Effective Evaluation on Urban road Collision Risk based on VANET

Symphorien karl Yoki Donzia\textsuperscript{1)}, Haeng-Kon Kim\textsuperscript{2)}

Abstract

When maneuvering a vehicle on two-lane roads in the same lane direction, the possible risk is that the vehicle can exceed other vehicles. However, little attention has been paid to issuing a warning about unsafe driving behavior, particularly in the case where two vehicles are likely to collide. Our work is about to reduce the crime of traffic accidents in our daily lives, especially for dangerous driving behavior that leads to vehicle crash. This study provides a framework for estimating the collision risk using an RGB-D camera. We define security requirements for the VANET, which is an emerging vehicle network technology that provides safe driving warning service based on road situation information through inter-vehicle connection environments and the VANET attacker model. After using the two proposed methods, we found that our framework is effective to estimate collision risks. The trajectory prediction error is very low, which is unlikely to have a significant impact. and the proposed framework is effective in estimating the risk of collision.

Keywords: Collision risk, RGB-D Camera, ARIMA, VANET Security and VANET attacker model.

요 약

동일한 차선 방향으로 2 차선 도로에서 차량을 조작 할 때 차량이 다른 차량을 초과 할 수 있는 위험이 있다. 기존의 연구는 두 대의 차량이 충돌 할 가능성이 있는 경우 안전하지 않은 주행 동작에 대한 경고를 발행하는데 주의를 기울이지 않았다. 본 연구는 차량 충돌로 이어지는 위험한 운전 행동을 위해 일상생활에서 교통 고의 범죄를 줄이려고 한다. 이 연구는 RGB-D 카메라를 사용하여 충돌 위험을 추정하기 위한 프레임 워크를 제공한다. 차량 간 연결 환경과 VANET 공격자 모델을 통해 도로 상황 정보를 기반으로 안전 운전 경고 서비스를 제공하는 신종 차량 네트워크 기술인 VANET에 대한 보안 요구 사항을 정의한다. 실험은 실제 차량의 데이터에 대해 수행된다. 연구결과는 도로 내에서 위치 및 속도 추정의 정확성을 보장 할 수 있으며 궤도 예측 오류는 매우 적으며 대부분의 상황에서 충돌 확률을 계산하는 데 큰 영향을 미치지는 않는다. 제안 된 두 가지 방법을 사용한 후 프레임 워크가 충돌 위험을 추정하는 데 효과적이라는 것을 알았다. 궤도 예측 오류는 매우 낮아서 큰 영향을 미치지는 않다.
1. Introduction

The VANET (Vehicular Ad-hoc Network) is the emerging vehicle network technology. This can provide a safe driving warning service, such as a collision warning, traffic information, emergency service, etc. according to the information on the situation of the road thanks to the connection between the vehicles. However, since the data packet which includes the node identification information and the location information includes the privacy information[1] in the data packet exchanged between the vehicles, there is a security problem on the part of the attacker who abuses this information. When drivers focus on traffic conditions and respect the rules of the road, which are Rules of the road, of course, to save lives and avoid injuries on our roads, such as wearing a seat belt, using restraints for children, never drive intoxicated obey the rules live. But here, in this work, this system is ignored to focus on the Dept. of Computer Science, rules of the road respected, since the incidence of traffic accidents increases according to these traffic conditions. Therefore, to improve efficiency, the types of sensors installed on / under the road detect the types of violations, such as driving at red speed. First we present that the cameras were originally introduced to reduce the incidence and severity of intersection accidents. Although there have been evaluations of the effectiveness of the Red Light camera program to reduce collisions at intersections. And the car’s radar installed in the vehicle is the most common of the sensors to guarantee the safety distance. There are two limitations to punishing the behavior of ignoring One of the main challenges in the design of an ad hoc vehicular network is the development of a dynamic routing protocol that can help disseminate information from one node (vehicle) to another. VANET routing is different from traditional MANET routing due to the highly dynamic and constantly evolving topologies in the former. Few protocols previously designed for the MANET environment have been tested in VANET. The challenge however The question is how to reduce the delay associated with the passage of information from one node to another. Overcoming these obstacles in MANET protocols can help implement real-time applications for the VANET environment. Other implications such as the reduction of overhead control costs should also be carefully considered. When monitoring the dynamic characteristics of VANET (as noted above)[11], The routing protocol must be able to withstand the unexpected and dynamic nature of the vehicle network topology. Perhaps the most difficult task of VANET routing is to find and maintain
optimal communication channels in the desired environments. Most routing protocols in VANET are closely related to the topology used in the network architecture, and performance varies every time there is a change in the network topology. The rest of this paper is organized as follows: the communication technologies and methods available to reduce VANET journey time are discussed in the following section, and the scope of this study and the details of its operational processes are explained in the section 3. Section 4 focuses on the performance of the evaluation system. A conclusion is presented in section 5.

2. Related Work

The term VANET was originally adopted to reflect the temporary nature of these very dynamic networks. But the temporary term Networks are widely associated with research on unicast routing, and discussions are currently underway among the pioneers in this field on the redefinition of the ad hoc network by redefining the VANET abbreviations. This discussion has not yet reached a consensus, so we will continue to mention VANET as inter-vehicle and inter-vehicle communications based on wireless LAN technology. The quantitative assessment of added value is difficult because of the human factors involved. Since such a prognosis must take into account feedback loops (for example, how humans react to these prognoses), road traffic has proven to be a very difficult task. Vehicles for safety related applications The Safety Communications (VSC) consortium has identified eight potential applications[12]. traffic light violation warning, curved speed warning, electronic emergency brake light, collision pre-detection, forward collision warning, left turn assist, lane departure warning and assistant sign stop motion. Four of them The application requires inter-vehicle communication, while the other four require communication with the road infrastructure. The derived technical requirements show the importance of broadcast communication at a hop (i.e. any vehicle that can simply send a packet and receive it directly is considered a neighbor at a hop). Periodic. Event messages are sent when a critical situation is detected. Periodic messages inform surrounding vehicles of their condition in advance.

Several studies have focused on real-time route planning with the help of VANET. A distributed route planning method has been advanced to alleviate the problem of congestion through the use of real-time data obtained from VANET, with increasing traffic flow. As for fuel economy in vehicles, it has designed a navigation system that helps drivers get away from congested roads. However, lack of coordination and selfish behavior of drivers could lead to
greater congestion when individual user manual patterns are implemented. Hence the need to jointly plan the routes of groups of vehicles to balance the traffic network. The planning of multiple vehicle routes is considered in[10]. However, this work does not pay attention to drivers’ preferences, nor to the average travel cost. Nor is it explained how VANET communications can affect the route planning algorithm.

VANET V2R and V2V communication methods have the ability to make real-time message delivery much faster, more efficient and more profitable than existing methods, even over shorter distances and thick networks. More importantly, the collection and distribution of data can be improved by the RSUs in the VANETs, which allows a coordinated planning of the routes to be carried out for groups of vehicles. In order to improve the quality of the experience, the multimedia transmission application can be compatible with a vehicle network based on the multimedia system, which could still be the victim of significant transmission delays[13].

3. Framework

As shown in FIG. 1, the system data is obtained from two types of cameras: one is the ordinary RGB camera installed on the road that faces the direction of movement of the vehicles to identify the identification of the vehicle using the registration recognition technique; the other is the RGB-D camera installed on the side of the road and orthogonal to the direction of the road[2]. The main risk calculation process consists of four steps: recognition of vehicle identification, segmentation of the vehicle, evaluation of the vehicle’s condition, analysis of dangerous behavior.

[Figure 1] The framework of RGB-D Camera collision risk value for urban road Farm
The main process of risk calculation includes four steps[3-4]: 1) recognition of vehicle identification; 2) segmentation of the vehicle; 3) Evaluation of the condition of the vehicle; 4) Analyze of dangerous behavior. 1) Recognition of vehicle identification; The license plates are the important identity of vehicles to send warning information and are unique in most situations. The technique of license plate recognition using video data, which is an important subclass of acquisition, is still at the forefront of research in the field of image processing. Given the real-time requirements, some excellent algorithms have been transplanted to cameras built into the camera. 2) segmentation of the vehicle; Objective of segmentation of the vehicle when separating the objective vehicle from the fund and other vehicles. This simplifies and transforms the representation of an image into something easier to analyze. Specifically, if the difference in depth between two pixels is less than a certain distance (define 20 cm in the experiment), they receive the same label. 3) Evaluation of the condition of the vehicle; Once the vehicles have been extracted from the original image by RGB depth and color information, the suit of the movement of a vehicle during the area covered by the camera is esteem. This trajectory is a set of discrete points, and each point is constituted from the position (x, y) and of the instantaneous speed (v) of the vehicle at that moment, which can be expressed by (x, y, v). 4) Analyze of dangerous behavior; We consider that it has mainly two types of danger, the danger in the short term, which means that collision may occur in a short time and present the highest risk value; Another is the long-term danger, in which the possibility of collision must be estimated on the basis of the expected attractiveness of the vehicle from the current data.

3.1 Dangerous Behavior Analysis

The method refers to the collision risk that will be calculated in two different situations[10]. The first is the emergency risk, which means that the collision can occur less than 1 s. In this situation, the method must be simple and must be processed in real time. The second is the recommendation risk, where the collision may occur a little later, but still within 3.5 s. In the network of urban roads, the average speed of traffic is about 30 km / h when it is in the central part of a road, so the vehicle will circulate about 30 minutes and 3.5 seconds. For this system, it is not necessary to calculate the risk when the vehicle has rolled until the vehicle leaves the camera during the 30 m. Therefore, VANET will be used to secure the requirement by protocol resolution (ARAN and Ariadne).

The challenges are the dynamic network topology based on vehicle mobility and the environmental impact on radio propagation. The latter must take into account the fact that the
low heights of the antenna and the attenuation / reflection of all the movable metallic bodies of the vehicle create unfavorable conditions for the radio channels. Together, the VANETs must operate properly under a wide range of conditions, including light and heavy traffic. There is a strong need for adaptive transmit power and speed control to achieve a reasonable degree of reliable communication and low latency. It is also difficult to balance security and privacy needs. On the one hand, recipients want to ensure that they can rely on the source of information. On the other hand, the availability of such trust could contradict the confidentiality requirements of a sender.

3.2 Emergency Vehicle Accident and Role of VANET

The number of patients with chronic diseases is increasing day by day. These patients are permanently readmitted to hospitals and health centers, which require significant medical care. To effectively treat patients, intelligent health systems are continuously improving. The applications Ad hoc emerging vehicle networks (VANET) can be used to provide improved communication capabilities in the ITS system to obtain real-time traffic information in a more efficient and cost-effective manner.

VANETs support the vehicle-to-road unit (V2R) and vehicle-to-vehicle communications, so real-time updates can be transmitted to and from vehicles and route units (MSW). This real-time information to be collected can be used accordingly for route planning on individual
vehicles, traffic flow management on motorways and vehicle location. Second, once traffic information is obtained in real time, several algorithms can be devised to discover the most efficient routes that individual vehicles can take. However, if route planning is implemented in an uncoordinated way, this could generate even more congestion. Although most of the available routes that include global algorithms pay attention to network improvements, they generally ignore driver preferences, such as distances and journey times. This is important, especially if reprogramming decisions are seen as a consequence of the need to avoid traffic congestion and traffic balancing rather than finding optimal routes. Therefore, some drivers may prefer to take longer routes, although this may involve higher costs[13]. Therefore, the design of the algorithms should be done in a way that takes into account both the reduction in the average cost of vehicle operation and network traffic.

4. Emergency Vehicle Accident and Role of VANET

4.1 Vehicle State Evaluation

In this section, the purpose of assessing the condition of the vehicle is to determine the vehicle’s path, which mainly includes position and speed. And it resumes in two parts: Calculation of the position and estimation of the speed. In the section, the purpose of assessing the condition of the vehicle is to determine the vehicle’s path, which mainly includes position and speed. And it resumes in two parts: Calculation of the position and estimation of the speed.

4.2 VANET Attacker Model

The VANET attackers[5-6] attack VANET’s security requirements. The first model of an attacker is camouflage. The attacking node is dragged to the credentials of another authenticated node. Attacking nodes are attacked to use network resources that are not available under normal circumstances or to interfere with the normal operation of the network. The second is a denial of service attack. An attacker can prevent a victim node from exchanging data with another node. The third is a repeat attack. The attacker attacks copying to another user of RSU (Road Side Unit) and continues transmitting the packet already transmitted. This threatens the authentication of the VANET security system. Finally, there is a routing attack in which the attacker intentionally deletes the data packet or interrupts the routing process of the network. Black hole attack, wormhole attack, and gray hole attack.
4.3 Efficient privacy and New Propagation

We estimated absolutely vehicle info, Occupants info and Accident info for emergency info elements. Furtherly new emergency rescue will controlled and evaluated in two part; before accident and after accident as indicated in [Table 1].

![Figure 3] Information to be transmitted in future emergency service

<table>
<thead>
<tr>
<th>Source ID</th>
<th>Vehicle and Occupants Info</th>
<th>Accident Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed, direction, Velocity</td>
<td>Speed, direction, Velocity</td>
<td>Location and time of day</td>
</tr>
<tr>
<td>Injuries information</td>
<td>Injuries information</td>
<td>Persons in the car</td>
</tr>
<tr>
<td>Location and time of day</td>
<td>Location and time of day</td>
<td>Driver and his conversation</td>
</tr>
<tr>
<td>Persons in the car</td>
<td>Persons in the car</td>
<td>Severity of damage</td>
</tr>
</tbody>
</table>

[Table 1] Future Emergency rescue

Our system is working through car black box technology consist sending after the crash such as snapshot of car speed, direction, acceleration, record of an voice made by driver prior to impact, record of weather condition and record of time of day.

Concerns about the data are generated due to the effectiveness and reliability of the information collection and exchange system between municipalities. Certainty For example, a caller may incorrectly mark an observation to gain an advantage (for example, vehicle V incorrectly informs that there is a traffic jam on the desired road R, so that other people avoid R and have a trip without agglomeration to V in R). It is recommended). More malicious reporters may pretend to be other vehicles or road infrastructure, causing security risks. The vehicle reduces this threat by creating a network that ignores and at least ignores the information of people who do not trust. Reliable communication generally implies Which two properties are satisfied
• The sender is determined to be a reliable source.
• The message content of the sender does not change during transmission.

You can find a general description of VANET safety in the Vehicle Safety Communications Application Project of the Current Association of Crash Prevention Metrics (CAMP), Vehicle Infrastructure Integration Project (VII), SeVeCom Project, Integrated car safety conference (ESCAR), others. IEEE standard test 1609.2 (formerly P1556) also covers VANET security services. The main challenge of VANET security is to provide caller authentication in broadcast communication scenarios. The so-called transmission authentication is difficult because the vehicle has not been fulfilled before and the loss of the link layer can affect several transmission receivers of different severity.

4.4 Evolution Experimental

The total number of test times is 10 × 16 = 160. A speed radar was adopted to measure the speed of the test vehicle and the result is considered to be the true value in the performance evaluation. This estimated value is applied to estimate the test error, which is defined in Figure.

The trajectory prediction performance is not easy to detect in a limited time when few camera numbers are used. The result of the vehicle trajectory prediction is illustrated in [Figure 4]. These experiments demonstrated the effectiveness of the position and speed estimation method.

![Figure 4] Trajectory prediction
5. Resolution of VANET security issue

First resolution is ARAN which[7] an attack from a neighboring node or a node of a third party Detects and Protects Behavior ARAN uses AODV-based protocols and uses shared-key cryptography to prevent counterfeit attacks. This technique requires an authentication server and all nodes must share a key. Also use a timestamp to make sure all the information is up to date. The operation of ARAN[8] is as follows. First, the originating node sends a route discovery packet (RDP) to the neighboring node, and each node records a list of nodes that received the message. Each node that receives a message sends it back to its neighbors with its own certificate and signature. When the message arrives at the destination node, the destination node unites the REP message to the source node where the message was received. All REP messages are signed by the sender node and verified by the next hop node. Here, no other node than the destination node can send a response to the RDP. In ARAN, each node has a routing table for its network neighbors. When data is received from a node that has not been received, an EPF error message is generated and the route is returned. Because the route authentication process is performed by leap-by-hop and signature and authentication are added each time, replay attacks and false attacks that threaten the authentication requirements can be resolved.

The second resolution is Ariadne; Ariadne[9] helps prevent many types of DoS attacks. Ariadne is based on the Dynamic Source Routing (DSR) protocol. This mainly involves the search and management of routes. Therefore, when there is no cached route from the source node to the destination node, the node itself searches for the source route to the destination node. In Ariadne, the source node and the destination node share two keys and the relative addresses are specified. To authenticate the route, the originating node sends a message containing unique data, such as a timestamp, uses it to calculate the message authentication code (MAC) and sends it to the destination node. In addition to MAC, digital signatures or TESLA are used for data authentication and routing.

6. Conclusion

In our work, RGB-D camera-based framework to estimate the risk of vehicle collision consists of four parts and that is effective to estimate the risk of collision. In this paper, we discuss also security issues in the VANET environment and the research being done to address these
security issues. We proposed an accident management system which employs cellular systems of the public transportation systems and VANETs to make efficient real-time communication between vehicles possible. Authentication, validity, consistency, the immutability of data, etc. There was a security requirement that had to be guaranteed in a special wireless communication environment called VANET. And replicate attacks that threaten the immutability and confidentiality of data. Two studies proposed as alternatives to these attacks were presented. ARAN uses cryptographic techniques against repetitive attacks and camouflage attacks. In the case of Ariadne, symmetric cryptography and MAC have been proposed as alternatives to DoS attacks, routing attacks, and repeated attacks. If a VANET that offers a safe driving service cannot defend against such an attack, a very deadly accident can occur.
References


