International Journal of
Geo-Information

Article

Early Detection of Suspicious Behaviors for Safe Residence from Movement Trajectory Data

Junyi Cheng [1], Xianfeng Zhang [1,*], Xiao Chen [1], Miao Ren [1], Jie Huang [1] and Peng Luo [2]

[1] Institute of Remote Sensing and Geographic Information Systems, Peking University, 5 Summer Palace Road, Beijing 100871, China
[2] Chair of Cartography, Technical University of Munich, 80333 Munich, Germany
* Correspondence: xfzhang@pku.edu.cn

Abstract: Early detection of people's suspicious behaviors can aid in the prevention of crimes and make the community safer. Existing methods that are focused on identifying abnormal behaviors from video surveillance that are based on computer vision, which are more suitable for detecting ongoing behaviors. While criminals intend to avoid abnormal behaviors under surveillance, their suspicious behaviors prior to crimes will be unconsciously reflected in the trajectories. Herein, we characterize several suspicious behaviors from unusual movement patterns, unusual behaviors, and unusual gatherings of people, and analyze their features that are hidden in the trajectory data. Meanwhile, the algorithms for suspicious behavior detection are proposed based on the main features of the corresponding behavior, which employ spatiotemporal clustering, semantic annotation, outlier detection, and other methods. A practical trajectory dataset (i.e., TucityLife) containing more than 1000 suspicious behaviors was collected, and experiments were conducted to verify the effectiveness of the proposed method. The results indicate that the proposed method for suspicious behavior detection has a recall of 93.5% and a precision of 87.6%, demonstrating its excellent performance in identifying the possible offenders and potential target places. The proposed methods are valuable for preventing city crime and supporting the appropriate allocation of police resources.

Keywords: suspicious behavior; trajectory data mining; community safety; ubiquitous computing; pattern detection; predictive policing

Citation: Cheng, J.; Zhang, X.; Chen, X.; Ren, M.; Huang, J.; Luo, P. Early Detection of Suspicious Behaviors for Safe Residence from Movement Trajectory Data. *ISPRS Int. J. Geo-Inf.* **2022**, *11*, 478. https://doi.org/10.3390/ijgi11090478

Academic Editors: Hartwig H. Hochmair and Wolfgang Kainz

Received: 6 July 2022
Accepted: 29 August 2022
Published: 3 September 2022

1. Introduction

There is a growing demand for community safety in cities, and predictive policing has received much attention in preventing crimes [1,2]. The early detection of suspicious behaviors can be used by law enforcement to efficiently deploy their resources to prevent criminal behavior [3]. Specifically, suspicious activity is any observed behavior that could indicate a person may be involved in a crime or about to commit a crime. Nowadays, citizens are encouraged to report suspicious behaviors in their neighborhood to help the police make the community safer, such as the Neighborhood Watch Program in the United States and the Safe Residence Program operated in the Algarve [4,5]. However, detecting suspicious behavior through police patrol and resident reports lacks automation and is time-consuming. Current studies of people's abnormal behavior detection have focused on identifying abnormal behaviors from video surveillance data that are based on computer vision [6,7]. Unfortunately, this approach is suitable for detecting ongoing violent behaviors, such as fights and brawls, but not for suspicious behaviors before committing crimes. The early detection of people's suspicious behaviors is crucial for reducing crimes and improving the overall quality of life.

Criminology studies explain why crimes are carried out at a particular place against a specific target, providing the theoretical foundation for suspicious behavior detection. Environmental criminology, including the rational choice theory [8], routine activity theory [9], and situational precipitators of crime [10], have emphasized the importance of an appropriate opportunity and a suitable target. Accordingly, the offender (e.g., theft) searches for a suitable crime scene and target to conduct criminal activities around places and the paths among them. Besides, crime studies increasingly adopt a foraging perspective when exploring criminal activities [11]. The adopted foraging perspective emphasizes that offenders learn about their environment when committing the first offence in a particular location [12]. The acquired knowledge reduces offenders' uncertainty about targets. For instance, a burglar or terrorist may loiter around and repeatedly observe the intended crime scenes. Consequently, even if criminals are aware of most of their behaviors, their pre-crime activities will be unconsciously reflected in locations and trajectories [13].

Due to advances in positioning technology and the increasing number of cameras, smart mobile terminals, and WLAN networks, large amounts of fine-grained personal trajectory data are collected. Such a large number of trajectories provide us with an unprecedented opportunity to automatically discover helpful knowledge [14,15], such as identifying suspicious movements and unusual activities. Therefore, crimes can be prevented if people's suspicious behaviors can be automatically detected by mining the semantic information that is hidden in the trajectory data.

Under the pressure of safety issues, some studies have tried to develop suspicious behavior detection methods using trajectories from unusual movement patterns in recent years [16,17]. However, to prevent crimes, the current methods for suspicious behavior detection from trajectory data suffer from the following problems: (1) they mainly focus on abnormal moving patterns, but suspicious behaviors include not only abnormal movement patterns but also unusual behaviors such as travel at unusual times; (2) the lack of detection methods that are adapted to the complexity of suspicious behaviors in real scenes, such as leaving midway while loitering around the crime scene; and (3) just presented some case studies but lacked quantitative accuracy assessment because there is a lack of trajectory datasets for validating detection algorithms of suspicious behaviors.

This study extends movement trajectory analysis to recognize people's suspicious behaviors that are likely to be a precursor to a crime. Moreover, we analyze the features of different behaviors and propose novel algorithms for detecting suspicious behaviors that are hidden in massive trajectory data. Rather than analyzing the causes of crime, we provide a method for detecting suspicious behaviors before committing a crime in this study. The contributions of this work can be summarized as follows:

(1) From the perspective of unusual movement patterns, unusual behaviors, and unusual gatherings, we introduce and characterize eight suspicious behaviors that could be reflected in the individual trajectory. This information is crucial for developing an urban safety-oriented early warning system and helping police make the community safer.

(2) Through analyzing the features of different suspicious behaviors, we propose and implement the corresponding detection algorithms with strong robustness for the complexity of real scenes. Specifically, the semantic information that is hidden in the trajectory is mined to recognize the suspicious behaviors based on spatiotemporal clustering, semantic annotation, trajectory pattern mining, outlier detection, and other methods.

(3) A real trajectory set containing more than 1000 simulated suspicious behaviors was collected and used to verify the proposed methods quantitatively.

2. Related Work

In this section, we briefly review the existing abnormal detection methods that are based on trajectories, which can be divided into outlier trajectory detection and anomaly behavior detection algorithms based on trajectory analysis [18].

2.1. Detection of Abnormal Trajectories Based on Outlier Detection

The main objective of outlier detection methods is to detect outlier trajectories with large local or global differences from other trajectories using a similarity metric. Outlier trajectory detection can be categorized as supervised classification-based, distance- and clustering-based, statistical model-based, and graph-based methods. The classification methods utilize labeled data for training machine learning or deep learning classifiers to classify the trajectory data. Since many labeled samples are required, and the model does not directly classify abnormal samples, this method is rarely used. The distance-based methods assume that a trajectory that is far from the other trajectories is an outlier [19]. However, the distance-based methods require a reasonable distance threshold to identify abnormal behaviors and consequently require subjective inputs. Therefore, some researchers have proposed semi-supervised or unsupervised clustering methods using the trajectory distance for clustering [20,21]. These methods assume that normal samples can be clustered into several clusters, whereas samples that are difficult to classify into any cluster are abnormal. The third method is based on a statistical model to infer abnormal behaviors, which assumes that a sample is abnormal if the probability of generating its trajectory by the model is low [22,23]. The graph-based methods transform the trajectory into a person-place-time graph and group the nodes by their similarity for abnormal trajectory detection [24].

The outlier detection method can effectively detect trajectories that differ significantly from other trajectories in shape or other similarity metrics. There have been various effective deep learning-based outlier detection methods in recent years [25]. However, in detecting suspicious behaviors, the similarity measurements are not shape-based but intention-based, which leads to a vague definition and may not be appropriate for applying common trajectory mining or outlier detection methods. Moreover, the people's behaviors before committing crimes are often complex, and a trajectory that differs from other trajectories does not necessarily indicate suspicious behavior and a threat to city safety. The detected outlier trajectory lacks semantic information, and further analysis is required. Besides, the high computational complexity and few suspicious behavior samples are key aspects, especially when the technique is applied in real-life. Therefore, it is challenging to identify suspicious behaviors that may endanger urban community safety only by using outlier detection methods.

2.2. Abnormal Behavior Detection Based on Trajectory Analysis

The main goal of anomaly behavior detection algorithms that are based on trajectory analysis is to extract the semantic information in the trajectory data using trajectory analysis methods combined with domain knowledge. Subsequently, the rationality of the behaviors is analyzed based on specific scenarios. For instance, pattern mining methods are frequently used to discover semantic locations that are important to an individual; visits to infrequent locations are then considered abnormal behavior. These methods have been widely applied in healthcare [26,27], urban transportation [28,29], and maritime transportation [30,31]. For instance, some studies in healthcare research defined specific moving patterns (e.g., pacing, lapping) of wandering behaviors that were exhibited by patients with diseases such as dementia and Alzheimer's and used machine learning methods (e.g., decision trees) to extract this behavior [27,32]. In addition to defining abnormal movement patterns of moving objects, some studies investigated abnormal patterns that were related to the relationship between moving objects and locations. For instance, dangerous behaviors between pedestrians and roads include crossing the road border, illegal stay, road crossing, moving along the curb, and entering the road [33]. Unusual behaviors between moving objects and locations were classified as surround, escape, and return [34].

Nevertheless, there are few studies on detecting suspicious behaviors before committing a crime because of the complexity and difficulty of defining pre-crime movement patterns. An interesting work describes the scenario of roaming behaviors that are related to planned crimes and then derives formal specifications for detecting suspicious roaming events from vehicle trajectories [16]. A recent study proposed the definitions of abnormal behaviors (e.g., wandering, scouting, and random walking) threatening social safety and used movement patterns to extract abnormal behaviors [17]. This is the closest work to our approach. However, this work only detected suspicious behaviors based on movement patterns and ignored the historical behaviors, and the proposed method was verified on simulated data and lacked quantitative evaluation on a real trajectory dataset. Finally, the existing research lacks underlying criminological theories of suspicious behaviors.

3. Methodology

Suspicious behaviors refer to individual behavior patterns that seem unusual or out of place, likely to be a precursor of a crime. We determined the types of suspicious behaviors for the following two reasons: (1) Practicality. We conducted investigations at multiple police stations and referred to government announcements in various countries [5,35–37], thereby identifying some practical suspicious behaviors that may be signs of crime. (2) We identify the behaviors that are hidden in trajectories from the three most commonly used aspects of trajectory analysis: movement patterns, historical behavior semantics, and group patterns. Considering that the focus of this study is to detect suspicious behaviors from personal trajectory data, those suspicious behaviors that are unsuitable for detection using trajectories are not included. Of course, we have to admit that the defined suspicious behaviors in this work are not all, and other suspicious behaviors may be detected better from other data sources. For example, someone peering into cars or windows is much easier to detect in video surveillance.

Based on the principles of the detection algorithms, we divide suspicious behaviors into three categories: unusual movement patterns, unusual behaviors, and unusual gatherings of individuals (Figure 1). The unusual movement patterns are movements that seem out of place, consisting of features in motion (e.g., multiple large-angle direction changes) and behaviors of individuals concerning locations (e.g., loitering around locations repeatedly). The unusual behaviors are certain behaviors that do not coincide with the historical activity of this person, including visiting unusual locations, traveling at unusual times, and unusual routes. Multiple individuals are gathered for longer than a certain period in a small area is defined as crowd gathering, and members can enter and leave this group at any time. In this paper, we propose the corresponding detection algorithm for the main features of each suspicious behavior, rather than a deep learning method that automatically extracts features. The main reasons are as follows: (1) Interpretability. It is essential for law enforcement agencies to make adequate inferences from the detected results and ensure that it is properly understood to develop appropriate strategies. Thus, we characterize suspicious behaviors under the guidance of criminological theory. (2) The difficulty of training. Suspicious behavior occurs much less often than regular behavior, so it is challenging to train a supervised machine learning model, especially a deep learning model. (3) Efficiency. Algorithms that are used in policing systems need low time complexity to avoid crimes effectively. Although these behaviors are not absolute confirmation of crimes, recognizing the potential crimes based on these suspicious behaviors will significantly reduce the crime rate.

In the following, we will clarify some of the key definitions that are used throughout this paper. A trajectory is defined as the path of a person consisting of multiple spatiotemporal points with time stamps. Each spatiotemporal point contains the location, time, and the ID of the person; it can be expressed as T = <($lon_1, lat_1, time_1, UserID$), ($lon_2, lat_2, time_2, UserID$), ... , ($lon_n, lat_n, time_n, UserID$)>. In practical applications, personal trajectories can be obtained from various sources, including smartphones, GPS positioning terminals, surveillance cameras, and smart bracelets.

A stop $SP = (x,y,t_{start},dur)$ represents the location that a person is visiting, consisting of a series of consecutive spatiotemporal trajectory points. In particular, a “stop” is not entirely stationary, rather it denotes staying in a relatively small neighborhood for an extended period. The coordinate (x,y) is the center position of the stop, which is obtained by computing the average positions of all spatiotemporal points during the stop. t_{start} represents the start time of the stop, and dur represents the duration of the stop, which is calculated as the difference between the end time and the start time of the stop.

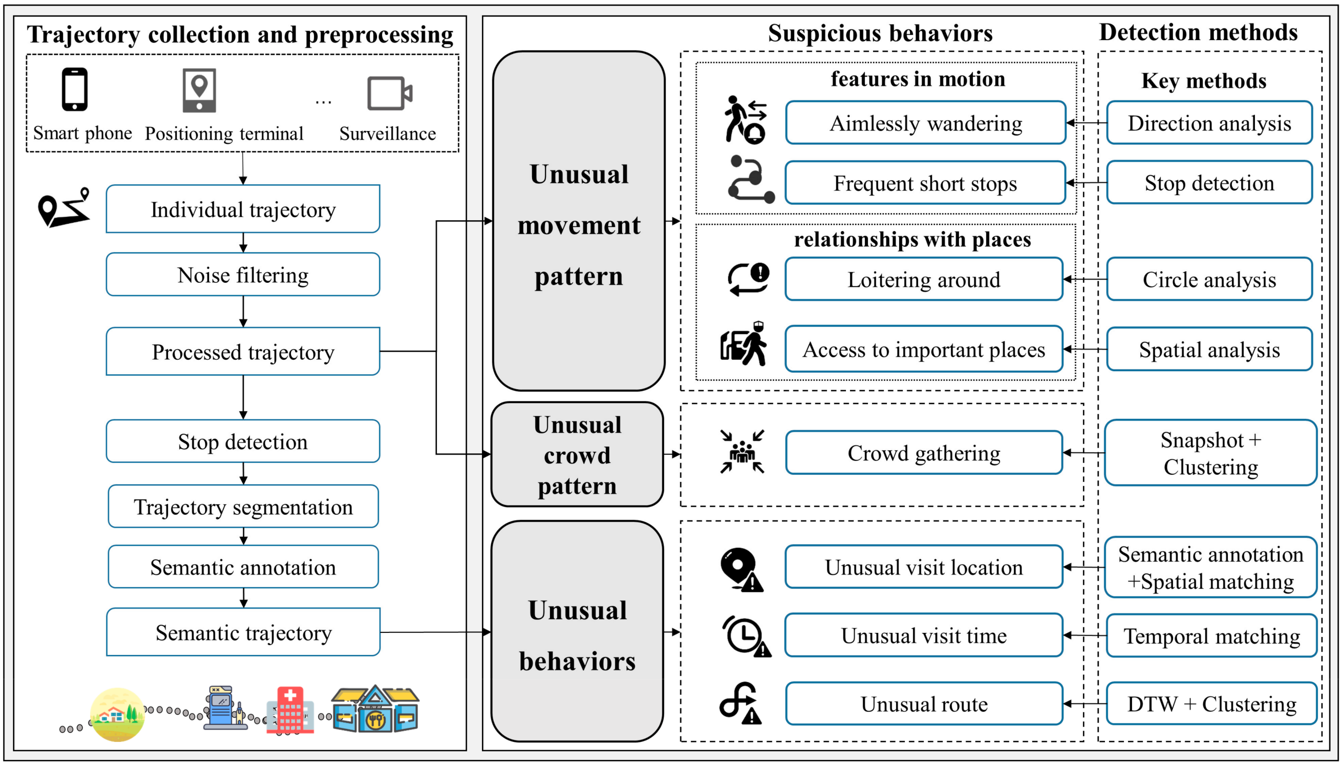

Figure 1. Flowchart of the proposed method for suspicious behavior detection from the trajectory data.

3.1. Algorithms for Detecting Unusual Movement Patterns

In order to recognize unusual movement patterns, we analyze the characteristics of four suspicious behaviors and propose the corresponding methods, including aimlessly wandering, frequent short stops, access to important places, and loitering around locations repeatedly. Furthermore, these four behaviors can be divided into unusual movement features and relationships with places.

3.1.1. Detection Based on Movement Features

(1) Aimlessly wandering

The routine activity approach assumed that for crimes to occur, there must be a convergence in time and space of three minimal elements: a likely offender, a suitable target, and the absence of a capable guardian against the crime [9]. The offender (e.g., theft and vandals) searches for a suitable crime scene and the target to conduct criminal activities [8]. Thus, it is important to notice a stranger wandering in the neighborhood or walking across the streets repeatedly and aimlessly. Aimlessly wandering is defined as abruptly changing direction many times in a short period in this work. The main feature of this type of suspicious behavior is that a person makes several large-angle changes in a short period (Figure 2). Generally, pedestrians do not make more than three large-angle turns in a short period. For instance, if people leave home and forget their keys, they only make two large-angle turns while turning back and leaving again.

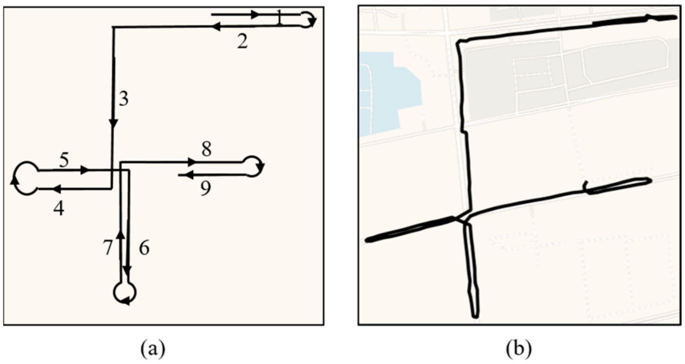

Figure 2. The schematic (**a**) and actual trajectory (**b**) of aimlessly wandering. Each curve in (**a**) corresponds to a large directional change.

Thus, the detection algorithm traverses each spatiotemporal point in the sequence to search for large-angle changes. Nevertheless, noise and short stops may also cause large changes in the heading angle (Figure 3). Therefore, it is necessary to analyze several spatiotemporal points before and after the current point to determine whether the large-angle change is correct. The velocity of the point p_i is v_i, the heading angle is h_i, and the conditions for determining whether there is a large-angle change in direction at point p_i are as follows:

(1) Does not belong to a stop: $\forall \mathrm{p} \in \{p_{i-3}, p_{i-2}, p_{i-1}, p_i, p_{i+1}, p_{i+2}, p_{i+3}\} \notin \mathit{any\ stop}$;
(2) Complete a large-angle change: $\sum_{j=i-1}^{3}(h_j - h_{j-1}) > angle$, $angle$ is the threshold of the turning angle.
(3) End of turning: $\sum_{j=i+1}^{3}(h_j - h_{j-1}) < angle$.
(4) The person is moving: $\frac{\sum_{j=i-1}^{3} v_j}{3} > speed$, $speed$ is the minimum speed threshold.
(5) Drift not caused by noise: $v_j < (v_{j-1} + v_{j-2})$ and $\frac{\sum_{j=2}^{2}(h_{i+j} - h_{i-j})}{2} > angle_{min}$, $angle_{min}$ is the mean angle difference threshold.
(6) Continue to travel a certain distance in the current direction after completing a large-angle turn.

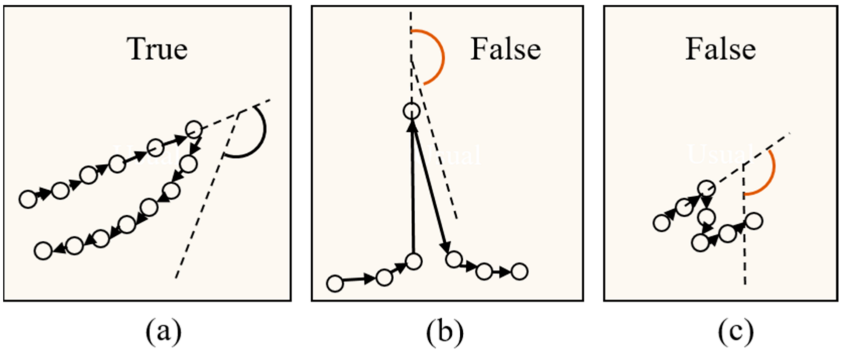

Figure 3. Several cases of large-angle changes in the heading angle. (**a**) correct large-angle change, (**b**) false large-angle change that is caused by noise, and (**c**) false large-angle change that is caused by a short stop.

(2) Frequent short stops

Crime pattern theory proposes that crime is perpetrated at those places and times where a motivated criminal's awareness space overlaps with the spatiotemporal distribution of attractive criminal opportunities [38]. It assumes that offenders should be aware of a location in order to be able to choose it as a target [39]. Besides, the foraging perspective also emphasizes that offenders learn about their environment when committing the first offence in a particular location [11]. For example, a possible drug dealer, sex offender, or burglar may observe the planned crime scenes without lights at night, around schools, residential streets, or playgrounds. The main feature is that a person moves slowly and exhibits multiple short stops in a short time, and this is defined as frequent short stops behavior. The person may not come to a complete stop but may move at a slow speed or move back and forth in a small area (Figure 4).

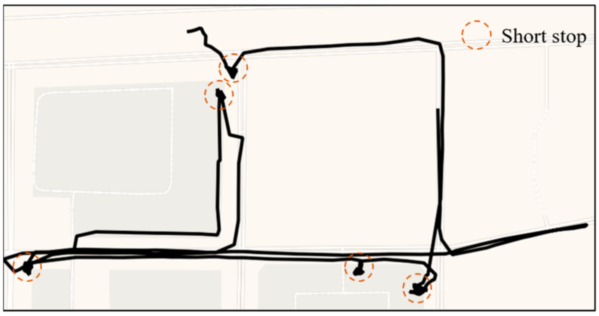

Figure 4. An example of a trajectory of frequent short stops. Each red circle indicates a short stop.

To identify this behavior, a spatiotemporal clustering algorithm is chosen to detect high-density clusters with strong aggregation in the spatiotemporal dimension. More specifically, the neighborhood of a spatiotemporal point is defined as the longest continuous subsequence starting from this point. The spatial distance from the starting point is less than the specified distance threshold d_1 for all points in the sequence. The neighborhood of point P_i can be expressed as:

$$Neighbor_{P_i} = \{P_{i+1}, P_{i+2}, \ldots, P_{i+n-1}, P_{i+n}\} \text{ st.} \forall P \in Neighbor_{P_i},\ distance_{P,P_i} < d_1, \quad (1)$$

where $Neighbor_{P_i}$ is the neighborhood of the spatiotemporal point P_i, and $distance_{P,P_i}$ is the spatial distance from P to P_i.

The density of the neighborhood is defined as the period of the sequence. Points with a density exceeding the period threshold t_1 were denoted as core points; otherwise, they were identified as noise. These definitions were integrated into the density-based spatial clustering of applications with noise (DBSCAN) algorithm to identify the stops in the trajectory [40]. Once the detection process was completed, all the stops that were adjacent in both time and space were merged to ensure that the entire stop would not be divided into several smaller stops.

Moreover, it is determined whether there are multiple short stops in the trajectory within a certain time interval after the extraction is completed. The time interval threshold is T, the stop duration threshold is D, and the minimum number of short stops is N. If there are frequent short stops, a set of stops occurs:

$$\text{stopset} = \{(x_1, y_1, t_{start1}, dur_1), \ldots (x_n, y_n, t_{startn}, dur_n)\}, \quad (2)$$

where $n \geq N$, $t_{startn} \leq t_{start1} + T$, and $\forall dur \in \{dur_1 \ldots dur_n\}$, $dur < D$.

3.1.2. Detection Based on the Relationship between Individuals and Places

(1) Loitering around a public place

Similar to frequent short stops, the optimal foraging and crime pattern theory can also explain the behaviors of loitering around a public place [11,38]. Loitering around refers to observing planned crime scenes repeatedly before committing crimes. The acquired knowledge reduces offenders' uncertainty about targets. Persons that are loitering around schools, parks, or secluded areas may be possible burglars, sex offenders, or drug dealers. The main feature is that the same person repeatedly loiters around a public place several times, forming a circular trajectory (Figure 5). The person may not observe the area continuously, e.g., they may go around a site in the morning and again in the evening or stop and leave the area briefly. In addition, there may be two circular trajectories in different directions. Therefore, the detection algorithm should be robust and adaptable to the complexity of real scenes.

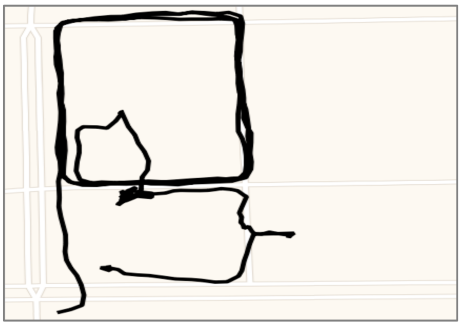

Figure 5. An example of a trajectory of loitering.

Since the main feature is repeatedly loitering around a place, the proposed loitering detection algorithm comprises of circle extraction and overlap detection. The objective is to find the sequence of circles in the trajectory and determine whether loitering behavior has occurred by detecting overlapping circles. The trajectories are mapped onto grids to solve the problem that the head and tail points of a circle may not be closed due to the positioning accuracy. This method is not affected by midway stops or noise fluctuations and has better robustness than only detecting lapping movement patterns. The specific steps are as follows:

Step 1: Starting from the first spatiotemporal point in the sequence and traversing backward, the algorithm searches for the point with the same position as the current point. After finding the point pair that meets the condition, if the time difference between the two spatiotemporal points does not exceed the threshold T_{max}, and the area of the polygon that is formed by the spatiotemporal point sequence between the two points is larger than the area threshold S_{min}, the polygon forms a circle, which is denoted as *Polygon.*

Step 2: If the data stack containing the detected circles is empty, or the point sequence of the polygon ($Polygon_s$) at the top of the stack does not have a time intersection with the sequence of the *Polygon*, the *Polygon* is added to the stack. The algorithm goes back to Step 1 and continues the traversal. If the time intersects, the algorithm proceeds to the next step.

Step 3: If there is almost no spatial overlap, the *Polygon* is added to the stack, and the traversal continues. If the *Polygon* overlaps with most of the $Polygon_s$ (e.g., more than 80%), it indicates that the same circle has been detected more than once. Thus, the circle is ignored, and the traversal continues. If there is partial overlap, the circle at the top of the stack is updated to the circle with the larger spatial area. The algorithm goes back to Step 1 and continues the traversal.

Step 4: After traversing all the spatiotemporal points in the detecting trajectory, the ratios of the overlapping areas of each of the two circles in the stack are calculated as follows:

$$r(i,j) = \frac{area_{Polygon_i \,\cap\, Polygon_j}}{\min\left(area_{Polygon_j}, area_{Polygon_j}\right)}, \tag{3}$$

where $r(i,j)$ denotes the proportion of overlapping polygons $Polygon_i$ and $Polygon_j$ in the stack, $\min\left(area_{Polygon_j}, area_{Polygon_j}\right)$ denotes the minimum area between $Polygon_i$ and $Polygon_j$, and $area_{Polygon_i \,\cap\, Polygon_j}$ denotes the area of overlap of $Polygon_i$ and $Polygon_j$.

If $r(i,j)$ is greater than the overlap ratio threshold r, loitering behavior occurs in $Polygon_i$ *and* $Polygon_j$.

The pseudo-code of this algorithm is shown in Algorithm 1:

Algorithm 1: The pseudocode of loitering detection

```
Input: $S$:Trajectory sequence   $T_{max}$:Maximum time interval   $S_{min}$:Minimum area
    $r$:Minimum overlapping area ratio
Output: Loitering sequences
set $N$ to length($S$) // N is total number of points in the sequence S
set $stack$ to $\emptyset$
for each point $s[i]$ in sequence $S$ do
    for $j$=i-1;$j \geq 0; j = j - 1$ do
        if the time difference between $s[i]$ and $s[j]$ is greater than $T_{max}$ then
            break
        if the coordinates of $s[i]$ and $s[j]$ are the same then
            set Polygon to the polygon formed by the points between $s[i]$ and $s[j]$ in sequence $S$
            if the area of Polygon is bigger than $S_{min}$ then
                if stack is empty then
                    add Polygon to the stack;
                else
                    set $Polygon_s$ to the polygon at the top of the stack;
                    if the sequence of Polygon and the sequence of $Polygon_s$ intersect then
                        if Polygon and $Polygon_s$ mostly overlap then
                            break
                        else
                            if Polygon and $Polygon_s$ rarely overlap then
                                add Polygon to the stack;
                            else
                                if the area of Polygon is bigger than the area of $Polygon_s$ then
                                    update the the polygon at the top of the stack to Polygon;
                    else
                        add Polygon to the stack;
    set $N_s$ to length($stack$) // $N_s$ is total number of polygons in $stack$
    set $result$ to $\emptyset$
    for each polygon $stack[i]$ in stack do
        for $j$=i+1;$j$ <$N_s$;$j$=j+1 do
            if the ratio of the overlapping areas of $stack[i]$ and $stack[j]$ is greater than $r$ then
                add the corresponding time sequences of $stack[i]$ and $stack[j]$ to $result$;
    return $result$;
    final
```

(2) Access to important areas

Crime opportunities are concentrated in space, and hot spots can drive up the local crime rate [41,42]. Thus, there are some important places to watch to prevent crimes. Access to important places refers to that a person intentionally approaches some areas, which are crime hot spots or crime generators. The important places to watch may include government buildings, schools, gas stations, and public transportations. For example, a person may remain in the vicinity of the key surveillance area of a police department longer than expected. The person may be stationary or move around the area slowly.

Herein, the spatial analysis between important places and trajectories should be conducted. Buffer zones are created around important areas. If the time of the trajectory inside the buffer zone exceeds a certain length, the trajectory is considered to have access to an important area.

3.2. Algorithms for Detecting Unusual Behaviors

Except for the above abnormal movement patterns in trajectories, some trajectories may be similar to others but contain different semantic information due to unusual locations or times. These unusual behaviors are certain behaviors that do not coincide with the historical pattern of this person, including unusual routes, visit locations, and travel times. Before analyzing behaviors, segmenting the trajectory into sequences in which "moving" and "stop" episodes alternately appear is necessary. The stop detection method that was used here is the same as the method that was described in frequent short stop detection in Section 3.1.1. It is assumed that if individuals have stopped, they must be doing meaningful activities at specific places, and therefore, the stops are considered as visiting places. After segmenting the trajectories into "moving" and "stop" episodes, whether the current behavior is unusual is analyzed using the following methods.

3.2.1. Unusual Route Detection

The route, which is different from the usual historical routes for the same start and end points, is termed an unusual route. This demonstrates that persons may have traveled to other locations or met with other people on the route. Suppose an unusual route passes through an important location, or it appears that other suspects are at the same location on the unusual route. In that case, the relevant authorities should investigate it further. Historical and unusual routes may not be unique (Figure 6), and the usual historical route is not necessarily the shortest but may be related to local road conditions.

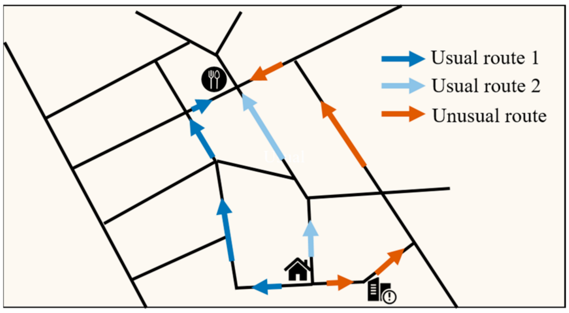

Figure 6. Schematic of an unusual route.

To determine whether the current route is unusual, we propose a clustering-based outlier detection method, which mainly includes trajectory distance calculation and clustering. The sequence of spatiotemporal points between two stops forms a route, and the searched routes, which are consistent with (or opposite to) the start and end of the current detecting route, form a historical route set. The distance between routes is calculated by the DTW strategy [43] and the Manhattan distance. Due to the difference in the sampling interval and moving speed, the sequence lengths of two identical routes differ, and the spatiotemporal points are difficult to align. The DTW method calculates the distance or similarity between the time sequences by extending and shortening the time sequence. The same point may match different points in another sequence. DTW uses the sum of the distances between all similar points, called the warp path distance, to measure the distance between the time sequences. To make the distance calculation more efficient, the trajectories are mapped onto grids to reduce the sequence length. Since the city layout is usually regular in blocks, the Manhattan distance is chosen to calculate the distance between matching spatiotemporal points. In the plane, the Manhattan distance between point *i* at coordinates (x_1, y_1) and point *j* at coordinates (x_2, y_2) is:

$$d(i, j) = |x_1 - x_2| + |y_1 - y_2|. \tag{4}$$

The core idea of DTW is to find the shortest warp route distance between the sequence Q = $(q_1, q_2, \ldots, q_n)$ and the sequence P = $(p_1, p_2, \ldots, p_m)$, and the solution is based on the dynamic programming algorithm. The recursive formula is as follows:

$$L_{min}(q_i, p_j) = \min\{L_{min}(q_{i-1}, p_j), L_{min}(q_i, p_{j-1}), L_{min}(q_{i-1}, p_{j-1})\} + d(q_i, p_j) \tag{5}$$

where $d(q_i, p_j)$ denotes the Manhattan distance between node q_i in route Q and node p_j in route P, $L_{min}(q_i, p_j)$ denotes the shortest warp distance between $(q_1, q_2, \ldots, q_i)$ and $(p_1, p_2, \ldots, p_j)$, where $L_{min}(q_1, p_1) = d(q_1, p_1)$.

After calculating the distance between every two routes in the historical route set, the DBSCAN algorithm [40] is used to cluster the routes. The distance threshold of the neighbor is set to the average distance between all the routes in the historical route set. If the current route is marked as noise by the DBSCAN algorithm, the route is considered an unusual route.

The code of the detection algorithm of the unusual route is shown in Algorithm 2:

Algorithm 2: The pseudocode of unusual route detection

```
Input:
    $s$: the current detecting route,a collection of point coordinates
    $s_{start}$: the coordinate of the start point of the current detecting route $s$
    $s_{end}$: the coordinate of the end point of the current detecting route $s$
Output:
    whether $s$ is an unusual route
set $useroute$ to $\emptyset$;
for each route $s[i]$ in the history route collection do
    if the start point of $s[i]$ is the same as $s_{start}$ and the end point of $s[i]$ is the same as $s_{end}$ then
        add $s[i]$ to $useroute$;
    else
        if the start point of $s[i]$ is the same as $s_{end}$ and the end point of $s[i]$ is the same as $s_{start}$ then
            add $s[i]$ to $useroute$;
add $s$ to $useroute$;
set $N$ to length($useroute$);
for each route $useroute[i]$ in $useroute$ do
    for $j$=$i$+1;$j \leq N$; $j = j + 1$ do
        calculate the DTW distance between $useroute[i]$ and $useroute[j]$;
set $average_d$ to the average distance between all routes in $useroute$;
DBSCAN($useroute, distance = average_d, MinPts = 3$);//clustering paths with DBSCAN
if $s$ is marked as Noise by the DBSCAN algorithm then
    return True
else
    return False
final ;
```

3.2.2. Algorithm for Detecting Unusual Visit Locations

Brantingham and Brantingham hypothesize that offenders may avoid targets immediately adjacent to their homes to avoid being recognized [44]. People who do not seem to belong in the workplace, neighborhood, campus, or anywhere are considered suspicious persons that are out of place [42]. The unusual visit location is featured by a person visiting locations that are never or rarely visited before, and locations of interest differ for different people. The algorithm searches for historical stops of the person with the same semantic meaning as the location of the current stop (e.g., the same university, the same neighborhood) or the close geographic location. Thus, the semantic annotation for visited places is needed after detecting stops. An unsupervised place annotation method [45] is used to infer the visited locations. In this method, a spatiotemporal probability model for the candidate places is created and decomposed into the spatial, duration, and visiting time probabilities. The spatiotemporal probability of a candidate place O_i corresponding to the stop point SP=$((x, y), t, dur)$ can be expressed as

$$P(O_i|(x,y),t,dur) = P(t|O_i)\cdot P(dur|O_i)\cdot P(O_i|(x,y))\cdot\frac{P((x,y))}{\mathrm{P}((x,y),t,dur)}, \tag{6}$$

where (x, y) is the coordinate of the stop center of *SP*; *dur* is the duration of *SP*; *t* is the visiting (start) time of *SP*; $P(t|O_i)$ is the visiting time probability; $P(dur|O_i)$ is the duration probability; $P(O_i|(x,y))$ is the spatial probability; and $\frac{P((x,y))}{P((x,y),t,dur)}$ is a constant for the same stop.

For each stop, the candidate place with the highest visit probability is marked as the visited place. If less than a certain number of stops meet the condition of the same visit place or close geographic location, it is considered an unusual visit location.

3.2.3. Algorithm for Detecting Unusual Visit Time

A given location may be ideal for crime at one time but unfavorable for crime at another [42]. For example, a street robber might be able to attack a victim at a darker time when others are absent. The unusual visit time refers to a person that is traveling at a time that occurs infrequently compared to travel history and visiting a specific location. Similarly, there may be differences in the usual travel times of different people. The sequence between two stops corresponds to one trip. The algorithm finds the historical trajectories with the close travel time to the current trajectory in the historical travels of the person. The visit time is considered unusual if the number of travels is less than a pre-setting value. The detected unusual visit time may indicate the person's abnormal behavior that is caused by some reasons such as committing a crime.

3.3. Detection Algorithm for Crowd Gathering

Multiple persons that are gathered together for longer than a certain period of time in a small area is defined as a crowd gathering. A gathering represents a crowd event or incident that involves a congregation of objects, such as celebrations, parades, traffic jams, and other public gatherings [46]. Discovering unusual gatherings over trajectories can help monitor and predict public safety issues.

We combine the spatiotemporal snapshot and density clustering to detect crowd gathering. If there exists at least *M* participators in each snapshot cluster of a spatial-closed crowd, it forms a gathering. Specifically, we begin at the detection start time t_{start} and search the positions of all persons at each time step $t_{interval}$(e.g., 1 min). The position at the *i*-th moment $(t_{start} + i * t_{interval})$ is the average position of all the spatiotemporal points of the people from the previous moment to that moment. Next, the DBSCAN algorithm is used to determine whether a cluster exists at each moment. The neighborhood sample threshold is set to the minimum number of participants, and the neighborhood distance threshold is set to 50 m. If a cluster exists, people are gathering at the current moment. If the total gathering time is longer than the time threshold N, crowd gathering is occurring.

As shown in Figure 7, crowd gathering occurs from T_2 to $T_{(2+N)}$ when there are more than five people.

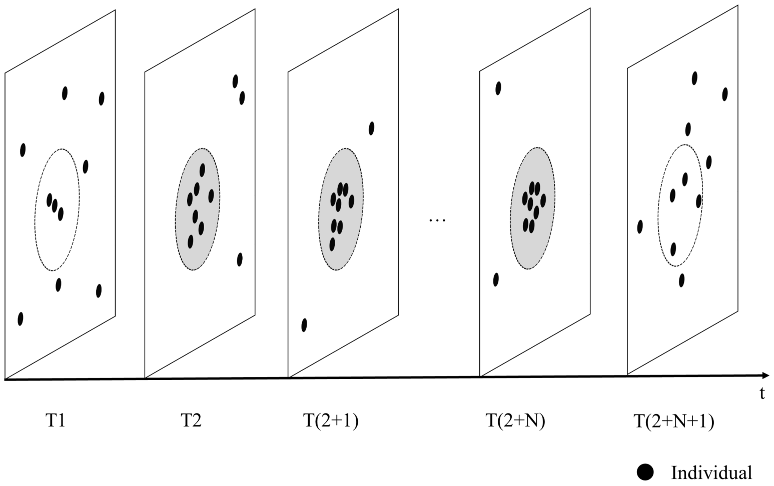

Figure 7. Schematic of crowd gathering. The gray circles show that people are gathering at the moment.

4. Experiments and Results

4.1. Trajectory Dataset with Suspicious Behaviors

An experiment was conducted to extract the suspicious behaviors from our collected trajectory dataset called TucityLife to evaluate the effectiveness of the proposed method. Since the high spatiotemporal-resolution trajectory data of real crimes is confidential and challenging to collect, we organized volunteers to conduct the above suspicious behaviors under the guidance and assistance of the police officers and collected the trajectories. The TucityLife dataset was collected by 28 volunteers in a city in west China from 17 July to 24 August 2021. The participants volunteered to record daily activities and suspicious behaviors over a period of more than four weeks. During everyday life, each volunteer randomly performed some suspicious behaviors anytime and anywhere. The volunteers that were involved in data collection were in different occupations, such as company employees, college students, and police officers. During the data collection, the geographic location information of each volunteer was collected using a custom-built location APP which was installed on Android smartphones, and the location data was uploaded and stored to the cloud database in real-time. As the GPS trackers collected private locations, a privacy protection contract was signed by each participant. A total of 2,907,951 spatiotemporal points were collected in the campaign. The time interval for positioning varies from 1 to 20 s, depending on the travel speed.

The volunteers completed a daily activity log every night, which included the time and type of daily activities and suspicious behaviors. The activity log was checked daily by playing back the trajectory to ensure the quality of the data collection. The activity log recorded more than 1000 suspicious activities, meeting the requirements of this study for verifying suspicious behaviors.

Noise is present in the original trajectory data due to signal blockages. Thus, preprocessing is required to remove the spatiotemporal point drift due to occlusion and duplicate uploads in case of a poor connection. Due to the fact that the noise in the trajectory is signal drift that is caused by the obstruction of buildings or other objects, therefore, the noise points are not located on the original route. The proposed method removes those noise based on three characteristics: positioning accuracy, speed, and a change in the heading angle. In the trajectory noise removal, the positioning accuracy threshold is 50 m, the maximum speed threshold is 100 km/h, and the maximum heading angle change is 150°.

4.2. Experiments for Suspicious Behavior Detection

4.2.1. Evaluation Indices

The suspicious behavior information that was recorded in the activity log of the TucityLife dataset was used as the true value, and the accuracy was checked by comparing the detected suspicious behavior with the true value. The precision, recall, and $F1$-score of the suspicious behaviors were calculated as follows:

$$\text{Precision} = \frac{TP}{TP + FP}, \tag{7}$$

where TP is the number of true positives, i.e., the detected suspicious behaviors that were successfully matched with the activity log, FP is the number of false positives, i.e., the detected suspicious behaviors unsuccessfully matched with the activity log.

$$\text{Recall} = \frac{TP}{TP + FN}, \tag{8}$$

where FN is the number of false negatives, i.e., the suspicious behaviors in the activity log that were not detected successfully.

$$F1 - \text{score} = \frac{2 * \text{precision} * \text{recall}}{(\text{precision} + \text{recall})}. \tag{9}$$

4.2.2. Parameter Setting

The parameter settings in the study are grouped into rule sensitivity and algorithm parameters. Rule sensitivity parameters refer to the parameters that are set in the rules, which determine the number of detected suspicious behaviors. These parameters can be adjusted, but it is important to note that the stricter the parameter value, the less suspicious behavior is derived. Algorithm parameters refer to the thresholds that are used in the algorithm to detect suspicious behavior. After performing some experiments, we define the parameters as follows.

(1) Rule sensitivity parameters

The detection rules for frequent short stops are a minimum of 3 stops of less than 10 min in 2 h. The minimum time for accessing an important area is 5 min. The minimum density of neighborhoods for unusual route clustering is 3. The detection rule for unusual visit locations is less than 3 visits to the same location or the same geographical area. An unusual visit time is defined as less than 3 travels with travel moments that are less than 15 min apart. The minimum number of participants for crowd gathering is 10, and the minimum gathering time is 30 min.

(2) Algorithm parameters

Loitering detection is performed by mapping the spatiotemporal points in 50 m × 50 m grids with a maximum time difference threshold of 120 min and a minimum area of 5 grids. Loitering occurs when the proportion of two overlapping polygons exceeds 50%. The angle threshold for aimlessly wandering is 150°, the speed threshold is 0.4 m/s, and the mean angle difference threshold is 100°. In the stop extraction, the distance threshold for the stop points is 60 m, and the time threshold is 300 s; the distance threshold for the merge is 60 m, and the time threshold is 240 s. In the semantic extraction, the search radius is 200 m. The sensitivity of the parameters will be analyzed in Section 4.4.

4.2.3. Compared Methods

To the best of our knowledge, this paper presents the first attempt at characterizing suspicious behaviors simultaneously from historical behaviors, movement, and crowd patterns. However, some existing abnormal behavior detection methods can be extended for comparison. To identify the wandering behavior of elderly people, Vuong proposed an algorithm to divide the trajectories into random, lapping, pacing, and random patterns [27]. Moreover, a recent work used this algorithm to recognize lapping patterns as wandering behaviors for crime prevention [17]. In this work, the lapping pattern is defined as circuitous locomotion revisiting, which is similar to loitering around a public place in our article. Thus, we compared the loitering detection accuracy with this work. A novel method called θ_WD was proposed to detect multiple sharp changes in moving directions in travel traces [47]. Consequently, we compared the aimlessly wandering detection accuracy with this method. In addition, the local outlier factor (LOF) [48] is usually chosen to identify outliers. Therefore, we compared the accuracy of using LOF and DBSCAN in unusual route detection. Since we did not find a similar method to detect other suspicious behaviors, no comparison was performed for those behaviors.

4.3. Results and Accuracy Assessment

A total of 215 incidents of access to important areas, 130 loitering incidents, 136 incidents of aimlessly wandering, 104 frequent short stops, 592 unusual visit locations, 229 unusual routes, 220 unusual visit times, and 1 crowd gathering behavior were detected in the TucityLife dataset. The accuracies of detecting the access to important areas, loitering, aimlessly wandering, frequent short stops, and crowd gathering were verified and the results are listed in Table 1. History-based suspicious behaviors must be analyzed using long-term historical information, which are easily mislabeled in an activity log; therefore, the unusual visit location and visit time were not checked for accuracy. The accuracy of detecting the unusual routes was verified by manually comparing the regular route clusters with the unusual route; the precision is shown in Table 1. The recall rate of all the six suspicious behaviors is 93.5%, and the precision is 87.6%; the recall and precision of all the categories are relatively high. Comparative experiments (Figure 8) show that our method outperforms the compared methods as described in Section 4.2.3 in detecting all three suspicious behaviors. By analyzing the detected results, we found that the compared method cannot effectively identify discontinuous loitering behaviors in detecting loitering, such as leaving briefly. In the detection of aimlessly wandering and unusual route behaviors, the comparison methods were more sensitive to noise. The results show that the proposed method could detect suspicious behaviors that were hidden in the massive trajectory data, providing decision support for the early detection of safety incidents. Identifying the possible offenders and potential target places in advance will play an essential role in urban safety management

Table 1. Accuracies of the detection algorithms for the suspicious behaviors.

Type of Suspicious Behaviors	Number of Logged Behaviors	Number of Detected Behaviors	Number of Correctly Detected Behaviors	Recall	Precision	*F*1-Score
Access to important areas	215	215	205	0.953	0.953	0.953
Loitering	123	130	118	0.959	0.908	0.933
Aimlessly wandering	120	136	106	0.883	0.779	0.828
Frequent short stops	93	104	86	0.925	0.827	0.873
Unusual route	-	229	198	-	0.865	-
Crowd gathering	1	1	1	1.000	1.000	1.000
Total	-	815	714	0.935	0.876	0.905

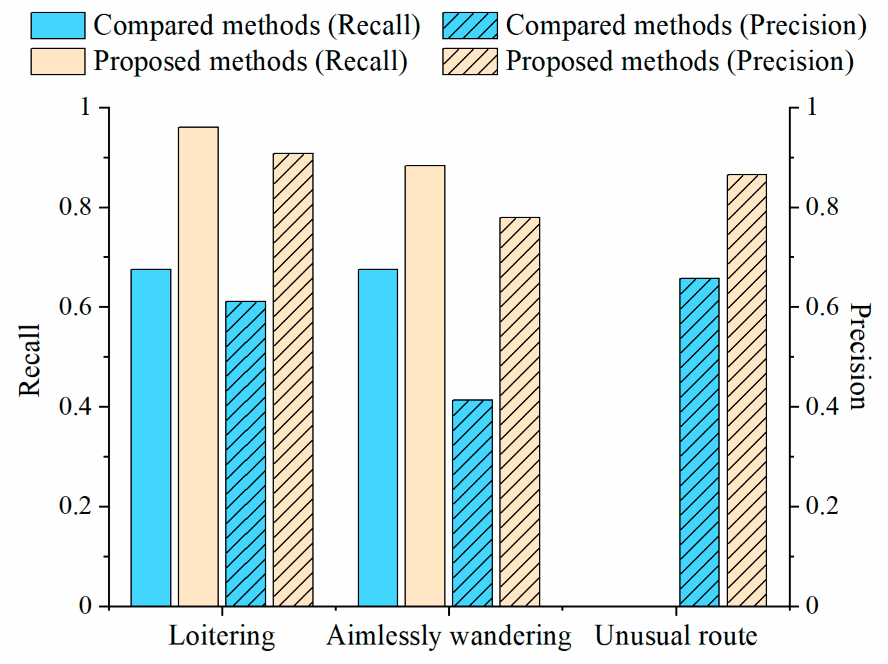

Figure 8. Comparison of the accuracy of different methods in suspicious behavior detection. The compared methods include the method that was proposed by Wu et al. [17] for loitering detection, θ_WD [47] for aimlessly wandering detection, and LOF [48] for unusual route detection.

4.4. Sensitivity Analysis of the Algorithm Parameters

Due to the complexity of suspicious behavior detection in real scenarios, some parameters should be determined according to the environment and application scenario. In this section, we compare the accuracies of varying parameters in aimlessly wandering and loitering detection (Figure 9). In aimlessly wandering detection, setting a small turning angle threshold and mean angle difference threshold may detect normal turns as suspicious ones. Moreover, when the conditions are too strict, some unusual behaviors may be missed by the algorithm. Thus, the turning angle threshold was set as 150°, and the mean angle difference threshold was set as 100° in the experiment. Likewise, in loitering detection, the grid size was set as 50 × 50 m, and the overlap ratio threshold was set as 0.5. Finally, we recommend that subsequent research uses the parameters as suggested.

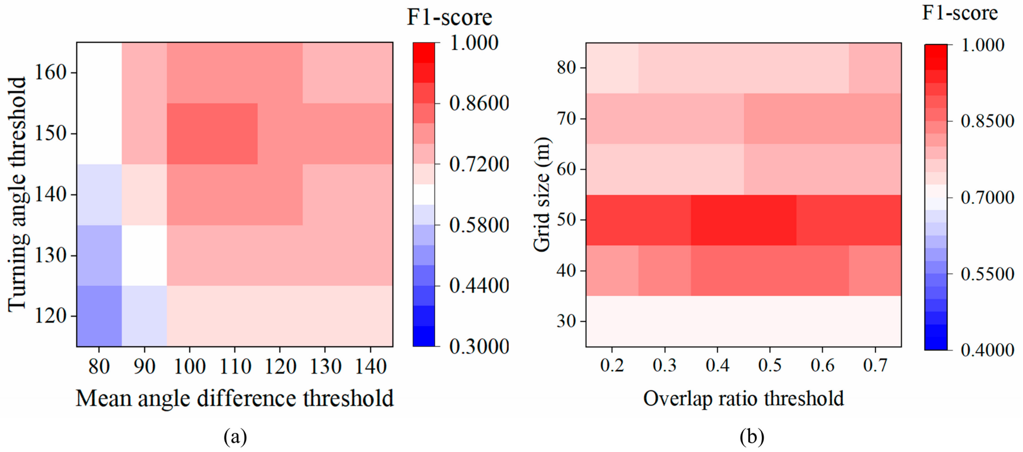

Figure 9. Accuracy of suspicious behavior detection with varying parameters from the TucityLife dataset. (**a**) aimlessly wandering; (**b**) loitering.

4.5. Typical Cases of the Suspicious Behaviors

The case studies for detecting suspicious behaviors are presented to demonstrate the effectiveness of the proposed method in identifying potential crimes.

Figure 10 shows examples of the trajectories of aimlessly wandering: (1) a person repeatedly meandering around the same street (Figure 10a–d); (2) a person changing direction multiple times to walk between multiple streets (Figure 10e–h); (3) a person changing direction multiple times while walking around an area (Figure 10i,j). These results are consistent with searching for suitable criminal targets and show that the proposed detection method can identify multiple types of aimlessly wandering behavior. Sometimes normal residents may also have a similar movement pattern, so when this pattern occurs, the police should comprehensively consider whether the person is a stranger in the neighborhood and whether the area is a high-risk area.

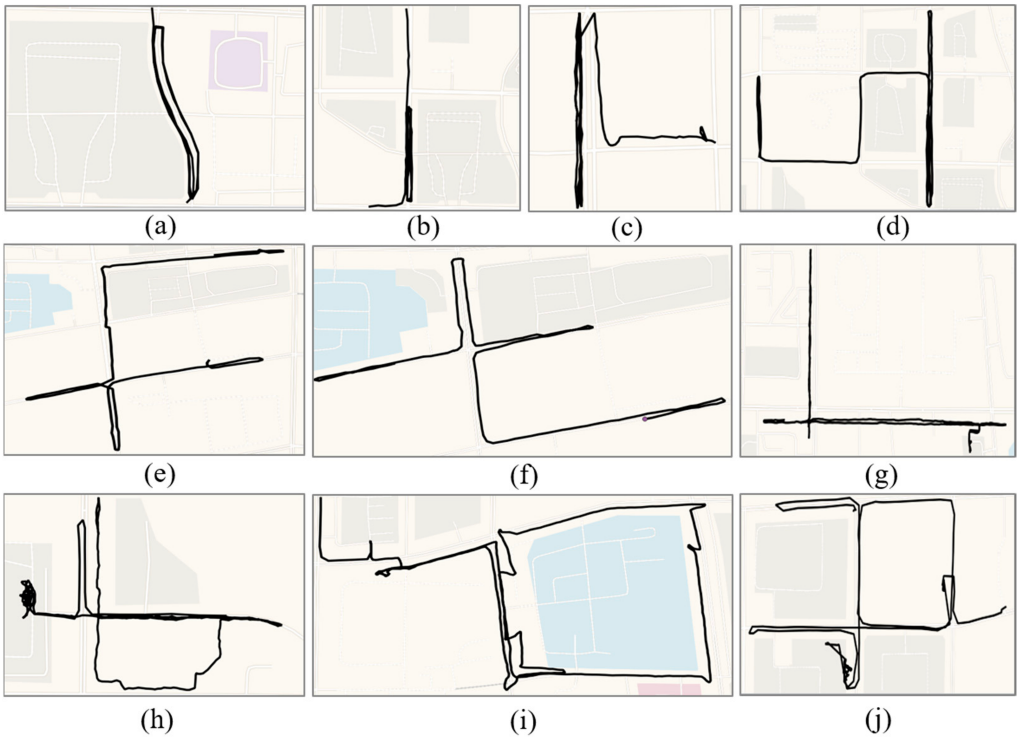

Figure 10. Examples of the trajectories of aimlessly wandering in the TucityLife dataset. Aimlessly wandering on the same road (**a**–**d**), on different roads (**e**–**h**), and in an area (**i**,**j**).

The examples of trajectories of loitering are shown in Figure 11. The circling behavior of a person while observing an area is often not continuous and may be accompanied by stops (Figure 11a) and departures (Figure 11c–f). In other words, it may be possible to visit an area once in the morning and again in the afternoon. A person may visit multiple areas at the same time when selecting a crime scene and revisit the intended area after a comparison (Figure 11g–i). The results demonstrate that the proposed loitering detection algorithm is robust and can identify the suspicious trajectory in these complex scenarios. A stranger loitering around schools, parks, or secluded areas that may become an offender should be noticed. The information can be used to help police to determine the potential crime scenes.

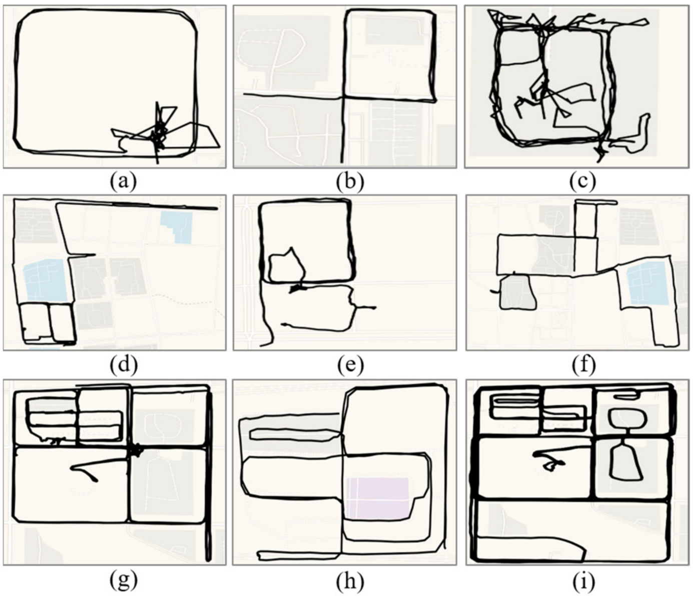

Figure 11. Examples of the trajectories of loitering that were extracted from the TucityLife dataset. (**a**) Loitering and stopping; (**b**) loitering; (**c**–**f**) loitering and leaving briefly; (**g**–**i**) multiple areas are examined simultaneously.

The trajectories of frequent short stops are illustrated in Figure 12. Several trajectories with multiple short stops occurring within a short time are shown. There are more short stops than normal trajectories, and aimless wandering and loitering may also occur. The stops that were detected by the proposed method show that the person observes the area and learns about the environment, corresponding to an offender observing the surrounding environment. This information can help police to detect suspicious behaviors before a crime occurs.

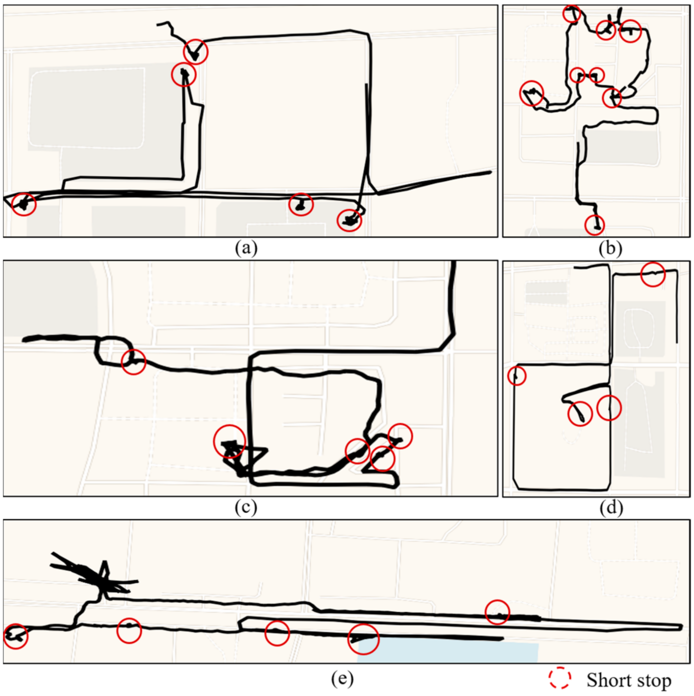

Figure 12. Examples of frequent short stops that were detected from the TucityLife dataset. (**a**–**e**) Several trajectories with multiple short stops (red circle) occurring within a short time.

The examples of detected unusual routes are shown in Figure 13. For routes with the same start and end points, several unusual routes are significantly different from the historical route, demonstrating that persons may have traveled to other locations or met with others on the route. If an unusual route passes through an important location, or it appears that other suspects are at the same location on the unusual route, the police should investigate it further.

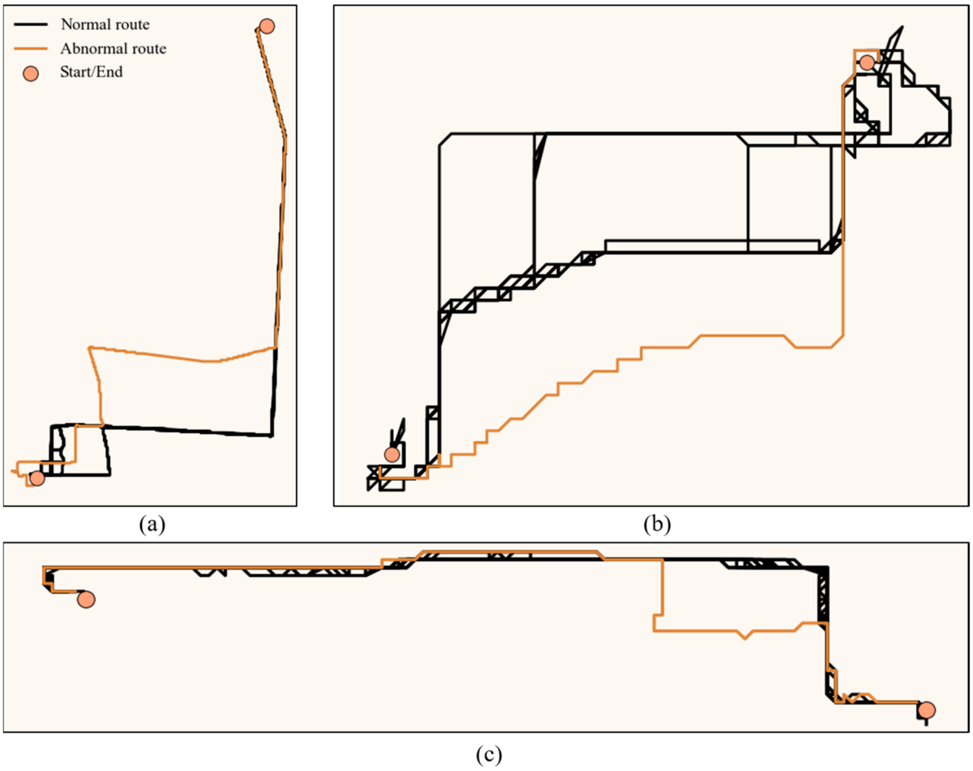

Figure 13. Examples of the unusual routes that were detected from the TucityLife dataset. (**a**–**c**) Several trajectories of unusual (brown) and normal (black) routes which are mapped on 50 m × 50 m grids.

5. Discussion

This work aims to help the police to recognize people's suspicious behaviors using personal trajectory data. In this way, resources can be deployed more accurately in place and time. Thus, we analyzed the characteristics of different behaviors and proposed the corresponding methods to capture the main features that were manifested in the trajectories. Someone might assume that criminals would be smart enough to vary where they spend their time, particularly if police use various information that may pinpoint the likelihood of a crime occurring in an area. Nevertheless, location preferences tend to be subtle and unconscious in many cases [13], even if humans are aware of a vast majority of their behaviors. In addition, the existing criminology theories were used to analyze what leads to these suspicious behaviors. It is important for law enforcement agencies to make adequate inferences from the data and to make sure that it is properly understood to develop fitting strategies. Thus, our method will be a good complement to the existing means, such as surveillance cameras.

The proposed method has the following advantages in suspicious behavior detection. First, to the best of the authors' knowledge, this is the first attempt at characterizing suspicious behaviors simultaneously from historical behaviors, movement, and crowd patterns. Moreover, we developed robust algorithms for detecting suspicious behaviors that were hidden in massive trajectory data by considering behavioral semantics and historical behavior, which will provide decision support for the early detection of safety incidents. Identifying the possible participants and potential places of a crime in advance will play an essential role in urban safety management. Finally, validation experiments on our trajectory dataset demonstrated the ability to detect suspicious behaviors. The case studies of detecting suspicious behaviors show that the proposed method can effectively identify the suspicious trajectory in these complex scenarios.

5.1. Practical Applications

It is expected that our method could become part of predictive policing. A growing body of research indicates that police departments are turning into the integration of data-driven decision-making to prevent crime [49]. Legal mandates for police to process data have expanded and allowed for more data collection, longer data retention periods, and data sharing [49]. On the one hand, the prevalent surveillance cameras and the widespread use of mobile phones provide data sources for trajectory data collection in public places. Several studies have discussed the right of the police to collect and use citizens' personal data for crime prevention [3,50], but this is not the focus of this article and, therefore, will not be discussed in detail. On the other hand, existing police systems can identify people in public places. Besides, offender-based modeling creates risk profiles for individuals, and geospatial modeling generates risk profiles for locations [51]. So our method can target high-risk people and locations, not all people. At the same time, our method does not use algorithms such as deep learning with high time complexity but a more efficient pattern mining method. For example, extracting all suspicious behaviors in a four-hour trajectory takes only a few seconds using a personal computer. Therefore, it can meet the requirements of the police system.

The proposed method can extract suspicious behaviors from trajectory data, but whether this behavior is likely to form a crime must be determined by incorporating multiple sources of information to reduce the number of false alarms. For example, the risks of frequent short stops in a park and a gas station are much different, and the risks of unusual visit locations of ordinary people and suspects are also different. Therefore, although our method can mine suspicious behavior patterns, it is necessary to assess the incident risk by considering information on people, time, location, and historical incidents in practical applications.

5.2. Limitations

Consequently, this work has some limitations in the following aspects. First, the characteristics of the input trajectories are crucial. For instance, since the movement patterns of the trajectories must be extracted, individual trajectories with a time interval of more than 30 s or spatial accuracy of more than 50 m are not suitable for analyzing the proposed suspicious behaviors. Similarly, trajectory datasets covering less than one week are not suitable for the proposed unusual route, visit location, and visit time detection. Second, due to the complexity of suspicious behavior detection in real scenarios, some parameters should be defined according to the environment and application scenarios. Although we have done sensitivity analysis on some parameters, further evaluation is still needed. Third, we identified eight suspicious behaviors that were suitable for trajectory detection from three aspects of trajectory analysis, but these are certainly not all. Fourth, due to the privacy of human trajectory data, we collected the trajectories of volunteers. Although we trained volunteers with the assistance of the police and tried to increase the randomness of the experiment, there still exist differences between our experiments and real crimes. Last, similar to the algorithms using video surveillance, our algorithm will fail to detect if experienced offenders try to avoid suspicious behaviors.

Future work will consider recruiting more volunteers to collect trajectory data and extend the verification in different cities. We will also consider using video surveillance data to obtain trajectories for multimodal suspicious behavior detection.

6. Conclusions

This work characterized several suspicious behaviors, including aimlessly wandering, frequent short stops, loitering, access to important areas, unusual routes, unusual visit time, unusual visit location, and crowd gathering, in perspective of unusual movement patterns, unusual behaviors, and unusual crowd patterns. Afterward, to capture the main features of each suspicious behavior, the corresponding algorithms were developed based on DBSCAN clustering, trajectory semantic annotation, movement pattern detection, and other methods. The proposed methods were verified with the TucityLife trajectory dataset that was collected in west China. The results of extracting the suspicious behaviors from this dataset using the proposed methods showed a recall of 93.5% and a precision of 87.6% for 815 detected suspicious behaviors, outperforming several other methods. The high accuracy of the proposed method indicates its effectiveness in helping police detect suspicious behaviors and identify the possible offenders and potential target places before it occurs. The case study showed that the proposed method was adaptable to complex practical situations and had high robustness and applicability. It is believed that the contributions and implementations of this study are valuable for preventing city crimes and supporting the appropriate allocation of police resources.

Author Contributions: Conceptualization, Junyi Cheng and Xianfeng Zhang; methodology, Junyi Cheng and Jie Huang; software, Junyi Cheng; validation, Junyi Cheng, Xiao Chen and Miao Ren; formal analysis, Xiao Chen and Miao Ren; data curation, Junyi Cheng, Jie Huang, Xiao Chen and Miao Ren; writing—original draft preparation, Junyi Cheng and Xianfeng Zhang; writing—review and editing, Junyi Cheng, Xianfeng Zhang, and Peng Luo; project administration, Xianfeng Zhang; funding acquisition, Xianfeng Zhang. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China, grant number 42171327 and the Xinjiang Production and Construction Corps, China, grant number 2017DB005.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data are available on request due to privacy restrictions.

Acknowledgments: We sincerely thank all the volunteers who participated in our data collection.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kalaiselvi Geetha, M.; Arunnehru, J.; Geetha, A. Early recognition of suspicious activity for crime prevention. In *Computer Vision: Concepts, Methodologies, Tools, and Applications*; IGI Global: Hershey, PA, USA, 2018; pp. 2139–2165.
2. Bartoli, G.; Fantacci, R.; Gei, F.; Marabissi, D.; Micciullo, L. A novel emergency management platform for smart public safety: A Novel Emergency Management Platform. *Int. J. Commun. Syst.* **2015**, *28*, 928–943. [CrossRef]
3. Meijer, A.; Wessels, M. Predictive Policing: Review of Benefits and Drawbacks. *Int. J. Public Adm.* **2019**, *42*, 1031–1039. [CrossRef]
4. GNR Safe Residence Program. Available online: https://www.safecommunitiesportugal.com/regional/algarve/gnr-safe-residence-program/ (accessed on 4 July 2022).
5. Capital Watch: What Is Suspicious Behavior? Available online: https://mpdc.dc.gov/whatssuspicious (accessed on 4 July 2022).
6. Pareek, P.; Thakkar, A. A survey on video-based Human Action Recognition: Recent updates, datasets, challenges, and applications. *Artif. Intell. Rev.* **2020**, *54*, 2259–2322. [CrossRef]
7. Chen, Z.; Cai, H.; Zhang, Y.; Wu, C.; Mu, M.; Li, Z.; Sotelo, M.A. A novel sparse representation model for pedestrian abnormal trajectory understanding. *Expert Syst. Appl.* **2019**, *138*, 112753. [CrossRef]
8. Clarke, R.V.; Cornish, D.B. Modeling Offenders' Decisions: A Framework for Research and Policy. *Crime Justice* **1985**, *6*, 147–185. [CrossRef]
9. Cohen, L.E.; Felson, M. Social Change and Crime Rate Trends: A Routine Activity Approach. *Am. Sociol. Rev.* **1979**, *44*, 588–608. [CrossRef]
10. Wortley, R. Situational precipitators of crime. In *Environmental Criminology and Crime Analysis*; Routledge: London, UK, 2016; pp. 81–105.
11. Vandeviver, C.; Neirynck, E.; Bernasco, W. The foraging perspective in criminology: A review of research literature. *Eur. J. Criminol* **2021**, 1–27. [CrossRef]

12. Bernasco, W.; Johnson, S.D.; Ruiter, S. Learning where to offend: Effects of past on future burglary locations. *Appl. Geogr.* **2015**, *60*, 120–129. [CrossRef]
13. McCue, C. *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*, 2nd ed.; Butterworth-Heinemann: Oxford, UK, 2015.
14. Yan, Z.; Chakraborty, D.; Parent, C.; Spaccapietra, S.; Aberer, K. Semantic trajectories: Mobility data computation and annotation. *ACM Trans. Intell. Syst. Technol. (TIST)* **2013**, *4*, 49. [CrossRef]
15. Mazimpaka, J.D.; Timpf, S. Trajectory data mining: A review of methods and applications. *J. Spat. Inf. Sci.* **2016**, *13*, 61–99. [CrossRef]
16. Shen, M.; Liu, D.-R.; Shann, S.-H. Outlier detection from vehicle trajectories to discover roaming events. *Inf. Sci.* **2015**, *294*, 242–254. [CrossRef]
17. Wu, H.; Tang, X.; Wang, Z.; Wang, N. Uncovering abnormal behavior patterns from mobility trajectories. *Sensors* **2021**, *21*, 3520. [CrossRef]
18. Meng, F.; Yuan, G.; Lv, S.; Wang, Z.; Xia, S. An overview on trajectory outlier detection. *Artif. Intell. Rev.* **2018**, *52*, 2437–2456. [CrossRef]
19. Belhadi, A.; Djenouri, Y.; Lin, J.C.-W. Comparative Study on Trajectory Outlier Detection Algorithms. In Proceedings of the 2019 International Conference on Data Mining Workshops (ICDMW), Beijing, China, 8–11 November 2019; pp. 415–423.
20. Yao, D.; Zhang, C.; Zhu, Z.; Huang, J.; Bi, J. Trajectory clustering via deep representation learning. In Proceedings of the 2017 International Joint Conference on Neural Networks (IJCNN), Anchorage, AK, USA, 14–19 May 2017; pp. 3880–3887.
21. Wang, Y.; Qin, K.; Chen, Y.; Zhao, P. Detecting anomalous trajectories and behavior patterns using hierarchical clustering from Taxi GPS Data. *ISPRS Int. J. Geo-Inf.* **2018**, *7*, 25. [CrossRef]
22. Shaikh, S.A.; Kitagawa, H. Efficient distance-based outlier detection on uncertain datasets of Gaussian distribution. *World Wide Web* **2013**, *17*, 511–538. [CrossRef]
23. Shi, H.; Xu, X.; Fan, Y.; Zhang, C.; Peng, Y. An Auto Encoder Network Based Method for Abnormal behavior detection. In Proceedings of the ACM International Conference Proceeding Series, Yokohama, Japan, 16–18 January 2021; pp. 243–251.
24. Ahmed, U.; Srivastava, G.; Djenouri, Y.; Lin, J.C.-W. Knowledge graph based trajectory outlier detection in sustainable smart cities. *Sustain. Cities Soc.* **2022**, *78*, 103580. [CrossRef]
25. Pang, G.; Shen, C.; Cao, L.; Hengel, A.V.D. Deep Learning for Anomaly Detection: A Review. *ACM Comput. Surv.* **2021**, *54*, 38. [CrossRef]
26. Shih, D.-H.; Shih, M.-H.; Yen, D.C.; Hsu, J.-H. Personal mobility pattern mining and anomaly detection in the GPS era. *Cartogr. Geogr. Inf. Sci.* **2016**, *43*, 55–67. [CrossRef]
27. Vuong, N.K.; Chan, S.; Lau, C.T. Automated detection of wandering patterns in people with dementia. *Gerontechnology* **2014**, *12*, 127–147. [CrossRef]
28. Long, Y.; Liu, X.; Zhou, J.; Chai, Y. Early birds, night owls, and tireless/recurring itinerants: An exploratory analysis of extreme transit behaviors in Beijing, China. *Habitat Int.* **2016**, *57*, 223–232. [CrossRef]
29. Carboni, E.M.; Bogorny, V. Inferring Drivers Behavior through Trajectory Analysis. In *Intelligent Systems'2014*; Springer International Publishing: Cham, Switzerland, 2015; Volume 322, pp. 837–848.
30. Lei, P.-R. A framework for anomaly detection in maritime trajectory behavior. *Knowl. Inf. Syst.* **2015**, *47*, 189–214. [CrossRef]
31. Rong, H.; Teixeira, A.P.; Guedes Soares, C. Data mining approach to shipping route characterization and anomaly detection based on AIS data. *Ocean Eng.* **2020**, *198*, 106936. [CrossRef]
32. Algase, D.L.; Moore, D.H.; Vandeweerd, C.; Gavin-Dreschnack, D.J. Mapping the maze of terms and definitions in dementia-related wandering. *Aging Ment. Health* **2007**, *11*, 686–698. [CrossRef] [PubMed]
33. Qianyin, J.; Guoming, L.; Jinwei, Y.; Xiying, L. A model based method of pedestrian abnormal behavior detection in traffic scene. In Proceedings of the 2015 IEEE First International Smart Cities Conference (ISC2), Guadalajara, Mexico, 25–28 October 2015; pp. 1–6.
34. Barragana, M.; Alvares, L.O.; Bogorny, V. Unusual behavior detection and object ranking from movement trajectories in target regions. *Int. J. Geogr. Inf. Sci.* **2017**, *31*, 364–386. [CrossRef]
35. Report Suspicious Activity | Safe Communities Portugal. Available online: https://www.safecommunitiesportugal.com/report-suspicious-activity/# (accessed on 8 August 2022).
36. What Is Suspicious Activity? Available online: https://www.cityofsanmateo.org/4361/What-is-Suspicious-Activity (accessed on 8 August 2022).
37. Reporting Suspicious Behaviour. Available online: https://www.suffolk.police.uk/sites/suffolk/files/reporting_suspicious_behaviour.pdf (accessed on 8 August 2022).
38. Brantingham, P.L.; Brantingham, P.J. situational crime-prevention in practice. *Can. J. Criminol.* **1990**, *32*, 17–40. [CrossRef]
39. Cornish, D.B.; Clarke, R.V. *The Reasoning Criminal: Rational Choice Perspectives on Offending*; Springer: Berlin, Germany; p. 1986.
40. Sander, J.; Ester, M.; Kriegel, H.-P.; Xu, X. Density-based clustering in spatial databases: The algorithm gdbscan and its applications. *Data Min. knowl. Discov.* **1998**, *2*, 169–194. [CrossRef]
41. Kinney, J.B.; Brantingham, P.L.; Wuschke, K.; Kirk, M.G.; Brantingham, P.J. Crime Attractors, Generators and Detractors: Land Use and Urban Crime Opportunities. *Built Environ.* **2008**, *34*, 62–74. [CrossRef]
42. Felson, M.; Clarke, R.V. *Opportunity Makes the Thief: Practical Theory for Crime Prevention*; Police Research Series; Research, Development and Statistics Directorate: London, UK, 1998.

43. Waterman, M.S. Time warps, string edits, and macromolecules: The theory and practice of sequence comparison. *Math. Biosci.* **1985**, *76*, 243–244. [CrossRef]
44. Brantingham, P.L.; Brantingham, P.J. Notes on the geometry of crime. In *Environmental Criminology*; Sage Publications: Beverly Hills, CA, USA, 1982; pp. 27–54.
45. Cheng, J.; Zhang, X.; Luo, P.; Huang, J.; Huang, J. An unsupervised approach for semantic place annotation of trajectories based on the prior probability. *Inf. Sci.* **2022**, *607*, 1311–1327. [CrossRef]
46. Zheng, K.; Zheng, Y.; Yuan, N.J.; Shang, S.; Zhou, X. Online Discovery of Gathering Patterns over Trajectories. *IEEE Trans. Knowl. Data Eng.* **2014**, *26*, 1974–1988. [CrossRef]
47. Lin, Q.; Zhang, D.; Huang, X.; Ni, H.; Zhou, X. Detecting wandering behavior based on GPS traces for elders with dementia. In Proceedings of the 12th International Conference on Control Automation Robotics & Vision (ICARCV), Guangzhou, China, 5–7 December 2012; pp. 672–677.
48. Breuniq, M.M.; Kriegel, H.-P.; Ng, R.T.; Sander, J. LOF: Identifying density-based local outliers. *SIGMOD Rec.* **2000**, *29*, 93–104. [CrossRef]
49. Jansen, F. Data driven policing in the context of Europe. Data Justice Lab. 2018. Available online: https://datajusticeproject.net/wp-content/uploads/sites/30/2019/05/Report-Data-Driven-Policing-EU.pdf (accessed on 8 August 2022).
50. Kutnowski, M. The ethical dangers and merits of predictive policing. *J. Commun. Saf. Well-Being* **2017**, *2*, 13. [CrossRef]
51. Shapiro, A. Reform predictive policing. *Nature* **2017**, *541*, 458–460. [CrossRef]