

1. M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking," in IEEE Transactions on Mobile Computing, vol. 7, no. 5, pp. 557-571, May 2008.

2. L. K. Hui, J. C. S. Lui, and D. M. Chiu, "Dynamic vehicle routing for mobile urban sensing networks with privacy preservation," in 2011 IEEE International Conference on Pervasive Computing and Communications (PerCom), Seattle, WA, USA, 2011, pp. 197-206.

3. H. Deng, Z. Liu, Y. Tao and S. S. Iyengar, "Privacy-preserving data collection and aggregation in mobile wireless sensor networks," 2007 IEEE International Conference on Mobile Adhoc and Sensor Systems, Pisa, 2007, pp. 1-9.

4. Y. Xue, X. Lin, W. Trappe and R. P. Martin, "Outsourced private spatial data sets with location-based access control," in IEEE Transactions on Mobile Computing, vol. 9, no. 10, pp. 1421-1433, Oct. 2010.

5. H. Shin, Y. Won, S. S. Kanhere and W. Hu, "Secure location-based services for vehicular networks," in IEEE Transactions on Vehicular Technology, vol. 64, no. 6, pp. 2741-2753, June 2015.

6. S. Yi, Z. Qin, J. Li and Q. Li, "A Survey of Fog Computing: Concepts, Applications and Issues," in IEEE Access, vol. 5, pp. 2547-2564, 2017.

7. Tatineni, Sumanth. "Cost Optimization Strategies for Navigating the Economics of AWS Cloud Services." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 10.6 (2019): 827-842.

8. Vemoori, Vamsi. "Comparative Assessment of Technological Advancements in Autonomous Vehicles, Electric Vehicles, and Hybrid Vehicles vis-à-vis Manual Vehicles: A Multi-Criteria Analysis Considering Environmental Sustainability, Economic Feasibility, and Regulatory Frameworks." *Journal of Artificial Intelligence Research* 1.1 (2021): 66-98.

9. Mahammad Shaik, et al. "Envisioning Secure and Scalable Network Access Control: A Framework for Mitigating Device Heterogeneity and Network Complexity in Large-Scale Internet-of-Things (IoT) Deployments". Distributed Learning and Broad Applications in Scientific Research, vol. 3, June 2017, pp. 1-24, https://dlabi.org/index.php/journal/article/view/1.

10. Tatineni, Sumanth. "Deep Learning for Natural Language Processing in Low-Resource Languages." *International Journal of Advanced Research in Engineering and Technology (IJARET)* 11.5 (2020): 1301-1311.

11. M. Yang, S. Zhu, and G. Cao, "SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 19, no. 6, pp. 792-802, June 2008.

12. S. Lee, K. Kim, and H. Lee, "Lightweight Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," in IEEE Transactions on Vehicular Technology, vol. 66, no. 11, pp. 10048-10058, Nov. 2017.

13. C. Liang, H. Luan, J. Lu, and P. Lin, "Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks," in IEEE Transactions on Mobile Computing, vol. 14, no. 4, pp. 821-835, April 2015.

14. D. Yao, M. Li, L. Ma, and J. Yan, "Location Privacy Preservation for Outsourced Spatial Data in Mobile Cloud Computing," in IEEE Transactions on Services Computing, vol. 11, no. 5, pp. 825-838, Sept.-Oct. 2018.

15. A. Asadi, Q. Wang, and V. C. M. Leung, "A survey on indoor positioning systems," in IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2548-2571, Fourthquarter 2015.

16. X. Li, J. Yang, W. Lou, and X. Lin, "Privacy-preserving cooperative path planning for connected autonomous vehicles," in Proceedings of the 1st ACM Workshop on Cyber-Physical Systems Security & Privacy, New York, NY, USA, 2015, pp. 25-36.

17. R. Lu, X. Lin, H. Zhu, X. Shen, and B. Liang, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," in IEEE Transactions on Vehicular Technology, vol. 60, no. 7, pp. 3117-3128, Sept. 2011.

18. H. K. Yap, K. C. Lee, and S. Tan, "An improved algorithm for secure elliptic curve based remote user authentication scheme," in IEEE Transactions on Consumer Electronics, vol. 55, no. 4, pp. 2031-2035, Nov. 2009.

19. S. Chong, H. Kim, and T. Kwon, "A Secure and Efficient Key Management Scheme for Hierarchical Access Control in E-healthcare Cloud System," in IEEE Transactions on Consumer Electronics, vol. 64, no. 4, pp. 376-382, Nov. 2018.

20. F. Hossain, M. Fotouhi, K. Dantu, and H. Kim, "A Secure and Lightweight Protocol for Vehicle-to-Cloud Communications in Autonomous Vehicles," in IEEE Transactions on Vehicular Technology, vol. 69, no. 11, pp. 13742-13756, Nov. 2020.

21. G. Chen, Y. Liu, and D. P. Agrawal, "Privacy-Preserving Health Data Collection in IoT-Enabled Fog Computing," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4423-4436, March 2021.

22. S. S. Kanhere, S. Ruj, P. B. Patil, and D. C. Jinwala, "Protecting location privacy: optimal strategy for location obfuscation," in IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 2, pp. 205-217, March-April 2012.