Vehicle Trajectory Obfuscation and Detection

Baihe Ma, Yueyao Zhao, Xu Wang, Zhihong Liu, Xiaojie Lin, Ziwen Wang,
Wei Ni, and Ren Ping Liu

Abstract A vehicle in road networks shares location data with other vehicles and location-based services (LBS) through Internet-of-vehicles (IoV). By analyzing the location data from vehicles, LBS providers can offer vehicles better services. However, fake trajectories created by adversaries and malicious drivers diminish the location data utility in IoV and breach the quality of LBS. Illegal trajectory detection is vital to ensure location data utility in IoV. Existing location privacy-preserving schemes like obfuscation schemes add noise to actual location data increasing difficulties in detecting illegal trajectories. In this paper, we detect illegal trajectory in the case that all drivers in road networks protect location privacy by using obfuscation. We propose a new personalized obfuscation mechanism to dynamically and adap-

Baihe Ma
Global Big Data Technologies Centre, University of Technology Sydney, 2007, Australia, e-mail: Baihe.Ma@uts.edu.au

Yueyao Zhao
Xidian University, Xian, China, e-mail: vmusen@outlook.com

Xu Wang
Global Big Data Technologies Centre, University of Technology Sydney, 2007, Australia, e-mail: Xu.Wang-1@uts.edu.au

Zhihong Liu
Xidian University, Xian, China, e-mail: liuzhihong@mail.xidian.edu.cn

Xiaojie Lin
Global Big Data Technologies Centre, University of Technology Sydney, 2007, Australia, e-mail: Xiaojie.Lin@uts.edu.au

Ziwen Wang
Xidian University, Xian, China, e-mail: wangziwen@stu.xidian.edu.cn

Wei Ni
Data61, CSIRO, Sydney, 2122, Australia, e-mail: Wei.Ni@data61.csiro.au

Ren Ping Liu
Global Big Data Technologies Centre, University of Technology Sydney, 2007, Australia, e-mail: RenPing.Liu@uts.edu.au

tively protect the location privacy of drivers in road networks. Considering uneven protection, we propose a trajectory detection scheme to classify trajectories in IoV. We evaluate our detection method with the data of real-world road networks, which is an important scenario of smart cities

. The experiment results show that the proposed classifier outperforms existing studies in detecting malicious obfuscated trajectories with at least 94% of the Area Under the Curve (AUC) score.

1 Introduction

Location-based services (LBS) have been extensively and deeply developed as an important part of smart cities to provide various services, e.g., traffic analysing and urban planning [1, 2]. Smart cities inevitably require spatio-temporal location data of vehicles, which is highly correlated with a driver's private information (e.g., home address, company address, and religion) [3]. Location-based services (LBS) providers rely on location data from drivers to offer various services [4]. However, adversaries can infer drivers' personal information by analyzing location data [5]. It is of necessity to protect location data in Internet-of-vehicles (IoV) for drivers' privacy while ensuring high quality of service (QoS).

Obfuscation schemes [6] and adaptive location privacy-preserving schemes [7] have been developed to protect location privacy. Obfuscation schemes add noise to obfuscate drivers' actual location data, which reduces the data utility of the location data. The obfuscated location data are indistinguishable from each other, which leads to the fact that LBS providers would collect illegal location data. The location privacy-preserving schemes aim to balance the QoS of LBS and privacy-preserving capability by analyzing the drivers' requirements.

Malicious drivers breach legal drivers' profit. For example, malicious drivers can occupy more benefits than they deserve by deliberately modifying their trajectory data in Taxi service [8, 9]. Malicious drivers also use location privacy-preserving schemes to protect their location data. By analyzing location data which concludes illegal location data, smart city applications cannot provide an acceptable QoS of LBS. Therefore, LBS should detect the illegal location data to ensure high QoS. If the malicious drivers employ location privacy-preserving schemes (e.g., obfuscation schemes) as the legal drivers, detecting illegal data becomes difficult.

We study the illegal location data detection and propose a personalized obfuscation scheme and an illegal trajectory detection mechanism. Our work has two-fold contributions as follows:

- We employ the differential privacy in the proposed personalized obfuscation scheme to protect drivers' location privacy adaptively and to provide high QoS of LBS in road networks.
- We propose a Convolutional Neural Network (CNN) based detection mechanism to detect illegal trajectories without requiring the drivers' actual location. The

proposed scheme has high accuracy in detecting illegal trajectories even if the drivers protect actual location data with various noise sizes.

We conduct experiments with the real-world road network dataset extracted from Open Street Map (OSM)[1] to evaluate the proposed scheme. The illegal trajectories are generated with fake speeds and paths with the real-world road network dataset. We also evaluate the proposed scheme in the case that the drivers adaptively protect their location data, i.e., using different privacy levels. The experimental results show that the proposed detection scheme achieves at least 94% Area Under the Curve (AUC) score when detects the illegal obfuscated trajectory.

The rest of this paper is organized as follows. Section 2 studies the existing works. Section 3 describes the proposed mechanisms. Section 4 evaluates the proposed mechanisms with real-world road network dataset. Section 5 concludes the paper.

2 Related Works

The existing smart city provides location-based services by mining trajectory data that are transmitted in vehicular networks [10]. Wang et al. have studied the privacy challenges in smart city and analyzed the privacy leakage in LBS [11]. The authors pointed out that the smart city can provide high quality of services if trajectory privacy is well protected.

The previous studies of location obfuscation mechanisms perturb a driver's actual location and report an obfuscated version to LBS. Derived from the differential privacy [12], scheme in [6] first developed the concept of geo-indistinguishability. The scheme follows the idea of geo-indistinguishability and uses Laplace distribution to add controlled noise for protecting location data locally. Yu et al. [13] improved the two-phase dynamic differential location privacy scheme by integrating the inference error expectation and geo-indistinguishability [14]. The improved framework effectively protects location privacy in a 2D map. The authors developed an adaptive location privacy-preserving mechanism in [7] to balance location privacy and utility. The mechanism calculates the amount of noise before adding noise to actual location data. The calculation is based on the correlation level between the driver's current location and the previous obfuscated locations. With the concept of differential privacy, Xiao et al. [15] improved a location-cloaking system to protect drivers' location data in a 2D map. The obfuscation locations generated by the existing 2D obfuscation mechanisms might locate at unreachable locations, e.g., in the river, which breaches the location privacy-preserving capability of the obfuscation mechanisms.

The existing illegal trajectory detection mechanisms are classified into the machine-learning-based detection and the rule-based detection. The illegal trajectory data is detected by utilizing GPS data in the rule-based detection mechanisms. Machine-learning-based detection mechanisms classify trajectory data as legal and

[1] Open Street Map is an open source database of the world's geographic map. https://www.openstreetmap.org/

illegal by using techniques like deep neural networks. In [16], Chen et al. improved an efficient real-time trajectory detection method with low processing overhead. The method uses the window size to estimate the partial trajectory that result in the anomalousness trajectory. The trajectory detection system with two-phase outliers upon trajectory data streams was improved in [17]. The two phases are the trajectory simplification and the outlier detection.

In [18], authors developed a trajectory detection method based on a recurrent neural network (RNN). The authors extracted drivers' behaviors within a sliding window and uses the deep representations that are fixed-length for the feature sequence. The authors grouped the representations into clusters before detection. CNN is first introduced in [19], which is further utilized in the fields such as the natural language processing and speech recognition. A CNN-based trajectory prediction method was improved in [20]. The method simplifies the network structure and utilizes the trajectory structure (spatio-temporal consistency). The experimental results show that the CNN-based trajectory prediction method can detect illegal trajectories with a high score of the AUC.

Our work obfuscates drivers' trajectories in the road networks to avoid the generation of the off-road obfuscated locations. Then, an illegal trajectory detection scheme based on CNN is proposed in this paper. The proposed scheme does not expose the drivers' actual trajectories and achieves high detection accuracy. The proposed scheme can detect illegal trajectories even if the drivers use various privacy parameters to obfuscate the locations. To the best of our knowledge, we are the first work that detects illegal locations in real road networks, which is almost the actual usage scenario of a smart city.

3 Proposed Scheme

In this paper, we start by proposing an adaptive obfuscation scheme to customized protect location privacy in road networks. Then, we propose an illegal trajectory detection system with CNN to identify the legal and illegal trajectory from the obfuscated trajectory. In our model, X_m is the m-th trajectory consists of the location points sequence $(x_{m1}, x_{m2}, \ldots, x_{mn})$. $x_{mi} = (lat_i, lon_i)$ is a tuple which stands for the coordinate (i.e., latitude lat_i and longitude lon_i) of a location.

3.1 System Model

The existing obfuscation studies [7, 21, 22] pay attention to protect the drivers' location data in a 2D map, which generate off-road locations (e.g., railroads and rivers). Adversaries can exclude the off-road obfuscated locations from real trajectory data when they identify the obfuscated locations that are off-road. The Euclidean distance between the obtained off-road location and the nearby road can be utilized by the adversaries to estimate the actual location. In this paper, we controlled the obfuscated candidates to avoid the off-road data and guarantee that all obfuscated locations are on-road.

3.2 Dynamic Obfuscation Scheme

Definition 1 Geo-indistinguishability [6]: Let P be a probabilistic function. Let X and Z be a set of the actual location candidates and obfuscated locations candidates, respectively. The K represents the mechanism that uses the probability $P(Z)$ to map an element in X to an element in Z. K is ϵ-geo-distinguishable, if and only if for all x, x' has:

$$d_{\mathcal{P}}\left(K(x), K\left(x'\right)\right) \leq \epsilon d\left(x, x'\right) \tag{1}$$

The $X_m = \{x_{m1}, \ldots, x_{mn}\}$ is the raw path that indicates the actual trajectories, while $Z_m = \{z_{m1}, \ldots, z_{mn}\}$ indicates the obfuscated trajectories. We utilize 2D Laplace noise $D_\epsilon(x)(z) = \frac{\epsilon^2}{2\pi} e^{-\epsilon d(x,z)}$ as obfuscation distribution in this paper. The reason is that the 2D Laplace noise ensures that z_{mi} is distributed around x_{mi}. The probability of z_{mi} with 2D Laplace noise decreases with the increasing of $d(x_{mi}, z_{mi})$ ($d(\cdot,\cdot)$ is the Euclidean distance in this paper). Theϵ-geo-distinguishable privacy condition is also satisfied with the 2D Laplace noise.

3.3 Adaptive location privacy-preserving scheme

A new adaptive location privacy-preserving scheme is proposed in this paper. The proposed scheme sets ϵ correlated to the generated obfuscated locations. By utilizing the proposed adaptive location privacy-preserving scheme, we boost the randomness of the noise generation, which increases the difficulty of inferring the actual location of a driver.

We configure ϵ into the high, medium, and low privacy levels. We set the average distance of the obfuscated location to r when there is a low level ϵ. A medium and a high level ϵ have an average distance of $1.5r$ and $2.25r$, respectively. The proposed scheme obfuscates every single location point in each continuous trajectory. As the starting location and destination are more sensitive to a driver, we set the highest privacy level for the two locations. For other locations x_i in the trajectory, the obfuscation parameters are related to the Euclidean distance $d(x_i, z_{i-1})$. We set two different thresholds $D1$ and $D2$ to divide $d(x_i, z_{i-1})$ into three types, where $D1 \neq D2$. When the value of $d(x_i, z_{i-1})$ is bigger than the values of $D1$ and $D2$, the correlation between x_i and z_{i-1} is weak. In this case, a low-level noise is added in the actual location data. When the value of $d(x_i, z_{i-1})$ is less than the values of $D1$ and $D2$, x_i and z_{i-1} is close in road networks (i.e., high correlation). Therefore, we add noise with a high privacy level when obfuscating actual locations in this scenario. Otherwise, we set ϵ as a medium privacy level in the proposed obfuscation scheme.

The proposed scheme reduces the correlation between x_i and z_{i-1}. Hence, the adversary cannot infer ϵ by analyzing the prior knowledge and the obtained obfuscated locations within a specific time window. The adversary cannot predict the driver's future locations because the value of ϵ is changing, which increases the difficulty of attacks.

The selection of ϵ in the proposed scheme aims to balance location privacy and data utility. A large amount of noise is required to achieve a high privacy level but leads to a low QoS of LBS. The different ϵ can provide customized geographic location accuracy which suit for various LBS requirements. For example, location-sensitive LBS (e.g., navigation) needs a high accuracy location data so that the scheme ought to utilize a high ϵ to provide a high data utility. For location-insensitive LBS, e.g., weather forecasts, the scheme can employ a low ϵ for a high privacy level.

The amount of the added noise is controlled in the proposed scheme to balance data utility and location privacy. we use z within a region based on x to set the upper-bound of the QoS loss and that of the capability of location privacy, i.e., $d_{max}(x, z)$. If the distance $d(x, z)$ between the actual location x and the obfuscated location z exceeds $d_{max}(x, z)$, the proposed scheme will obfuscate the driver's actual location again.

The proposed scheme generates obfuscated locations $z_{m1}, \ldots, z_n$ and maps the obfuscated locations to the nearest road. Therefore, the proposed scheme obfuscates actual trajectories to reachable on-road locations.

3.4 Illegal trajectories detection based on CNN

A two-dimensional convolutional neural network (2D-CNN) model is applied in the proposed scheme to detect illegal trajectories. The proposed model is shown in Fig. 1.

One-dimensional CNN (1D-CNN) consists of the convolutional layer, the subsampling layer, and the optional fully-connected layers. In convolutional neural networks, the convolutional layer is the major part that analyzes the inpu data to extract classification features. The Separate feature extractor contains multiple convolution kernels. The convolutional layer of the CNN model can extract the Spatial-temporal correlation of the trajectory. After extracting features in convolutional layer. pooling step starts. The weight parameter redundancy is solved by the local connection and weight sharing. However, the over-fitting problems arise due to the CNN model degrades in the generalization performance. With the extracted features from the convolution layer and pooling, CNN model can reduce the data dimension while retaining the value of the principal feature map.

Our work improves the architecture of 1D-CNN with 2D-CNN model, which is widely utilized in classification of images (e.g., ResNet [24], VGG [25], and GoogleNet [26]). The proposed model is described as follows.

- In advance of the maximum pooling layer, two convolutional layers are employed in our model. Thus, the proposed model can extract features effectively.

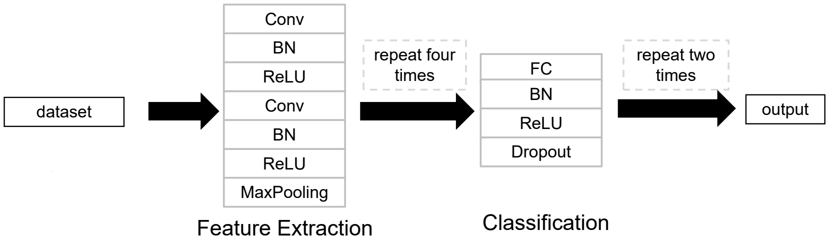


Fig. 1 Our CNN model architecture [23].

- We add a normalization (BN) layer after the two convolutional layers to retain the spatial-temporal correlation of locations. The fully connected (FC) layers are combined with the dropout layers and BN in the proposed model to avoid the FC layers leading to over-fitting issue.

4 Evaluation

4.1 Original Dataset

We employ real-world road network information of Porto, which is extracted from OpenStreetMap (OSM) to evaluate the proposed scheme. OSM is popular in LBS applications, such as the route planning and the geocoding of address [27]. The extracted road network is shown in Fig. 2. The Portugal taxi trajectory dataset[2], whose recorded location data has 15 seconds time interval to build the trajectory, is used in our experiment.

4.2 Illegal trajectories

As far as we know, no public dataset are labeled with illegal and legal trajectories. Three methods are popular to generate illegal trajectories according to legal trajectories.

1. Insertion trajectory from other sources of trajectory dataset as the illegal trajectories [28].
2. Division the trajectories data into legal and illegal dataset [29].
3. Combination the above two methods [21].

[2] Portugal taxi trajectory dataset[Online]. Available: https://www.kaggle.com/c/pkdd-15-predict-taxi-service-trajectory-i

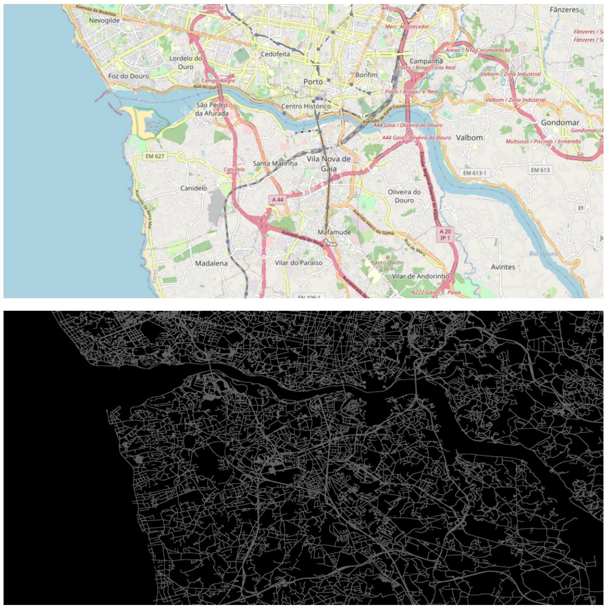


Fig. 2 Generation of the road network. Upper: real road map in OSM; Bottom: the generated road network [23].

In this paper, we generate illegal trajectories by utilizing legal trajectories. The generated illegal trajectories are employed in our classification experiments. Hence, legal and illegal trajectories in the training and detection come from the same dataset to reduce deviation.

4.3 Simulation results

We evaluate the detection capability of the proposed scheme with the generated trajectory data and the public trajectory dataset of the Portugal taxi. In the experiment, we configure ϵ to control the level of Laplace noise.

4.3.1 Experimental setting

We use the public real-world trajectory dataset and the synthetic data as follows.

Real-world trajectory: We employ the public trajectory dataset of Portugal taxi which has approximate 1.7 million trajectory data.

Synthetic data: We extract half of the trajectory data from the Portugal taxi dataset to generate the illegal data. In this paper, the illegal trajectories considered have two forms, speed anomaly and path anomaly. The two forms represent malicious actions, i.e., speeding and detour, respectively. The illegal trajectories are generated as follows:

- **Speed anomaly**: The maximum speeds of vehicles are limited in road networks. Malicious drivers drive faster than the limitations to obtain more profit within a period. The utilized trajectory dataset contains timestamp, we delete x_i in the selected continuous trajectory X with a certain probability and reassign the timestamp. The the trajectory X has a higher speed than the speed limitation.
- **Path anomaly**: Malicious drivers can also select a longer route than the recommended route, i.e., path anomaly. We utilize multiple legal trajectories (e.g., three trajectories X_a, X_b, X_c) to generate path anomaly illegal trajectories. The starting location and destination of X_a are denoted as x_{a1} and x_{an}, respectively, at shown in Fig. 3. We employ the trajectories X_b and X_c to intersect[3] the trajectory X_a at location x_{ai}, x_{aj}. We also combine the trajectories X_b and X_c at location x_{bl}. Then, we obtain an illegal trajectory which is a path anomaly. The starting location and destination of the generated trajectory are x_{a1} and x_{an}, respectively, but the route distance between x_{a1} and x_{an} is longer than it should be. In this paper, the length of the generated trajectories are set to be at least 1.6 times as long as that of the legal trajectories.

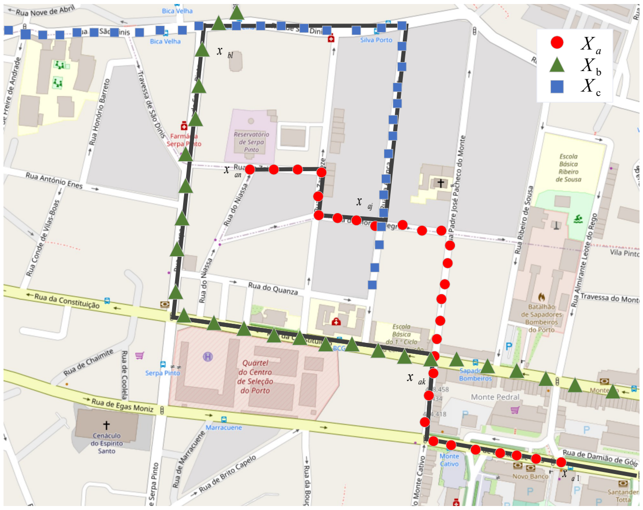


Fig. 3 Example of a anomaly generated path [23].

[3] The intersection stands for the points of the two trajectories whose distance are within a certain range.

The above types of illegal trajectories include the most categories of malicious activities in the road networks. We use more than 600,000 legal and illegal trajectories to evaluate our proposed detection scheme.

4.3.2 Implementation

The configurations of the proposed mechanism that implemented in our experiments are as follows.

We use $\epsilon_0 = 0$ to stand for the non-protected situation. We configure the obfuscation radius as the average Euclidean distance between x_i and z_i when using noise level ϵ_i. When $\epsilon_0 = 0$, the average obfuscation radius is 0 m. We set ϵ_1 and ϵ_2 with obfuscation radii 100 m and 1000 m, respectively.

4.3.3 Experimental results

We use Python to conduct the experiments. We take the average value of the experiment results after running the experiment for five times.

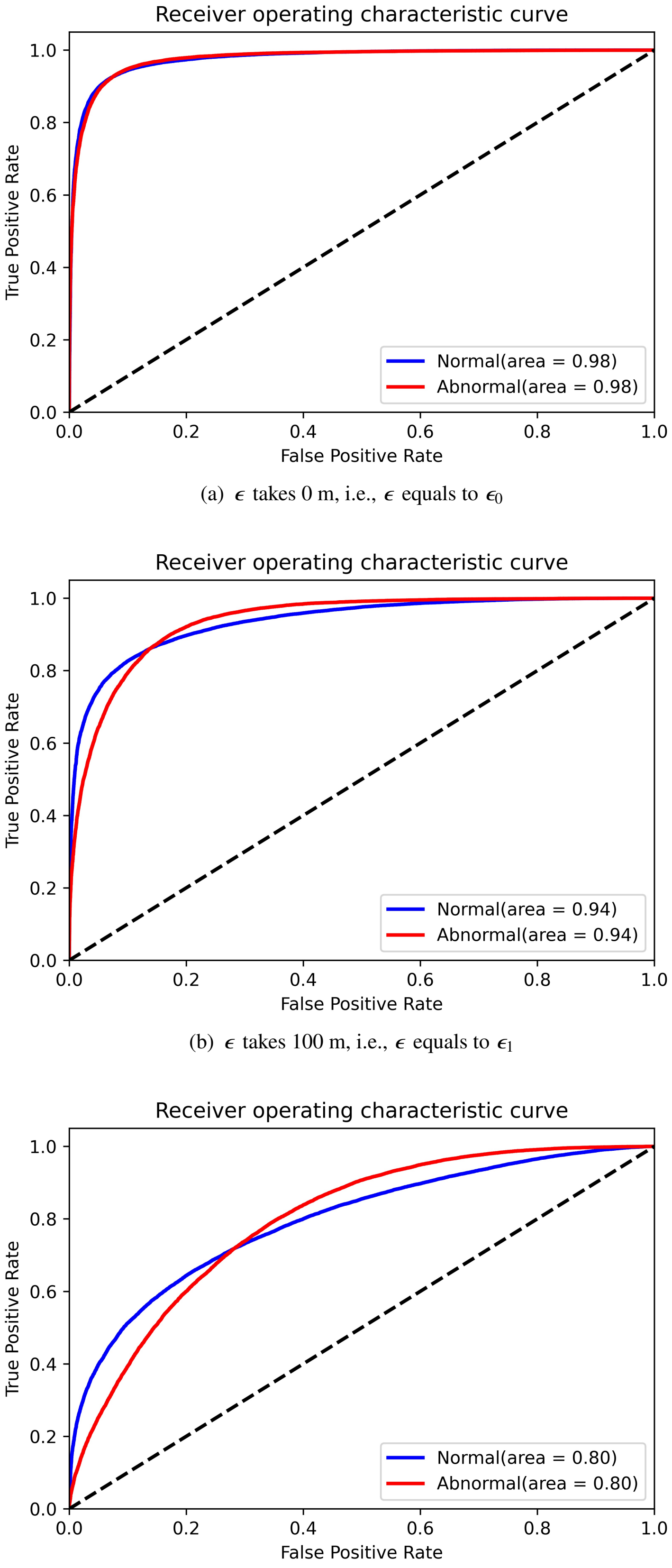
Table 1 Experimental Accuracy

ϵ	**Average value of the noise radius**	**Accuracy**
ϵ_0	0 m	93.1%
ϵ_1	100 m	86.1%
ϵ_2	1,000 m	72.5%

A large amount of noise decreases the accuracy rate of the CNN model, as shown in Table. 1. We compare the receiver operating characteristics curve (ROC) with various setting of ϵ, as shown in Fig. 4. When applying ϵ_1 and ϵ_2, the proposed scheme achieves a high-value accuracy rate of 0.94 on the AUC score. Compared with that of ϵ_1, the AUC score of ϵ_2 has been reduced by 0.14 to 0.80.

4.4 Contrast

We use the same trajectory dataset as the existing related work [21]. When detecting illegal trajectories, the proposed scheme achieves higher accuracy rate than the scheme developed in [21]. The proposed scheme considers a more complex environment, i.e., road networks, than the 2D plane environment considered in [21] The proposed scheme utilizes a different obfuscation process and recognition dataset, so we do not compare the accuracy of the two schemes. Compared with the schemes in [21], the proposed scheme has advantages as follows.



(a) ϵ takes 0 m, i.e., ϵ equals to ϵ_0

(b) ϵ takes 100 m, i.e., ϵ equals to ϵ_1

(c) ϵ takes 1,000 m, i.e., ϵ equals to ϵ_2

Fig. 4 ROC under three different parameters [23].

- The scheme in [21] employs fixed parameters in obfuscation process, while the proposed scheme dynamically calculate the parameters. The dynamically calculated parameters provide higher privacy protection capability and high data utility than the scheme in [21].
- The scheme in [21] manually inject trajectories to generate illegal trajectories. The illegal trajectories trajectories generated in this paper are closer to the real world than that of the scheme in [21]. The generated illegal trajectories in this paper are indistinguishable from the real trajectories which increases the difficulty to detect illegal trajectories. Under the strict assumption, the proposed scheme still achieve a higher accuracy rater than the existing work [21].
- We employ the real-world dataset and road networks to evaluate the proposed scheme. Thus, the proposed scheme in this paper has practical meaning.

5 Conclusions

In this paper, we first propose a new scheme to adaptively protect location data in real-world road networks, which is an important scenario of smart cities. Then, we proposed an illegal trajectory detection scheme to detect illegal locations in the case that all drivers are protected in road networks. The privacy parameters of the proposed scheme was calculated by considering the correlation of the actual location and the obfuscated location. Thus, the adversary cannot infer utilized privacy parameters and the actual locations. We generated illegal trajectory data with speed anomaly and path anomaly to simulate the real-wold malicious driving. The 1D-CNN model with 2D-CNN architecture is proposed in detecting illegal trajectories. According to our experiment results, the proposed detection scheme achieve better performance (e.g., the AUC score is above 0.94) than the existing works in road networks.

In the future work, we will balance the data utility and location privacy to maximize the data availability while satisfying the requirements of drivers' privacy. Moreover, we will assess the privacy levels of driver's privacy and develop a new system to protect location data privacy with the capability to handle most drivers' requirements.

References

1. Haojun Teng, Mianxiong Dong, Yuxin Liu, Wang Tian, and Xuxun Liu. A low-cost physical location discovery scheme for large-scale internet of things in smart city through joint use of vehicles and uavs. *Future generation computer systems*, 118:310–326, 2021.
2. Laxmi Sharma, Abhishek Javali, Rahul Nyamangoudar, R Priya, Pallavi Mishra, and Sudhir K Routray. An update on location based services: Current state and future prospects. In *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, pages 220–224. IEEE, 2017.

3. Yingjie Wang, Zhipeng Cai, Xiangrong Tong, Yang Gao, and Guisheng Yin. Truthful incentive mechanism with location privacy-preserving for mobile crowdsourcing systems. *Computer Networks*, 135:32–43, 2018.
4. Zhaoman Liu, Lei Wu, Junming Ke, Wenlei Qu, Wei Wang, and Hao Wang. Accountable outsourcing location-based services with privacy preservation. *IEEE Access*, 7:117258–117273, 2019.
5. Zuobin Xiong, Zhipeng Cai, Qilong Han, Arwa Alrawais, and Wei Li. Adgan: protect your location privacy in camera data of auto-driving vehicles. *IEEE Transactions on Industrial Informatics*, 17(9):6200–6210, 2020.
6. Miguel E Andrés, Nicolás E Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. Geo-indistinguishability: Differential privacy for location-based systems. In *Proc. of the 2013 ACM SIGSAC conference on Computer & communications security*, pages 901–914, 2013.
7. Raed Al-Dhubhani and Jonathan M Cazalas. An adaptive geo-indistinguishability mechanism for continuous lbs queries. *Wireless Networks*, 24(8):3221–3239, 2018.
8. Yemisi Adegoke. Uber drivers in lagos are using a fake gps app to inflate rider fares. *Quartz Africa, November*, 13, 2017.
9. Yong Ge, Hui Xiong, Chuanren Liu, and Zhi-Hua Zhou. A taxi driving fraud detection system. In *2011 IEEE 11th International Conference on Data Mining*, pages 181–190. IEEE, 2011.
10. Ibrahim Abaker Targio Hashem, Victor Chang, Nor Badrul Anuar, Kayode Adewole, Ibrar Yaqoob, Abdullah Gani, Ejaz Ahmed, and Haruna Chiroma. The role of big data in smart city. *International Journal of information management*, 36(5):748–758, 2016.
11. Shengling Wang, Qin Hu, Yunchuan Sun, and Jianhui Huang. Privacy preservation in location-based services. *IEEE Communications Magazine*, 56(3):134–140, 2018.
12. C. Dwork. Differential privacy. volume 2006, pages 1–12. ICALP, 2006.
13. Lei Yu, Ling Liu, and Calton Pu. Dynamic differential ;ocation privacy with personalized error bounds. In *Network and Distributed System Security Symposium (NDSS)*, 2017.
14. Reza Shokri, George Theodorakopoulos, Jean-Yves Le Boudec, and Jean-Pierre Hubaux. Quantifying location privacy. In *2011 IEEE symposium on security and privacy*, pages 247–262. IEEE, 2011.
15. Yonghui Xiao, Li Xiong, Si Zhang, and Yang Cao. Loclok: Location cloaking with differential privacy via hidden markov model. *Proc. of the VLDB Endowment*, 10(12):1901–1904, 2017.
16. Chao Chen, Daqing Zhang, Pablo Samuel Castro, Nan Li, Lin Sun, and Shijian Li. Real-time detection of anomalous taxi trajectories from gps traces. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking, and Services*, pages 63–74. Springer, 2011.
17. Jiali Mao, Tao Wang, Cheqing Jin, and Aoying Zhou. Feature grouping-based outlier detection upon streaming trajectories. *IEEE Trans. Knowl. Data Eng.*, 29(12):2696–2709, 2017.
18. Di Yao, Chao Zhang, Zhihua Zhu, Qin Hu, Zheng Wang, Jianhui Huang, and Jingping Bi. Learning deep representation for trajectory clustering. *Expert Systems*, 35(2):e12252, 2018.
19. Yann LeCun, Léon Bottou, Yoshua Bengio, and Patrick Haffner. Gradient-based learning applied to document recognition. *Proc. of the IEEE*, 86(11):2278–2324, 1998.
20. Nishant Nikhil and Brendan Tran Morris. Convolutional neural network for trajectory prediction. In *Proc. of the European Conference on Computer Vision (ECCV) Workshops*, 2018.
21. Dajiang Suo, M Elena Renda, and Jinhua Zhao. Quantifying the tradeoff between cybersecurity and location privacy. *arXiv preprint arXiv:2105.01262*, 2021.
22. Mayra Zurbarán, Karen Avila, Pedro Wightman, and Michael Fernandez. Near-rand: Noise-based location obfuscation based on random neighboring points. *IEEE Latin America Trans.*, 13(11):3661–3667, 2015.
23. Yueyao Zhao, Baihe Ma, Ziwen Wang, Zhihong Liu, Yong Zeng, and Jianfeng Ma. Trajectory obfuscation and detection in internet-of-vehicles. In *2022 IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, pages 769–774. IEEE, 2022.
24. Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In *Proc. of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 770–778, June 2016.

25. Karen Simonyan and Andrew Zisserman. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*, 2014.
26. Ramprasaath R. Selvaraju, Michael Cogswell, Abhishek Das, Ramakrishna Vedantam, Devi Parikh, and Dhruv Batra. Grad-cam: Visual explanations from deep networks via gradient-based localization. In *Proc. of the IEEE International Conference on Computer Vision (ICCV)*, pages 618–626, Oct 2017.
27. Gunther Maier. Openstreetmap, the wikipedia map. *REGION*, 1(1):R3–R10, Dec. 2014.
28. Min-hwan Oh and Garud Iyengar. Sequential anomaly detection using inverse reinforcement learning. In *Proc. of the 25th ACM SIGKDD International Conference on Knowledge Discovery & data mining*, pages 1480–1490, 2019.
29. Kathryn Gray, Daniel Smolyak, Sarkhan Badirli, and George Mohler. Coupled igmm-gans for deep multimodal anomaly detection in human mobility data. *arXiv preprint arXiv:1809.02728*, 2018.