Enhancing Service Quality and Reliability in Intelligent Traffic System

Abdullahi Al Kafee Chowdhury

A dissertation submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy

School of Science, Engineering and Information Technology
Federation University, Australia

16 January 2020

Except where otherwise indicated, this thesis is my own original work and has not been submitted for any other degree.

Abdullahi Al Kafee Chowdhury

16 January 2020

Dedicated to my parents and sister for their love, encouragement and support while I was far away from home during my PhD program.

Dedicated to my wife and son for their patience, love and support over the years that helped me to complete this dissertation.

Acknowledgements

Praise be to Allah, the most gracious, the most merciful, who has blessed me with the intellect, courage, strength, energy, and patience to complete this thesis successfully. I would like to express my profound gratitude and gratefulness to my supervisors Dr. Gour Karmakar and Prof Joarder Kamruzzaman for their tireless efforts in ensuring the quality of my research and scholarly guidance from beginning to the end of the research work. Without their constant inspiration, encouragement, valuable suggestions, endless patience, energetic supervision, constructive criticism, this research would not have been completed.

I am also thankful to all staff and postgraduate students at Gippsland Campus for their cordial support and inspiration. Discussions with them have enriched my conception and knowledge about this research work.

I would like to thank Federation University Australia for giving me the opportunity to carry out my research in an excellent environment. I also thank Federation University and Gippsland Campus for providing me with the necessary resources, materials, financial supports, and scholarships.

My heartiest love and gratitude to my parents Mr. Nazir Ahamed Chowdhury and Begum Lutfunnahar Chowdhury for their endless love, inspiration, and sacrifice and for always keeping me in their prayers. My sincere thanks go to my only sister Dr Chowdhury Nurunnahar who has been a source of joy and inspiration. I am also thankful for my parents-in-law MA Aziz and Mrs. Lutfun Nahar Aziz, and my only brother-in-law MD Morinozzaman Khan for their inspiring words, kind support, and encouragement. I also thank my friends for their moral support and inspiration.

Last but not least, my deepest gratitude goes to my wife Samima Chowdhury and son Adyan Chowdhury for their love, patience, care, and understanding during my candidature.

Abdullahi Al Kafee Chowdhury was supported by an Australian Government Research Training Program (RTP) Fee-Offset Scholarship through Federation University Australia.

Abstract

Intelligent Traffic Systems (ITS) can manage on-road traffic efficiently based on real-time traffic conditions, reduce delay at the intersections, and maintain the safety of the road users. However, emergency vehicles still struggle to meet their targeted response time, and an ITS is vulnerable to various types of attacks, including cyberattacks. To address these issues, in this dissertation, we introduce three techniques that enhance the service quality and reliability of an ITS.

First, an innovative Emergency Vehicle Priority System (EVPS) is presented to assist an Emergency Vehicle (EV) in attending the incident place faster. Our proposed EVPS determines the proper priority codes of EV based on the type of incidents. After priority code generation, EVPS selects the number of traffic signals needed to be turned green considering the impact on other vehicles gathered in the relevant adjacent cells.

Second, for improving reliability, an Intrusion Detection System for traffic signals is proposed for the first time, which leverages traffic and signal characteristics such as the flow rate, vehicle speed, and signal phase time. Shannon's entropy is used to calculate the uncertainty associated with the likelihood of particular evidence and Dempster-Shafer (DS) decision theory is used to fuse the evidential information.

Finally, to improve the reliability of a future ITS, we introduce a model that assesses the trust level of four major On-Board Units (OBU) of a self-driving car along with Global Positioning System (GPS) data and safety messages. Both subjective logic (DS theory) and CertainLogic are used to develop the theoretical underpinning for estimating the trust value of a self-driving car by fusing the trust value of four OBU components, GPS data and safety messages.

For evaluation and validation purposes, a popular and widely used traffic simulation package, namely Simulation of Urban Mobility (SUMO), is used to develop the simulation platform using a real map of Melbourne CBD. The relevant historical real data taken from the VicRoads website were used to inject the traffic flow and density in the simulation model. We evaluated the

performance of our proposed techniques considering different traffic and signal characteristics such as occupancy rate, flow rate, phase time, and vehicle speed under many realistic scenarios. The simulation result shows the potential efficacy of our proposed techniques for all selected scenarios.

Contents

List of Figures

List of Tables

Acronyms

AU	Application Unit
ACC	Adaptive Cruise Control
ATCSs	Adaptive Traffic Control Systems
ATS	Adaptive Traffic Signal
CACC	Cooperative Adaptive Cruise Control
cITS	Cooperative Intelligent Transport System
DSRC	Dedicated Short Range Communication
ECU	Electronic Control Unit
EVPS	Emergency Vehicle Priority System
GNSS	Global Navigation Satellite System
GSM	Global System for Mobile communication
I2I	Infrastructure to Infrastructure
I2X	Infrastructure to Everything
IMS	Incident Management System
ITLs	Intelligence Traffic Lights
ITS	Intelligent Traffic Systems
IVWS	Intersection Violation Warning System
Lidar	Light Detection and Ranging
MaaS	Mobility as a Service
MANET	Mobile ad-hoc Networks

Acronyms

OBU	On-Board Units
QoS	Quality of Service
RFID	Radio Frequency Identification
RSU	Road Side Unit
SCATS	Sydney Coordinated Adaptive Traffic System
STLC	eSmart Traffic Light Control system
SUMO	Simulation of Urban Mobility
TMS	Traffic Management System
TPM	Trusted Platform Module
TRIP	Trust and Reputation Infrastructure based Proposal
USDOT	US Department of Transportation
V2I	Vehicle to Infrastructure
V2P	Vehicle to Pedestrian
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
VANET	Vehicular ad-hoc Network
VD	Vehicle Detector

Nomenclature

$\aleph_j$	Number of vehicles passing through the signal j
$\amalg N$	False-Negative
$\amalg P$	False-Positive value
$\breve{n}_m$	Number of cars in cell m
χ	Number of successful outcome of observation
$\delta(g)$	Length of cell g
μ	Mean value
$\neg N$	Proposition being abnormal
Φ	Number of successful outcome of observation
ρ	Density
σ	Standard deviation
ϑ	Average Speed
bel	Belief function DS theory
C	Capacity of cell
c	Certainty in CertainLogic
$E(t)$	Observed event at time t
$E_w(t)$	Observed event of w at time t

$E_F(t)$ Observed event of flow rate at time t

$E_P(t)$ Observed event of phase time at time t

$E_S(t)$ Observed event of vehicle speed at time t

F Flow Rate in Chapter 4

f Initial expectation in CertainLogic

I Number of Interventions

j Signal number

k Number of observed cell adjacent (both in left- and right-hand side) to j^{th} signal

l_j Length of the cells

m_{jw} probabilistic value of a mass function for w^{th} event ($E_w(t)$) in j_{th} intersection

N Proposition being normal

$N \wedge \neg N$ Null hypothesis

$N \vee \neg N$ Proposition being uncertain

n_s #signals btw an EV and incident spot

O Occupancy rate of the cell

P Phase Time in Chapter 4

p State of the phase

pl Plausibility

q Flow rate

R ID of a sensor

S Vehicle Speed in Chapter 4

S_j	Average space headway
t	Average Rating in CertainLogic
T_j^e	EV travel time from j^{th} cell to incident place
T_m	Time headway of cell m
TN	True-Negative value
TP	True-Positive value
T_j^c	Average clearance time of j^{th} signal
w	Different observation
z	z value

Introduction

Over the past few decades, the number of vehicles has significantly increased, which has resulted in populated roads. With the ever-increasing population and vehicles in urban areas, traffic congestion is becoming one of the major as well as challenging issues in big cities around the world. This massive traffic load has significantly increased road accidents, which has consequently raised injury and death rates worldwide. Besides, traffic congestion not only delays the journey but also brings detrimental impacts on the environment by polluting air, the economy by wasting working hours and fuel, and traveler's personal life by increasing stress level [1]. Traffic signals play an essential role in managing traffic congestion. The idea of developing traffic signals began in the 1800s. The first gas-lit traffic lights were installed outside the Houses of Parliament in London on December 10, 1868. In 1914, the first electric traffic lights were installed in the United States of America. With the invention of computers, traffic lights started to become computerized in the 1960s. These digital signals were using static and pre-defined phase times. Traffic signals during that period were standalone and not connected to the central traffic controller. The phase times were controlled by an electronic circuit board installed inside the traffic signal posts.

The continuous congestion level increase on public roads during peak time is a critical problem in most countries and acute in many cities. The growing congestion is becoming a significant concern to transportation specialists and decision-makers. This is why congestion control is regarded as the heart of traffic management, which ensures that users will have their desired quality of service. It is challenging to control congestion

when traffic conditions cannot be predicted in advance. The traffic-light-sequence is still a predefined recurring feature (static) of most current traffic lights systems.

The recurrent congestion generated by the excess road occupancy demand is a part of the traffic management problem. Congestion is also caused by irregular occurrences, such as traffic incidents, vehicle disablement, and spilled loads and hazardous materials. An incident can be an occurrence that affects roadway capacity [2]; especially severe are incidents on high-speed highways. Over half of the nonrecurring traffic delay in urban areas and almost 100% in rural areas are attributed to incidents. The likelihood of secondary incidents increases with the amount of time it takes to clear the initial incident, stressing the need for incident clearance. Traffic flow dynamics are highly useful in estimating the travel time of vehicles to predict traffic congestion. The effect of delay on traffic flow dynamics has been investigated both analytically and numerically in traffic flow literature using various traffic models [3] [4] [5]. The general conclusion from these studies is that increasing delay destabilizes traffic flow. The static traffic light systems, surveillance, and control are not adequately efficient in terms of performance, cost, maintenance, and support. To manage the traffic congestion efficiently, decrease the impact of delay due to traffic congestion, and manage incidents effectively, ITS was introduced.

ITS is the future direction of the smart transportation system. ITS have been developed since the beginning of the 1970s. In the last decades, ITS has emerged as an efficient way to improve the performance of vehicle flow on the roads. The goal of ITS is to provide comfortable driving, road safety, and near-real-time distribution of updated information about the traffic condition.

The success of ITS largely depends on the platform used to access, collect, and process accurate traffic data. Many ITSs have been developed that can integrate a broad range of systems, including sensing, communication, information dissemination, and traffic control. Vehicle detection tasks in ITS include counting the number of vehicles, vehicle speed measurement, identification of traffic accidents, and traffic flow prediction. ITS uses dedicated hardware such as inductive loop detectors, radar detectors, laser detectors to detect vehicles. Timely and accurate traffic flow information collection is

crucial for transportation management. Data collection components gather all observable information from the transportation system (e.g., traffic flow at a particular point of the road network, average travel time for a particular road section, road hazards) for further analysis of the current traffic conditions.

Real-time traffic monitoring ability, vehicle detection facility, and the improved communication option between the vehicle and infrastructure enables an ITS to offer various services. Such services, for example, dynamic traffic signal control, emergency vehicle priority, public vehicle priority, pedestrian safety, incident management service, variable speed limit, and freeway ramp signals.

There are many cars with semi-autonomous and driving assistive features, such as the smart parking assistance system, lane-keeping assistance system, and Adaptive Cruise Control (ACC), already available in the market [6] [7]. Fully autonomous driving, also known as self-driving, represents the next big leap in human transport technologies. Several companies (e.g., Tesla, Apolong, BMW) are manufacturing and testing self-driving private, public, and commercial vehicles to run smoothly on the road [8], [9]. This sophisticated new technology entirely relies on the automation of vehicle sensing and driving functions, where a human driver is no longer required and effectively becomes a passenger.

Traffic light change anticipation system, bus rapid transit development, share the road with autonomous vehicles, Mobility as a Service (MaaS) using Autonomous Vehicle (AV), and green wave System for EV are some of the major research projects in ITS to provide safe, smart, and faster transportation services [10] [11] [12]. These major research projects can be broadly categorized into four main groups - (i) Traffic Management System (TMS), (ii) ITS communication system, (iii) Incident Management System (IMS), and (iv) ITS security issues. These groups are described in the following section.

1.1 Research on ITS

1.1.1 Traffic Management

ITS uses the [13] to improve the way of managing traffic data received from sensors from automated vehicles and road-side infrastructures. It aims to introduce different innovative TMS to make the road safe for the commuters, use the existing transport network efficiently, and make the TMS more coordinated by providing real-time and better dissemination of traffic information.

For further analysis of the current traffic conditions, Adaptive Traffic Signal (ATS) gathers all observable information from the transportation system (e.g., traffic flow at a particular point of the road network, average travel time for a particular road section, number of passengers boarding a transit line). Collected data is sent to the central traffic controller via the roadside infrastructure. There are different projects to utilize TMS for efficient, safe, and faster traffic management services. The services include public transport priority, bi-cycle lane priority, dynamic phase time control, and IMS [14] [15]. To make TMS more smart and efficient, many issues still need to be addressed. The prominent issues are: (i) providing proper and timely detour notice to the commuter during different events (e.g., accident, road work, natural disaster), (ii) improving Road Side Unit (RSU) to adopt autonomous cars on the road, (iii) adjusting traffic signals in intersections to provide priority to public vehicles, and (iv) giving safe shared route to bicycles and pedestrian. Transportation authorities in different countries are investigating, planning, and running projects to ensure road users (e.g., pedestrians, bicycles, and human-driven vehicles) and self-driving vehicles can use the road safely and efficiently. For example, highly automated driving vehicle partnership, Victoria, Australia [16]; GEAR 2030 strategy and the Cooperative Intelligent Transport System (cITS) [17] platform, Europe; and Self-Driving Transport (SDT) projects, Dubai are some of the major government initiated trials [18] for the safe and secure road for self-driving vehicles for using the road infrastructure. To accelerate such initiatives around the globe, innovative technologies surrounding ITS are on the rise, valuing the

Global ITS market at the amount of US$ 21,481.4M in 2017, and projected to reach US$ 70,798.4M by 2027, indicating a compound annual growth rate of 12.7% [19].

1.1.2 ITS Communication System

Future ITSs will certainly be applied in mixed AVs and Regular Human-piloted Vehicles (RHVs) environment. AVs are new technologies that integrate smart vehicles with road infrastructure. Connected and autonomous vehicles incorporate a range of different technologies, facilitating the safe and efficient movement of people and goods. AV enabled traffic systems have demonstrated great potential to mitigate congestion, reduce travel delay, and enhance safety performance.

In ITS, different wireless communication systems like Dedicated Short Range Communication (DSRC) and cellular networks are being used for the vehicles and road infrastructure communications. There are mainly four components in ITS: (a) On-Board Unit (OBU), (b) RSU, (c) Vehicle Detector (VD), and (d) Signal Controller (SGC). These components mainly use wireless technologies to communicate with each other. Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications are based on ad-hoc wireless communications. Vehicular ad-hoc Network (VANET) play an essential role in ensuring safe, reliable, and faster transportation in an ITS. Currently, intelligent vehicles are equipped with GPS, OBUs, and digital maps for V2V and V2I communications. Vehicles also can access the Internet via RSUs and V2I communications through the IEEE 802.11p Wi-Fi standard [20] [21].

There are many research projects available in the literature for V2V, V2I, Infrastructure to Infrastructure (I2I), Infrastructure to Everything (I2X), and Vehicle to Everything (V2X) communications. Some of these important research projects are: cooperative awareness [20], emergency vehicle warning [22], forward collision warning [23], cooperative maneuver platooning [24], cooperative adaptive cruise control [6], and cooperative intersection control [21].

However, some of the significant concerns in ITS communication system are - (i) Providing an efficient method to collect probe data, (ii) Establishing communication

between the automated and regular vehicle, (iii) Making platoon in a highly congested area, and (iv) Understanding the driver behavior in human-driven and driver-less driving environment.

1.1.3 Incident Management

Traffic congestion can also be life-threatening when the emergency vehicles must travel through congested areas, which may prevent them from reaching accident spots on time. In every major city or state, services offered by ambulance, fire, and other emergency services usually have a strict target response time and Quality of Service (QoS) to meet while attending incidents [25]. Congestion can severely hinder the response time and QoS in rendering those services. The determination of the green light sequence in some ITSs does not consider an emergency vehicle's presence. Thus, if the fire service vehicles, police cars, and ambulances are stuck in traffic, delaying to reach their destination can cause the loss of life and property.

For most incidents, emergency vehicles like ambulance, police, fire service, state emergency service, or other traffic incident assisting service, need to attend the incident place. Monitoring the impact of an incident once occurred, and effective incident management by sending the right emergency support vehicle(s) to the incident place as quickly as possible will decrease incident clearing time, improve roadway safety and decrease traffic delays.

The prime purpose of IMS is to detect an incident. For the detection, ITS uses the road safety cameras used in ATS. The European transportation authority is imposing autonomous vehicles to eCall [26], which can notify the incident to the emergency control room. Clearing the incident place is the next important thing in IMS. Different incident management teams [27] work on major roads to attend incidents quickly. To aid emergency service vehicles to travel quickly, many ITSs have been proposed in the literature, notably Green Wave [11], ITS Integration model [28], Usage-Base model [29], Smart Congestion Avoidance (STLC) [30] and Smart Collision Avoidance (SCA) [31].

All these methods attempt to reduce traffic congestion by making only one traffic signal green for emergency vehicles as they travel along the road. They all consider

emergency vehicles as one type without differentiating among types of emergency vehicles (e.g., ambulance, police, fire service) or priority levels of their services in relevance to the severity level of an incident.

1.1.4 ITS Security Issues

It is conceivable that attacks on ITS can create enormous traffic congestion, malfunctioning of an autonomous vehicle or RSU, even cause a life-threatening accident. For example, a false obstacle data injection in the radar, Light Detection and Ranging (Lidar), or camera may force a car to stop suddenly on a freeway and can cause a fatal accident with the following vehicle [23] [32]. ITS supports the deployment of autonomous driving technologies with cooperation between vehicles. Both existing applications, as well as envisioned future developments, present a host of new security challenges. One of these is the reliability and correctness of transmitted information that is exchanged wirelessly between vehicles and other vehicles or infrastructure. This communication happens within a highly dynamic and heterogeneously managed ad-hoc network. To provide safe and efficient services, ITS needs to protect the integrity of the transmitted data and maintain the accuracy of the data [33], [34].

Existing traffic control systems are very vulnerable to cyberattacks because of the systematic lack of security consciousness. For example, an Argentinian security expert showed that the vehicle detection system of the traffic system is vulnerable to cyberattacks. The vulnerabilities the expert found allowed anyone to take complete control of the devices and send fake data to the traffic control systems [35]. There are many more attacks that happened on different ITS components. Some of the major attacks of the current ITS is detailed in Section 2.4.1

Different autonomous vehicles, Stanford autonomous vehicle [36], Oxford RobotCar [37], AnnieWAYs autonomous vehicle [36], use different combinations of OBU components. Many research projects have investigated the potential cyberattacks on the autonomous vehicle by listing the attack surfaces and describing what attacks can be performed on these autonomous vehicles. Even though there exist many projects, still

now, up to our knowledge, the approaches that can detect an attack in traffic signals and self-driving cars lack in the current literature.

Incident management and ITS security can create more impact on humans in terms of life loss and congestion incurring on the road compared with other research topics (e.g., traffic management and communication systems). Therefore, the research on incident management and ITS security is becoming imminent because of the huge potentiality of self-driving and assistive vehicles becoming a reality shortly. For this reason, this dissertation mainly focuses on the research of incident management and ITS security areas.

1.2 Motivation

ITSs are of paramount importance as they use the dynamic traffic control system to provide safer, smarter, and faster traffic flow. For the dynamic characteristics of on-road traffic, it is hard to manage traffic during the time of an incident. As a consequence, even with the current priority techniques, emergency vehicles cannot meet their targeted response time during peak traffic conditions. As ITSs are becoming more and more intelligent, and smart vehicles are equipped with wireless sensors and communication technologies, the risk of cyberattacks is being increased with time. To address these issues, this dissertation is motivated by the following two key factors:

M1. For the reduction of human cost or impact, improving the EV response time while concomitantly reducing the impact on other on-road traffics is a long-time desire. However, because of its complexity, still, it remains a major research issue.

M2. The increasing use of wireless communications and sensor technologies, and autonomous driving are making an ITS progressively smarter, but consequently, they are also turning it extremely vulnerable to cyberattacks. Increasing reliability of an ITS by improving its resilience against cyberattacks is a pressing need, but yet to be resolved.

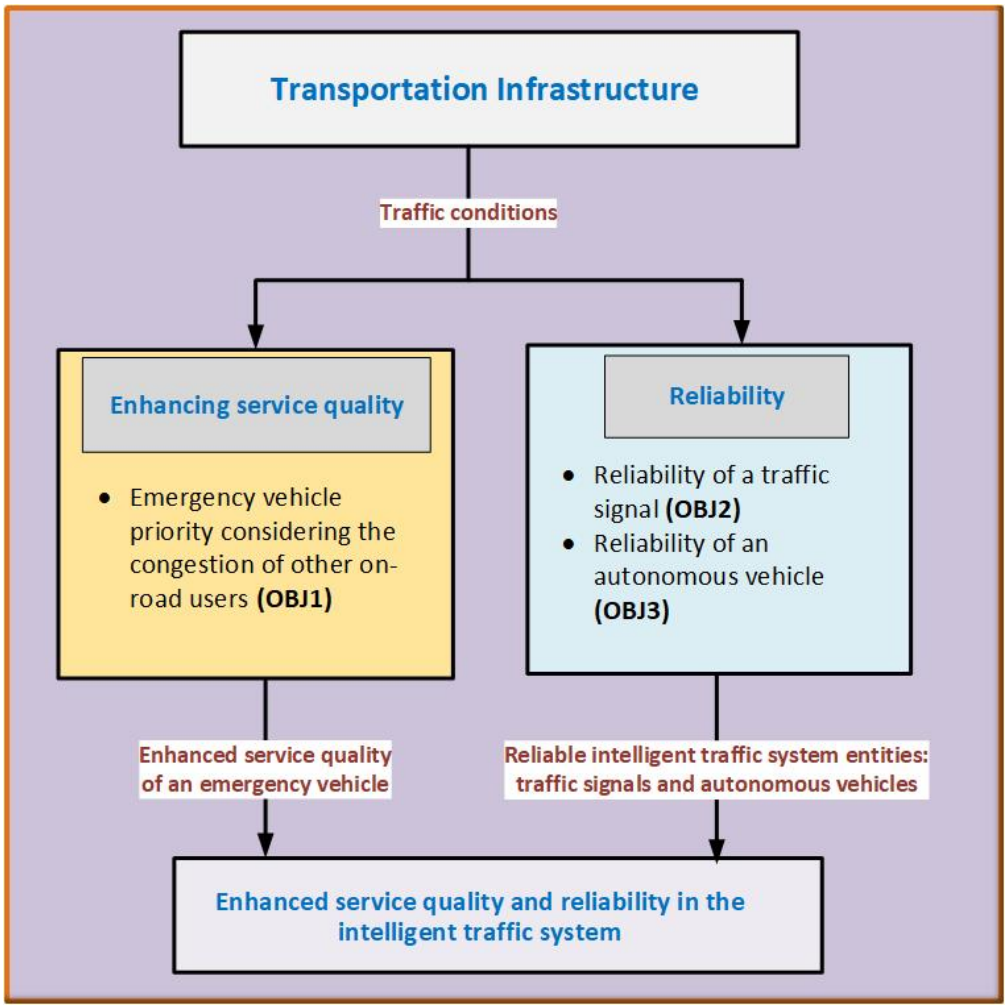


Figure 1.1: An overview of the enhanced service quality and reliability for the intelligent traffic system aimed in this thesis

1.3 Research Objectives

Based on the two motivating factors discussed in Section 1.2, this dissertation aims to address the following three research objectives:

OBJ1. For motivating factor M1, to develop an approach considering the impact on surrounding traffics, which will enable emergency vehicles to reduce the gap between their actual response time and the targeted response time.

OBJ2. To investigate the vulnerabilities of state-of-the-art traffic systems to make them more resilient against attacks. This objective aims to provide the solution of a part of the research issue articulated in motivating factor M2.

OBJ3. Self-driving cars are vulnerable to cyberattacks, and thus their integration into an ITS will make it extremely unreliable. Therefore, as a part of M2's research problem, in this objective, the thesis aims to explore techniques to assess and improve the trustworthiness of a self-driving car on the fly.

To show how the objectives aimed in this thesis are logically connected and will contribute to advancing an intelligent traffic system, an overview of the primary research issues is illustrated in Fig. 1.1. This dissertation specifically focuses to enhance two major aspects of an intelligent traffic system: (i) service quality (OBJ1) and (ii) reliability (OBJ2 and OBJ3).

1.4 Overview of Contributions

An overview of the contributions made in this thesis is given below:

i) To address research objective OBJ1, an Emergency Vehicle Priority System (EVPS) is developed to determine the priority level of the emergency vehicles in relevance to the type and severity of an incident. This system will assist the traffic system to manage light signals in such a way so that the most appropriate emergency vehicle can reach to the incident place sooner. Such preference to the emergency vehicles should be executed intelligently without causing or minimizing any detrimental impact on other on-road vehicles. Therefore, the main part of the proposed EVPS is to calculate the number of signals that need to be turned green in such a way so that it provides a faster route to an emergency vehicle, and at the same time, it reduces the waiting time of other vehicles on the road. We analyze the vehicular traffic flow interrupted by incidents by applying the macroscopic traffic models and developed a simulation model using a traffic simulation tool, namely SUMO [38]. The initial version of this project has been published in [39].

ii) To achieve OBJ2, for the first time, this thesis introduces an Intrusion Detection System (IDS) to detect the attacks in traffic signals. This system is theoretically modeled

using the most popular and widely used theory for information fusion, namely the Dempster-Shafer (DS) decision theory [40]. The proposed IDS considers the instantaneous observations of vehicle flow rate, the speed at intersections, the phase time of traffic signal changes, and their corresponding historical data recorded by transportation authorities. Shanon's entropy is used to determine the uncertainty in estimation. For the verification and validation of our IDS, we developed a simulation model based on SUMO using many real scenarios and the data collected by the Victorian Transportation Authority, Australia, called VicRoads. We published the preliminary version of our proposed IDS in [41].

iii) To enhance the accuracy of assessing the reliability of a self-driving car (refer to OBJ3), an innovative trust measurement model is presented in this thesis. Along with GPS and warning messages, the proposed model measures the trust level of the main four components of a self-driving car's OBU: (1) Lidar, (2) Acoustic sensor, (3) Radar and (4) Camera. The uncertainty associated with the trust values of these six components is measured using the Shannon information theory. These trust values are fused using the DS decision theory. To compare and contrast the trust values obtained using a subject logic (DS theory), we also use CertainLogic [42] to estimate the trust value of a self-driving car. The proposed trust model was simulated using SUMO, and the relevant real VicRoads historical data and its preliminary version has been published in [43] and full version have been published in [44].

iv) For all objectives (OBJ1-3), we developed a realistic simulated environment capable of emulating real-life traffic and road networks on the SUMO platform. The VicRoads's historical data on real traffic and the real road map of a location in Melbourne CBD in Victoria were used in our simulation platform. We selected the peak-time density, flow rate, and vehicle speed in our simulation using the real traffic historical data from VicRoads during 08:00 am to 09:00 am Monday (52 Mondays of 2016) at five busy corners of Melbourne CBD: (a) Lonsdale and Russel street, (b) Collins and Kings St, (c) Elizabeth and Latrobe St, (d) Collins and Swanston St, and (e), Flinders and Swanston St Melbourne. We selected different incidents like car breakdown places in the monitored area, unusual vehicle stops due to OBU component malfunctions or

malicious behavior, and compromised RSU components using 11 different scenarios, five different occupancy rates, and three different time slots. Each vehicle type was individually modeled. Each vehicle had its route and moved individually. Vehicle type (e.g., private, public, tram, emergency vehicles, delivery van), pedestrian numbers, road conditions (e.g., dedicated bus lane, one-way traffic) were considered.

1.5 Structure of this Thesis

This section provides an overview of how the remainder of the thesis is organized.

Chapter 2 includes a contemporary review of traffic signal systems, traffic flow models, applications and projects of ITS, security issues, and recent attacks on ITS. Two conference papers and one book chapter on the review of different types of cyberattacks in the cyber-physical system have been published in [45], [46], and [47].

Chapter 3 proposes an innovative system named Emergency Vehicle Priority System (EPVS), which can be easily integrated into an existing ITS. There are two major operational parts in EPVS. In the first part, the system determines the priority code of an EV based on the type and severity of the incident. In the second part, the proposed EVPS system calculates the number of interventions needed in the green signal phase time to provide priority to EV by considering the additional congestion created with other traffics. The result shows that the intervention recommendation provided by our proposed EVPS reduces the EV travel time by up to 15.4% from the currently implemented green light system [15] [11].

Chapter 4 presents an intrusion detection system for the traffic signals. This chapter uses the DS decision theory to fuse the combination of different numbers and types of evidential observations derived from traffic signal characteristics. The performance metrics indicate that our proposed IDS can detect the intrusion with 91.1% overall accuracy.

Chapter 5 presents a novel approach to determine the trustworthiness value of a self-driving car using all four main components of an OBU: (i) Lidar, (ii) Acoustic sensor, (iii) Radar and (iv) Camera along with GPS data and warning messages using both subjective

and CertainLogic. This chapter finds that CertainLogic has better performance than the DS decision theory measuring the trustworthiness of a self-driving car.

Chapter 6 presents concluding remarks of this dissertation and outlines possible future research directions.

Chapter 2

A Review of an Intelligent Traffic System: Approaches and Security Mechanisms

According to the research objectives of this dissertation presented in Section 1.3 of Chapter 1, in this chapter, we review the contemporary and relevant approaches and security mechanisms introduced for an ITS.

In ITS, different signal controller units are used to communicate between the signals in adjacent intersections, maintain the phase time, cycle time, and the operational status provided by the central traffic controller. Roadside sensor systems and different driver assistance systems installed in modern vehicles can communicate with an RSU to receive and provide information to increase road safety and smart traffic management. For these reasons, different types of Adaptive Traffic Control Systems (ATCSs) such as Sydney Coordinated Adaptive Traffic System (SCATS), Optimization Policies for Adaptive Control (OPAC), Real-time Hierarchical Optimized Distributed Effective System (RHODES), Adaptive Control Software Lite (ACSLite) and InSync adaptive traffic system [13] [48] that use real-time traffic data to optimize the cycle time of a traffic signal to reduce travel time and congestion are discussed in details. These systems are at risk of having under different types of a cyberattack through the exploitation of their wireless communication technologies. As a consequence, we survey a broad range of traditional traffic flow models used in simulations and ATCSs, attacks on an ITS, and trust management issues that are relevant to this research project. From the critical analysis and examinations of the approaches and security issues and mechanisms presented in this chapter, we

identify some further research challenges that are also articulated in this chapter. These research challenges enable us to select the research objectives of this thesis.

The chapter is organized as follows. This chapter begins by providing a detailed discussion about Traffic Queuing Models in Section 2.1. Communication infrastructure and entities of ITS are discussed in 2.2. Section 2.3 presents the dynamic traffic control system used by the transportation authority of Victoria (VicRoads). The security issues including trust related to an ITS and self-driving cars are described in Sections 2.4 and 2.5. Next, in Section 2.6, we present some further research challenges. We finally conclude this chapter.

2.1 Traffic Flow Models

Since the early 1900s, several traffic flow models were developed to increase traffic management procedures. There exist four major types of traffic flow models in the literature. The first model, fundamental relation, was introduced in the 1930s. Second and third models, microscopic and macroscopic, were started their journey simultaneously in the 1950s. After a decade later, in the 1960s, the mesoscopic model was introduced. These four models are described below.

2.1.1 Fundamental Relation Model

Greenshields [49] introduced the first traffic flow theory in 1934 by showing the relationship between two basic traffic characteristics, vehicle speed and the space between the fronts of two consecutive cars. In 1935, Greenshields showed that density, traffic flow also can be used with the vehicle speed and the space between two cars and developed a fundamental relation model. del Castillo [50] describes a fundamental relationship with the following properties:

- The range of vehicle speed (ϑ) and density (ρ) is from zero to maximum.
- Vehicle speed is maximum in lowest density and velocity is zero with maximum density, $\rho(0)=\vartheta_{max}$ and $\vartheta(\rho_{max})=0$

- Flow rate (q) is zero with extreme density, $q(0) = q(\rho_{max}) = 0$ This fundamental relationship model is the base of the other traffic flow models described below.

2.1.2 Microscopic Model

Microscopic models [51] incorporate the response of individual vehicles to changes in their surrounding traffic such as acceleration, lane changes, and deceleration. Each vehicle follows and adjusts speed and distance between cars according to its leading vehicle. Hence most of the earlier models are car-following models based on longitudinal behavior and did not consider the vehicle and driver action and consequently failed to imitate real traffic dynamics and produced inaccurate results.

Pipes [52] is one of the pioneers of the microscopic models based on a safe distance approach [51]; this model did not incorporate the unpredictable behavior of the leading vehicle. Gipps in [53] proposed a model that includes the characteristics of the driver and the vehicle to minimize the gap between simulation and actual scenarios. This model successfully imitates real traffic scenarios, adds the apparent driver, and vehicle characteristics without making the calibration process more complicated. It also sets a safe speed according to the position, speed, and traffic density associated with the predecessor. A sudden disruption in the speed of the predecessor, the vehicle can avoid an accident and come to a safe stop following this model. Similar conditions are observed for braking behavior. For example, a vehicle might not apply brakes unless its predecessor starts to decelerate. This model generates results faster than others as the model calculates speed using less complicated mathematical equations. In the late nineties, multi-class and multi-anticipation models gained popularity to incorporate the heterogeneity of vehicles, which lead to vast development in this area, and many authors worked to enhance this approach. Another simplified categorization of microscopic models is the cellular-automata model. These models partition a road into cells of a fixed length, which may or may not have a vehicle at a given time. The first model of this nature was designed in 1986 and further improved by combining it with a car following the optimal velocity model and with the three-phase traffic theory

as discussed and compared by the authors in [54]. The main advantage of microscopic models is that it incorporates various behavioral characteristics of the vehicle/driver and parameters such as safe distance, stimulus-response, the relative position of vehicles, vehicle classes, and reaction margin. This makes these models more accurate and detailed, but a more significant number of parameters make these models hard to calibrate and computationally slow while increasing the processing cost [55].

2.1.3 Macroscopic Traffic Modelling

The macroscopic model [56] is designed based on the continuum fluid flow models, where traffic flow is treated the same way as particles (atoms/molecules) of a fluid of continuum flow. The model considers three fundamental variables: speed (ϑ), density (ρ), and flow (q), and assumes that traffic flow is solely dependent upon the traffic density. Speed and density are inversely proportional, and minimum traffic speed indicates maximum traffic density, which is also known as jam density. Lighthill and Whitham proposed the first simple macroscopic traffic flow model and further improved independently by Richards. This model is known as LighthillWhithamRichard (LWR) model. [57] [58].

The LWR model revolved around the concept of traffic equilibrium, although it captured the essential dynamics of traffic flow but failed to describe scenarios that lie outside the equilibrium conditions. The main equation of the model is based on the conservation law of vehicles formulated based on entropic solutions due to which it does not correctly depict acceleration and deceleration of traffic. Furthermore, the LWR model defines acceleration to be unbounded, implying that vehicles have infinite acceleration due to which it fails to model jam conditions correctly. The author in [59] extends the LWR model to address its shortcomings. The proposed solution includes setting an upper bound for acceleration so that it does not exceed the maximum acceleration. By introducing non-entropic solutions to the existing LWR model, the author [54] shows that the model can provide analytical solutions for both equilibrium and non-equilibrium conditions.

Furthermore, the author lists various two-phase extension models of the LWR model and compares their results and limitations with his proposed solution. His model provides analytical solutions for all the essential causes of a traffic jam, capacity drop, hysteresis, sudden traffic state changes, scattering of traffic, etc. The drawback of this model is that it is deterministic, so it can only detect but cannot explain the discrepancies of traffic flow.

The LWR model relies on the existence of an equilibrium speed-concentration relationship $\vartheta = \vartheta_e \rho$ or equivalently a flow-density $q = \rho\vartheta = q_e(\rho)$ or flow-speed relationship $q = \rho_e \vartheta$ (because $q = \rho\vartheta$). With such a relationship, the model becomes a first order, nonlinear partial differential equation of hyperbolic type:

$$\frac{\partial \rho(x,t)}{\partial t} + q'(\rho)\frac{\partial \rho(x,t)}{\partial x} = 0 \tag{2.1}$$

where $q'(\rho) = \frac{dq_e}{d\rho}$.

The simplest macro model is the LWR model is expressed by:

$$\rho_t + (\rho\vartheta_e(\rho))_x = 0 \tag{2.2}$$

where $\rho, \vartheta_e(\rho)$ are respectively the density and equilibrium speed. Equation (2) can simulate the formation and evolution of shock wave, but it cannot be used to study non-equilibrium traffic flow as the speed in the model cannot deviate from $\vartheta_e(\rho)$ To conquer this drawback, many Distance Gradiant (DG) and Space Gradiant (SG) models were developed to explore non-equilibrium traffic flow. The classical DG model is the Payne model [60]:

$$\begin{cases} \rho_t + (\rho\vartheta)_x = 0 \\ \vartheta_t + \vartheta\vartheta_t = \frac{\vartheta_e - \vartheta}{\tau} - \frac{\vartheta}{\rho_\tau}\rho_x \end{cases} \tag{2.3}$$

where τ is the relaxation time, and $\vartheta = -0.5\vartheta'(\rho)$ is the anticipation coefficient.

The advantage of macroscopic models is that it is easy to model due to lesser parameters, minimum complexity, fast and efficient performance and, low computation

cost as compared to microscopic and mesoscopic traffic flow models. However, these models require characteristics (such as vehicle specification, traffic flow conditions at the time 't,' and nature of the driver) to be incorporated in the model design to achieve a more detailed and accurate result not compromising on the simplistic design and easy calibration of macroscopic models [59].

2.1.4 Mesoscopic Model

The Mesoscopic model of traffic flow was introduced to bridge the gap between the macro- and microscopic models, this model divides traffic into groups and study the behavior of vehicles in aggregate terms combining the positive aspects of both macro- and microscopic models. A very popular branch of mesoscopic models is gas kinetic models, similar to the theory of particles in motion in a gas. The model was first introduced by Prigogine and Andrews [61], who used partial differential equations to derive the basic formula, which was then improved by Paveri-Fontana [62] by considering correlated behavior of adjacent vehicles as well. There are two conventional approaches to mesoscopic models, first in which the traffic is divided into multiple packages, e.g., CONTRAM simulator that came in 1989, and second in which the dynamics of individual vehicles derive the flow dynamics of the model such as in DYNASMART simulator proposed in 1994 [63]. In these models, the link is commonly divided into two parts; running part and queue. In the early 1990s, researchers estimated that the time a vehicle exits a link is dependent upon the traffic density in the queue. The gas kinematic models cannot be implemented without modifications, they are converted into continuum gas kinematic models before simulation, due to which continuum gas kinematic models gained popularity, and many researchers started work to improve these designs.

The mesoscopic model provides a more accessible approach to microscopic models based on the non-continuum approach and macroscopic models based on the continuum approach and is relatively faster. It is not dependent upon a large number of parameters such as in microscopic models and is much more efficient systems. The modeling of mesoscopic models seems quite complicated due to various assumptions and the use

of partial differential equations. The major disadvantage is that these models are only limited to simulators and laboratory tests; the future research on mesoscopic models requires more work to be done on applications of this model [55].

Traffic flow models play an important role in identifying the issues and possibilities to improve the service provided by traffic management authorities. To improve the service and adopt the new available technologies, ITS was introduced. The next section will discuss the applications, entities, communication architecture, adaptive traffic system, and the security issues of an ITS.

2.2 Intelligent Traffic System

Different types of applications are provided to the users in ITSs. This section provides an overview of the ITS applications, architecture, and entities.

2.2.1 ITS Applications

ITSs are providing many different services to make the road journey faster, safer, and smarter. Both roadside infrastructures and autonomous vehicles are giving various applications, as shown in Figure 2.1. ITS applications is broadly categorized into four main classes: (i) traffic management; (ii) road safety; (iii) autonomous driving applications; and (iv) infotainment and comfort [32, 64, 65].

2.2.1.1 Infotainment and Comfort Applications

One primary function of infotainment and comfort application is to bring about a better driving experience with the aid of information about the driving environment. Passengers of autonomous vehicles are provided with many free and value-added services. To make this service seamless and practical, these service providers are ensured to be the ones who make provisions for the corresponding. Therefore, when their applications are installed on a vehicle's application unit, the transmission process will

be likely to experience little or no hitch. Application units link up with the remote Service providers' data centers through their OBUs. They do this by using a range of Vehicle-to-Infrastructure communication technologies in the form of 3G,4G/LTE, and 5G [66].

Driverless cars are newly emerging technology in the automobile industry, which is cost-effective and efficient. With this new technology transportation system will enter into a new era of advancement with a different method. In driverless cars, a person will call upon a car from his mobile phone with the help of an app and will ride to a destination without any involvement of the second person. Moreover, as some cities are preparing for fleets of cars, which will be owned by a small number of peoples and a large number of consumers will use that which may change the whole scenario of the current system. SAE J3016_201806 standard for the level of driving automation, cars are divided into five levels. SAE Level 1 car requires a driver for every action means zero automation gradually increasing with little to full assistance as Level 5 vehicles are fully driverless and operate independently in every situation [67].

For the autonomous function of a vehicle, an autonomous car requires a lot of technologies to combine at the same place for safety and accuracy. Detection of objects, their location, and shape, making decisions, and other works are required to be done accurately for safety. A successful driverless car needs to locate the path, its position, different vehicle position and intentions, position of surrounding objects, and other traffic participants like pedestrians and traffic signals. Cameras, high sensitive GNSS, WLAN, infrared, tactile, and combine polar systems, UWB and RFID, can be used for recognition of object and transfer data depending upon range and accuracy. Mid-range and long-range radars, ultrasonic, 3D video camera, infrared camera, and laser scanner are used for the identification of traffic participants and the environment [68] [69] [12]. With the wireless OBUs installed in the autonomous cars, it can connect with the APs and routers of the RSUs and can connect to the Internet. Fixed cameras can broadcast the live stream of videos or receive video during the events or incidents. Smart GPS and GNSS can provide tourist spots, emergency service locations, and other services (e.g., shopping centers, parking locations). Brief description of different components of OBU

used in self-driving cars is describer in Section 2.2.2..

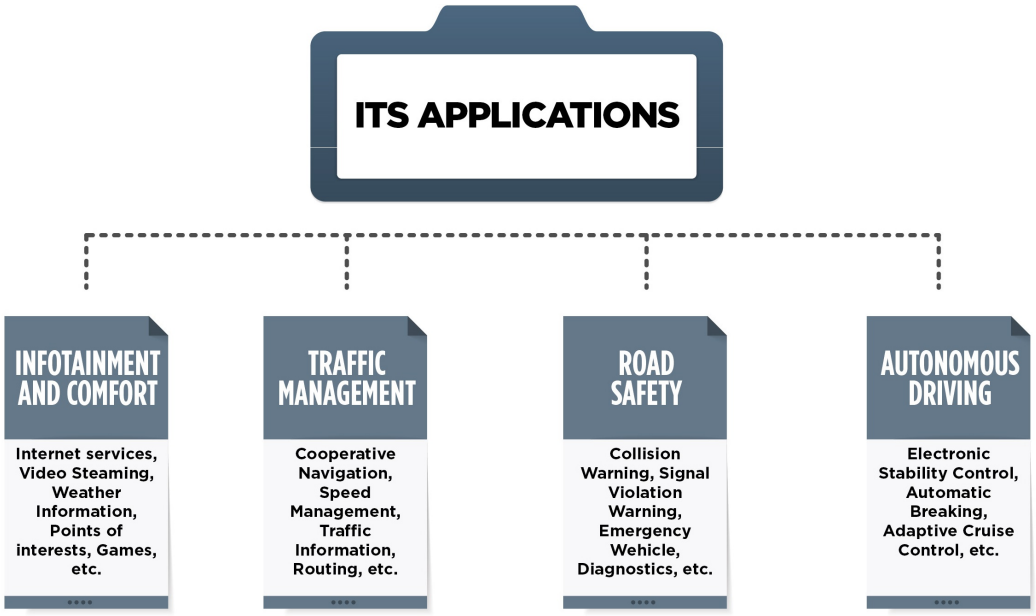


Figure 2.1: ITS applications

2.2.1.2 Traffic Management Applications

The main objectives of traffic management applications are to (i) enhance the management and coordination of traffic flows and (ii) provide cooperative navigation services to drivers. These applications rely on the collection and analysis of the exchanged ITS messages between ITS entities (refer to Section 2.2.2 about the details of ITS entities) [70]. Traffic signals are one of the main contributors to provide these services.

The Intelligence Traffic Lights (ITLs) is a constituent of the warning messages under the smart city framework. It moreover updates the driver on the status of the traffic conditions, makes routes decisions and modulates the traffic information. Vehicle monitoring systems receive accurate GPS information as a provision of the new scheme. Each level of the proposed technique performs an integrity check to assess the GPS positioning output quality. The car's velocity integrity check is done through the GPS

Doppler information for there to be a resultant improvement on the map matching process.

The Zig bee module provides wireless communication CC2500 to link the traffic controller and emergency cars like ambulances. Different combined input tests came to play on the system prototype, and the experimental results were amicable. The telematics role in the transport system is highlighted in [71]. They reduce harmful impacts while strengthening transport characteristics. Through it, the transport system challenges like unnecessary congestion, energy use, and air pollution reduction [72]. ITS uses an adaptive traffic control system to gather traffic data, process the data, and control the traffic signals. The details of the adaptive traffic system are discussed in Section 2.3.1.

2.2.1.3 Road Safety Applications

Road safety application aims to manage the ITS entities (e.g., vehicles, road infrastructures) in such way to reduce the traffic accidents and protect drivers and pedestrians from road hazards [73].

Four typical examples of emerging ITS road safety applications are (i) collision warning, (ii) signal violation warning, (iii) emergency vehicle priority, and (iv) vehicle monitoring.

The development and utilization of the Intelligent Disaster Decision Support System (IDDSS), together with its ability to responding and planning during a natural disaster, provides a smarter incident management service. Thus the disaster management concepts of resiliency, susceptibility, and risk can be improved through IDDSS [74]. The IDDSS equips each car with an RFID tag. Network congestion is easy to determine through vehicle counts on a specified duration using the RFID readers. The information moreover aids in deciding the green light duration for the set path. If the course of car theft, the data will also help in its depiction.

In-vehicle Intersection Violation Warning System (IVWS) was introduced by the US Department of Transportation (USDOT) warns a driver the risk of failing to stop for a

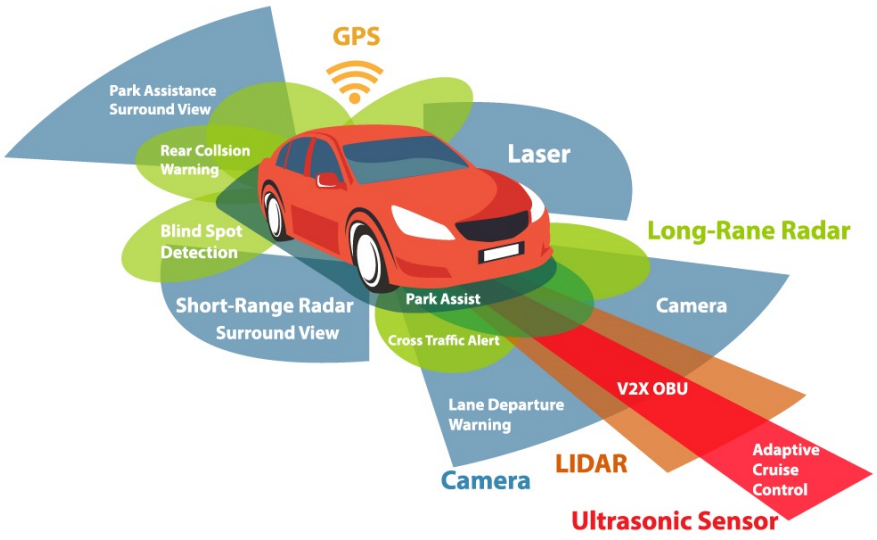


Figure 2.2: Key technologies used in autonomous vehicle

red light or stop sign [75]. The risk determination is based on algorithms that consider current vehicle operating conditions, intersection geometry, GPS differential corrections, and signalized intersections, the status of the traffic signal phasing [32] [64]. Managing incidents is one of the significant and challenging tasks to provide safety to the road user. The description of the incident management service is provided in Section 2.3.5.

2.2.1.4 Autonomous Driving Applications

Autonomous driving, also known as self-driving, technology is expected to be fully functional by 2030. As shown in Figure 2.2, autonomous driving cars integrate many different technologies. The key technologies differ depending on the make and model of the vehicle. The technologies used in autonomous cars are: (i) ultrasonic sensors to detect the presence of obstacles; (ii) Lidar and radar to create a 360-degree field view to prevent accidents; (iii) high definition cameras to spot road hazards such as pedestrians and animals crossing in real-time; (iv) Global Navigation Satellite System (GNSS) receivers to provide highly accurate instantaneous location of cars; and (v) V2X com-

munication technologies to enable a car to communicate with the surrounding vehicles, road infrastructures, remote services providers and trusted third parties. Automatic braking, collision avoidance, lane detection, and lane change technology, adaptive cruise controls are some of the major techniques provided by the autonomous driving applications [32] [76–78]. Autonomous vehicles communicate with the RSUs using the OBUs to sense the traffic data, process current traffic information, and make decision execute autonomous driving. The significant entities of an ITS will be discussed in the next section.

2.2.2 ITS Entities

As growing urban drivers and commuters put pressure on our road network, cities in the constant battle will need new and better tools to avoid congestion and ensure driver safety. The ever-growing ITS revolution represents a new way of looking at the management of traffic and road network. From a security perspective, an ITS system can attract many different entities, including drivers, OBUs, RSU, third parties, attackers, and infotainment systems [79] [80]. Figure 2.3 shows different entities of ITS. Those entities are outlined below:

2.2.2.1 Road Side Units

The major components of the roadside units consist of different in-road sensors (e.g., vehicle counting sensor, speed detection sensors, traffic flow monitoring sensors [81]), warning display system (e.g., warning for road works, incident warning), video detection system (e.g., road safety camera, redlight camera), and traffic signals. Figure 2.3 shows the differents RSUs. Road sensors and cameras send traffic data to the regional traffic controller. The regional controller then sends the data to the central traffic controller for data processing. The central controller then sends appropriate information to traffic signals and display monitors through regional computers and ATCSs (refer to Section 2.3.1 for details about ATCS). The main functions of an RSU are to:

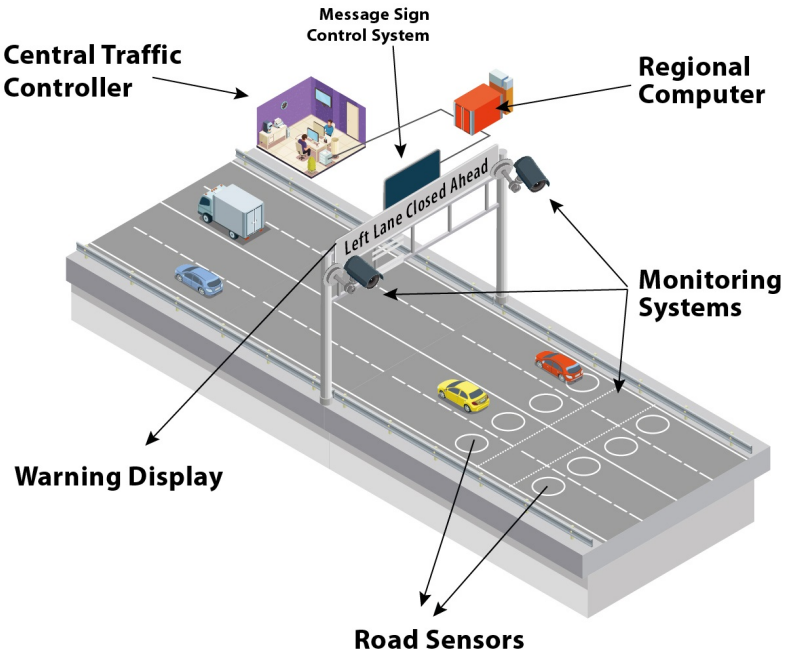


Figure 2.3: ITS entities

- Extend the communication range
- Provide Internet connectivity to onboard units, and
- Equip with safety applications such as accident warning

A vehicle with all these components can not only reduce the number of accidents but also robustly maintain the three most essential security requirements termed CIA -Confidentiality, Integrity, and Availability. All these are done by using a fixed infrastructure unit called RSU. An RSU is responsible for registering vehicles willing to participate in a VANET group. It connects with the Internet and produces the needed information for the vehicles it connects to. A vehicle can identify nearby RSUs by using its digital positioning system, and upon being identified, it sends them a hello packet for confirmation. An RSU's responsibility is to issue a secret token to each vehicle during registration, which is later used by the vehicle to authenticate itself to the RSU. Since tokens are used to authenticate vehicles, those must be protected. For example, to prevent malicious vehicles from revealing their tokens to attackers, each token is a unique integer dynamically generated by the RSU. All keys and tokens are delivered to vehicles after successful registration, except for warning messages which are delivered even without registration [82].

2.2.2.2 Drivers

Drivers are the essential components of the ITS system because they interact with driver support systems to ensure a safe and quick passage and make essential decisions. For a fully autonomous vehicle, the vehicle itself plays the role of the driver, and for a semi-autonomous vehicle, a human is a driver. In both cases, the driver is the important entity of an ITS for safe driving practice.

2.2.2.3 OBU

An OBU keeps track of all communication information for a given flight as it has storage space to store recorded, evaluated, and transmitted events to other OBUs such as an

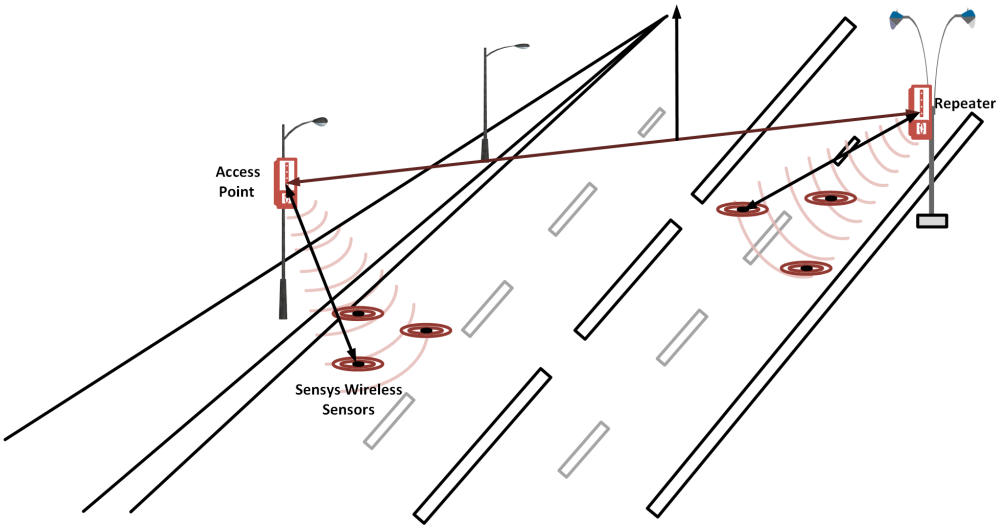


Figure 2.4: ITS sensors and signals

aircraft black box. Figure 2.2 different types of OBUs used in autonomous vehicles. Different vehicles use different storage facilities such as the Adaptive Traffic System Capture to stores traffic information such as the number of cars crossing an intersection and pedestrian data to provide an improved and efficient traffic management service. An OBU has a short-range wireless communication network device based on the IEEE 802.11p standard, and a user interface for connecting to other OBUs. It also includes a transceiver for 5.9 GHz DSRC, Electronic Control Unit (ECU), Trusted Platform Module (TPM), a GNSS unit (e.g., GPS), an Application Unit (AU), an application processor and a Human-Machine Interface (HMI).

- **Lidar** is used for measuring the distances between the vehicle and the surrounding objects. It can send 400000 pulses in a second and can create a 3D map. Lidar is used to create 3D maps of surroundings in autonomous cars for better performance as it can operate at tough conditions like low visibility, fog, and even in complete darkness. Lidar uses infrared light pulses to detect the object's shape and distance in 360 degrees around the car. Lidar creates high-resolution images and maps as compare to radars and other technologies. Two types of Lidars are used based on covering distance on sides of cars medium distance Lidars 20m-40m are used while

on front and back 150m-400m long-range Lidars are used. Currently available, Lidars can scan the only maximum up to 120m ahead, which is far less than a camera mounted system, which can cover up to 500m. Velodyne HD Lidar system is available with good specifications like 100m range, full accuracy, and complete 360-degree scan with 30 degrees vertical. But their power consumption is more, and the price is also high. This issue can be eliminated by selecting architecture sensors like silicon detectors. There are two standards based on a safety level named IEC-60825-1 and ANSI Z136.1, which gives the maximum permissible exposure for such systems. In order to maintain safety, there are limitations for pulse repetition and energy levels because when the repetition rate is high, it will be considered as a continuous source of energy, increasing power level, which is hazardous for eyes. Due to such limitations, specifications of systems cannot be maintained for better performance. This problem can be covered by using Short-wave Infrared (SWIR) light as its wavelength is more than visible light and does not harm the human eye. Moreover, SWIR has less scattering during tough weather conditions and minimum cluttering by solar radiation [83] [84].

- **ECUs** collect data of car dynamics (for example, position, speed, headroom, car size), control a vehicle's functionality, and the next environmental parameter within the vehicle domain (for example, the number of adjacent cars, local traffic circumstances). These ECUs work together by exchanging messages with the various OBUs and AUs and defining an on-board system (also called on-board network).

- **AU** is a device that is installed in a car and is responsible for running remotely from the transmitting units of corresponding OBU applications provided by the manufacturer. An AU must carry out a program in which its transmission medium involving an EV and its OBU is also wired or wireless, to enable an OBU's communication capability. An OBU monitors transfer with a network adapter, and thus assumes responsibility for all mobility and network tasks for which an AU communicates via the OBU over the network. An AU communicates with other

nearby ITS entities using its associated OBU and can be a committed gadget for security applications, or a different tool such as a Personal Digital Assistant (PDA).

- **TPM** of a vehicle enables secure and efficient communications and manages various keys and certificates [65]. The HMI is interactive and non-intrusive, i.e., it should be not used by a driver while driving. Therefore, an OBU should have a touch screen that restricts its use when a car is moving. To enable its use during driving, a voice-based interaction has already been included in a vehicle to avoid distraction [85].

2.2.3 Communication Between ITS Entities

Their primary functions of ITS communication are wireless radio access, ad-hoc and geographic control, network interference control, reliable transmission of messages, data protection, and IP mobility [86]. To ensure seamless communication between V2I and V2, it must be equipped with one or more wireless communication transceivers, as an OBU provides both V2I and V2V. Older data is overwritten after a certain period, but an OBU may frequently transmit a status message to other OBUs to make safety applications mandatory for vehicles [85, 87]. The communication architecture is given in the next section.

2.2.4 ITS Communication Architecture

2.2.4.1 Communication Domain

The architecture of ITS comprises three main communication domains: (i) In-vehicle, (ii) V2X, and (iii) Infrastructure domains, as shown in Figure 2.5. In the In-vehicle domain, a vehicle contains OBUs mounted on the top of the vehicle itself. The communication units of an OBU communicate with each other to ensure vehicle functionality. The V2X domain forms an ad-hoc network amongst OBUs and RSUs deployed along with the road's ITS infrastructure. The information collected at the OBUs is exchanged in real-time with nearby ITS entities (e.g., OBUs, RSUs) using various vehicular communication

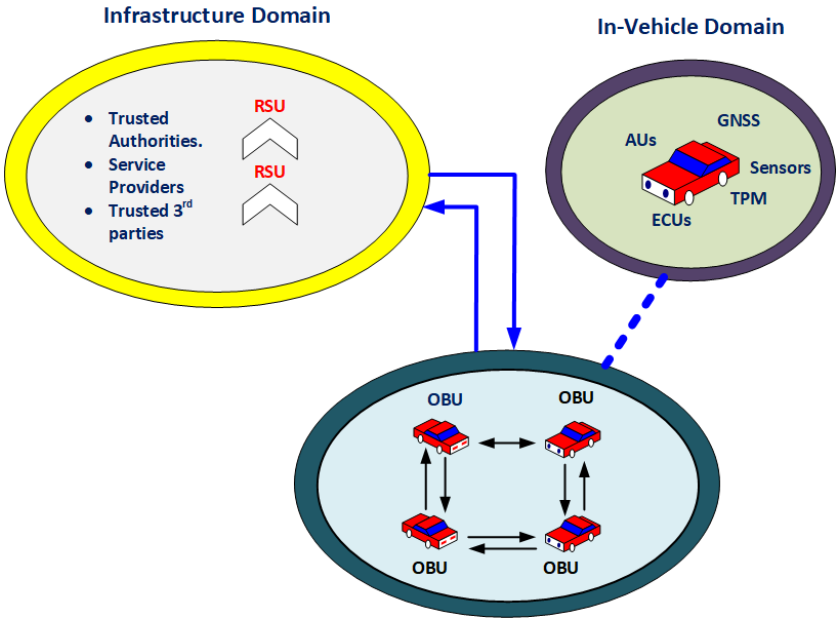


Figure 2.5: ITS architecture with main communication domains

technologies (V2X), including (i) V2V communications among neighboring vehicles, (ii) V2I communications mainly among the surrounding OBUs and RSUs; and (iii) Vehicle to Pedestrian (V2P) communications between the OBUs/RSUs and the surrounding pedestrians [64].

The main component of the infrastructure domain is the RSUs located along the roadside. Each vehicle connects to the nearest RSUs through its OBU, and hence an RSU is regarded as the bridge between vehicles [65]. ITS is recognized as a game-changer that will contribute to traffic safety, passengers' accidental protection, and traffic overcrowding resolving by functional convergence of Information Communication Technology (ICT) and transport systems. As mentioned before, in ITS, OBU and RSU communicate with each other. As shown in Figure 2.4, the communication between RSU and OBU is bidirectional and can be wired or wireless. The communication within this domain forms VANET and Mobile ad-hoc Networks (MANET).

2.2.4.2 Communication Protocols

VANET is a fundamental technology on which the ITS is based. It is the largest MANET application where the nodes are presented as vehicles with implemented sensors, intelligence, and communication capabilities. Nowadays, VANET solutions are based on wireless interfaces like DSRC and Long Time Evolution (LTE) that are built-in vehicles and supporting road infrastructure as well.

IEEE has improved IEEE 802.11 protocol versions and defined IEEE 802.11p, in agreement with the DSRC band, forming Wireless Access in Vehicle Environment (WAVE) stations. WAVE stations are developed according to specific network needs and shaped in a family of IEEE 1609 protocols in order to provide physical layer and medium access layer of VANETs, interfaces, information exchange, and all other details necessary for network functionality.

The typical range for V2V DSRC radio communication is from 300m to 1000m. Basic Safety Message (BSM), as a representative of a beacon message, is transmitted via DSRC, every 100ms. It contains information about vehicle location, speed, maintains the list of neighbor vehicles and other details that help to avoid collisions, and generate alerts for improved safety. The DSRC frequency band consists of seven 10 MHz sub-bands and a 5 MHz guard band in the beginning. One of these bands is reserved for BSM, but even this dedicated channel can be congested very quickly if the traffic is heavy and when the number of nodes is significantly increased with many vehicles broadcasting their BSMs. This mutual awareness between vehicles makes driving safe, even in hard conditions with zero visibility, and represents road-map to driver-less cars [88].

As stated above, ITS entities communicate with each other to collect, transfer, and share traffic-related information. The next section will discuss the role of ATS in ITS. We will discuss the system called SCATS used by the road authority of Victoria, Australia.

2.3 Adaptive Traffic System

SCATS is designed to meet the different traffic management demands of small, medium, and large cities. A typical SCATS system is shown in Figure 2.6, contains a single

regional computer that can control signals at up to 250 intersections. The following three components are essential to implement the SCATS system:

- Central Traffic Controller (CTC) to manage global traffic data, access control, graphics data as well as data backup,
- Traffic Signal Controller (TSC) that is compatible with SCATS, and
- a reliable communications network so that the CTC can share data with all TSCs, and at every intersection, usually in the form of rings.

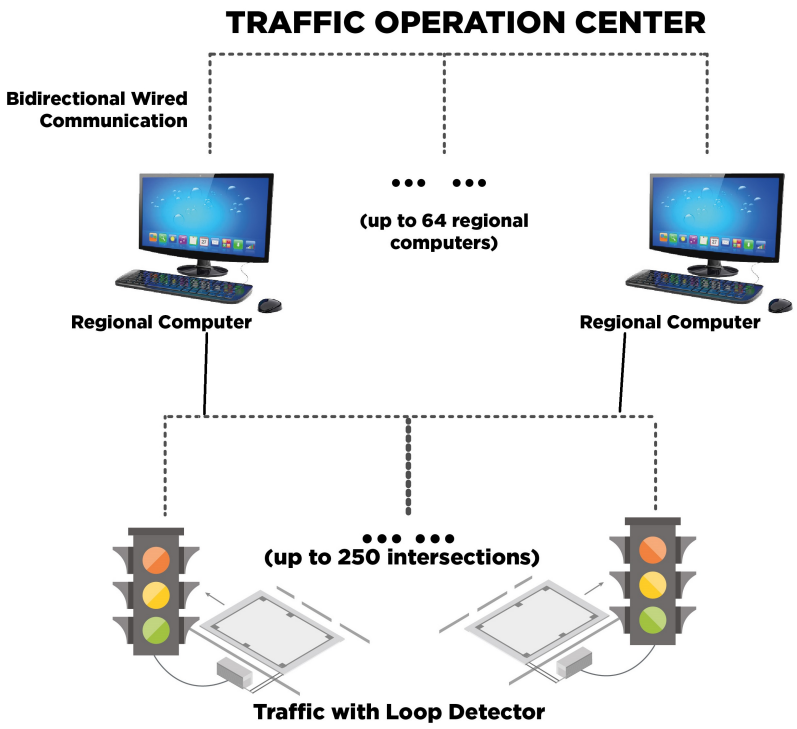


Figure 2.6: SCATS system

SCATS collects data from different sources and analyze the data to dynamically set the cycle and phase time as per current traffic demand. The data collection methods are described below:

2.3.1 SCATS data collection method

There are four main methods used to collect data on transport routes using a "floating car" or "probe." These include (i) the triangulation approach, (ii) re-identifying vehicles, (iii) GPS methods, and (iv) smartphone-based costly monitoring. In the early 2010s, because of the system cost and complexity, the popularity of the triangulation process based on a signal variation from a moving car's internal telephone decreased. Re-identifying vehicles: The installation of roadside detectors is required for this method. In this technique, a unique serial number is found at a single point of the car equipped device and is then collected further down the road. Traveling time and speed are calculated using pairs of sensors to measure the detection time of a particular device. It can be done by using Bluetooth or other devices ' MAC addresses, or the RFID serial number of Electric Toll Collection (ETC) to identify devices in the vehicle (also known as "toll tags") [89].

GPS methods: An increased number of vehicles have two-way communication with a traffic data provider using satellite navigation systems. For the calculation of vehicle speed, position readings for these vehicles are used.

Smartphone-based rich monitoring: Accelerometers are monitored for traffic speed and road quality from smartphones used by drivers. Smartphone audio and GPS beacons are used to identify traffic density and traffic congestion. They have been employed as part of the Nericell Research Experimental System in Bangalore, India.

2.3.2 SCATS Operation Modes

SCATS has different operation modes. They are (i) Master Link, (ii) Flexi Link, (iii) Isolated, (iv) Hurry Call, and (iv) Manual Operation. Depending on the traffic conditions and demand, SCATS can operate on any of these operation modes.

In Masterlink mode is an adaptive control mode. Regional computers determines the sequences and time of the phases based on real-time traffic demand. This mode also controls the timing of pedestrian crossing lights, public vehicle priority light, and

traffic light for trams. Masterlink changes or skips any sequence of the phase depending or the traffic density and demand to make sure the maximum utilisation of the green time. The main purpose of controlling the green phase time is to minimise the stop time of the road users at any red signal. When the phase sequence is determined by the regional computers, local controller make sure that the safety interval times are being satisfied (e.g., minimum green, pedestrian clearance). Once the transition to the new phase is complete, the local controller determines the minimum intervals of a green and minimum walk and waits for a regional computer end-of-phase command. Once the command is received, the local controller decides for the end of this phase (e.g., yellow, all-red) regardless of the distance intervals required. These security configurations prevent communication errors or regional computer failures, which prevent the local controller from displaying hazardous signals on the local controller, such as reduced greens or all red times. The cancellation of pedestrian walk signals is also controlled by the regional computer so that the walk timing can be adjusted according to the conditions of traffic demand.

When regional computer breakdown or communication loss occurs, local controllers can return to Flexilink, time-based coordination. The phase sequence and the length of the walking displays are calculated according to the current plan on a daytime basis. In this mode, local vehicle actuation is still operational. The isolated mode can be used as an emergency operating mode since this mode is used as a backup unless the central connection and the flexible link do not work. SCATS is also available in a preset mode called' hurry call' where the local controller usually enters a pre-programmed mode linked to a local emergency pre-emption phase such as a train or tram phase [14].

2.3.3 Degree of Saturation

The adaptive SCATS 6 is based on a traffic demand measurement, known as the Degree of Saturation (DSAT), which represents the efficiency of road use in that context. Under congested conditions, DS-values greater than unit (insufficient green time to meet request) is produced, and SCATS will respond to this saturation situation quickly. To

keep the DSAT at the fast lane with maximum saturation, the cycle time is increased or reduced by about 0.9. The time for this cycle can be 20 to 240 seconds. The lower limit for cycle time is considered (usually 30 to 40 seconds), and an upper limit (usually 100 to 150 seconds), is specified by the TMS. We can vary Cycle time up to 21 seconds, but this upper limit is resisted unless a strong trend is recognized.

2.3.4 Phase Time

The signal cycle is divided into various phases and is labeled with letters from A to Z. The sequence of the phases can be implemented in any sequence. Any phase, except for that on the most critical road, can be skipped if no vehicle is waiting for the green on that phase (for example if no vehicle is waiting for B phase, B phase is skipped; consequently, the sequence would be A–C–A). The sequence of the phase time is defined by the local controller in Isolated and Flexilink modes. The regional computer determines the sequence of phase time in Masterlink mode [14].

ATSs aim to provide efficient and safe traffic management. One of the most important services is to provide proper incident management service. Brief details of IMS is provided below.

2.3.5 Incident Management System

In this section, we present several intelligent traffic systems, with emphasis on facilitating faster travel by emergency vehicles.

An ITS based on a green wave system using Radio Frequency Identification (RFID) Technology, Global System for Mobile communication (GSM) modules, and high-speed microcontrollers has been presented in [90]. The primary objective of this system is to identify the emergency vehicle and track its location so that the system can provide a wave of green signals to the emergency vehicle by turning the signal light to green when an emergency vehicle approaches it. In this way, an emergency vehicle is assured all green signals on-route.

The system proposed in [90] is based on image processing and uses on-road video cameras to process images to identify emergency vehicles. However, image-based identification makes the system less robust against bad weather and/or poor visibility (windy weather, heavy rain, fog, etc.), making it difficult to identify the correct emergency or stolen vehicle. To address this, RFID based green wave system has been introduced. It uses Atmel's Atmega16 microcontroller along with low-frequency RFID reader (125 kHz) and passive transponders based on EM4102 [91]. RFID based green wave provides better results to determine the emergency vehicle compared to its image processing-based counterpart. This system assumes that, along with emergency vehicles, stolen vehicles are to be equipped with RFID tags. But this will not be able to detect vehicles that have RFID tags attached. The major disadvantage of the green wave is that, when the synchronization of the traffic signal is not maintained, it can generate huge traffic jams (over-saturation) [14].

To reduce the impact of not having proper synchronization, another RFID based traffic control system capable of identifying all vehicles with or without having a RFID tag attached has been recommended. If a vehicle has a RFID tag attached, it is required to identify the vehicle with the analysis of its RFID signal or number plate. In [92], Yang and Lei introduced a vehicle detection and classification system for low-speed congested traffic based on the low-cost triaxial anisotropic magnetoresistive sensor. The work proposed a collaborative traffic information collection, fusion, and storage for smart city traffic systems using a WSN, which provides a better solution by reducing more traffic congestion compared to the current traditional traffic signal systems. It also discussed the incident response model and the way to provide a clear way for an emergency vehicle by making the signal phase time green for one signal ahead. However, this model doesn't address the issue of how the additional congestion will be cleared, which is accumulated due to the signal timing interference created by emergency vehicles. Moreover, it cannot handle dynamic traffic. Traffic light control can be categorized as static and dynamic. Usually, for static traffic lights, the phases have a fixed duration based on historical traffic data. The green time can be varied between the pre-timed minimum and maximum lengths depending on flows. Due to the advent of dynamic

traffic control systems, such as SCATS and Split Cycle Offset Optimisation Technique (SCOOTS), nowadays, many cities around the world use dynamic traffic control systems. As a dynamic traffic control system uses the real traffic condition rather than historical data, this system reduces the response time in an emergency situation better than a static traffic control system. The optimization of real-time response for incident management is derived by using the real-time traffic pattern and as well as their historical data by using the traffic pattern derived from sensing information [14].

Another dynamic traffic monitoring system [93], which optimized the road traffic flow with the aim of meeting the current and future necessities for road travel. This system increases the efficiency of monitoring the road traffic conditions by providing permanent knowledge of the meteorological parameters of different zones. Even though it improves congestion conditions in the future, but doesn't consider traffic signals to the vehicles and vehicle to vehicle communications.

To assign a lane to a particular way based on specific traffic conditions, authors proposed a novel fixed threshold state machine algorithm based on signal variance to detect vehicles within a single lane and segment the vehicle signals effectively according to the time information of vehicles entering and leaving the monitoring area. The results show that the proposed algorithm can detect up to 99.05% of vehicles accurately, and the average classification accuracy is 93.66%. However, the effectiveness of this algorithm depends on the condition of the vehicle signals and the value of a manually selected threshold. To overcome these limitations, an RFID-based technique has been proposed. For this, the quick accident recovery and response using RFID have also been articulated in several research projects [94] [95]. They proposed to install RFID tags and readers to the ambulance and the traffic system, respectively.

When an ambulance approaches a traffic signal system, the RFID reader reads the RFID tag and then turns the traffic signal to green for an emergency vehicle. The process of finding the quickest path for the emergency vehicle has been reported in a recent project described in [96]. However, it was not clearly mentioned, if an emergency vehicle approaches a traffic signal without having any emergency whether the signal light

remains green. In real-life situations, emergency vehicles do not have any priority if they do not have to respond to any incident recovery.

With the increased use of wireless technologies in ITS, the traffic system is becoming vulnerable day by day. The next section will discuss the security issues in ITS.

2.4 ITS Security Issues

The successful deployment of an ITS in real-world applications requires diverse security requirements to ensure secure communications within ITSs yielding safe driving [97] [98] [99]. The communication platform of ITS are mainly wireless; entities can be highly mobile and uses low powered computing system. The major characteristics of the network in ITSs are given below:

- High Mobility - the nodes move at high speeds in the VANET network, affecting the determination of their position, real-time critical information distribution, and making more complex security and privacy issues.
- Dynamic network topology – the nodes are mobile in nature, and the speed of vehicles is changing according to the traffic conditions, making the dynamic and unpredictable wireless network topology. Dynamic wireless network topology is influencing security issues and makes it hard to find nodes misbehavior in the network.
- Network coverage – affects the availability of the wireless transmission medium. VANET networks can be deployed for a city, several cities, and main traffic lines in the area or the whole country. Since it is wireless communication, dedicated Radio-frequency bandwidth, transmission power, and propagation delays caused by Doppler Effect, multipath reflections, and other propagation losses affect the coverage.
- Frequent information exchange - since the VANET is a generic Mobile ad-hoc Network (MANET), nodes are exchanging information continuously between the

vehicles and also roadside units (network infrastructure elements). The VANET nodes have no issue of energy, computing capacity, or storage failure. The available throughput in wireless communication is influencing service availability and the need for frequent information exchange between fast-moving nodes.

As alluded before, because of the high-security threat expected for autonomous vehicles, a number of attacks on self-driving cars have already been reported in the recent literature. These attacks are described in the following section.

2.4.1 Recent Attacks On Self-Driving Cars

Since the beginning of self-drive tests, there have been many various types of attacks on individual units of a car. Some of these include; the internal unit, the Lidar, the GPS, the AU and thrusters, and the alert messages. Several incidents have been reported up until now. These include incidents in which a vehicle could not plan a safe movement sequence to navigate in confined spaces. Garcia et al. [86] have demonstrated that almost 100 million Volkswagen vehicles sold from 1995 to 2016 are vulnerable to remote and unlocked hacking. Volkswagen vehicles are dependent on several global keys to recover from ECUs. Thus, the attacker can clone a remote Volkswagen control, which allows unauthorized access to the car through intercepting a single signal from the original remote control. Through vulnerabilities in the mobile application Nissan Connect, which controls electric vehicles from Nissan Leaf, attackers took control of the heater of the vehicle. They turned it on repeatedly to discharge the battery. This occurrence forced Nissan to disable the request [100].

An attacker within the Wi-Fi range has enabled SmartGate to steal car information in the car Skoda [101]. Additionally, from the SmartGate system, the attacker can block the car owner. In 2015, Chris Urmson, director of the Google Self-Driving Cars project, said that if "the program sensed an anomaly somewhere in the network that could have potential security consequences, it immediately passed vehicle control on to our test driver" [102]. As mentioned in Table 2.1, the autonomous vehicle of the BMW 7 series

could not be parked in a parking lot because the hacker had taken control of the car, making it hit.

2.4.1.1 Attack On GPS

With a precision level of one meter, GPS provides absolute position data. GPS is an open standard available in the public domain; however, coded signals are utilized in limited GPS systems such as GPS systems for the military. GPS is universal, but malicious signals can easily be generated to annoy and block a GPS device (interference, spoofing) because of its transparent architecture. GPS spoofing is a rather complicated process involving the generation of incorrect GPS signals to confuse GPS receptors. An attack by spoofing will, for example, start with the transmission of signals synchronized with the correct signals found in the target recipient. The strength of the phishing signals is increased, and the position is changed from the target progressively. GPS units are usually programmed to use the highest signal because this signal is probably more reliable in an ideal world. This sounds relatively straightforward in principle; however, the hardware required to generate realistic signals is a complicated operation. As the potential benefits of GPS spoofing increase, the generation of simplified plugs and play controls will become a reality. The public domain already holds a complete theory on how to spoof GPS attacks. For example, the literature on successful attacks has been published [103].

Currently, however, the literature only contains examples of "proof of concept" attacks. For example, students at Texas University in 2013 showed how false GPS signals could be generated, which overloaded GPS signals progressively in their theses and thus deviated the path of a superyacht. The superyacht control reacted then by warning the crew of the position deviations to change the GPS signal and started correcting it by setting a new course. The device used for that attack was developed and is the only GPS forgery reported in the public literature capable of accurately generating fake GPS signals, as Humphreys and his collaborators acknowledged themselves [104]. GPS use should be redirected to a large scale or stolen for activities such as high-value vehicles or

vehicles carrying goods. Since GPS has been developed as an open standard technology, research has been carried out to develop GPS counterfeiting measures. Numerous simple validation mechanisms can be implemented to prevent spoofing attacks. Monitoring identification codes, satellite signals, and time slots, for example, may help detect attempts at spoofing. O'Hanlon et al. [105] explains in detail how approximately 163 decibels of signal strength can be observed. A GPS simulator, such as the one developed by Humphreys et al. [106], would provide several magnitude orders more significant than the signal strength of any satellite on Earth's surface. GPS signals can also be monitored so that their relative change is within a threshold. O'Hanlon et al. [107] also discuss whether a GPS signal is monitored to verify that its forces vary according to expectations and that they are not perfect. However, if the attack is sufficient to make its sophistication authentic, the validation tests will fail, and the GPS device will be usurped. It is widely accepted that spoofing will be stopped only by the military-level encryption [106].

2.4.1.2 Attack On Warning Messages

It is essential to make sure that the safety of Vehicle to Vehicle messages, particularly data legitimacy and dependability due to the messages' nature exchanges in V2V communication (for example, acceleration, velocity, and position) because they are safety-critical. To ensure that the data content's legality is ambiguous and it is not possible to do it traditionally, although source authenticity message veracity can be guarded by cryptographic means. Harsh effects will include undermining the advantages of V2V communications if false data is received from another car. A dangerous circumstance can occur. For example, crashing accidents from the rear end can occur if, for instance, recent studies [34] [108] prove that in a CACC setting, feeding false data to a wireless conduit can cause a malevolent car to increase or reduce the speed of other vehicles incorrectly.

It is imperative to make sure that cars sense and filter data from other motor vehicles, given that a linked car's decision-making process much depends on the received V2V messages. When drafting a trust framework for secure V2V data authentication, many

challenges are present. Cars should be able to detect false messages and approximate the true states in real-time as the attackers may feed incorrect data from another car at any given time. Detection of untruthful data should be done in a manner that is confined and decentralized as a substitute for depending on national infrastructures to gather universal information such as the trusted roadside components. With the number of surrounding vehicles being small and the possibility of collusion, we cannot presuppose a candid, more significant part of the one-hop area of a car. To sum it up, since not all cars are fitted with highly developed detectors like radars, which are costly, the solutions are going to cost less. In VANETs traditional trust framework cannot gratify the suitable requirement without responding to every message in real-time since they are only needed to assess the long term trust of the other fellow vehicles. A Mitsubishi Outlander PHEV was hacked, and the investigators of safety at Pentest Partners executed a man in the middle attack to know the one responsible between the PHEV's cell phone application and the Plug-in Hybrid Electric Vehicle Wi-Fi AAP. They were able to find out the binary protocol that was used for messaging after repeating the different messages from the mobile app. The attackers were able to switch on and off the lights, immobilize the entire burglary alarm system, thus making the car at risk of more attacks.

Table 2.1: Recent attacks on self-driving cars

Name of the attack	**Exposed vulnerability**	**Impact**	**Type of attacks**	**Mitigation approach taken by manufacturer**	**Violated security requirement(s)**
Attacks on AV software [109]	Software flaw (Weak message propagation algorithm)	Sensitive information leakage	Malware (Bug)	Updating antivirus and sandbox approach	Availability /Authentication

Continued on next page

Table 2.1 – *Continued from previous page*

Name of the attack	**Exposed vulnerability**	**Impact**	**Type of attacks**	**Mitigation approach taken by manufacturer**	**Violated security requirement(s)**
Attack on OBU [110]	OBU vulnerability on Lane Change Unit	Unauthorised manipulation of routing table	Jamming attacks on OBU	Frequency hopping and multiple radio transceivers	Availability
Speed control of Tesla from outside [111]	Vehicular hardware flaws of speed control sensor	Disclosure of sensitive information	Sensor impersonation	Implemented performance monitoring system	Authentication
Google car hacked [112]	OBU's what component vulnerabilities and sensors malfunctions	Network flooding with wrong information	Bogus information	Elliptic Curve Digital Signature Algorithm (ECDSA)	Authentication /Integrity
Attack on GPS [113]	Software flaws and weak password	Sensitive data leakage	Social engineering-based	Encrypted and strong password for message communication	Integrity /Privacy
Jeep was remotely controlled by hackers [114]	Ethical hackers accessed the vehicle remotely	Tricked sensors to sense false data	Remote access	Access control and redesign the cars to make them robust against cyberattacks	Authentication

Continued on next page

Table 2.1 – *Continued from previous page*

Name of the attack	**Exposed vulnerability**	**Impact**	**Type of attacks**	**Mitigation approach taken by manufacturer**	**Violated security requirement(s)**
Ignition auto-start – Benz [115]	Wireless-enabled OBU vulnerabilities and thus insecure wireless communication	Revelation of an user's identity	Attack on privacy	Holistic approach for data transmission	Privacy /Authentication
Attack on wireless-enabled OBUs [116]	Insecure wireless communication channel	Messages alterations	Impersonation	Identity-based batch verification scheme	Authentication
Driver losing steering control [117]	Non-encrypted messages and insecure wireless communication channel	Injected false messages	Man-in-the-middle (MITM)	Strong cryptographic techniques	Availability /Confidentiality
Incorrect GPS location [113]	Flaws in routing table and non-encrypted messages	Data leakage on back-end wired channel	Sybil	Position verification of neighbouring nodes, VANET PKI [118] and RobSAD [119]	Authentication /Availability

Continued on next page

Table 2.1 – *Continued from previous page*

Name of the attack	**Exposed vulnerability**	**Impact**	**Type of attacks**	**Mitigation approach taken by manufacturer**	**Violated security requirement(s)**
Unable to control brake [120]	Hardware vulnerabilities	Message alterations en-route to other vehicles via RSU and CTC.	MITM attacks between RSU and CTC.	Strong cryptographic techniques	Confidentiality /Availability
Attacks on ECU [107] [121]	Vulnerable ECU software	Control Vehicle components remotely by reprogramming ECU software.	Remote Access	Update system software	Authentication
Attacks on UConnect system [116, 122]	Security issues with third party software and vulnerable to data injection.	Taking on board unit operational control from driver or car remotely.	Unauthorized Access	Change firmware settings.	Authentication /Data Integrity
Malicious data to Controller Area Network (CAN) bus [123] [124]	Compromising security keys used by ECU	Several OBU stopped functioning or started malfunctioning.	Unauthorized remote access.	Controlled OBUs remotely	Availability /Non-Reproduction

Continued on next page

Table 2.1 – *Continued from previous page*

Name of the attack	**Exposed vulnerability**	**Impact**	**Type of attacks**	**Mitigation approach taken by manufacturer**	**Violated security requirement(s)**
Attack on Mitsubishi Outlander [125]	Messaging protocol is not secured.	Turn on and off light, disable anti-theft alarm.	Man in the middle alarm	Update firmware and messaging software.	Availability /Confidentiality
Attack on Volkswagen keyless entry system [86]	Global master key information retrieved from ECU	Able to gain unauthorized access to many Volkswagen cars	Eavesdropping	Update master key information.	Authentication /Data Integrity
Attack on Nissan Leaf cars [100]	Vulnerable Nissan Connect application.	Able to drain the battery of the car which makes car stopped middle of the road.	Unauthorized access.	Nissan disabled the application	Availability /Non-Reproduction

2.4.1.3 Attack On OBUs

Lidar technology can generate 3D maps of environments quickly, enabling the creation of a 3D computer model. This model can be used to identify objects and trajectory routes. However, as there is no guarantee that the 3D model built is correct, it opens the door to attacks, including spoofing, hacking, and jamming with cheap hardware. This technology has proven to be a useful aid in autonomous vehicles. There are wave-length mitigation techniques that try to reduce the risk of jamming and identity theft through the use of commercially available laser devices and increased hardware required for

the attack. The use of V2V communication to share collaborative measurements [126]is another mitigation mechanism. Such a connection with V2V can, however, lead to false measures outside the compromised vehicle. Another, perhaps more feasible solution is a random analysis to make it difficult to synchronize their laser at the correct frequency since this allows the device to change the interval of the frequencies repeatedly [127].

If attacks happen on a monitoring unit of a self-driving car, they will have less or no time to notify the driver to take control and run the vehicle in manual mode. This is an area that is relatively unexplored, and there is an absence of literature informing on how vehicle safety measures can intervene and prevent cyber-attacks. The volume of literature on attacking and compromising vehicles indicates the absence of robust cyber-specific control mechanisms and safe-mode. There is a lack of research detailing how the vehicle or driver may react upon detecting a potential cyber-attack [128]. Will a vehicle have a safe mode in which the vehicle can enter to ensure that a safe level of control can be maintained? Furthermore, if a vehicle could detect that it has been compromised, how would it pass control back to the driver with enough information for the driver to quickly make sense of the situation?

AU comprises many important applications, including remote vehicle diagnostic applications. Therefore, an attack on AU can lead to manipulating the detection of the safety defect of a car. Mostly, password and key attacks happened on AU [129–131]. Based on the recent attacks described above, the following section presents the countermeasures that have been taken or need to be taken for the types of attacks that happened or could happen in the future on the self-driving cars.

Researchers at the University of Michigan [35] have found that systemic weaknesses in traffic control systems make them vulnerable to attack. Those weaknesses include the use of unencrypted wireless signals to control the lights, the use of default usernames and passwords on these control systems, and a vulnerable traffic controller that controls the lights and walk signs. Some of the possible attacks that can happen in ITSs are described below.

- **Denial of Service (DoS)**: VANET provides communication between (1) nearby vehicles and (2) vehicles and nearby roadside equipment. VANET is one of the

prime targets of the DoS attacks nowadays. In VANET, the attackers use jamming communication channel, network overloading, and packets dropping to perform DoS attacks. DoS attack to the computing systems of the traffic controller can happen from multiple sources. DoS to a single system from multiple sources is called DDoS [132].

- **Sybil Attack**: VANET supports the services associated with drivers' safety, such as the information transmission between vehicles, the rear-end collision between vehicles, and the warning about dangerous situations in real-time. In a Sybil attack, a compromised node claims multiple identities to misguide other nodes in that network by providing misleading or incorrect information. In a Sybil attack where an attacker or malicious node sends false or misleading information to the nearby nodes or Sybil nodes, as shown in Figure 2.7. This information can be false incident notification, incorrect road work notification, or misleading traffic congestion information. The purpose of this attack is to mislead the nearby vehicles in VANET [20]. Many literature researchers correspondingly focus on Sybil attack detection. Golle et al. [133], devised adversarial parsimony as a heuristic approach. It was a new solution for the Sybil attacks. Its intention was towards the detection of Sybil attacks on a vehicular network. It informally translates to the discovery of the most preferred explanation to corrupted data received. After the improvement of the capabilities of the nodes' sensors, like using the light spectrum and the cameras to exchange data, it is possible to determine the existing nodes. The collected sensor data is applicable in reaching the information that will assist in distinguishing the nodes. Figure 2.7 represents a basic scenario of a Sybil attack. After the vehicles exchange information, a heuristic mechanism in place will detect any inconsistencies that might result from a Sybil attack. It is through the comparison of the data received to the maintained VANET model on each vehicle. The mechanism acts as a reference to all the VANET knowledge. The detection mechanisms, however, neither have an in-depth explanation nor simulation support.

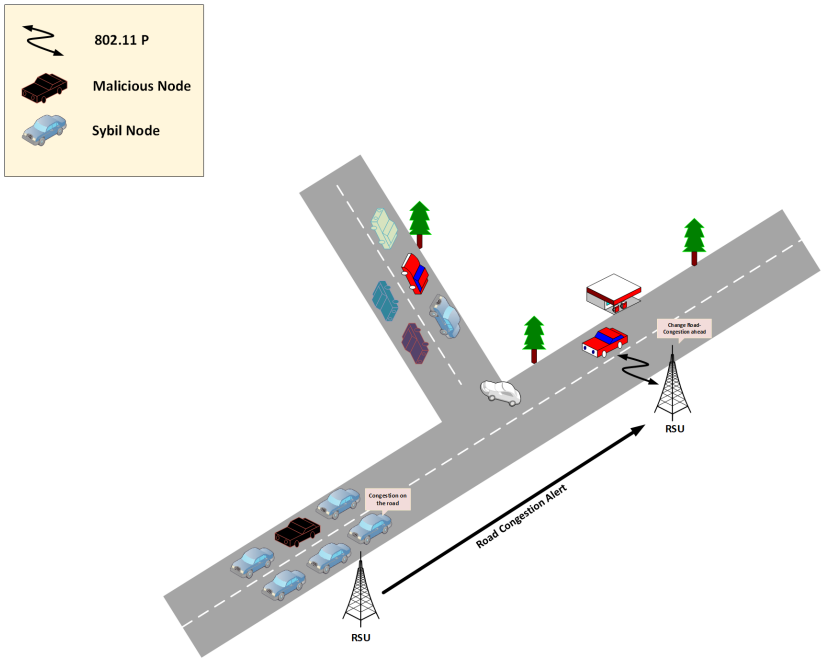


Figure 2.7: Sybil attack

- **GPS hacking**: GPS is not only used for general transportation but also extensively used for navigation of robotics such as driverless cars, drones, and industrial robots. An ITS has lots of automated cars, self-driven cars, drone ambulance and traffic controller that depends on proper GPS signal to locate an incident place and the quickest route. If GPS is hacked, hackers can divert an emergency vehicle to a different destination [104] [105].

2.4.1.4 Major Reported Incidents

Table 2.1 shows different types of major attacks reported in different ITSs, their dates, duration, affected ITS Units, and possible losses. The authors found that data spoofing attacks are highly effective for the signal control algorithm with the default configurations in the Intelligent Traffic Signal System (I-SIG) used by the U.S. Department of Transportation. The spoofed trajectory data from one single attack vehicle is able to increase the total delay by as high as 68.1%, which completely reverses the benefit of

using the I-SIG system (26.6% decrease) and cause the mobility to be even 23.4% worse than that without using the I-SIG system [41]. A major artery in Israel's national road network located in Haifa suffered a cyber attack that caused serious logistical problems and hundreds of thousands of dollars in damage. The tunnel which was under attack is a strategic thoroughfare in the third-largest city of the country. The attackers used malware to hit the security camera apparatus in the Carmel Tunnels toll road on Sept. 8, 2013, to gain its control. The attack caused an immediate 20-minute lockdown of the roadway. Attackers shut down the roadway again during morning rush hour. It remained shut for eight hours, causing massive congestion [134],

As mentioned before, I2V or V2I and V2V communication systems are being used in VANETs. Vehicle collisions, road accidents, reliable safety messages (e.g., weather conditions, road works, road hazards) transmission, and safe driving of self-driving cars are some major concerns of VANETs. These concerns indicate for reliable transmission and driving. The security of VANETs is a critical issue, which can be addressed by measuring the trustworthiness of the different aspects of VANETs. Such a trustworthiness measure is described in the following section.

2.5 Trust Management

The trustworthiness measure in a VANET has been mainly done in three ways by measuring the value of the: (i) Entity-centric trust, (ii) Data-centric trust, and (iii) Combined Trust.

2.5.1 Entity-Centric Trust

To assist road users with reliable and real-time information, ITS heavily uses GPS devices to gather data such as speed, location, road car density, and road condition with the support of service providers (for example, Google Maps, road authority like VicRoads in Victoria, Australia). The focus of Entity-centric trust is to model vehicle trustworthiness with the aim of analyzing their behavioral attitudes. So far, in the

literature, the entity-centric trust uses the only GPS in terms of an entity. This usually identifies the malicious or corrupt vehicles to make sure a reliable collection and message delivery between peers. It was observed that enabling GPS trust is one of the main issues in providing secure routing for data delivery in VANETs. The entity-centric trust model is used to collate the trust value based on direct interactions between vehicles and other relevant recommendations provided by others. The author in [135] proposed the use of a watchdog algorithm with techniques to detect interruptions in establishing trust management. The watchdog algorithm is sent to neighboring nodes to monitor them with IDs. The value of trust is then recorded in a trust table. The major drawback of this technique is information overload on the network. If a node has many neighbors, it will be forced to store a lot of data about all the neighbors.

Cong et al. [136] introduced an approach to establish the trustworthiness based on reporting incidents in VANETs communication. The authors used a simulator called GrooveNet to record the details (e.g., time, location, severity, duration) of the incident-based on the report of RSU. These details of the incident are then compared with the vehicle sensors (e.g., radar, camera, Lidar) based on the detection diameter. The trustworthiness of the vehicle is measured by the crowd information in the V2V and V2I network. This work did not consider the trustworthiness of the individual component of the vehicle and also didn't did consider the normal behavior of the traffic condition without the incident. Zhou et al. [135] proposed the establishment of a dynamic trust token for co-operation among nodes using a watchdog algorithm. The author described that a node could behave abnormally in four different ways. First of all, a node can behave normally for a long time and gain trustworthiness and then start behaving abnormally, secondly, the node can behave differently to different other nodes or sensor, the third one is the node will report a malicious node as normal node, and finally, node can be under Sybil attack, where the compromised node is under control of the attacker. The authors measured the trustworthiness of the node in three different ways. Firstly they calculated the trustworthiness of the node based on the past behavior of the node. Then they calculated the trusted accuracy of the node by determining the information loss while transferring a message from one node to another node. Finally, the trust

robustness was calculated based on the performance of the node while there is an attack on the network. Even though there was a dynamic trust token is used to calculate the trustworthiness of a node, the simulated WSN was static. This work needs to be tested further in a highly mobile network like VANET.

Trust and Reputation Infrastructure based Proposal (TRIP) algorithm for traffic analysis was introduced by Marmol et al. [137]. This approach aimed at identifying malicious vehicles spreading bogus information in the network. A traffic warning message is normally sent to a vehicle in the network to check its trustworthy value using the Fuzzy logic. However, it is hard to track the trust value and behavior of all nodes, and thus, at times, malicious nodes go scot-free.

In measuring the trustworthiness of GPS vehicle data received from VANET, there are many techniques to choose from. These techniques are divided or classified into two categories:

(a) **Centralized:** In the centralized technique, a central unit is used to control the entire VANETs like that of trust management. Wang et al. [138] introduced a module called misbehavior detection module used for the eviction of faulty and misbehaving vehicles so as to improve the trust level in VANETs [139].

(b) **Distributed** In the distributed scheme, VANETs uses V2V interaction to compute and update trustworthiness in another vehicle. Wang et al. [138] used a single interaction in vehicles for trust management, but that may lead to a false alarm. False alarms are verified using the data from other vehicles, central traffic, and RSUs controller information. The inability to identify false information earlier will cause congestion or accidents.

2.5.2 Data-centric trust

Data-centric trust, also known as event-centric trust, is used to determine the trustworthiness of the information relating to events like accidents, detour, and traffic congestion (e.g., warning alert) as well as identifying the false information in VANETs. From reviews [140]- [141], transmitting reliable and secured data is one of the vital and main

concerns VANETs applications, while trusted safety and updated data with location information are vital to efficient traffic management. It is evident that data are dynamic in nature. The available data-centric trust models are mainly defined based on the type of event. The number of reports obtained for the same event and the type of event is considered to measure trust for this type of trust model. Though the above indicates that data are vital ITS, it is very hard to know whether the received data are trustworthy or not from only one message [142].

Majority Voting [143] uses the principle of majority voting to measure the trustworthiness of the data. Most Trusted Report [144] calculates the trustworthiness of data based on the maximum trusted value from the trusted report. Weighted Voting [143] method takes the maximum vote but also considers the weight of the vote and then calculates the trustworthiness. Bayesian Inference [145] takes the posterior probability and different evidence for the same event to measure the trustworthiness. DST calculates the trustworthiness based on human reasoning, considering the uncertainty of the event.

Raya et al. [146] used the weighing method to calculate the trustworthiness of the data. They have used the data-centric method by collecting different pieces of evidence and weighed them differently to measure the trustworthiness. Wu et al. [147] used the RSU and the self-driving car sensors to measure the trustworthiness using V2I communication to collect data. The authors have calculated the number of sensors available in the vehicle, their sensing power, and then weighted the trustworthiness according to the capability of the self-driving car to monitor the data they are transmitting. Ding et al. [148] classified different vehicles into different groups. Each group of vehicles was provided with a dynamic role for transmitting different types of messages. They have shown that this classification can reduce the number of false or incorrect information.

Since the trust of a vehicle depends on both data and node trust, to improve the reliability of the entity and the data transmitted by that entity in VANET, the combined trust has been introduced.

2.5.3 Combined trust

With the combined trust, there is a wide usage of trust of an entity to assess the trustworthiness of the information and uphold the trust of the entity over time. It is well-known that data's trust evaluation depends on entity trust. Other peer nodes in the same VANET confirm the trustworthiness of the data. With the available trust models in this category, entity, as well as data, trusts frequently interrelate with each other. RSU and the beacon-based trust management models create entity trust by intensely examining the credibility of event messages and beacon-based messages. These models can prevent internal intrudersfrm by transmitting the manipulated message. Presently, there are very few combined trust models available for VANETs [138].

There exists a trust management scheme using three aspects [149] [150], namely: social network impact on the network, policy control, and proactive trust establishment. The social aspect deals with the opinion of the nearest nodes/vehicles so as to set trust among each other. The policy aspect deals with data entry trust attributes. Proactive trust deals with the communication history to determine the trust value.

Even though ITS will have great potential in the near future, there are many open research challenges and issues that need to be addressed to deploy effective and safe ITS operations. The limitations of the existing literature and the research challenges are given below:

2.6 Limitations of Existing Works and Research Challenges

Below we outline the limitations of the existing ITSs highlighting the research challenges.

1. **Incident-Based Emergency Vehicle Priority**: There exist many IMSs (refer to 2.3.5) to detect the incident place, provide a safety warning message to the road users, and send incident recovery vehicles to the incident place. None of the IMS is designed to provide incident management service based on the type of incident. Detecting the type of incident will allow the traffic control system to send the

proper EV to the incident place to clear the incident place and restore normal traffic conditions inefficient way.

2. **Communication Between Emergency Department and Central Traffic Controller**: The communication between different emergency departments and the central traffic controller during the incident time is very important. Existing systems and proposed methods in literature do not address the issue. For proper and quicker routing for EV, provide the real-time traffic and incident condition, there needs to be proper communication method between the emergency vehicles and the traffic controllers.

3. **Selection of Green Signals**: Existing emergency vehicle priority systems described in [11] provides a green wave to an emergency vehicle once the emergency vehicle comes close to the traffic signals. These systems do not consider the real-time traffic conditions while providing priority to the EV. It is important to consider the density, traffic flow, and the magnitude of the incident to reduce the waiting time for other vehicles using the road.

4. **Crash Detection**: Monitoring real-time traffic condition and type of the incident will be very beneficial to detect the incident early, and monitoring the incident continuously. There is an existing model in ATSs to monitor the incident place, where there exist road safety cameras. Further research can be done to extend the monitoring by sending cameras using a drone or using the cameras of autonomous cars.

5. **Intrusion Detection in ITS**: Though reported attacks on ITS currently are limited to attacks on computers in the traffic controller, safety cameras installed in the RSU, and processing units installed in the signals of the intersection, undoubtedly such attacks will be on the rise in the future. There are no IDS found in the current literature to detect attacks on traffic signal units and ITS in general.

6. **Driving Behaviour Analysis**: As the real-time traffic condition can vary for many reasons, determining the normal behavior of traffic is a very challenging task. The

traffic flow is dynamic and complicated, therefore predicting the traffic information about it is one of the most complex and resource-demanding elements of the traffic control system. Several works have been done [7] [69] to predict human driver behavior. The further research scope is there to predict the behavior drivers and vehicles in the co-existence of self-driven and human-driven vehicles.

7. **Intelligent Congestion Management Using Probe Data**: Several GPS companies are using probe data to get real-time traffic information and providing an alternate route for vehicles. Currently, the central traffic controller depends on the RSUs and inroad sensors to receive traffic data. TMSs can use the probe data to manage an inefficient congestion manner. The main challenge to use probe data is to validate the accuracy of the provided information.

8. **Using OBUs of Self-Driving Cars to detect Intrusion**: Several studies have studied individual vehicles, but the whole ITS is not only about vehicles. ITS has vehicles, roadside infrastructures, road sensors, and OBUs. There are many reported attacks on individual OBUs, as described in Table 2.1. Many instances of hacking OBU components of a vehicle have been reported, and this emphasizes the pressing need to measure the trustworthiness of OBU components and overall vehicle for safe driving.

9. **Uncertainty Due to External Factors**: The road conditions, with all their stability, have unpredictable factors, both in terms of weather-climatic parameters deviations and in road parameters. It is an important but big challenge for the researchers to measure the trustworthiness of a self-driving car or the traffic control system using information from the sensors in OBUs and RSUs considering the uncertainty of the traffic condition.

2.7 Conclusion

In this chapter, we present mainly the state-of-art of the different components and their contemporary approaches and the main applications of an ITS. Different traffic modeling

techniques used to evaluate the performance of traffic systems. A review of different attacks of ITS and self-driving cars is performed. Techniques used to protect ITS from external attacks also been investigated. The trustworthiness measure of autonomous vehicles is explored and articulated in this chapter.

From the investigation of these approaches, many further research challenges are identified. Some of these research challenges are chosen to fulfill the research objectives presented in Section I-V (Chapter 1). The possible solution for these selected research challenges will be presented in the next three chapters.

The next chapter will introduce a smart ITS to provide priority to EV considering the type of incident and the impact on the other vehicles surrounding the EV travel path to the incident place.

Chapter 3

A Smart Priority-Based Traffic Control System for Emergency Vehicles

From the literature review (Chapter 2), we have observed that there have been many ITSs presented in the literature to provide one green signal ahead of an ambulance for its quick travel. The current ITSs consider emergency vehicles as one type without differentiating them (e.g., ambulance, fire service, police) or priority levels of their services in relevance to an incident type.

In most major cities or states, emergency services usually have a strict target response time and QoS requirement. Congestion can severely hinder their response time and QoS. For example, in Victoria, Australia, the average actual response time of the 90^{th} percentile is much higher than the targeted one [25]. Traffic congestion affects not only the response time, but it can also become life-threatening when emergency vehicles fail to reach the incident place within time, as dictated by the severity of the incident.

To address the issue mentioned above, in this dissertation, we frame a research objective (OBJ1) in Chapter 1. To achieve this objective, we introduce an Emergency Vehicle Priority System (EVPS) in this chapter. The proposed EVPS determines the priority level of an EV based on the type and the severity of an incident and estimates the number of signal interventions while considering the impact of those interventions on other associated on-road traffics. We present how EVPS determines the priority code, and a new algorithm to estimate the number of green signal interventions needed to

provide an EV quickest travel path and reduce the impact on the other on-road vehicles accumulated in the surrounding of that travel path. To analyze the vehicular traffic flow interrupted by incidents, we developed a simulation model with a real map in SUMO [38] and real-time traffic data [151]. We used five different occupancy rates (0, 30, 50, 70, and 100%) to validate the efficacy of our proposed EVPS. Simulation results show that EPVS can reduce both the emergency vehicle response and clearance time with its selected number of signal interventions.

The organization of the chapter is as follows. Sections 3.1 provides the fundamental components and their logical connection to our proposed model. Section 3.1.1 presents the steps to select the priority code, while the calculation of the appropriate number of signal interventions is given in Section 3.1.2. Section 3.2 outlines the simulation setup. The performance of our proposed method based on the simulation results is provided in Section 3.3. Finally, Section 3.4 concludes the chapter.

3.1 Proposed Emergency Vehicle Priority System

Reaching the destination as fast as possible in case of emergency results in the reduction of risks to lives and possessions so that critical conditions can be attended in time and adequately by mobilizing required resources. Even though various research works propose different approaches to give a green signal or a clear pathway to emergency vehicles, they assume that only one emergency vehicle is coming from one direction. Most research projects provide priority to an ambulance the only [11]. In real-life scenarios, in most cases, police stations, fire service offices, and hospitals are not located at the same or nearby place. In case of a fatal accident, emergency vehicles of these three departments generally need to attend the scene through the different paths from different locations. The existing models available in the literature only provides one green light to an EV as the vehicle advances. The incident information, including its type and severity, current traffic congestion, and time (e.g., peak, off-peak), need to be considered to provide efficient incident management service. To provide proper priority to the appropriate vehicle based on the current traffic condition (e.g., density,

flow rate, incident type), we propose an emergency vehicle priority system. Traffic on road changes dynamically depending on the travel time such as peak and off-peak and the occurrences of incidences. To manage such a dynamic system, the followings are needed:

- Estimating the type of incident occurred.
- Collecting information about the incident and storing that into a dynamic traffic controller.
- Gathering information about the current traffic condition.
- Determining the priority level of emergency vehicles considering the type and information of the incident.
- Depending on the priority levels and existing traffic conditions, the controller calculates the optimal route and sets the appropriate traffic light signals along and other relevant roads.
- The controller brings all signals back to normal operation after receiving confirmation from an emergency vehicle that the incident has been cleared.

The basic operating principles of our model are depicted in Figure 3.1. This process starts when an incident is reported to the emergency control room. The emergency control room receives the information (e.g., place, type, number of cars involved, type of injuries) about the incident. If there is not enough information to determine the priority, more information is requested. If road safety cameras are operating near the incident place, road authority and the emergency control room can have additional incident information from them. Once the emergency control room receives sufficient information about the incident, the priority code is determined, which is shown in a process called "Determine priority code." The priority code determination process is described in Section 3.1.1.

After generating the emergency code, the emergency control room sends the information to the central or regional traffic controller. The traffic controller then sends

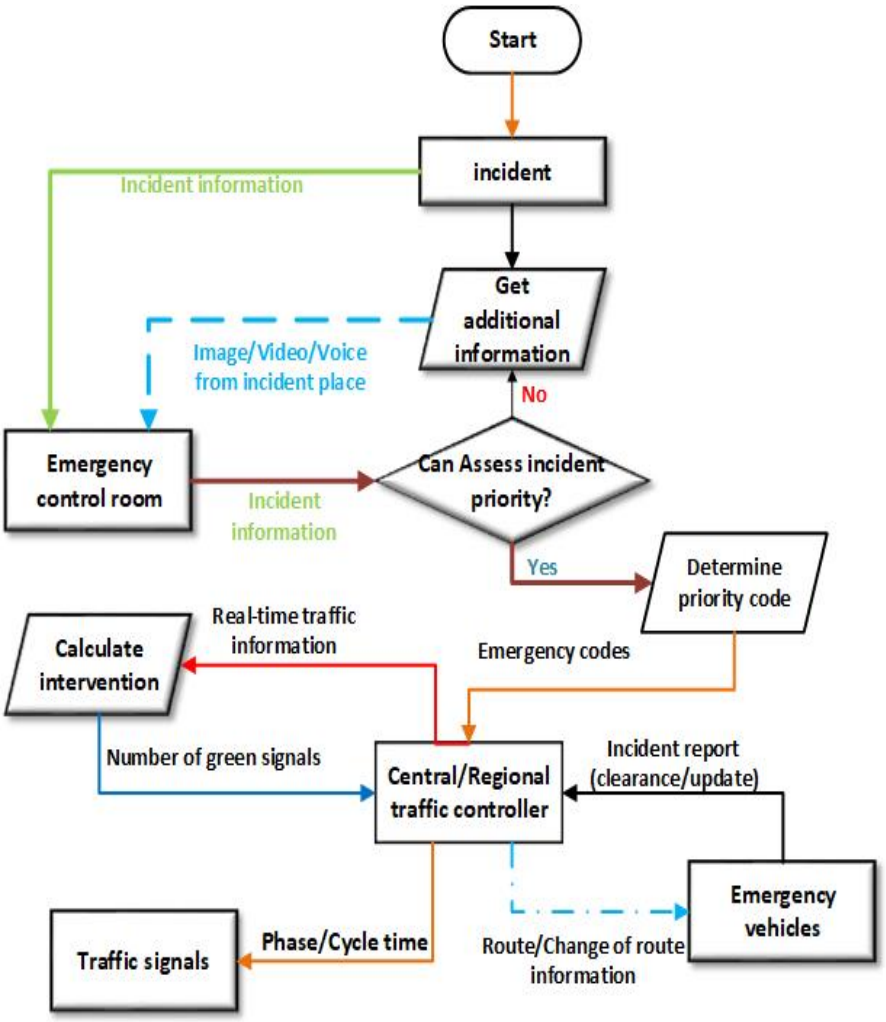


Figure 3.1: System flowchart for our proposed Emergency Vehicle Priority System (EPVS)

real-time traffic information (e.g., flow rate, congestion level, incident location) to a process, namely "Calculate intervention," which uses Algorithm 1 to determine the number of signals needs to be green considering the time required to clear the incident place. Algorithm 1 is detailed in Section 3.1.2.1.

The central traffic controller then sends the route information to the EV, regional traffic controllers, and traffic signals. The regional traffic controller maintains the cycle time of the traffic signals as requested by the central traffic controller for the EV. Traffic signals also adjust the phase time of the signals as requested by the central traffic

controller. The EV follows the route information provided by the central traffic controller. Once the EV reaches the incident place and incident place is cleared, the EV sends the information to the central traffic controller. Central traffic then sends the information to the regional traffic controllers and the traffic signals to restore the phase time and the cycle time to the normal operational mode.

3.1.1 Priority Code Selection

The model generates priority code (e.g., Code A, Code B, Code C) considering the type and severity of an incident. Three specific scenarios having a separate header with the scenario for Codes A-C are shown in Figure 3.2. The interpretation of these scenarios to determine the appropriate priority levels for an emergency vehicle is as follows:

For Code A, an ambulance is assigned Priority 1, while a fire service and police vehicles are assigned Priority 2 and Priority 3, respectively. This is because an ambulance needs to reach the site first to assist patients immediately, and then the police can reach the site for incident reporting, and if requires (e.g., for removal of the oil spill or fire hazard), fire service vehicles will render its service. For Code B, a fire service vehicle has Priority 1, as without handling the fire, paramedics are not able to reach or assist the injured persons. A scenario like this may arise in case of accident vehicle caught fire, and the passengers/driver are stuck inside. For Code C, a police car receives Priority 1, and an ambulance and fire service are given to Priority 2 and Priority 3, respectively. Examples include incidents involving crowd control issues, such as a fight between groups where police car needs to go there first to clear crowd for an ambulance. Based on other different incident scenarios (e.g., flood, bush fire, bomb threat, and suicide threat), other emergency codes can be generated, and an emergency code database can be updated.

After having the code information from the emergency control room and setting them in the system, the central traffic controller uses the code for resetting all relevant traffic signals phase time around the incident place. The central traffic controller monitors the incident, and if needed, changes the traffic signals or an EV route according to the current traffic condition, which is presented in the following section.

	Scenario for Code A	Scenario for Code B	Scenario for Code C
Life Threatening Medical issue	YES	YES	YES
Fire Threat	YES	YES	YES
Fire preventing access	NO	YES	NO
Crowd Control needed first	NO	NO	YES
Priority 1	Ambulance	Fire Service	Police
Priority 2	Fire Service	Ambulance	Ambulance
Priority 3	Police	Police	Fire service

Figure 3.2: Sample Priority Code

3.1.2 Calculating number of interventions

As shown in Figure 3.1, our system calculates the number of signals that needs to turn green (the number of interventions) to reduce the travel time of an EV to reach the incident location. Turning all signals green on the route from the beginning for an EV to the incident place produces its minimum travel time. However, turning signals green in this way will create additional traffic congestion in the surround signals of the EV travel route. The challenge is how to calculate the minimum traveling time of an EV that produces the less possible impact on the other associated traffics. In this chapter, we introduce an algorithm (Algorithm 1) exploiting the minimum clearance time (refer to Algorithm 2) to determine the number of interventions (I). In theory, for an EV in front of j^{th} signal, we can formulate the problem as:

$$I = argmin(\textsc{Cls\_Time}(j, i)) \tag{3.1}$$

where, $0 \leq i \leq n$ and subject to: $\textsc{Cls\_Time}(j, i) < \textsc{Cls\_Time}(j, i + 1)$.

Eq. (3.1) increases the value of i until the clearance time ($\textsc{Cls\_Time}()$) becomes a minimum and then selects $I = i$. The constraint $\textsc{Cls\_Time}(j, i) < \textsc{Cls\_Time}(j, i + 1)$ of the objective function defined in (3.1) represents that for some sequential values of i, the objective function may decrease when i increases.

Algorithm 1 Number of signal intervention estimation

1: **function** CALCULATEIN(j) ▷ j= The ID of the signal in front of an EV
2: I=1 ▷ consider one intervention
3: $T_j^c \longleftarrow$ CLS_TIME(j, I) ▷ calculate CLS_TIME for I=1 intervention
4: **while** $I < (n_s - 1)$ **do** ▷ n_s = #signals btw an EV and incident spot.
5: $T_{j+}^c \longleftarrow$ CLS_TIME$(j, I+1)$ ▷ find CLS_TIME for $I+1$ interventions
6: **if** $T_{j+}^c < T_j^c$ **then**
7: $T_j^c \longleftarrow T_{j+}^c$
8: $I \longleftarrow I + 1$
9: **else**
10: Return I
11: **end if**
12: **end while**
13: Return I
14: **end function**

3.1.2.1 Algorithm 1

When an EV starts from j^{th} signal, our proposed algorithm calculates the number of interventions (I) to minimize the delay to clear the incident. It checks how many signals should be turned green starting from no intervention (normal traffic condition) to turning all signals green in front of an EV, based on the updated traffic condition when the EV crosses a signal until it reaches the incident place. The algorithm is detailed as follows:

Steps 1-3: In these steps of the algorithm, the system takes the ID of the signal in front of an EV as j (Step 1), set the number of initial interventions as $I = 1$ (Step 2) and calculates the clearance time (CLS_TIME(j, I)) using Algorithm 2 (Step 3).

Steps 4-13: These steps implement the objective function defined in (3.1). Once the number of signals from the incident place to an EV's location (n_s) is known, the system uses a while loop to calculate the number of interventions (I). In Step 5, using the updated traffic condition, the cell clearance time T_j^c for $I + 1$ interventions is calculated using Algorithm 2. Steps 6-7 are the main part for calculating minimum cell clearance time. The algorithm returns the value of I when it achieves the minimum cell clearance time (Step 8) or exits while loop normally (Step 13).

The heart of this algorithm is how to calculate the clearance time considering an EV's

Algorithm 2 Estimating signal clearing time

function CLS_TIME(j, I) ▷ Calculate the clearance time for I interventions
  $T_j^e, T_j^c \longleftarrow 0$ ▷ Assuming initial EV travel time and clearance time as 0
  for g = j to n **do** ▷ For I interventions, find EV travel time from j^{th} signal to incident
    Estimate **average speed** $\vartheta(g)$ from in-road sensors or using (3.5)
    Estimate **the length of the cells** $\delta(g)$ **associated with** j^{th} **signal**
    $T_j^e \longleftarrow T_j^e + \frac{\delta(g)}{\vartheta(g)}$ ▷ Add EV travel time for each cell
  end for
  for $m = j$ to $j + I - 1$ **do**
    Estimate **time headway** T_m using (3.2)
    Estimate **number of cars** $\breve{n}_m$ from in-road sensors or using (3.4)
    Calculate m^{th} **signal's clearance time** $T_m^c \longleftarrow \breve{n}_m \times T_m$
    $\breve{n}_m^l, \breve{n}_m^r, T_m^{sl}, T_m^{sr}, T^l_m, T^r_m, T^s_m(0) \longleftarrow 0$
    for x= 1 to k **do** ▷ k cells of each side of the current signal
      Estimate **time headway** $T_m^l(x)$ and $T_m^r(x)$ using (3.2)
      $T_m^l = T_m^l + T_m^l(x)$
      $T_m^r = T_m^r + T_m^r(x)$
      Get **number of cars** $\breve{n}_m^l(x)$, $\breve{n}_m^r(x)$ from in-road sensors or using (3.4)
      $T_m^{sl} \longleftarrow \breve{n}_m^l(x) \times T_m^l$ ▷ Calculate the clearance time for the left side cells
      $T_m^{sr} \longleftarrow \breve{n}_m^r(x) \times T_m^r$ ▷ Calculate the clearance time for the right side cells
      $T_m^s(x) = max(T_m^s(x-1), T_m^{sl}, T_m^{sr})$
    end for
    $T_m^s \longleftarrow T_m^s(x) + T_m^c$ ▷ Add side cells clearance time with cell clearance time
    $T_m^c \longleftarrow$ **max**(T_j^e, T_m^s) ▷ Calculate the clearance time
    if $T_m^c > T_j^c$ **then**
      $T_j^c = T_m^c$
    end if
  end for
  Return T_j^c ▷ Return the clearance time
end function

traveling time, and the impact of the intervention on other on-road traffics. The details of such calculation are provided in the following algorithm (Algorithm 2).

3.1.2.2 Algorithm 2

In this algorithm, for the start of an EV from j^{th} signal and a specific number of interventions (I), we estimate the clearance time by comparing the maximum value between the EV traveling time to the incident place and the associated side cells clearance time

of the interrupted signals. The decision to take maximum time for an EV's travel and side cells' clearance starts simultaneously. Once we get all of the maximum values for each intervention, our proposed system will consider the intervention providing the lowest maximum value to send the EV to the incident place quicker, and other vehicles need less time to clear the cell. Note, in this algorithm, we calculate the clearance time assuming the signal of a cross intersection, as shown in Figure 3.3. However, with minor modifications, clearance time for any intersection can be calculated. Steps of the algorithm (Algorithm 2) are as follows:

Steps 1-2: The CLS_TIME(j, I) function of Algorithm 2 receives the ID (j) of the signal in front of an EV and the number of interventions (I) as input from Algorithm 1 in Step 1. The initial travel time of an EV T_j^e and the clearance time T_j^c are set to 0 (Step 2).

Steps 3-7: The travel time for an EV from its dispatch place to the incident location is calculated in these steps. The function sets a loop (Step 3) to calculate the EV travel time from j^{th} signal to n^{th} signal. The average speed is calculated using (3.5) (Step 4), and the length of the cells (δ) associated with j^{th} signal is obtained from the real map in Step 5. The vehicle speed is acquired from the in-road speed sensors. If there is no speed sensor available, the system can also calculate the speed from the current density and flow rate by using (3.6). Next, the travel time T_j^e is calculated by dividing the length of the cells by the average speed (Step 6).

Steps 8-12: To find out the clearance time, these steps estimate the two major elements - (i) time headway and (ii) the number of cars. Step 8 starts the outer loop to calculate the clearance time considering each of the I interrupted signals. The first part of the outer loop estimates the time headway T_m (Step 9) of m^{th} signal by using (3.2). The number of vehicles in the cells associated with m^{th} signal is determined in Step 10. Multiplying the number of those vehicles by the time headway provides the time to clear the cells associated with that signal (Step 11). Step 12 sets the initial value of $\breve{n}_m^l, \breve{n}_m^r, T_m^{sl}, T_m^{sr}, T_m^l, T_m^r, T_m^s(0)$ to 0.

Steps 13-21: Step 13 starts the inner loop from 1 to k to calculate k number of side cells' clearance time for both in the left and right sides of an EV's travel path. The

reason for estimating such clearance time is to consider the impact of an incident and the travel time of an EV on the adjacent cells. Depending on the magnitude of an incident, road condition, time (peak or off-peak), and geographical condition, road authority can choose the appropriate value of k.

Step 14 shows the time headway computation using (3.2) for the cells in left (T^l_m) and right (T^r_m) sides of an EV's travel path. In Steps 18 and 19, for both sides of m^{th} signal, the clearance time is estimated from the in-road vehicle counter sensors.

Once the number clearance time is calculated for the cells of each side, the system determines the time required to clear side cells in Step 20. The reason for taking maximum value in Step 20 is justified by the fact that the cells on both sides start clearing at the same time.

Steps 22-29: As the side cells and m^{th} signal clearing occurs sequentially, Step 22 adds side cells clearance time (see Step 20) with m^{th} signal clearance time (see Step 11). In Step 23, as explained before that an EV's travel and cell clearance happens concurrently, the maximum value of cell clearance time, and an EV's travel time is taken as m^{th} signal clearance time. For the same reason, the final clearance time is regarded as the maximum clearance value for I number of interrupted signals, which is measured by statements of Steps 24-26 within the outer loop.

Step 28 returns the clearance time T^c_j to Step 5 of Algorithm 1 to estimate the required number of interventions. Step 29 ends the function CLS_TIME().

In Algorithm 2, we need to use the time headway, the number of cars, and the average speed of vehicles. How to assess the values of these parameters considering the instantaneous condition of an ITS is described in the following sections.

3.1.2.3 Estimating time headway

Time headway (T) is the difference between the time when the front of a vehicle arrives at a point and the time the front of its next vehicle arrives at the same point. The average time headway T_j for cells associated with j^{th} signal can be calculated as [152]:

$$T_j = \frac{S_j}{\vartheta_j} \tag{3.2}$$

where S_j and ϑ_j are the average space headway and the average speed of the vehicles associated with signal j, respectively.

Space headway (S) [152] is difference in position between the front of a vehicle and the front of the next vehicle (in meters). Space headway (S_j) in signal j can be calculated by using the following equation:

$$S_j = \frac{l_j}{\breve{n}_j} \tag{3.3}$$

where l_j is the length of the cells associated with signal j and $\breve{n}_j$ is the number of cars in those cells.

3.1.2.4 Estimating number of cars

There are in-road vehicle-counting sensors [81] that can count the number of vehicles in a cell. If a cell doesn't have the vehicle counting sensors, the number of cars $\breve{n}_j$ in the cells related to j^{th} signal is estimated from their occupancy rate and capacity. The capacity of a cell is defined to be the maximum number of vehicles that can be accommodated in that cell at any given time. Let the maximum capacity and occupancy rate of the cells related to signal j be C_j and O_j, respectively. Then the number of cars $\breve{n}_j$ can be found by [152]:

$$\breve{n}_j = C_j \times O_j \tag{3.4}$$

3.1.2.5 Estimating average speed

The speed of a vehicle in traffic flow is defined as the distance covered per unit time. It is hard and resources intensive to record the speed of each vehicle on the road. Thus, our system considers the average speed of the vehicle at any given signal. The average vehicle speed of signal j can be calculated by [153]:

$$\vartheta_j = \frac{\sum_{i=1}^{\breve{n}j} \vartheta_i}{\breve{n}_j} \tag{3.5}$$

where ϑ_i is the speed of i^{th} vehicle determined from the relevant speed sensors.

If there is no speed sensor installed, ϑ_j also can be determined by using the following equation [153]:

$$\vartheta_j = \frac{q_j}{\rho_j} \tag{3.6}$$

where q_j and ρ_j represent the flow rate and density associated with j^{th} signal, respectively.

Flow rate is defined as the number of vehicles that pass through a given point on the roadway in a given time, which is usually an hour. Traffic flow is usually measured by observing a road and counting down the number of vehicles passing through that given point on the roadway.

Let the duration of the green state of a phase p in seconds in signal j be G_j^p. Similarly, R_j^p and Y_j^p represent the duration of the red and yellow states of that phase, respectively. If $\aleph_j$ is the number of vehicles passing through the signal j in G_j^p time, for j^{th} signal, the flow rate in vehicles per hour can be defined as [153]:

$$q_j = \aleph_j \times \frac{3600}{W} \tag{3.7}$$

where, W = $G_j^p + R_j^p + Y_j^p$ is the phase time (the combination of time for signal state Green, Yellow, and Red) of j^{th} traffic signal. Figure 3.3 shows four different phases. In this figure in Phases 1 and 2, northbound and southbound traffics turn left and right from the middle, and no vehicles pass straight. In Phases 3 and 4, no vehicles turn left or right from the middle, but vehicles cross straight.

Density refers to the number of vehicles per unit length of the road. Normally, it is expressed as vehicles per kilometer. Let $\breve{n}_j$ be the number of vehicles that are occupied in the length l_j of j^{th} signal. Then density in signal j can be represented as [153]:

$$\rho_j = \frac{\breve{n}_j}{l_j} \tag{3.8}$$

In a real-life scenario, there are a number of sensors available to monitor the flow rate, detect vehicle speed, calculate average speed, monitor occupancy rate, and counting

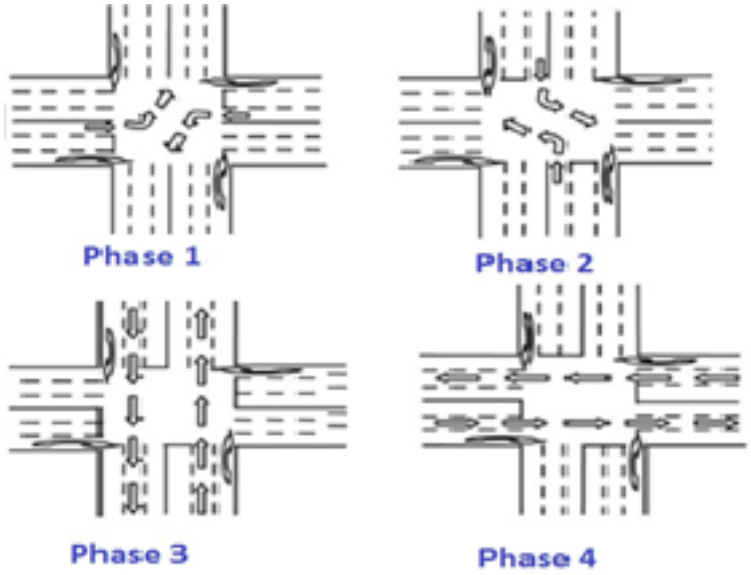


Figure 3.3: Signal Phases

pedestrian. For example, Sensmetrics, Sensturn, SensID, Sensbike, and FlexID are some of the critical sensors manufactured by Sensys providing signal traffic flow count, counting the number of turning vehicles, calculating travel time counting bicycles, and traffic signal performance monitoring, respectively at signals [81]. Different transportation authorities use different types of sensors based on their requirements and budget. To validate our proposed model, we created a simulated environment in SUMO. Section 3.2 discusses the simulation environment we use to evaluate our system.

3.2 Simulation Environment

For simulation, we used the microscopic version of the Simulation of Urban Mobility (SUMO). SUMO is an open-source, multi-modal traffic simulation platform. The microscopic version of SUMO was developed by Stephan Kraus [154], which allows modeling each vehicle explicitly with its route and movement ability. We implemented our model on the SUMO platform and simulated it on a real map to evaluate the performance of

our proposed model. The following parameters were considered while setting up the simulation environment.

3.2.1 Simulation Parameters

- **Map**

  This simulation was set up using a real map of Melbourne CBD. JOSM editor for OpenStreetMap [155] [38] was used to convert the real map to the SUMO network file, as shown in Figure 3.4. Two different incident places were used to simulate the incidents - one that occurred at a shorter distance having ten signals and another at a longer distance having 20 signals from an EV's dispatch point. These incident places are marked with a square box and a circle, respectively, in Figure 3.4. An EV's dispatch point is shown with a down arrow button.

Figure 3.4: Map of Melbourne CBD used in SUMO

- **Density**

  Five different traffic densities were considered where 0, 30, 50, 70, and 100% road were occupied. Traffic density changes over time and with events such as

on and off-peak time, school and non-school days, working and non-working days (weekends and holidays), and special events. The simulation results were produced in both low (30% occupied), medium (50% occupied), and high density (70% occupied) conditions. We also used 0% and 100% occupancy rates to check the performance at the free flow and for difficult incident situations, respectively.

- **Vehicle type**

  To simulate a realistic environment, we also used different types of vehicles. For example, the percentage of vehicles on the road was taken as 65, 20, 15, and 5% respectively for passenger vehicles, delivery vans, bus (both public and free shuttle services), and tram. Some pedestrians were also added randomly.

- **Traffic data**

  In the simulation, we considered three different times (05:30 am, 01:00 pm and 05:00 pm) of a working day (Monday) in Melbourne CBD for low, medium, and high occupancy rates. Real traffic flow data were used in the simulation. These flow rates were taken from VicRoads data available online [151].

- **Car following model**

  Krauss [154] established a model based on the safe speed, without considering that acceleration and deceleration in different vehicles are different. Han and Chen [155] proposed a new model that considers the gradual process of deceleration in vehicle braking based on Kraus' model. In our implementation, we used the car following the model proposed by Han and Chen.

- **Assumption**

  To mimic a realistic environment, we assume that 20, 20, and 60% vehicles turn left, turn right, and go straight when a signal turns green.

3.3 Simulation Results

We observed the average speed, density, and time headway to calculate an EV travel time from its dispatch position to incident place as well as the clearance time of vehicles in the cells adjacent to the travel path for $0\%, 30\%, 50\%, 70\%$, and 100% occupancy rate. We created two different incident places in the simulation, one having a shorter distance (ten signal points) from the EV dispatch point than the other (20 signal points). In the simulation, we used two right and two left side cells ($k = 2$ in Algorithm 2) for each signal of the EV travel path. For the near incident place, the number of observed cells was 55, while it was 110 for the distant incident place. Simulation results for the EV travel time (i.e., response time), number of cars in the observed cells, total cell clearance time for short and long distant incidents are shown in Table 3.1, 3.2, 3.3 and Table 3.4, respectively.

As discussed earlier, our main purpose is to reduce an EV's travel time, but we also need to consider that other vehicles do not have to wait an excessively long time to give away to the EV. Except for the 0% occupancy rate, the increased number of interventions to provide green phase time to an EV decreases the EV travel time, but it naturally raises the number of vehicles in the adjacent cells of the EV travel path. The increase of vehicles is mainly in the cells located on the left and the right-hand side of green phases on the EV travel path. Total clearance time not only depends on the number of vehicles in the observed cells but also on the time headway. Table 3.1 shows the time for an EV to reach the incident place (i.e., response time), and Table 3.2 shows the number of vehicles in the observed cells.

For the short and long-distant incident places, five different occupancy rates, and five interventions, Table 3.1 shows an EV travel time from its dispatch location to the incident place. IN (0) intervention is when in the simulation, we did not intervene any signal's phase time change. Similarly, IN (n) intervention means where we made consecutive n signals green in front of the EV's route towards the incident place until the EV pass through that signal. This process repeated until the EV reached the incident place. For no intervention and 100% occupancy rate, the EV travel time becomes the

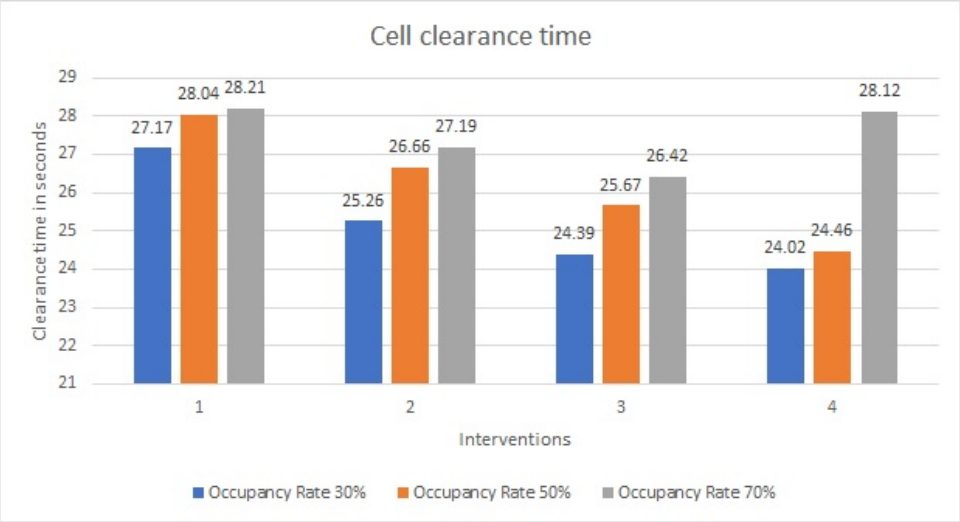


Figure 3.5: Average cell clearance time in 7^{th} cell in different occupancy rate with different interventions

maximum value of 3392 and 3762 seconds for short and long-distance incident places, respectively. However, as expected, with increased interventions, the EV travel time decreases. For example, for four interventions, the EV travel time is much lower than that with no intervention. For 100% occupancy rate, the EV travel times decrease to 2086 and 3658 seconds for short and long distances, respectively. However, applying more interventions generally creates more congestion to the cells nearby the EV travel path. Figure 3.5 shows the cell clearance time for a left side cell of the 7^{th} signal at different occupancy rates and four different interventions. In 30% and 50% occupancy rates, the cell clearance time decreases when interventions increase, but for 70% occupancy rate, the cell clearance time increases for four interventions. One of the main reasons for this is the growing number of vehicles waiting in those cells affected by the incident and providing green signals to the EV.

From Table 3.2, we can see that for both short- and long-distant incidents, the number of cars in the observed cells increases as the number of intervention increases. In a 0% occupancy rate, only one vehicle is the EV. For 0 intervention and 30%, 50%, 70%, and 100% occupancy rates, the vehicle numbers are 1190, 1340, 1690, and 2600 for short-distant, respectively, while they are 2320, 2586, 3430, and 5200 for the long-distant

Table 3.1: Travel time for an EV in seconds for different occupancy rates and interventions.

OR (%) →	0		30		50		70		100	
IN ↓	short	long	short	long	short	long	short	long	short	long
0	230	480	643	1247	815	1505	1410	2619	3392	3762
1	230	480	585	1181	764	1419	1359	2531	3275	3701
2	230	480	550	1075	703	1351	1321	2452	3221	3684
3	230	480	517	1023	671	1257	1287	2404	3180	3672
4	230	480	495	571	982	703	1209	1213	2086	3658

OR = Occupancy rate, IN= Intervention

Table 3.2: Number of cars in observed cells for both short and long distant incident for different occupancy rates and interventions.

OR (%) →	30		50		70		100	
IN ↓	short	long	short	long	short	long	short	long
0	1190	2320	1340	2586	1690	3430	2600	5200
1	1230	2354	1376	2714	1758	3840	2600	5200
2	1260	2380	1418	2820	1774	3820	2600	5200
3	1289	2420	1452	2860	1885	4100	2600	5200
4	1302	2465	1487	2917	1943	4185	2600	5200

OR = Occupancy rate, IN= Intervention

incident. This growing number of vehicles leads to increasing density and decreasing flow rate and average speed in those cells. When the number of intervention rises, the flow rate of EV travel path and average speed increase, however, consequently, the density reduces.

For short distance, Table 3.3 shows for a 0% occupancy rate, the time to clear is the same for all interventions. In this case, turning all signals into the green provides the same clearance time, 230 seconds, as no intervention. In both real-life and simulation,

Table 3.3: Clearance time (in seconds) when an EV is within the short distance (ten signals) of an incident place

IN / OR (%)	0	1	2	3	4	5	6	7	8	9	10
0	230	230	230	230	230	230	230	230	230	230	**230**
30	643	585	550	517	**495**	578	676	781	826	885	921
50	815	764	703	**671**	743	795	942	997	1036	1084	1129
70	1410	1359	**1321**	1355	1392	1502	1676	1822	1887	1951	2072
100	**3392**	3581	3646	3899	3972	4082	4123	4233	4432	4567	4676

OR = Occupancy rate, IN= Intervention

since an EV goes through the red signals without stopping, and in a 0% occupancy rate, there is no other vehicle surrounding the cell, an EV's travel time is not impacted by the interventions at all.

For 30% occupancy rate and zero to ten interventions, Table 3.3 shows the clearance times are 643, 585, 550, 517, 495, 578, 676, 781, 826, 885 and 921 seconds. As up to four interventions, clearance time decreases, and after that, it increases. Since the clearance time becomes the lowest (495 seconds) for four interventions, our proposed system recommends four as the number of interventions for the incident located in a short distance at this occupancy rate. Similarly, for 50% and 70% occupancy rates, the lowest clearance times (671 and 1321 seconds) were obtained for three and two interventions, respectively. Therefore, the suggested intervention numbers are three and two for these two occupancy rates, which indicates, as expected, the number of interventions decreases with the higher occupancy rate.

A 100% occupancy rate means all cells are filled with vehicles. The number of interventions only make clearance time higher. Even if the travel time for an EV reduces, the clearance time rises for the fact that the number of vehicles in the observed cells becomes high. More vehicles also accumulate in the adjacent of the observed cells as the number of interventions increases. Flow rate and average speed are reduced in the

observed cells if more vehicles gather in their surrounding cells. The minimum clearance time is 3392 seconds for no (0) intervention. However, because of the reasons explained before, the clearance time starts growing with the increased number of interventions.

The distance from an EV to an incident place also has an impact on the selection of intervention numbers. Table 3.4 shows the simulation results for an incident happening at a longer distance.

Table 3.4: Clearance time (in seconds) when an EV is within the long distance (20 signals) of an incident place

IN / OR (%)	0	1	2	3	4	5	6	7	8	9	10
0	480	480	480	480	480	480	480	480	480	480	480
30	1325	1247	1181	**1037**	1067	1135	1202	1284	1335	1382	1457
50	1575	1505	**1418**	1475	1523	1593	1625	1675	1814	1905	1954
70	2723	**2619**	2684	2779	2807	2893	2955	3012	3085	3143	3195
100	**3762**	4153	4348	4804	5123	5242	5323	5424	5513	5627	5716

OR = Occupancy rate, IN= Intervention

Similarly to the short distance, the number of interventions was chosen as 3, 2, 1, and 0 for 30, 50, 70, and 100 occupancy rates, respectively. In this case, intervention number reduces with a higher amount of occupancy rate. For the same occupancy rate, if we compare the number of interventions chosen from Table 3.3 and Table 3.4, it exhibits that, for a long distant incident, intervention numbers are less compared with those for a shorter distance. For example, for 50% occupancy rate, intervention numbers are three and two for short and long-distant incidents, respectively. The longer the EV's traveling path, the higher its traveling time and the more accumulation of vehicles are. This increases the density and thus reduces the flow rate and average speed of an EV and other vehicles. As a consequence, EV's traveling time and clearance time decrease up to a fewer number of interventions. For this reason, when an EV takes a longer time to reach the incident place, it increases the clearance time; hence, the number of

interventions is reduced.

Figure 3.6 shows the average speed change in different cells at the 50% occupancy rate. Here, Cell 1 is the cell next to the EV start position. Cells 5 and 10 are next to Signals 5 and 10 of the EV travel path, respectively. The incident place is near to Cell $n = 55$ for short distant incident place. We can see that the average speed of the vehicles reduces early for the cells that are near to the incident place. For example, the average speed of Cell n reduces sharply within 2-3 minutes (close to 2-3 phase time) as the flow rate decreases as soon as an incident happens. Average speed starts decreasing sharply in Cells 10, 5, and 1 in 6-7, 13-14 and 17-18 minutes, respectively. This means an EV needs more time to reach the incident place as its speed reduces more on the way. This sharp fall of speed caused a delay in both EV traveling and cell clearance. The impact of the change of this clearance time due to occupancy rate, distance, and average speed is described below.

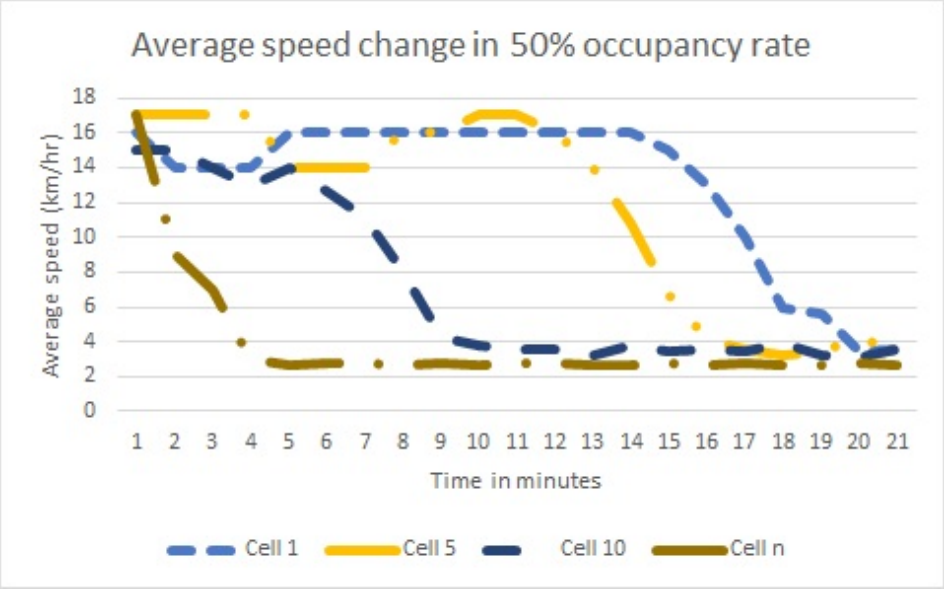


Figure 3.6: Average speed change in different cells in 50% occupancy rate

Our system recommends the number of interventions considering both EV travel time and clearance time for other vehicles. If we consider the 70% occupancy rate in the short-distant incident, Table 3.1 shows the EV travel time is 1287 seconds and 1208

seconds for three and four interventions respectively and for long-distance, the EV travel time is 2779 seconds and 2807 seconds for three and four signals respectively. The EV travel time is low in four or three interventions, but our system recommends two interventions for short distance and one intervention for long-distance. For short distance, if we increase to intervention number from two to three, it increases the clearance time from 1355 seconds to 1392 seconds. These results reflect that the intervention that our system recommends lowers the EV travel time but also trades off the clearance time for other vehicles. From these results, we find that the number of intervention recommendations depends on both the distance from EV dispatch place to the incident location and occupancy rate. The number of intervention recommendation changes when the occupancy rate or distance changes.

3.4 Conclusion

In this chapter, we introduce the Emergency Vehicle Priority System to provide an appropriate priority with an EV to reach an incident place faster. This system considers two major processing steps. In the first step, an appropriate priority code is provided to an EV based on the type and severity of an incident. In the second step, this system estimates the cell clearance time to determine the number of interventions needed to reduce an EV's travel time while concomitantly considering the cell clearance time for other associated vehicles. We monitor the traffic condition (e.g., flow rate, density, time headway) at the signals through which an EV reaches the incident place. We also consider the left and right-side cell clearance time at each of the signals that are made green for an EV's traveling. For the simulation model, SUMO is used to create a simulation environment in a real map of Melbourne CBD with real traffic data available on the VicRoads website. Five different occupancy rates are used to validate our system in different scenarios. The simulation result shows an EV's travel time decreases with the increased number of interventions, but when we consider the impact on other vehicles in the monitored cells, the number of interventions depends on the occupancy rate and the distance of the EV location from the incident place. The result shows our system can

recommend appropriate intervention number that assists an EV in reducing response time even with the consideration of clearance time of other vehicles. Therefore, it is expected that our proposed system will play an important role in saving human life by sending an EV quicker to the incident place while clearing the holding traffic quickly.

ITS is using more and more wireless technologies (e.g., wireless sensors, wireless traffic signals) to improve the quality of traffic management service. These wireless technologies are providing better and smarter services but also making ITS more vulnerable to cyber-attacks. A traffic signal is one of the most critical components of ITS. It is becoming an important issue to detect intrusion in the traffic signals as quickly and efficiently as possible to make an ITS more reliable. The next chapter will introduce an intrusion detection system for traffic signals of an ITS.

Chapter 4

Detecting Intrusion in the Traffic Signals of an Intelligent Traffic System

In Chapter 3, we discussed that our proposed Emergency Vehicle Priority System uses ITS to estimate the number of interruption needed in traffic signals to provide a faster route for an EV considering the impact on other vehicles. As alluded in Section 2.4.1, many traffic signals across the world were under attack [156], indicating the importance of intrusion detection. Though reported attacks on ITS were limited to attacks on computers in the traffic controller, safety cameras installed in the RSU, and processing units installed in the signals of the intersection, undoubtedly such attacks will be on the rise in future [35] [69]. Up to our knowledge, there are no IDS available in the current literature that can detect attacks on traffic signal units.

Motivated by the above facts, to make an ITS more reliable and thus the fulfillment of research Objective 2 (OBJ2) specified in Chapter 1, in this chapter, we introduce an IDS for the traffic signals of an ITS for the first time. We theoretically model our proposed system using the DS decision theory considering the instantaneous observations of vehicle flow rate, the speed at intersections, the phase time of traffic signal changes, and their relevant historical data recorded by transportation authorities. We also use Shanon's entropy to determine the uncertainty associated with the observations. For the verification and validation of our proposed IDS, we developed a simulation model based on the traffic simulator called SUMO [38] using many real scenarios and the data

collected by the Victorian Transportation Authority, Australia (VicRoads). Simulated results show the overall detection accuracy of our proposed system is 91.1%. Therefore, our proposed IDS can successfully detect most intrusions on the traffic signals with a very small number of false alarms.

The rest of the chapter is organized as follows. The chapter begins by presenting an overview of the proposed intrusion detection system in Section 4.1. Section 4.1.2 formulates the theoretical model to monitor the status of a traffic signal . Next in Section 4.1.3, development of probability mass function is described. The evaluation process of the intrusion detection for the traffic signals is given in Section 4.2. Sections 4.2.1 and 4.2.2 details the simulation environment and performance metrics. Section 4.2.3 analyzes the simulation results, Section 4.3 concludes the chapter.

4.1 Proposed Intrusion Detection Method

4.1.1 Overview of the proposed IDS.

Our proposed system mainly monitors the status of a current traffic signal, which is statistically determined considering the flow rate and the density of vehicles, and the signal phase time of that traffic signal.

To assess whether the traffic signal is behaving as normal or unusual, the current status is compared and contrasted with the relevant status of that traffic signal derived from the corresponding historical data recorded by its TMS. The basic operating principle of the proposed system is shown in Figure 4.1. To reduce the false alarms in detection, firstly, the proposed system checks whether there is any software or hardware malfunction. If the deployed mechanism signals no software or hardware malfunction, the system then further verifies whether the MAC address is registered in the system. If the MAC address is not registered, it sends a message to the control system that the data is coming from an unauthorized sensor. Otherwise, our system checks whether the current observation data sufficiently deviates from the corresponding historical observation pattern. If it sufficiently deviates, it confirms that there is an intrusion in

that traffic signal. However, there may be special events (e.g., sports, festival) occurring seasonally and/or periodically throughout the year, which may affect the signal. To reduce the impact of those special events, the relevant historical data for a similar time that was affected by those events are chosen in our proposed system. Our proposed system consists of mainly two parts –(i) monitoring the status of the traffic signal and (ii) evaluating the traffic signal to detect intrusion. Those components are described below.

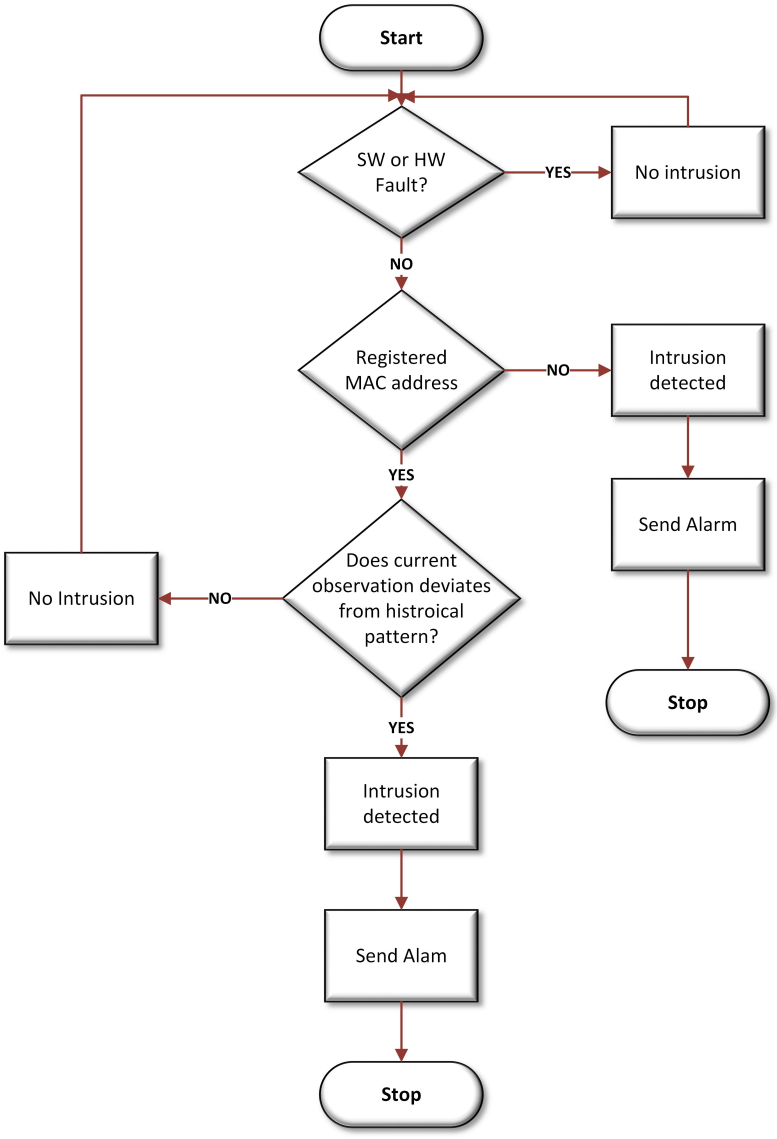


Figure 4.1: An Overview of the proposed intrusion detection system. SW=Software and HW=Hardware

4.1.2 Monitoring the Status of the Traffic Signal

The traffic signal is monitored in two phases. In the first phase, we use the MAC address of the sensors. People (e.g., hackers) can use external devices equipped with sensors to connect with the TMS network through wireless communication infrastructure to exploit the system vulnerability and alter traffic data. Therefore, in the first stage, we can verify whether the MAC address of a particular sensor belongs to the list of registered MAC addresses. This verification process ensures to detect where any unregistered sensor is attempting to send signal data raising suspicion. In the second phase, our proposed approach determines whether a registered sensor has been compromised. For this, we can exploit historical traffic pattern probability mass function that has not been manipulated by an intruder at a particular time within a particular time window (e.g., from 08:00 am to 09:00 am on Monday).

In this project, since we aim to use historical data to monitor the status of a current traffic signal at a particular time, we collected all required and relevant data from Vic Road's traffic data [151]. How the probability mass function of these data for a particular time window can be approximated, is detailed later.

For detecting the intrusion in this phase, we need to calculate the continuous observed values of some signal attributes. For this project, we have chosen the observed value of the flow rate and phase time of a signal and vehicle speed. This is because the flow rate and phase time can be used to obtain additional green time for creating traffic signal disruption or having illegal benefits. For example, hackers can extend signal phase time to create disruption for plotting a terrorist activity, or a thief can extend a green signal phase time to pass quickly by the stolen vehicle. Vehicle speed is selected as it is also profoundly affected by traffic signal disruption. Other attributes (e.g., vehicle type, pedestrian count) are not significant as they are not so effective like flow rate and phase time to make a significant change in signal timing or affected as vehicle speed. The impact of their changes only stays for one or two-cycle time, not being sufficient to create considerable disruption.

Here, we need to use an inference method to assess the status (e.g., normal or not normal) of a traffic signal. There are many methods available in the literature for

inference, such as Bayesian theory, rule-based inference system, and Dempster-Shafer (DS) decision theory. We have chosen the DS decision theory because it is based on generalized Bayesian theory and provides distributing support for different propositions using temporal data. For our proposed system, the frame of discernment is defined as:

$$H = (N, \neg N, N \vee \neg N) \tag{4.1}$$

where, N, $\neg N$, and $(N \vee \neg N)$ represent the proposition of the current observation being normal, not normal, and uncertain, respectively.

Since the flow rate, vehicle speed, and phase time are measured by respective individual sensor data, the belief function contributing to a particular preposition needs to be statistically measured for each sensor.

Let R_{jw} be the id of a sensor placed in intersection j having sensor type w, where, w=1, w=2, and w=3 represent flow rate, vehicle speed, and phase time, respectively. Since we observe events such as flow rate, vehicle speed, and phase time of a particular intersection over time (e.g., the observed event in this case $E_w(t)$ at time t at a particular day), we observe the data in a time window (e.g., 08:00 am -09:00 am) of a day considering working and non-working days, we need to use the probability mass function of the historical data corresponding to that time window of that day to find out the probability of a particular observation being normal. Therefore, the lower limit of the probabilistic value of j^{th} intersection being normal for y events can be defined using the belief function of the DS theory [40]:

$$bel_j(N) = \frac{1}{1-k} \times \sum_{\cap E_w(t)=N \neq \emptyset} \prod_{1 \leq w \leq y} m_j(E_w(t)) \tag{4.2}$$

where, k is defined as:

$$k = \sum_{\cap E_w(t)=\emptyset} \prod_{1 \leq w \leq y} m_j(E_w(t)) \tag{4.3}$$

According to the Shannon information theory, the uncertainty is the highest when $m_j(E_w(t)) = m_{jw}(N)$=0.5. Note, here, $m_{jw}(N)$ denotes the probabilistic value of a mass

function for w^{th} event ($E_w(t)$) having j^{th} intersection being normal. If the value of $m_{jw}(N)$ moves in either direction from 0.5, the uncertainty decreases. Applying the principle of Shannon information theory, the uncertainty associated with $m_{jw}(N)$ i.e., the probability, m_{jw} $(N \vee \neg N)$ is defined as:

$$\begin{aligned} m_{jw}(N \vee \neg N) = -m_{jw}(N) log_2 m_{jw}(N) - \\ (1 - m_{jw}(N)) log_2 (1 - m_{jw}(N)) \end{aligned} \tag{4.4}$$

Since, $m_{jw}(N \wedge \neg N)$ denotes the null hypothesis i.e., $m_{jw}(N \wedge \neg N)$=0, $m_{jw}(\neg N)$ is derived as,

$$m_{jw}(\neg N) = 1 - m_{jw}(N) - m_{jw}(N \vee \neg N) \tag{4.5}$$

The upper limit (plausibility) of j^{th} intersection being normal is defined as:

$$pl_j(N) = 1 - bel_j(\neg N) \tag{4.6}$$

For obtaining the uncertainty value and then the belief value using (4.4) and (4.2), respectively, we need to calculate $m_j(E_w(t))$ for the flow rate, vehicle speed and phase time.

Either or all of the sensors can be compromised by the hackers. As mentioned before, to determine whether they have been attacked, individually or multiple, we can compare and contrast their observed values with their corresponding and authentic (e.g., not attacked or forged) historical values. This accentuates the development of probability mass function $m_j()$ used in the DS theory based fusion approach defined in (4.2) and (4.6).

The development of $m_j()$ using the VicRoads's historical traffic signal data uploaded Victoria's state government website [151] is described in the following section.

4.1.3 Development of the Probability Mass Function

The special event usually happens in a particular period of a year. The occurrence of a special event can increase the likelihood of having unusual historical data than normal data during that specific time frame. This implies that we need to use historical traffic signal data with and without the occurrence of events for both pieces of evidence. We calculated histograms and their corresponding best fit normal distribution curves of the historical data for both flow rate, vehicle speed, and phase time as below. Without any event occurring, the histogram of the flow rate per hour, average sped, and phase time on working Mondays from 08:00 am - 09:00 am in 2017, and their corresponding best fit normal distribution curves of three different intersections are shown in Fig 4.2 a-c, respectively. All of the figures for flow rate, average vehicle speed, and the phase time show that all probability mass functions are approximately normally distributed. This is indicated by their corresponding well fitted normal probability mass functions for all curves.

Using the probability mass functions developed from the historical data, we need to calculate the probability of observed evidences (flow rate, vehicle speed and phase time) which is described below.

4.1.4 Calculating probabilities of the observed evidences

In this section, we need to calculate the probabilities of the observed evidences for both flow rate and phase time, respectively. Since, as explained before, the probability mass functions are normally distributed, the probability of an evidence for observed value x_w for w^{th} event can be calculated as,

$$m_j(x_w) = \begin{cases} 1 - \int_0^{z_w} \frac{1}{\sqrt{2\pi}} e^{\frac{x_w^2}{2}} dx_w \text{ if } z_w \geq 0 \\ 1 - \int_{z_w}^{0} \frac{1}{\sqrt{2\pi}} e^{\frac{x_w^2}{2}} dx_w \text{ Otherwise} \end{cases} \tag{4.7}$$

where, $z_w = (x_w - \mu_w)/\sigma_w$, $x_w = E_w(t)$, and μ_w and σ_w are the mean and standard deviation of the probability mass function shown in Fig 4.2 for j^{th} event, respectively.

Once the probability of a particular evidence is calculated, we use this to evaluate the status of the traffic signal which is described in the next section.

4.2 Evaluating the Traffic Signal to Detect Intrusion

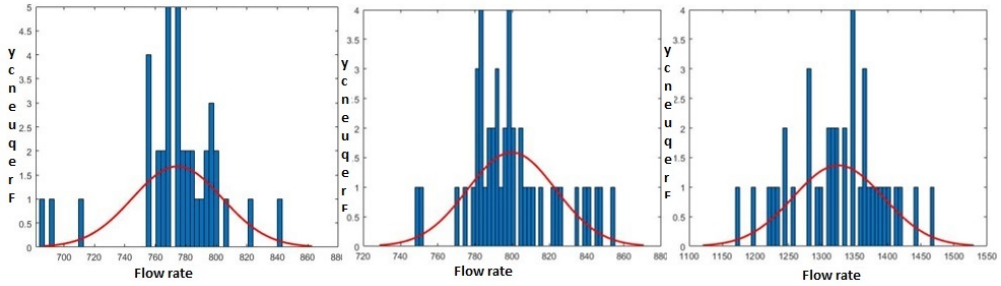
To detect an intrusion in the traffic signal, we need to evaluate the status of the traffic signals. This status is used in our system to determine the normal behavior of a traffic signal based on the historical data. If we know the value of current events (e.g., $E_F(t)$, $E_S(t)$, $E_P(t)$), we can calculate their probabilities as $m_j(E_F(t))$,$m_j(E_P(t))$, and $m_j(E_S(t))$ using (4.7) and the μ and σ of their corresponding probability mass functions. Then next, the probability of being N i.e., $bel_j(N)$ fined in (4.2) needs to be determined. If $bel_j(N) \geq \emptyset$, the traffic signal of j^{th} intersection is assumed to be normal, otherwise, it is intruded.Here Ø is an intuitively selected threshold. The sensitivity and accuracy of our proposed depend on the value of Ø. However, in the average case, Ø can be considered 0.5.

4.2.1 Simulation Environment

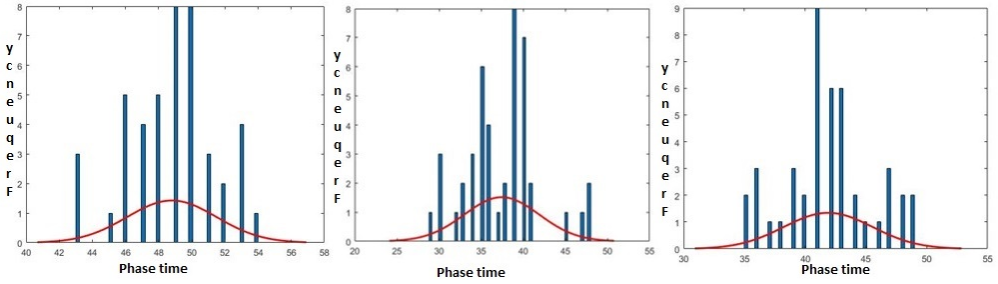
We instigated our system on the SUMO and simulated using a real road map on SUMO to weigh the intrusion detection performance of our system. Fig. 4.3 shows a screen-shot of our simulation platform. In the simulation, the vehicle flow was generated using the real-time traffics derived from VicRoad's historical data. Figs. 4.3a and b show the traffic flow of Intersection 1 for its normal and intruded conditions, respectively. The following parameters were considered while setting up the simulation environment.

Map: We used the road map of Melbourne CBD and VicRoads' real traffic data available in [38]. We have used five different intersections in Melbourne CBD. The intersections are (i) Lonsdale and Russel street, (ii) Collins and Kings St, (iii) Elizabeth and Latrobe St, (iv) Collins and Swanston St, and (v), Flinders and Swanston St Melbourne.

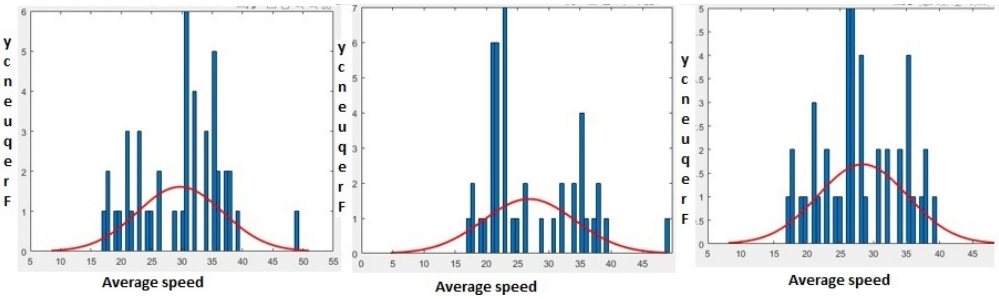
Density and flow rate: We selected the peak-time phase time, average vehicle speed, and flow rate in our simulation using the traffic data from 08:00 am to 09:00 am Monday



(a) Histograms and their corresponding best fit normal distribution curves for flow rate



(b) Histograms and their corresponding best fit normal distribution curves for phase time



(c) Histograms and their corresponding best fit normal distribution curves for vehicle speed

Figure 4.2: Histograms and their corresponding best fit normal distribution curves for flow rate, phase time and vehicle speed

at five busy corners of Melbourne CBD. The phase time, average vehicle speed, and flow rate of an intersection at time t were calculated in the simulation using a popular microscopic traffic model presented in [155].

Vehicle type and traffic distribution: We considered mixed vehicle types where 65% vehicles were passenger vehicles, 20% delivery vans, 15% bus (both public and free shuttle services), 5% tram, and some random pedestrians.

Car following model: We used the Krauss car following model in our simulation.

Krauss car following model considers that cars follow gradual deceleration while braking [154].

Normal and intrusion scenarios: For normal conditions, the flow rate, vehicle speed, and phase time of an intersection for a particular scenario were derived through our above-mentioned simulation model developed using SUMO. In the simulation model, traffic distributions were initiated with the respective and non-compromised historical information of VicRoads online data [151]. To emulate the current traffics in the simulation, the density, vehicle speed and phase time of incoming and outgoing traffics of an intersection of interest were randomly selected from the range of [minimum, maximum] value of the respective historical data for that day and time period collected through a year (2017) available in VicRoads website.

For simulating intrusions to the traffic signals, the flow rate of an intersection for a particular scenario was changed by intuitive induced phase time and vice versa. The induced average vehicle speed of an intersection was also inserted. If the intersection is intruded for a very short time (e.g., less then one cycle time), flow rate, vehicle speed, and phase time data will remain within the range of 68% to 95% confidence intervals. If the duration of the intrusion is higher, flow rate, vehicle speed, and phase time will go outside 95% confidence interval. To consider both cases (e.g., short and long time intrusion), the flow rate, vehicle speed or phase time were induced in such a way so that it remains within 68% to 95% confidence intervals in some cases (Scenario 2 and Scenario 4) and outside 95% confidence intervals of the relevant historical data for the other cases.

The mean (μ) and standard deviation (σ) of those normal probability mass functions for all curves are shown in Table 4.1.

Figure 4.2 shows the histogram and the corresponding fitting normal curves of different flow rates, phase time, and vehicle speed of three different intersections.

In this project, we aim to use historical data to monitor the status of a current traffic signal at a particular time. We have tested 40, 41, 39, 42, and 44 numbers of pieces of evidence (e.g., flow rate, phase time, and vehicle speed) for respective Scenarios 1

Table 4.1: Mean (μ) and standard deviation (σ) of flow rate, vehicle speed, and phase time of Intersections 1-5

	Flow Rate		Vehicle Speed		Phase Time	
Intersection	μ	σ	μ	σ	μ	σ
1	774.359	29.4694	23.34	3,43	36.6279	3.8011
2	1108.703	15.2003	36.13	4.13	52.4545	4.4432
3	811.3488	27.0122	29.76	6.21	41.8864	13.3589
4	938.1818	27.8687	31.54	4.69	47.7955	3.0238
5	799.6818	23.6562	28.97	4.12	38.2727	2.6795

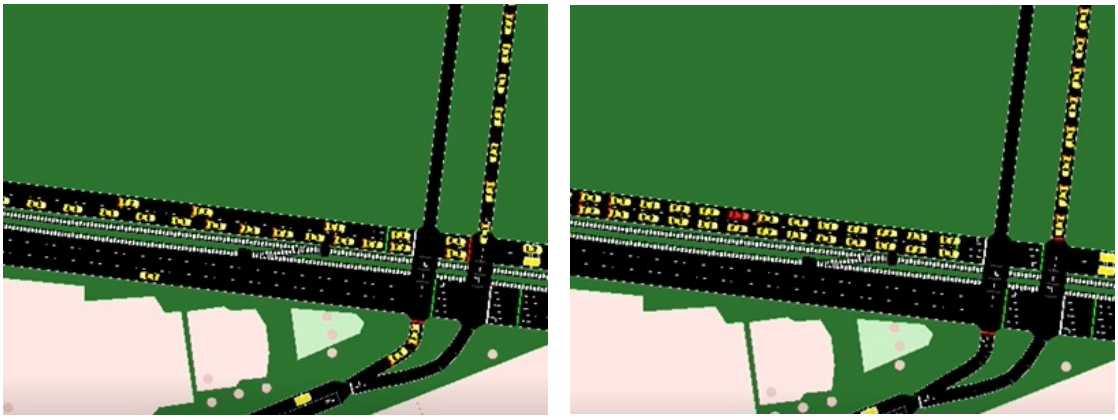
to 4 described in Section 4.2.3. We initially set up the simulation as per the normal historical data available on the VicRoads website [151]. Using this data set, we then selected different incidents, vehicle breakdown places in the monitored area, an unusual vehicle stops because of sensor malfunctions or malicious behavior. Additionally, in the simulation, we included instances and locations where untrustworthy vehicles or hackers can enter and provide false information about traffic conditions, which may lead the following vehicles to crash or change the route or increase congestion by sudden stop.

Our proposed approach considers the traffic condition as normal if the observed flow rate falls within the 95% confidence interval of the normal distribution curve, as shown in Figure 4.2.

4.2.2 Performance Metrics

We evaluated our intrusion detection results for all scenarios using the standard performance metrics widely used in event detection, such as specificity, sensitivity, overall accuracy, and F-score.

Specificity, sensitivity, accuracy, and F-Score were calculated using the True Positives (TP), False Positive (IIP), True Negative (TN), and False Positive (IIP) values. When an



(a) Traffic in normal scenario (b) Traffic in intruded scenario

Figure 4.3: Simulation environment for Intersection 1 for normal and intruded cases

intersection is operating in a normal condition, and the system detects it as normal, it is counted as TP value. Otherwise, it is treated as $\amalg N$. Similarly, for intruded intersection, if an intersection is found as intruded, it is considered TN. Otherwise, it is regarded as $\amalg P$. These specificity, sensitivity, accuracy, and F-Score are defined as follows:

$$Specificity = \frac{TN}{TN + \amalg P} \tag{4.8}$$

$$Sensitivity = \frac{TP}{TP + \amalg N} \tag{4.9}$$

$$Accuracy = \frac{TN + TP}{TP + TN + \amalg P + \amalg N} \tag{4.10}$$

$$FScore = 2 \times \frac{Sensitivity \times Precision}{Sensitivity + Precision} \tag{4.11}$$

4.2.3 Results and Analysis

As mentioned before, we have tested 40, 41, 39, 42, and 44 observations for Intersections 1 to 5, respectively. As a representative sample, Table 4.2-4.5 shows the probabilities of signals being normal (N), not normal ($\neg N$), and the uncertainty ($N, \neg N$) for Scenarios 1-4 having various flow rates, average speed, and phase times.

We have used four different types of combinations for two different observations (normal and not normal) of an intersection. Four different combinations of two observa-

tions are (i) flow rate and phase time (FP), (ii) flow rate and vehicle speed (FS), (iii) phase time and vehicle speed (PS), and (iv) flow rate, phase time, and vehicle speed (FPS).

Tables 4.2 and Table 4.4 present the intrusion detection results and their uncertainty values produced by our system for Scenarios 1 and 3, where no intrusions happened in any of the five intersections. Note, since uncertainty values are shown separately in all tables, throughout the chapter, belief values obtained by (4.2) denote the results. In contrast, Tables 4.3 and 4.5 show the results for Scenarios 2 and 4 where intersections were intruded. Therefore, Scenarios 1 and 3 represent normal intersections, while Scenarios 2 and 4 are for the intruded intersections. The probability values highlighted with bold text shows which combination provides the best result. It also shows the combinations that have the lowest uncertainty.

In the case of intrusion in an intersection, results produced by combining two pieces of evidence (e.g., FP, FS, PS) provide better detection than the results achieved using all three pieces of evidence (FPS). For example, in Table 4.5, our proposed method obtained the maximum detection probability values (e.g., 0.74, 0.72, 0.921, 0.73) for being not normal for four intersections using FP, while for Intersection 5, it (e.g., 0.62) is for FS. In contrast, for FS, the probability values are lower compared with those for FP. Table 4.5 also show the lowest uncertainty values (e.g., 0.10, 0.07, 0.04) was obtained for maximum number of intersections (3/5) using FP. Table 4.3 also supports a similar trend in the results. The detection probabilities obtained using FPS for Intersection 1 of Scenario 2 (see Table 4.3) and Intersection 5 of Scenario 4 (refer to Table 4.5) are 0.41 and 0.40, respectively that are lower the selected threshold 0.50 indicating the ineffectiveness of exploiting all three pieces of evidence for capturing intrusion. These results indicate that phase time is a major factor for intrusion detection. If a hacker can intrude on the sensor to change the phase time, it creates more congestion. Phase time impacts the traffic flow and average vehicle speed immediately. In the simulation, Intersection 5 and Intersection 2 had intruded phase time in Scenario 2 and Scenario 4, respectively. For Intersections 5 and 2, Tables 4.3 and 4.5 present the high detection values exhibiting the efficacy of phase time consideration in spotting intrusion.

When the intersection is not intruded, i.e., normal, combination for all three pieces of

evidence (FPS) provides better detection results than those for others. These results are above 0.50 for all intersections of the two scenarios. For example, for PS, the probability value for Intersection 1 shown in Table 4.2 is 0.49, while it is 0.58 for FPS. Table 4.4 show the probability values for Intersection 2 are 0.42, 0.48, and 0.43 for FP, FS and PS, respectively compared with 0.56 for FPS. These superior detection outcomes vindicate the use of FPS (three or more pieces of evidence) for the accurate detection of normal traffic conditions. The only loophole of FPS utilization is that its uncertainty value is higher than others but not that high as its maximum value is 0.12. This higher uncertainty value is justified by the fact that in a normal scenario, real traffic condition is dynamic. Traffic conditions may change due to many different reasons, such as different times (peak, off-peak), weather conditions, special events (e.g., road works, sports events), and school time. Flow rate, average vehicle speed, and phase time are affected because of the dynamic characteristics of the traffic condition.

From the results discussed so far, it is evident that FPS is effective to identify normal traffic conditions, but not so potential for intruded intersection detection. However, if we use the maximum probabilistic values highlighted with bold of an intersection in Tables 4.2-4.5, our proposed system is able to detect the correct state (normal or intruded) of all intersections. For example, for intersections being normal, the maximum value for Intersection 1 in Table 4.2 and Intersection 2 in Table 4.4 are: max (0.53, 0.58, 0.49, 0.58) = 0.58 and max (0.42, 0.48, 0.43, 0.56) =0.56, respectively. Note, since for both intersections, these two maximum values (0.58 and 0.56) are above 0.50, our proposed system can detect normal traffic conditions accurately.

Table 4.2: Detection results for Scenario 1. In the simulation, all intersections operated in normal condition

	Normal (N)				Not Normal (¬ N)				Uncertainty (N ∨¬ N)			
j	FP	FS	PS	FPS	FP	FS	PS	FPS	FP	FS	PS	FPS
1	0.53	0.58	0.49	**0.58**	0.41	0.34	0.45	0.3	**0.06**	0.08	**0.06**	0.12
2	0.85	0.78	0.83	**0.88**	0.13	0.19	0.14	0.02	**0.02**	0.03	0.03	0.1
3	0.645	0.625	0.68	**0.72**	0.301	0.321	0.27	0.19	0.05	0.06	**0.04**	0.09
4	0.735	0.752	0.698	**0.76**	0.255	0.17	0.16	0.25	**0.04**	0.08	0.06	0.08
5	0.887	0.824	0.805	**0.91**	0.093	0.16	0.17	0.06	**0.02**	0.04	0.03	0.03

j=Intersection, F= Flow Rate , P = Phase Time, and S = Vehicle Speed

Table 4.3: Detection results for Scenario 2. In the simulation, all intersections were intuitively intruded (not normal)

	Normal (N)				Not Normal (¬ N)				Uncertainty (N ∨¬ N)			
j	FP	FS	PS	FPS	FP	FS	PS	FPS	FP	FS	PS	FPS
1	0.37	0.42	0.33	0.45	0.58	0.53	**0.66**	0.41	**0.05**	0.06	0.07	0.14
2	0.31	0.35	0.29	0.36	0.62	0.55	**0.65**	0.52	**0.07**	0.08	**0.07**	0.12
3	0.32	0.36	0.43	0.38	**0.60**	0.59	0.501	0.54	0.08	**0.05**	0.07	0.08
4	0.12	0.14	0.21	0.18	0.83	**0.87**	0.76	0.75	0.05	**0.03**	**0.03**	0.07
5	0.018	0.012	0.016	0.13	**0.94**	0.87	0.88	0.83	0.01	**0.01**	0.02	0.04

j=Intersection, F= Flow Rate , P = Phase Time, and S = Vehicle Speed

Table 4.4: Detection results for Scenario 3. In the simulation, all intersections operated in normal condition

	Normal (N)				Not Normal (¬ N)				Uncertainty (N ∨¬ N)			
j	FP	FS	PS	FPS	FP	FS	PS	FPS	FP	FS	PS	FPS
1	0.68	0.61	0.59	**0.74**	0.27	0.33	0.35	0.2	0.05	0.06	**0.04**	0.06
2	0.42	0.48	0.43	**0.56**	0.51	0.42	0.51	0.32	0.07	0.1	**0.06**	0.12
3	0.645	0.58	**0.65**	0.51	0.301	0.36	0.34	0.47	0.05	0.06	0.06	**0.03**
4	0.67	**0.71**	0.65	**0.71**	0.255	0.20	0.26	0.16	**0.04**	0.09	0.09	0.13
5	0.65	0.63	0.67	**0.69**	0.33	0.35	0.30	0.25	**0.02**	0.02	0.03	0.06

j=Intersection, F= Flow Rate , P = Phase Time, and S = Vehicle Speed

Table 4.5: Detection results for Scenario 4. In the simulation, all intersections were intuitively intruded (not normal)

	Normal (N)				Not Normal (¬ N)				Uncertainty (N ∨¬ N)			
j	FP	FS	PS	FPS	FP	FS	PS	FPS	FP	FS	PS	FPS
1	0.20	0.24	0.22	0.215	**0.74**	0.71	0.65	0.6	0.06	**0.05**	0.12	0.14
2	0.18	0.16	0.17	0.14	**0.72**	0.65	**0.72**	0.70	**0.10**	0.19	0.11	0.16
3	0.012	0.022	0.019	0.09	**0.921**	0.91	0.88	0.78	**0.07**	**0.07**	0.11	0.13
4	0.23	0.22	0.18	0.27	**0.73**	0.67	0.72	0.56	**0.04**	0.11	0.10	0.17
5	0.31	0.26	0.34	0.38	0.53	**0.62**	0.57	0.40	0.16	0.11	**0.09**	0.22

j=Intersection, F= Flow Rate , P = Phase Time, and S = Vehicle Speed

For showing how our proposed system works to detect both traffic conditions for each intersection, we calculate the average value of the probabilities for both scenarios. Figs. 4.4 and 4.5 show these average detection results for the normal and intruded traffic conditions, respectively. In Figs. 4.4 and 4.5, for each intersection, there are 12 bars. The first four bars represent the probability of an intersection being normal, bars 5-8 denote the probability of an intersection being not normal, and the last four bars show the uncertainty values. For the normal traffic conditions, as with the results shown in Tables 4.2 and 4.4, for FSP, the detection probabilities shown in Fig. 4.4 are higher and above or equal to 0.57 for all interactions except Intersection 3. For these intersections for FSP, Fig. 4.4 also shows higher uncertainty values. However, for the intruded traffic conditions, the probability values for FSP for all intersections are less than others having higher uncertainty values except Intersection 4.

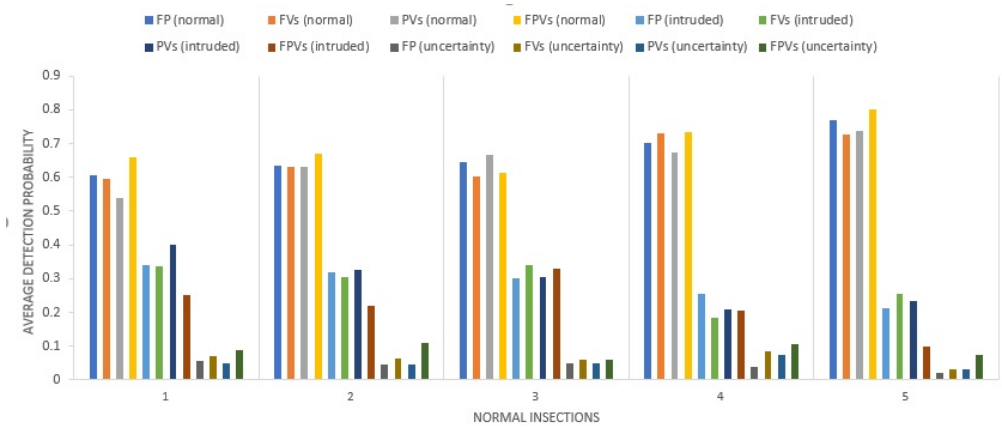


Figure 4.4: Average detection probability for normal intersections

As we know, the wider separation gap between the value of two decisive parameters makes the system decide more accurately and robust. For this reason, to show the robustness of our system in deciding whether an intersection is normal or not normal, we calculate the separation gap between the average probability values for all pieces of evidence being normal or not normal for any particular intersection. The separation band of the values of an intersection being normal or intruded is shown in Figs. 4.6 a and b, respectively. The highest gap calculated is for Intersection 3, shown in Fig. 4.6b, has the probability of being not normal is 0.792, and normal is 0.203. Therefore, the gap is

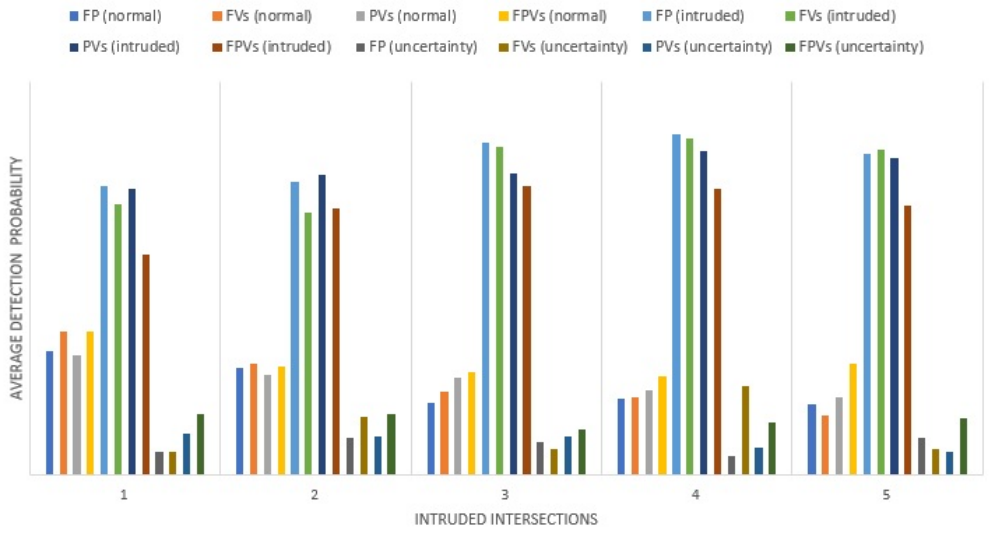
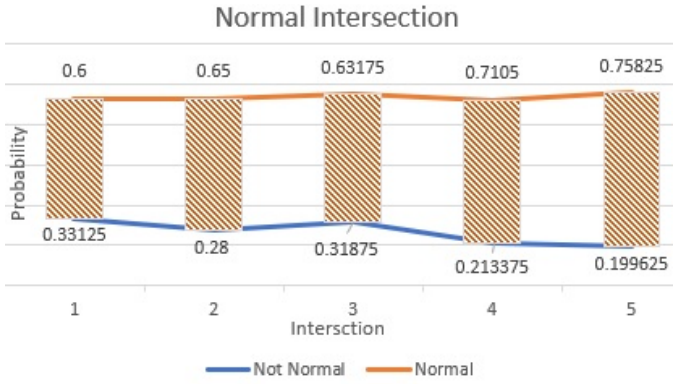


Figure 4.5: Average detection probability for intruded intersections

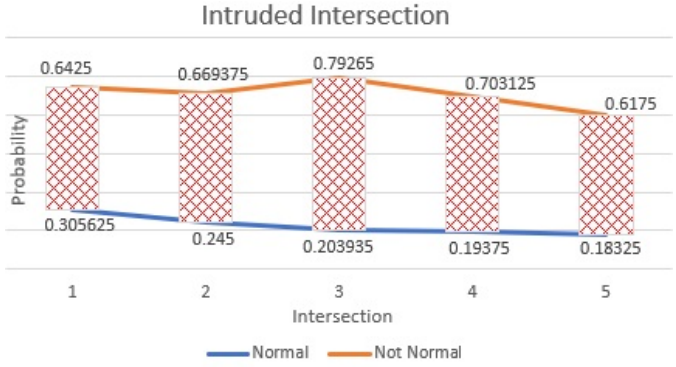
0.589. The lowest gap is for Intersection 1 in Table 4.6 a. The probability of being normal is 0.6, and not normal is 0.331, and thus the lowest gap is 0.269. The wide separation gap ranging from 0.269 to 0.589 vindicates that our system can conveniently differentiate the normal and intruded intersections.

We used 206 observations for the five intersections for each piece of evidence (FP, FS, PS, and FPS) and scenario. Therefore, the total number of observations we used is $206 \times 4 \times 4 = 3296$. We calculate the value of four performance metrics - sensitivity, specificity, accuracy, and FScore) using equations (4.8-4.11), which is shown in Table 4.6. The performance values are within the range of 0.86 to 0.95, which exhibits the superior performance of our proposed system.

Since the initial and instantaneous traffic distributions were induced in the simulation from the corresponding historical data, our proposed system is able to successfully determine most normal cases correctly except a few of them. Where in the simulation SUMO created normal traffic condition that deviates largely from historical value, our system detected those scenarios as a false negative. This happened because if the traffic condition deviates highly from historical data, it can cause disruption in normal traffic management. The results of Table 4.6 show that none of the evidence pieces achieves



(a) Separation gap for normal traffic condition



(b) Separation gap for intruded traffic condition

Figure 4.6: Separation gap between the probability of intersection being normal and intruded scenarios.

superior performance in terms of all metrics. This is because, as mentioned before, there are some situations where our system could not detect normal traffic conditions accurately.

For Intersection 5, the value for all performance metrics is slightly lower than that of others because, for this intersection, the historical data used to generate traffic in SUMO for the specific time period (08:00 am to 09:00 am, Monday) during which an event occurred. The occurrence of such an event created more deviations of the flow rate and phase time produced by SUMO from their corresponding historical data distributions for the similar events that occurred in that time period throughout a year.

Table 4.6: Detection results in terms of standard performance metrics

	Intersection	Sensitivity	Specificity	Accuracy	FScore
FP	1	0.904	0.947	0.923	0.925
	2	0.9523	0.901	0.923	0.926
	3	0.951	0.894	0.919	0.923
	4	0.952	0.904	0.926	0.925
	5	0.869	0.904	0.883	0.886
PS	1	0.913	0.87	0.891	0.898
	2	0.947	0.919	0.934	0.923
	3	0.924	0.943	0.934	0.919
	4	0.926	0.938	0.929	0.918
	5	0.897	0.928	0.903	0.895
PS	1	0.940	0.947	0.905	0.919
	2	0.950	0.909	0.929	0.927
	3	0.914	0.923	0.921	0.918
	4	0.905	0.947	0.905	0.909
	5	0.864	0.900	0.881	0.884
FPS	1	0.900	0.864	0.881	0.878
	2	0.950	0.909	0.929	0.927
	3	0.944	0.833	0.881	0.872
	4	0.909	0.950	0.929	0.930
	5	0.890	0.887	0.894	0.896
Overall		0.917	0.906	0.911	0.914

4.3 Conclusion

In this chapter, we introduced a system to detect an intrusion in ITSs for the first time. Our proposed IDS can detect any anomaly of traffic flow, signal phase, and average vehicle speed at a time that can make considerable disruption in the traffic system. Our system is based on the estimation of probability mass functions of traffic flow, phase time, and average vehicle speed from the historical data collected from an ITS and fusion of those variables using DS theory. We also used an approach based on Shannon's entropy to calculate the uncertainty. To test the efficacy of the system, we developed a simulation system considering the real traffic flow rate, signal phase time, and vehicle speed using the real map of Melbourne CBD and the historical data provided by VicRoads. The simulation system was built on SUMO, a known road traffic simulator. We created various traffic signal scenarios including induced intrusions by making either flow rate,

phase time, or vehicle speed or all intentionally shorter or longer than their designed permissible duration. We assessed the performance of the IDS using the standard performance metrics such as specificity, sensitivity, accuracy, and F-Score. Our proposed system can achieve an overall detection accuracy of 0.914 and 0.914 for intruded and normal traffic conditions, respectively. Currently, our system misses intrusion when the intrusion duration is very short (i.e., 1 or 2 cycles) time. The reason being, such short interruption does not have any noticeable impact on the traffic system and hence on the collected traffic data to show sufficient deviation from the normal signal.

Future ITSs will have self-driving vehicles, smart road infrastructure, and various sensors wirelessly connected to TMS, which will attract researchers to work on detecting the vulnerability of future ITSs. One of the main components of the future ITSs is a self-driving car which requires to communicate with traffic signals, other cars/vehicles, and roadside infrastructures, and recognize roadside signs. The performance of the future ITSs is heavily dependent on the reliability of a self-driving car. To assess the reliability of a self-driving car, the next chapter will present a new approach to measure its trust value.

Chapter 5

Trustworthiness of Self-Driving Cars for Intelligent Transportation Systems

Detecting intrusion in the traffic signals is presented in the previous chapter (Chapter 4). As mentioned in Chapter 2, the number of self-driving cars is increasing rapidly and thus increasing ITS unreliability. There exist many techniques to measure a self-driving car's trustworthiness by exploiting the trust of GPS data and probe data [40] [113] [157] [158]. Like warning messages and GPS data, an OBU of a car is also very susceptible to hacking. Many instances of hacking OBU components have been reported [41]. For safe driving, this hacking report emphasizes the pressing need to measure the trustworthiness of a self-driving car considering OBU components along with GPS data and safety messages. However, up to our knowledge, OBU components have not been taken into account in measuring the trust level of a self-driving car.

To address the above-mentioned crucial issue (OBJ3 articulated in Chapter 1), we propose an innovative trust measurement model for a self-driving car, which estimates the trust level of each of the four major OBU components (Lidar, Acoustic sensor, Radar and Camera). The uncertainty of the trust of six items (four OBU components, GPS data, and safety messages) is determined by Shannon's entropy [159]. These six trust values are fused using the popular and widely used subjective logic, namely the DS decision theory [40] [160]. Similarly, the trust values of these items and their corresponding certainty values are also calculated and combined by CertainLogic [42].

Model validation and evaluation for the assessed trust levels were performed using the SUMO and VicRoads historical traffic data [151] considering many real-world scenarios. Simulation results show both subjective logic and CertianLogic-based models produce meager trust value (well below 0.5) if one of the six items is compromised for all scenarios considered in this chapter. As expected because of the implication of applied logical operators, the trust values produced by the model based on CertainLogic are more sensitive to the breached components than those for the subject logic.

The chapter is organized as follows: in Section 5.1, we discuss our proposed model, while the trust models using CertainLogic and subjective logic are discussed in Section 5.1.1 and Section 5.1.2, respectively. Evaluation of the trust models is described in Section 5.2, and Section 5.2.2 analyzes the result. Finally, conclusion and future work are highlighted in Section 5.3.

5.1 Proposed Trust Model for a Self-Driving vehicle

Along with GPS and warning messages, we consider the four components of an OBU: (i) Lidar, (ii) acoustic sensor, (iii) Radar, and (iv) camera to measure the trustworthiness of a self-driving vehicle. The reason for this consideration is that these are the essential components of a self-driving vehicle.

Self-driving vehicles use three steps process to operate safely on the road. These steps are - (i) sensing, (ii) planning, and (iii) acting. Lidar, radar, cameras, and acoustic sensors provide information about the core issues involved in driving including the vehicle's current position (e.g., what street is the vehicle currently on and in which lane?), movement (e.g., what is the vehicle's current speed and direction?), nearby movable obstacles (e.g., are there moving or stopped vehicles, pedestrians, or bicycles nearby?), nearby fixed obstacles (e.g., are there curbs, signs, or buildings in the near vicinity?), and surrounding traffic-safety features (e.g., are there relevant traffic lights, stops signs, or lane markings that need to be observed?). Lidar of an autonomous vehicle can rapidly rotate 360- degrees to detect movable and fixed obstacles. Lidar systems use laser and can take up to a million readings every second. Lidar can detect a tiny object within a

100-meter range of the vehicle. In addition to Lidar, self-driving vehicles use radar to detect the position and speed of surrounding objects. Radar performs better than Lidar in performing the positioning tasks. For one, the range of a radar is much higher, up to several hundred meters or more. Moreover, radar systems detect the speed of different moving objects (e.g., pedestrian, bicycle, moving cars) very efficiently [83]. In self-driving vehicles, video cameras detect the location and speed of nearby obstacles. A typical arrangement involves two or more video cameras spaced around the vehicle at known distances. Spacing multiple video cameras in this way allow an OBU to receive parallel images of the same objects but from slightly different angles [161]. Acoustic sensors sense different predefined sounds (e.g., the crash of a vehicle, emergency vehicle siren, surface condition) to determine any traffic hazards or risk while driving [162]. These sensors work internally to provide safety information by observing road conditions surrounding the self-driving vehicles. The GPS of a self-driving vehicle gathers location and road conditions (e.g., traffic condition ahead) of the surrounding area and the route to the destination. Self-driving vehicles also use the messaging system to send or receive road safety information to and from the nearby vehicles [84] [68]. This messaging system is also used to capture road safety messages from the RSUs and Central traffic controllers. From the discussion, it is evident that the trustworthiness of a self-driving vehicle equally depends on the trust value of each of the above mentioned six components.

There exist many approaches for measuring the trustworthiness of GPS data and safety messages. Up to now, there is no work except our preliminary works [43] to assess the trust of a self-driving vehicle considering an OBU's components, GPS data, and safety messages. In [43], the uncertainty associated with the trust measure is taken manually, and only the DS theory is used for the decision fusion.

The trustworthiness of a self-driving vehicle can be measured using two prominent evidence-based information-theoretic approaches – (i) CertainLogic and (ii) Subjective logic. How to develop the theoretical frameworks for modeling the trust level of a self-driving vehicle considering four OBU components, GPS data, and safety messages using these two approaches are described in the following section.

5.1.1 Trust model using CertainLogic

Ries et al. [42] introduced a model named CertainLogic for evaluating propositional logic terms that are subject to uncertainty by defining the standards for the operator of propositional logic (AND, OR, and NOT). Since the trustworthiness measure of a self-driving vehicle contains massive ambiguity, CertainLogic is a better candidate to employ for evaluating a self-driving vehicle's trust. Average rating (t), initial expectation (f), and certainty (c) used in CertainLogic are independent. This independence characteristic allows the CertainLogic to handle the uncertainty better way compared with its counterpart, namely subjective logic (e.g., the DS decision theory). The main cause of this is the dependency of probabilities of trust, non-trust, and uncertainty as the sum of these terms is 1 in the subject logic.

In the following, we describe a CertainLogic-based approach considering the OBU's components of a self-driving vehicle, GPS data, and safety messages. This approach shows how the trustworthiness of a self-driving vehicle can be carried out with the propositional logic terms [42].

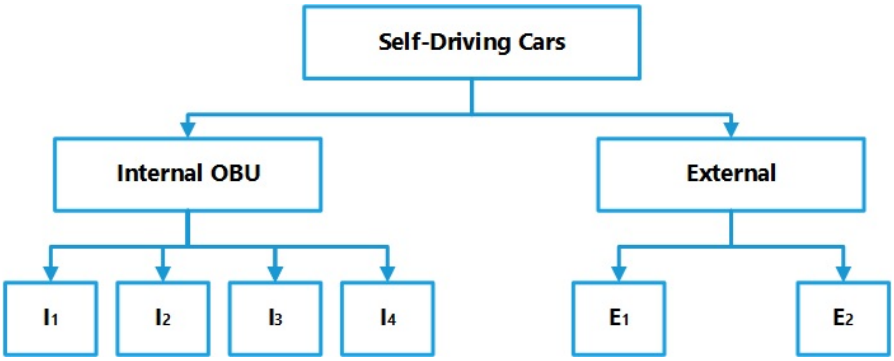


Figure 5.1: Self-driving vehicle Trust

Fig. 5.1 shows the trustworthiness of a self-driving vehicle directly depends on two subsystems - (i) Internal (I) and (ii) External (E) subsystems. Here I contains trust values of OBU components, which depend on the internal observations (e.g., object detected by an onboard camera) of a self-driving vehicle. E exploits the external observation values (e.g., location data from satellite, safety messages from CTC). Therefore, as shown in

Fig. 5.1, subsystem I consists of four OBU components - (i) Lidar (I_1), (ii) Camera (I_2), (iii) Acoustic Sensor (I_3), and (iv) Radar (I_4). Subsystem E comprises two units- (i) GPS (E_1) and (ii) Message (E_2). As alluded before, the trust of a self-driving vehicle depends on the combined trust of these six components. If the trust value of any component decreases, the trust value of the self-driving vehicle decreases. Any compromised or malfunctioning OBU component creates an impact on the traffics like changing the instantaneous flow rate and speed of vehicles in the adjacent areas of a self-driving vehicle of interest. According to the earlier description, the trust of a self-driving vehicle can be carried out by evaluating the following propositional logic term:

$$(I_1 \wedge I_2 \wedge I_3 \wedge I_4)) \wedge (E_1 \wedge E_2) \tag{5.1}$$

w$here, I_1, I_2, I_3, I_4, E_1$ and E_2 are within [0,1].

Since all of the six components of (1) are combined using the AND operator to become a self-driving vehicle trustworthy, all of them need to be trustworthy. Therefore, one of the non-trustworthy components makes the self-driving vehicle non-trustworthy. For this reason, CertainLogic is very sensitive to the level of the trustworthiness of those individual components. CertainLogic is developed based on a model called CertainTrust. CertainTrust model is used for expressing opinions and construct modeling probabilities that are subject to uncertainty. Though CertainTrust is developed for evidence-based trust, it can also represent an uncertain value. In CertainTrust, the expectation (trust value) of opinion can be defined as:

$$\varepsilon(t, c, f) = tc + (1 - c)f \tag{5.2}$$

where $\varepsilon(t, c, f) \in [0, 1]$.

The average rating (t) is the level of support for the truth of proposition from the past observation. Certainty (c) indicates the degree to which average rating will be in the future. Initial expectation (f) represents the truth of a proposition if there is no evidence supporting or denying it. We need to estimate the trust of the six components and thus find out the number of evidence supporting (s) or denying (n) the truth.

Considering the standard profiles of supporting and denying the truth and instantaneous observations, we can calculate the value of (s) and (n). s_0 and n_0 also represent the amount of supporting and contradicting the truth, respectively, but are derived from prior knowledge. From these four values, t, c and f can be calculated as:

$$t = \begin{cases} 0.5, \text{if s+n=0} \\ \frac{s}{s+n}, \text{else} \end{cases} \tag{5.3}$$

$$c = \frac{s+n}{s+n+2} \tag{5.4}$$

$$f = \frac{s_0}{s_0+n_0} \tag{5.5}$$

Up to now, the theoretical model for assessing trust level of the individual component has been derived. To determine the trust value of a self-driving vehicle, we need to combine trust values $\varepsilon(t,c,f)$ of six components using a logical AND operator. The combined trust value can be calculated using the following formulas:

$$t_{I_1} \wedge t_{I_2} = \begin{cases} \frac{1}{c_{I_1} \wedge c_{I_2}} c_{I_1} c_{I_2} t_{I_1} t_{I_2} + d, \text{ if } c_{I_1} \wedge c_{I_2} = 0 \\ 0.5, else \end{cases} \tag{5.6}$$

where $d = \frac{c_{I_1}(1-c_{I_2})(1-f_{I_1})f_{I_2}t_{I_1} + (1-c_{I_1})f_{I_1}(1-f_{I_2})t_{I_2}}{1-f_{I_1}f-I_2}$

$$\begin{aligned} c_{I_1} \wedge c_{I_2} = c_{I_1} + c_{I_2} - c_{I_1}c_{I_2} - \\ \frac{(1-c_{I_1})c_{I_2}(1-f_{I_1})t_{I_2} + c_{I_1}(1-c_{I_2})(1-f_{I_2})t_{I_1}}{1-f_{I_1}f_{I_2}} \end{aligned} \tag{5.7}$$

$$f_{I_1} \wedge f_{I_2} = f_{I_1} f_{I_2} \tag{5.8}$$

where, t_{I_1}, c_{I_1} and f_{I_1} represent the value of t, c and f for I_1. Since an AND operator follows associative law, we can derive the truth (trust) value of (5.1) by applying 5.6-5.8 repeatedly.

To obtain the value of $\varepsilon(t, c, f)$ defined in (5.2), we need to derive the values of s, s_0, n and n_0 . s_0 and n_0 represent the prior evidence and hence they can be determined from their relevant historical data. s and n can be calculated by mapping CertainLogic into Beta Distribution Function (BDF). Before discussing this mapping, we present the BDF in this section. The BDF is a commonly used distribution for a random variable $0 \leq P \leq 1$. The Beta probability density function f (P, Φ, χ) is defined as:

$$f(P|\Phi, \chi) = \frac{\Gamma(\Phi + \chi)}{\Gamma(\Phi\chi)} P^{(\Phi-1)} 1 - P^{(\chi-1)} \tag{5.9}$$

Here, Φ and χ indicate the number of successful and unsuccessful outcomes for a particular event. How to measure Φ and χ for a self-driving vehicle using the traffic characteristics (e.g., flow rate, speed) is detailed in Section 5.1.3

The expected value of BDF given in (5.10) is defined as:

$$E(f(P|\Phi, \chi)) = \frac{\Phi}{\Phi + \chi} \tag{5.10}$$

Now, mapping the CertainLogic into BDF is defined as: $(t, c, f) = m^B_{CT}(s, n, s_0, n_0)$,

where, s= Φ and n= χ. Thus, the equation of t, c, and f can rewritten as:

$$t = \begin{cases} 0.5, \text{ if } \Phi + \chi = 0 \\ \frac{\Phi}{\Phi+\chi}, \text{ else} \end{cases} \tag{5.11}$$

$$c = \frac{\Phi + \chi}{\Phi + \chi + 2} \tag{5.12}$$

Note that f is defined in (5.5).

Using (5.2), (5.5), (5.11) and (5.12), we can calculate the trust value of each component of OBU. After this, we can use (5.6), (5.7) and (5.8) repeatedly to calculate the trust of a self-driving vehicle.

So far, the theoretical model for estimating the trust value of a self-driving applying CertainLogic is completed. Now, how to assess its trust value using the subjective logic is articulated in the following section.

5.1.2 Trust model using Subjective Logic (the DS theory)

There are many methods related to subject logic available in the literature, such as Bayesian theory, rule-based inferences system, and DST. We have chosen the DST because it is based on the generalized Bayesian theory and provides support for different propositions using temporal data. For our proposed model, the frame of discernment is defined as:

$$H = (T, \neg T) \tag{5.13}$$

where T and $\neg T$ represent the proposition of the current observation being trustworthy and not trustworthy, respectively.

Assuming j=1, j=2, j=3, j=4 , j=5 , and j=6 represent Lidar, acoustic sensor, radar, camera, GPS data, and transferred messages, respectively. The lower limit of the trust value of i^{th} self-driving vehicle can be defined using the belief function of the DS theory [40] as:

$$bel_i(T) = \frac{1}{1-k} \times \sum_{\cap B_i = T \neq \emptyset} \prod_{1 \leq i \leq 6} m_{ij}(B_i) \tag{5.14}$$

where, B_i is a set of observable outcome for each component of the self-driving vehicle and k is defined as:

$$k = \sum_{\cap B_i = \emptyset} \prod_{1 \leq i \leq 6} m_{ij}(B_i) \tag{5.15}$$

Here, for $T \in B_i$, $m_{ij}(B_i) = m_{ij}(T)$ represents the mass function (the trust value) of j^{th} component (e.g., $I_1, I_2, or E_2$). Using BDF, we can define $m_{ij}(T)$ as:

$$m_{ij}(T) = \frac{\Phi_{ij}}{\Phi_{ij} + \chi_{ij}} \tag{5.16}$$

where, Φ_{ij} and χ_{ij} represent the successful and unsuccessful outcomes for the j^{th} component of i^{th} self-driving vehicle, respectively. As mentioned before, how to derive the values of these two parameters is detailed in Section 5.1.3.

According to the Shannon information theory, the uncertainty is the highest when $m_{ij}(T)$=0.5. If the value of $m_{ij}(T)$ moves in either direction from 0.5, the uncertainty decreases. Applying the principle of Shannon information theory, the uncertainty associated with $m_{ij}(T)$ i.e., the probability, $m_{ij}\ (T \vee \neg T)$ where $(T \vee \neg T) \in B_i$ is defined as [163]:

$$\begin{aligned} m_{ij}(T \vee \neg T) = -m_{ij}(T) log_2 m_{ij}(T) - \\ (1 - m_{ij}(T)) log_2 (1 - m_{ij}(T)) \end{aligned} \tag{5.17}$$

where, the probability, $m_{ij}(\neg T)$ is:

$$m_{ij}(\neg T) = 1 - m_{ij}(T) - m_{ij}(T \vee \neg T) \tag{5.18}$$

The upper limit (plausibility) of i^{th} self-driving vehicle trust value is:

$$pl_i(T) = 1 - bel_i(\neg T) \tag{5.19}$$

5.1.3 Estimating parameters of Φ and χ

The compromised or malfunctioning OBU component(s) create an impact on the traffic patterns like changing the instantaneous flow rate and speed of vehicles in the adjacent areas of interest for a self-driving vehicle. Note, different types and amount of impacts

can be manifested on traffic patterns and a transportation system for various compromised OBU components. We can use the relevant impacts to estimate the value of Φ_{ij} and χ_{ij} for j^{th} component. For example, we can consider the impact of each of the six breached components on the traffic flow rate and the speed of vehicles. An approach to calculate the value of Φ_{ij} and χ_{ij} would be as follows:
If the observable flow rate falls within the 95% confidence interval of the normally distributed historical flow rate as shown in Section 5.2, Φ^f_{ij} will increase by 1; otherwise, χ^f_{ij} will increase by 1. Where, Φ^f_{ij} and χ^f_{ij} indicate the number of successful and unsuccessful outcomes for the flow rate, respectively. Similarly, following the normal distribution of the speed, we can calculate the number of successful and unsuccessful outcomes (Φ^s_{ij}, χ^s_{ij}) for the speed.

5.1.4 Fusion for the flow rate and speed for each OBU component

For CertainLogic, $\varepsilon^f_{ij}(t, c, f)$ values of t, c, f derived using Φ^f_{ij}, χ^f_{ij} , Φ^s_{ij} and χ^s_{ij} using (5.5), (5.11) and (5.12). In this CertainLogic, for the flow rate, we can calculate $\varepsilon^f_{ij}(t, c, f)$ including t,c, and f using the values of Φ^f_{ij} and χ^f_{ij}.

In the similar way, for the speed, we can calculate $\varepsilon^s_{ij}(t, c, f)$ including t, c and f using the values of Φ^s_{ij} and χ^s_{ij}.

For the combined trust value, we can calculate $\varepsilon_{ij}(t, c, f)$ of $\varepsilon^f_{ij}(t, c, f)$ and $\varepsilon^s_{ij}(t, c, f)$ can be calculated by using (5.6)-(5.8) and (5.2).

Similar to the CertainLogic, we can calculate m^f_{ij} (T) and $m^s_{ij}(T)$ using (5.16) and then fuse them using to obtain $m_{ij}(\mathrm{T})$

5.2 Evaluation of The Trust Model

5.2.1 Simulation Environment

In order to analyze the performance of our proposed method, we require to use either a real traffic network or a realistic simulated environment capable of emulating real-life

traffic and road networks. We chose the latter and developed such a simulated model using SUMO and the VicRoads's historical data on real traffic and the road map of a location in Melbourne CBD in Victoria. VicRoads is a road and traffic authority in the state of Victoria, Australia. SUMO is an open-source, microscopic, multi-modal traffic simulations. It allows us to simulate traffic scenarios through a given road network and using various vehicle types, flow rates, densities, and other traffic parameters. Each vehicle is modeled explicitly, has its route, and moves individually. While implementing our model on the SUMO platform using real traffic on the road network in a city, the following parameters were considered in setting up the simulation environment. We selected the peak-time density and flow rate in our simulation using the traffic data from VicRoads during 08:00 am to 09:00 am Monday at five busy corners of Melbourne CBD: (i) Lonsdale and Russel street, (ii) Collins and Kings St, (iii) Elizabeth and Latrobe St, (iv) Collins and Swanston St, and (v), Flinders and Swanston St Melbourne.

Figure 4.2(a) in Section 4.2 shows the histogram and the corresponding fitting normal curves of different flow rates of Intersection 1.

In this project, since we aim to use historical data to monitor the status of a current traffic signal at a particular time, we collected all required and relevant data from VicRoads traffic data [38]. We have tested 40, 41, 39, 42 and 44 samples for scenarios 1 to 6 described in Section 5.2.2. We initially set up the simulation as per the normal historical data available on the VicRoads website [151]. Using this data, we then selected different incidents, vehicle breakdown places in the monitored area, unusual self-driving vehicle stops due to OBU component malfunctions, or malicious behavior. Additionally, in the simulation, we included instances and locations where an untrustworthy self-driving vehicle can enter and provide false information about traffic conditions, which may lead the following vehicles to crash or change the route or increase congestion by sudden stop. Our proposed approach considers the traffic condition is normal if the observed flow rate falls within the 95% confidence interval of the normal distribution curve, as shown in Figure 4.2 (a).

5.2.2 Results and Analysis

We have monitored six different scenarios in our simulation, and there are different cases in each scenario. The scenarios are described below:

• **Scenario #1**: A pedestrian was crossing, and the self-driving vehicle's camera was unable to detect that on time. As a result, the vehicle failed to slow down to provide a pedestrian giveaway. We assumed that there was no collision and no major change in traffic condition occurred.

• **Scenario #2**: Radars failed to detect the gap between the monitored self-driving vehicle and the following vehicle while changing the lane. There was no collision, but it forced the following vehicle to slow down. It caused other vehicles further behind to slow down as well, resulting in a reduction in the average speed of the road.

• **Scenario #3**: A malfunctioning GPS was showing the wrong location, forcing the self-driving vehicle to take a wrong turn. There was no overall effect on the VANET, but the trustworthiness of the GPS was reduced.

• **Scenario #4**: In this scenario, an acoustic sensor of the self-driving vehicle heard a wrong crash sound and stopped suddenly on the road. The radar also failed to determine the safe distance between this self-driving vehicle and the following vehicle. This sudden stop caused a crash with the following vehicle, and the traffic congestion increased due to the crash.

• **Scenario #5**: Both the Lidar and cameras were unable to detect an object on-road, and the self-driving vehicle crashed with the object. Self-driving vehicles sent incorrect traffic condition messages that caused prolonged congestion.

• **Scenario #6**: The GPS was showing the incorrect location, and also other OBU components were unable to detect the correct location. As a result, the vehicle made a wrong turn and collided with roadside infrastructure.

In all the scenarios mentioned above, we have calculated the change of trust for each concerned OBU component of the self-driving vehicle. The self-driving vehicle acted abnormally and consequently caused road hazard in some cases. From the simulation,

Table 5.1: Scenario 1

Component	CertainLogic				DST	
	t	c	f	ε (t,c,f)	T	u
1	0.975	0.953	0.975	0.976	0.976	0.096
2	0.146	0.953	0.170	0.171	0.159	0.212
3	0.927	0.953	0.786	0.786	0.855	0.211
4	0.927	0.953	0.902	0.902	0.915	0.185
5	0.927	0.953	0.902	0.902	0.915	0.185
6	0.881	0.955	0.951	0.951	0.916	0.18

Table 5.2: Scenario 2

Component	CertainLogic				DST	
	t	c	f	ε(t,c,f)	T	u
1	0.976	0.953	0.976	0.976	0.976	0.096
2	0.902	0.953	0.927	0.904	0.915	0.185
3	0.927	0.953	0.786	0.920	0.855	0.211
4	0.293	0.953	0.317	0.294	0.305	0.158
5	0.927	0.953	0.902	0.926	0.915	0.185
6	0.881	0.955	0.951	0.884	0.916	0.184

we have determined the effect of that change by measuring the change of flow rate, and speed was. From SUMO, we found the change in speed and flow rate. The changes were used to calculate the Φ, χ, s_0, and n_0 values. As mentioned before, in a realistic environment, the supporting evidence of a component may have a certain level of uncertainty. Using Eqs. (5.2), (5.5), (5.10), (5.11), (5.12), and (5.14), we have calculated the trust value and uncertainty of the individual OBU component for all six different scenarios.

Table 5.3: Scenario 3

Component	CertainLogic				DST	
	t	c	f	ε(t,c,f)	T	u
1	0.976	0.953	0.976	0.976	0.976	0.096
2	0.976	0.953	0.927	0.973	0.951	0.144
3	0.927	0.953	0.786	0.920	0.855	0.211
4	0.927	0.953	0.902	0.926	0.915	0.185
5	0.268	0.953	0.293	0.269	0.280	0.173
6	0.881	0.955	0.951	0.884	0.916	0.184

Table 5.4: Scenario 4

Component	CertainLogic				DST	
	t	c	f	ε(t,c,f)	T	u
1	0.976	0.953	0.976	0.976	0.976	0.096
2	0.951	0.953	0.854	0.947	0.902	0.194
3	0.268	0.953	0.146	0.263	0.207	0.205
4	0.293	0.953	0.317	0.294	0.305	0.158
5	0.927	0.953	0.902	0.926	0.915	0.185
6	0.881	0.955	0.951	0.884	0.916	0.184

Table 5.5: Scenario 5

Component	CertainLogic				DST	
	t	c	f	ε(t,c,f)	T	u
1	0.049	0.953	0.171	0.054	0.110	0.201
2	0.146	0.953	0.171	0.147	0.159	0.212
3	0.927	0.953	0.786	0.920	0.855	0.211
4	0.927	0.953	0.902	0.926	0.915	0.185
5	0.927	0.953	0.902	0.926	0.915	0.185
6	0.122	0.953	0.171	0.124	0.146	0.211

Table 5.6: Scenario 6

Component	CertainLogic				DST	
	t	c	f	ε(t,c,f)	T	u
1	0.098	0.953	0.195	0.102	0.146	0.211
2	0.146	0.953	0.171	0.147	0.159	0.212
3	0.073	0.953	0.146	0.077	0.110	0.201
4	0.122	0.953	0.171	0.124	0.146	0.211
5	0.927	0.953	0.902	0.926	0.915	0.185
6	0.881	0.955	0.951	0.884	0.916	0.184

Table 5.7: Uncertainty Comparison for CertainLogic and Dempster-Shafer

Scenario	CertainLogic				Dempster-Shafer	
	t	c	f	ε(t,c,f)	T	u
1	0.100	0.962	0.101	0.1	0.419	0.04
2	0.194	0.963	0.193	0.194	0.358	0.04
3	0.64	0.969	0.18	0.126	0.214	0.037
4	0.121	0.982	0.033	0.12	0.048	0.0117
5	0.002	0.905	0.003	0.002	0.012	0.007
6	0.008	0.995	0.003	0.003	0.004	0.003

Tables 5.1-5.6 show the trust values and the uncertainty measures for each component of the self-driving vehicle for all six scenarios. It reveals that, for all cases, uncertainty is higher in the DST. CertainLogic can calculate the certainty in a better way considering the real scenarios. In Table 5.1, it shows that the trust value of the camera of the self-driving vehicle is 0.294 in the CertainLogic while it is 0.305 in the DST. Uncertainty in the CertainLogic is 0.047, and in the DST, the uncertainty is 0.158. The overall trust of a self-driving vehicle for scenario #1 attains 0.1 for the CertainLogic and 0.419 for the DST. Similarly, the overall trust scores for the self-driving vehicle are 0.194, 0.126, 0.12, 0.002 and 0.003 for scenarios#2 to #6, respectively for the CertainLogic, while those are 0.358, 0.214, 0.048, 0.012, and 0.004 for the DST. Since a self-driving vehicle is responsible for the safe, smart, and reliable travel for the passenger, the trust level of all components should be higher for it to maintain the safety of the passenger as well as other road users. The CertainLogic was able to detect the trust label in a better way with lower uncertainty. The overall trust of a self-driving vehicle does not only depend on the reliability of the OBU components but also depends on the trustworthiness of the message they are transferring to the other vehicles of the VANET. Our model takes the trustworthiness of the GPS data and the message to reduce the possibilities of a self-driving vehicle being act as a malicious node in the VANET. Comparing the data provided by the OBU units of the self-driving vehicle with the real-time flow rate and the average speed of the

dynamic traffic situation estimates the trustworthiness of the self-driving vehicles more accurately.

Table 5.7 shows the comparison of the CertainLogic and the DST for trust value and uncertainty for all different scenarios. We can see that the uncertainty value is more sensitive in CertainLogic. If more than one components have less trust value, it reduces the trust values sharply in CertainLogic. As we mentioned above, if the trust value moves to 0 or 1 from 0.5, the certainty increases. As we used the AND logical operator to calculate the overall value of the trust and certainty of self-driving vehicles, it is more sensitive when more than one component is used.

5.3 Conclusion

In this chapter, we introduce a model to measure the trust value of a self-driving car, which employs the OBU components along with GPS data and safety messages. The impact of an untrustworthy OBU component on traffic conditions (e.g., traffic flow change and speed change) is used in many different intersections under different scenarios to measure the trustworthiness of OBU components. Results demonstrate that the combined trust scores calculated by both subjective logic and CertainLogic change with the trust level of OBU components, safely messages, and GPS data. If the trust value of multiple OBU components decreases, the overall trust score decreases sharply, and CertainLogic delivers better uncertainty information than the DS decision theory when all relevant information is fused.

So far, in this thesis, we introduce an emergency vehicle priority system that provides priority to an EV considering the impact on other on-road relevant vehicles. To increase the reliability of the current and future ITS, we introduce an IDS for the traffic signals for the first time and accessing the trust value of a self-driving car, respectively. However, as with other research projects, there are a few ways these proposed techniques can be improved further. Some of the further research challenges associated with these techniques are described in the next chapter (the final chapter of the thesis).

Chapter 6

Conclusion and Future Works

6.1 Conclusions

Efficient traffic management is a very complex task because of the dynamic characteristics of traffic on-road. Emergency services are taking more than the recommended response time to reach to the incident place for the traffic congestion. The increasing number of vehicles, mainly in the urban areas, use of the roadside infrastructure with smart and wireless sensors, and the introduction of self-driving cars on the road also make the full ITS vulnerable to the cyber-attack.

This thesis has directly addressed these issues by introducing an emergency vehicle priority system, an intrusion detection system for traffic signals, and a trust measurement model for self-driving cars.

In the course of achieving the research objectives as outlined in Chapter 1, the key achievements of this thesis, along with the significance of the proposed systems and models are summarised below:

- An incident reduces the traffic flow, average vehicle speed, and increases traffic congestion and hence, causes additional traffic congestion in the surrounding cells of the incident place. Emergency vehicles struggle to meet their targeted response time because of this additional traffic congestion. Our proposed EPVS, introduced in Chapter 3, can determine the priority code based on the type of incident. Sending the right emergency vehicle with proper priority code reduces the impact of an incident and expedites its clearance. Our system also calculates

the number of interventions required for an EV's faster travel, considering the delay of other vehicles on the surround cells of the EV travel path. For an incident that occurred in short distance (ten signals), our proposed system reduces EV travel time by 15.4, 8.6, and 0.8% for 30, 50, and 70% occupancy rates, respectively, compared with one intervention used in [11] and [15]. Similarly, for long-distance (20 signals), the reduction rates are 13.4 and 4.8% for 30 and 50% occupancy rates, respectively. For occupancy rate 70% in long-distance, EV travel time remains similar to that of produced by [11] and [15]. The traffic signal is one of the most critical components of an ITS. A disruption in traffic signal operation caused by an incident, hardware malfunction, or intrusion can increase traffic congestion and delays the emergency vehicle response time. Consequently, it can be life-threatening. This critical issue leads us to introduce an intrusion detection system for a traffic signal.

- Modern traffic signals are equipped with many wireless sensors to collect data from the RSUs and the smart vehicles on the road, process these data, and send these collected data or decisions derived from them to the central traffic controller. Application of these wireless technologies in these traffic signals improves the quality of the services they provide, but also put the traffic signals in the risk of being cyberattack. To make traffic signal reliable in this thesis, we introduce an Intrusion Detection System (IDS) for a traffic signal. Our proposed IDS uses three major instantaneous observational traffic data (flow rate, vehicle speed, and signal phase time) and their respective historical data. The Dempster-Shefar (DS) theory fuses the evidence derived from observational data. Shannon's entropy is used to determine the uncertainty associated with the evidence. To test and evaluate the system, we created two normal and two intruded scenarios in five different traffic signal intersections. Result shows using all three pieces of evidence provide a better detection result for normal traffic conditions, while two pieces of evidence provide better detection results for an intruded traffic signal. Our proposed system can detect intrusion with 91.1 % overall accuracy and 91.7% sensitivity. The operation of traffic signals in ITS relies on the traffic information (e.g., flow rate, speed,

density) provided by the in-road sensors and the reliability of semi-autonomous and autonomous vehicles. This motivated us to introduce a novel model to measure the trust level of a self-driving car based on the trustworthiness of its OBU components along with GPS data and safety messages.

- The number of self-driving cars is increasing sharply day by day. These self-driving smart vehicles are dependent on different types of OBUs to communicate with other vehicles and the roadside infrastructures. Many studies (e.g., [164]) have been done so far that focus mainly on data integrity, accuracy, and reliability. The trustworthiness of the GPS information and safety messages of an autonomous vehicle is measured in [40], [113] and [158]. Up to our knowledge, there exists no method which considers the trustworthiness of OBU components in measuring the trustworthiness of driverless cars. Our proposed model presented in 4 use four OBU components, GPS data, and the safety messages to enhance the accuracy of assessing the reliability of a self-driving car. For modeling, we use both CertainLogic and subjective logic (DS theory). The result indicates that CertainLogic is more sensitive to the distrust level of individual components than subjective logic (DS theory). All of the six different scenarios we have used show the more OBU components have less trust value, the more sharp decrease of overall trust value of a self-driving car is.

- We evaluated and tested all of the techniques mentioned above using the simulation environment created in SUMO. A real map of Melbourne CBD was used in the SUMO platform. Historical morning peak-time traffic data of 52 different Mondays taken from VicRoads' website were used to inject the traffic flow and density in the simulation model. Two different incident locations, one of them is ten signals away from the EV dispatch location and the other one 20 signals away, were created to test and evaluate the performance of our proposed EVPS. We evaluated the performance of our proposed IDS considering different traffic and signal characteristics such as occupancy rate, flow rate, phase time, and vehicle speed in five different intersections. Four different, two normal and two intruded,

scenarios were used in evaluating and validating our proposed trust measurement model. Results show the high accuracy of our proposed techniques under all selected scenarios.

6.2 Threats to Validity

Efficient traffic management faces number of threats and challenges due to the dynamic characteristics (e.g., change of flow rate, incidents, events, vehicle speed change) of on-road traffic. Some of the threats where our proposed model may not perform to their desired expectation are given below:

- In Chapter 3, our proposed EVPS provides priority to the emergency vehicle based on a single incident. If more than one incidents occur in close vicinity, it will increase the emergency vehicle travel time and incident clearance time.
- Our proposed EVPS uses Algorithm 2 to calculate the cell clearance time for number of interruptions needed. Two left and two right cells (denoted as k) were considered to calculate the cell clearance time. If the value of k is increased to calculate the cell clearance time based on more than two cells, the calculation complexity will increase and may change the number of interruptions depending on the traffic conditions (e.g., occupancy rate, average vehicle speed).
- The trust measurement system proposed in Chapter 4 measures the trust of the overall vehicle. If the traffic signal or the traffic controller system malfunctions or security breach occurs, it will affect the traffic conditions (e.g., flow rate, vehicle speed, and phase time) and result in the vehicle of interest being untrustworthy.
- Our proposed intrusion detection system introduced in Chapter 5 detects the intrusion of a traffic signal by comparing the historical traffic data and real-time traffic data. If the traffic condition vastly changes due to external factors (e.g., change of weather and road condition, vehicle break down), this may increase false positive rate.

6.3 Future Works

There are many potential areas that could be explored further to extend the research projects presented in this thesis. Some of the future research directions are highlighted as follows:

- We have used priority for emergency vehicles, but the proposed fundamental concept of this priority scheme can be extended for other relevant vehicles (e.g., public transport priority) and pedestrian crossing. For example, the green signal phase time for pedestrian crossing can be used for providing priority to the pedestrians waiting in the signal. Providing priority to public vehicles will increase the quality of service provided by public transportation authorities while providing proper priority to pedestrians will increase the safety of the road users.

- Our proposed EVPS discussed in Chapter 3 considers one EV vehicle coming from one direction. For saving lives and reducing the damage caused by severe incidents with high magnitude, multiple EVs from the same emergency service department or multiple departments need to travel to an incident place from different directions. Therefore, our proposed EVPS can be extended further to determine the number of interventions needed in multiple directions. Providing priority to multiple EVs from multiple directions in case of critical emergencies (e.g., bush fire, terrorist attack) will save lives and reduce property damage.

- If a traffic signal is intruded for a long time, it can cause huge congestion and collision. The collisions can be fatal and cause a human loss. Shortly, it is important to measure the impact of an intrusion in a traffic signal. For making a traffic signal more reliable, the quick recovery from an intruded system needs to be introduced yet.

- Traffic flow rate, vehicle speed, and signal phase time have been used to detect an intrusion in a traffic signal. There are many more traffic conditions and other factors that can change the traffic flow at an intersection. The impact of other

evidential traffic data, for example, traffic density, weather conditions, and road works, can be investigated further. This investigation will allow researchers and the traffic control departments to perceive the impact of other traffic and relevant data on changing the dynamic characteristic of the traffic conditions.

Publications from PhD Research

Articles that have been Published

Peer Reviewed International Conference Papers:

1. Chowdhury, A. (2016, September). Priority based and secured traffic management system for emergency vehicle using IoT. In *2016 International Conference on Engineering & MIS (ICEMIS)* (pp. 1-6). IEEE. **Best Paper Award in IEEE International Conference on Engineering & MIS** Available at: https://ieeexplore.ieee.org/document/7745309

2. Chowdhury, A. (2016, October). Recent cyber security attacks and their mitigation approaches–an overview. In *International conference on applications and techniques in information security* (pp. 54-65). Springer, Singapore. Available at: https://link.springer.com/chapter/10.1007/978-981-10-2741-3_5

3. Chowdhury, A. (2017, February). Cyber attacks in *mechatronics systems based on Internet of Things. In 2017 IEEE International Conference on Mechatronics (ICM)* (pp. 476-481). IEEE. Available at: https://ieeexplore.ieee.org/document/7921154

4. Chowdhury, A., Karmakar, G., Kamruzzaman, J., & Saha, T. (2018, October). Detecting Intrusion in the Traffic Signals of an Intelligent Traffic System. In *International Conference on Information and Communications Security* (pp. 696-707). Springer, Cham. **(Core Ranking: B)**. Available at: https://link.springer.com/chapter/10.1007/978-3-030-01950-1_41

5. Chowdhury, A., Karmakar, G., & Kamruzzaman, J. (2019, August). Trusted Autonomous Vehicle: Measuring Trust using On-Board Unit Data. In *2019* 18^{th} *IEEE International Conference On Trust, Security And Privacy In Computing And Communications/*13^{th} *IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 787-792). IEEE. **(Core Ranking: A)** Available at: https://ieeexplore.ieee.org/document/8887412

Peer Reviewed Book Chapter:

1. Chowdhury, A., Karmakar, G., & Kamruzzaman, J. (2017). Survey of recent cyber security attacks on robotic systems and their mitigation approaches. In Detecting and Mitigating Robotic Cyber Security Risks (pp. 284-299). IGI Global. Avialable at: https://www.igi-global.com/gateway/chapter/180078

Journal Paper:

1. Chowdhury, A., Karmakar, G., & Kamruzzaman, J., "Trustworthiness of Self-Driving Vehicles for Intelligent Transportation Systems in Industry Applications," *IEEE Transactions on Industrial Informatics*, 2020.**(Impact Factor: 7.377), (Quartiles: Q1)**

Bibliography

[1] RACV. (2016) Racv redspot survey & traffic congestion on vicroads. (Last accessed on: 28/8/2019). [Online]. Available: https://www.racv.com.au/membership/member-benefits/expert-advice/advocacy-for-members/improving-victorias-roads-transport/congestion.html

[2] A. Skabardonis, "Control strategies for transit priority," *Transportation Research Record*, vol. 1727, no. 1, pp. 20–26, 2000.

[3] G. Barney and L. Al-Sharif, *Elevator Traffic Handbook: Theory and Practice*. Routledge, 2015.

[4] C. Daganzo and C. Daganzo, *Fundamentals of transportation and traffic operations*. Pergamon Oxford, 1997, vol. 30.

[5] J. F. Shortle, J. M. Thompson, D. Gross, and C. M. Harris, *Fundamentals of queueing theory*. John Wiley & Sons, 2018, vol. 399.

[6] M. Jagielski, N. Jones, C.-W. Lin, C. Nita-Rotaru, and S. Shiraishi, "Threat detection for collaborative adaptive cruise control in connected cars," in *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2018, pp. 184–189.

[7] L. Chen, Z. Yang, J. Ma, and Z. Luo, "Driving scene perception network: Real-time joint detection, depth estimation and semantic segmentation," in *2018 IEEE Winter Conference on Applications of Computer Vision (WACV)*. IEEE, 2018, pp. 1283–1291.

[8] M. R. Endsley, "Autonomous driving systems: A preliminary naturalistic study of the tesla model s," *Journal of Cognitive Engineering and Decision Making*, vol. 11, no. 3, pp. 225–238, 2017.

[9] R. Sell, A. Rassõlkin, R. Wang, and T. Otto, "Integration of autonomous vehicles and industry 4.0." *Proceedings of the Estonian Academy of Sciences*, vol. 68, no. 4, 2019.

[10] W. Goodall, T. Dovey, J. Bornstein, and B. Bonthron, "The rise of mobility as a service," *Deloitte Rev*, vol. 20, pp. 112–129, 2017.

[11] A. K. Mittal and D. Bhandari, "A novel approach to implement green wave system and detection of stolen vehicles," in *2013 3rd IEEE International Advance Computing Conference (IACC)*. IEEE, 2013, pp. 1055–1059.

[12] T. Litman, *Autonomous vehicle implementation predictions*. Victoria Transport Policy Institute Victoria, Canada, 2017.

[13] P. Aavani, K. Mithun, S. Sneha, and S. Rohit, "A review on adaptive traffic controls systems," *International Journal of Latest Engineering and Management Research*, vol. 2, no. 1, pp. 52–57, 2017.

[14] A. Lidbe, E. Tedla, A. Hainen, A. Sullivan, and S. Jones Jr, "Comparative assessment of arterial operations under conventional time-of-day and adaptive traffic signal control." *Advances in Transportation Studies*, vol. 42, 2017.

[15] H. Xie, S. Karunasekera, L. Kulik, E. Tanin, R. Zhang, and K. Ramamohanarao, "A simulation study of emergency vehicle prioritization in intelligent transportation systems," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*. IEEE, 2017, pp. 1–5.

[16] Austroads. (2019) Trials. (Last accessed on: 16/5/2019). [Online]. Available: https://austroads.com.au/drivers-and-vehicles/connected-and-automated-vehicles/trials

[17] G. Meyer, "European roadmaps, programs, and projects for innovation in connected and automated road transport," in *Road Vehicle Automation 5*. Springer, 2019, pp. 27–39.

[18] A. Stocker and S. Shaheen, "Shared automated mobility: early exploration and potential impacts," in *Road Vehicle Automation 4*. Springer, 2018, pp. 125–139.

[19] D. Pojani and D. Stead, "Sustainable urban transport in the developing world: beyond megacities," *Sustainability*, vol. 7, no. 6, pp. 7784–7805, 2015.

[20] A. Bazzi, B. M. Masini, A. Zanella, and I. Thibault, "On the performance of ieee 802.11 p and lte-v2v for the cooperative awareness of connected vehicles," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 419–10 432, 2017.

[21] I. H. Zohdy and H. A. Rakha, "Intersection management via vehicle connectivity: The intersection cooperative adaptive cruise control system concept," *Journal of Intelligent Transportation Systems*, vol. 20, no. 1, pp. 17–32, 2016.

[22] T. Petrov, M. Dado, P. Kortis, and T. Kovacikova, "Evaluation of packet forwarding approaches for emergency vehicle warning application in vanets," in *2018 ELEKTRO*. IEEE, 2018, pp. 1–5.

[23] J. B. Cicchino, "Effectiveness of forward collision warning and autonomous emergency braking systems in reducing front-to-rear crash rates," *Accident Analysis & Prevention*, vol. 99, pp. 142–152, 2017.

[24] Z. Huang, D. Chu, C. Wu, and Y. He, "Path planning and cooperative control for automated vehicle platoon using hybrid automata," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 3, pp. 959–974, 2018.

[25] V. A.-G. Report. (2015) Emergency service response times. (Last accessed on: 15/05/2018). [Online]. Available: http://www.audit.vic.gov.au/publications/20150319-Emergencyservice/20150319-Emergency-service.pdf

[26] R. Oorni and A. Goulart, "In-vehicle emergency call services: ecall and beyond," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 159–165, 2017.

[27] A. Karndacharuk and A. Hassan, "Traffic incident management: framework and contemporary practices," in *Australasian Transport Research Forum (ATRF), 39th, 2017, Auckland, New Zealand*, 2017.

[28] K. Nellore and G. Hancke, "A survey on urban traffic management system using wireless sensor networks," *Sensors*, vol. 16, no. 2, p. 157, 2016.

[29] P. Händel, J. Ohlsson, M. Ohlsson, I. Skog, and E. Nygren, "Smartphone-based measurement systems for road vehicle traffic monitoring and usage-based insurance," *IEEE systems journal*, vol. 8, no. 4, pp. 1238–1248, 2013.

[30] B. Ghazal, K. ElKhatib, K. Chahine, and M. Kherfan, "Smart traffic light control system," in *2016 third international conference on electrical, electronics, computer engineering and their applications (EECEA)*. IEEE, 2016, pp. 140–145.

[31] V. Pattanaik, M. Singh, P. Gupta, and S. Singh, "Smart real-time traffic congestion estimation and clustering technique for urban vehicular roads," in *2016 IEEE region 10 conference (TENCON)*. IEEE, 2016, pp. 3420–3423.

[32] W. Sun, J. Liu, and H. Zhang, "When smart wearables meet intelligent vehicles: Challenges and future directions," *IEEE wireless communications*, vol. 24, no. 3, pp. 58–65, 2017.

[33] S. S. Albouq and E. M. Fredericks, "Lightweight detection and isolation of black hole attacks in connected vehicles," in *2017 IEEE 37th international conference on distributed computing systems workshops (ICDCSW)*. IEEE, 2017, pp. 97–104.

[34] B. DeBruhl, S. Weerakkody, B. Sinopoli, and P. Tague, "Is your commute driving you crazy?: a study of misbehavior in vehicular platoons," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2015, p. 22.

[35] Y. Feng, S. Huang, Q. A. Chen, H. X. Liu, and Z. M. Mao, "Vulnerability of traffic control system under cyber-attacks using falsified data," in *97th Annual Meeting of the Transportation Research Board*, 2018.

[36] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2014.

[37] W. Maddern, G. Pascoe, C. Linegar, and P. Newman, "1 year, 1000 km: The oxford robotcar dataset," *The International Journal of Robotics Research*, vol. 36, no. 1, pp. 3–15, 2017.

[38] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of sumo-simulation of urban mobility," *International Journal On Advances in Systems and Measurements*, vol. 5, no. 3&4, 2012.

[39] A. Chowdhury, "Priority based and secured traffic management system for emergency vehicle using iot," in *2016 International Conference on Engineering & MIS (ICEMIS)*. IEEE, 2016, pp. 1–6.

[40] Y. Wu, F. Meng, G. Wang, and P. Yi, "A dempster-shafer theory based traffic information trust model in vehicular ad hoc networks," in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. IEEE, 2015, Conference Proceedings, pp. 1–7.

[41] A. Chowdhury, G. Karmakar, J. Kamruzzaman, and T. Saha, "Detecting intrusion in the traffic signals of an intelligent traffic system," in *International Conference on Information and Communications Security*. Springer, 2018, pp. 696–707.

[42] S. Ries, S. M. Habib, M. Mühlhäuser, and V. Varadharajan, "Certainlogic: A logic for modeling trust and uncertainty," in *International Conference on Trust and Trustworthy Computing*. Springer, 2011, pp. 254–261.

[43] A. Chowdhury, G. Karmakar, and J. Kamruzzaman, "Trusted autonomous vehicle: Measuring trust using on-board unit data," in *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2019, pp. 787–792.

[44] A. Chowdhury, G. C. Karmakar, J. Kamruzzaman, and S. Islam, "Trustworthiness of self-driving vehicles for intelligent transportation systems in industry applications," *IEEE Transactions on Industrial Informatics*, 2020.

[45] A. Chowdhury, "Recent cyber security attacks and their mitigation approaches–an overview," in *International conference on applications and techniques in information security*. Springer, 2016, pp. 54–65.

[46] A. Chowdhury, G. Karmakar, and J. Kamruzzaman, "Survey of recent cyber security attacks on robotic systems and their mitigation approaches," in *Detecting and Mitigating Robotic Cyber Security Risks*. IGI Global, 2017, pp. 284–299.

[47] A. Chowdhury, "Cyber attacks in mechatronics systems based on internet of things," in *2017 IEEE International Conference on Mechatronics (ICM)*. IEEE, 2017, pp. 476–481.

[48] N. Moganarangan, N. Balaji, R. S. Kumar, S. Balaji, and N. Palanivel, "Study on static and dynamic traffic control systems," *International Journal of Pure and Applied Mathematics*, vol. 119, no. 12, pp. 565–579, 2018.

[49] B. D. Greenshields, J. Thompson, H. Dickinson, and R. Swinton, "The photographic method of studying traffic behavior," in *Highway Research Board Proceedings*, vol. 13, 1934.

[50] J. M. del Castillo, "Three new models for the flow–density relationship: derivation and testing for freeway and urban data," *Transportmetrica*, vol. 8, no. 6, pp. 443–465, 2012.

[51] M. Treiber, A. Kesting, and D. Helbing, "Delays, inaccuracies and anticipation in microscopic traffic models," *Physica A: Statistical Mechanics and its Applications*, vol. 360, no. 1, pp. 71–88, 2006.

[52] L. A. Pipes, "An operational analysis of traffic dynamics," *Journal of applied physics*, vol. 24, no. 3, pp. 274–281, 1953.

[53] P. G. Gipps, "A behavioural car-following model for computer simulation," *Transportation Research Part B: Methodological*, vol. 15, no. 2, pp. 105–111, 1981.

[54] L. Leclercq and J. A. Laval, "A multiclass car-following rule based on the lwr model," in *Traffic and Granular Flow'07*. Springer, 2009, pp. 151–160.

[55] T. M. Sider, A. Alam, W. Farrell, M. Hatzopoulou, and N. Eluru, "Evaluating vehicular emissions with an integrated mesoscopic and microscopic traffic simulation," *Canadian Journal of Civil Engineering*, vol. 41, no. 10, pp. 856–868, 2014.

[56] G.-l. Chang and Z. Zhu, "A macroscopic traffic model for highway work zones: formulations and numerical results," *Journal of advanced transportation*, vol. 40, no. 3, pp. 265–287, 2006.

[57] C. F. Daganzo, "The cell transmission model, part ii: network traffic," *Transportation Research Part B: Methodological*, vol. 29, no. 2, pp. 79–93, 1995.

[58] P. I. Richards, "Shock waves on the highway," *Operations research*, vol. 4, no. 1, pp. 42–51, 1956.

[59] A. Aw and M. Rascle, "Resurrection of" second order" models of traffic flow," *SIAM journal on applied mathematics*, vol. 60, no. 3, pp. 916–938, 2000.

[60] H. Payne, "Mathematical models of public systems," in *Simul. Counc. Proc. Ser*, vol. 1, 1971, pp. 51–61.

[61] I. Prigogine and F. C. Andrews, "A boltzmann-like approach for traffic flow," *Operations Research*, vol. 8, no. 6, pp. 789–797, 1960.

[62] S. Paveri-Fontana, "On boltzmann-like treatments for traffic flow: a critical review of the basic model and an alternative proposal for dilute traffic analysis," *Transportation research*, vol. 9, no. 4, pp. 225–235, 1975.

[63] A. Alnajajreh, M. Marinelli, and S. Sinesi, "A dynamic mesoscopic network loading model for spillback queuing assessment," in *2019 IEEE International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe)*. IEEE, 2019, pp. 1–5.

[64] A. M. Dahod, A. Schoener, K. Chowdhury, L. Schwartz, M. H. Harper, K. E. Virgile, and A. Gibbs, "Adaptive intelligent routing in a communication system," Feb. 7 2017, uS Patent 9,565,117.

[65] Y. Tang, C. Zhang, R. Gu, P. Li, and B. Yang, "Vehicle detection and recognition for intelligent traffic surveillance system," *Multimedia tools and applications*, vol. 76, no. 4, pp. 5817–5832, 2017.

[66] R. Kolandaisamy, R. Md Noor, I. Ahmedy, I. Ahmad, M. Reza Z'aba, M. Imran, and M. Alnuem, "A multivariant stream analysis approach to detect and mitigate ddos attacks in vehicular ad hoc networks," *Wireless Communications and Mobile Computing*, vol. 2018, 2018.

[67] M. A. Appel and Q. Ahmed, "Intelligent vehicle monitoring for safety and security," SAE Technical Paper, Tech. Rep., 2019.

[68] D. C. Jenn, *Radar and laser cross section engineering*. American Institute of Aeronautics and Astronautics, Inc., 2019.

[69] D. Ding, Q.-L. Han, Z. Wang, and X. Ge, "A survey on model-based distributed control and filtering for industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 2483–2499, 2019.

[70] A. Y. Shahrah and M. A. Al-Mashari, "Adaptive case management framework to develop case-based emergency response system," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 4, pp. 57–66, 2017.

[71] K. P. Sanketh, S. Subbarao, and K. A. Jolapara, "I2v and v2v communication based vanet to optimize fuel consumption at traffic signals," in *13th International IEEE Conference on Intelligent Transportation Systems*. IEEE, 2010, pp. 1251–1255.

[72] X. Hu, Y.-C. Chiu, J. A. Villalobos, and E. Nava, "A sequential decomposition framework and method for calibrating dynamic origin—destination demand in a congested network," *IEEE Transactions on intelligent transportation systems*, vol. 18, no. 10, pp. 2790–2797, 2017.

[73] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, and A. Tuncer, "Uav-enabled intelligent transportation systems for the smart city: Applications and challenges," *IEEE Communications Magazine*, vol. 55, no. 3, pp. 22–28, 2017.

[74] A. Rajabifard, R. G. Thompson, and Y. Chen, "An intelligent disaster decision support system for increasing the sustainability of transport networks," in *Natural resources forum*, vol. 39, no. 2. Wiley Online Library, 2015, pp. 83–96.

[75] J.-A. Jang, K. Choi, and H. Cho, "A fixed sensor-based intersection collision warning system in vulnerable line-of-sight and/or traffic-violation-prone environment," *IEEE Transactions on Intelligent Transportation Systems*, vol. 13, no. 4, pp. 1880–1890, 2012.

[76] R. S. Raw, M. Kumar, and N. Singh, "Security challenges, issues and their solutions for vanet," *International journal of network security & its applications*, vol. 5, no. 5, p. 95, 2013.

[77] M. Teichmann, M. Weber, M. Zoellner, R. Cipolla, and R. Urtasun, "Multinet: Real-time joint semantic reasoning for autonomous driving," in *2018 IEEE Intelligent Vehicles Symposium (IV)*. IEEE, 2018, pp. 1013–1020.

[78] L. Hobert, A. Festag, I. Llatser, L. Altomare, F. Visintainer, and A. Kovacs, "Enhancements of v2x communication in support of cooperative autonomous driving," *IEEE communications magazine*, vol. 53, no. 12, pp. 64–70, 2015.

[79] S. Mirri, C. Prandi, P. Salomoni, F. Callegati, A. Melis, and M. Prandini, "A service-oriented approach to crowdsensing for accessible smart mobility scenarios," *Mobile Information Systems*, vol. 2016, 2016.

[80] S. H. Bouk, S. H. Ahmed, D. Kim, and H. Song, "Named-data-networking-based its for smart cities," *IEEE Communications Magazine*, vol. 55, no. 1, pp. 105–111, 2017.

[81] Sensys. (2020) Sensys network products. (Last accessed on: 6/1/2020). [Online]. Available: https://sensysnetworks.com/products

[82] R. Zhang, F. Schmutz, K. Gerard, A. Pomini, L. Basseto, S. B. Hassen, A. Jaiprakash, I. Ozgunes, A. Alarifi, H. Aldossary *et al.*, "Increasing traffic flows with dsrc

technology: Field trials and performance evaluation," in *IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2018, pp. 6191–6196.

[83] L. Zhou and Z. Deng, "Lidar and vision-based real-time traffic sign detection and recognition algorithm for intelligent vehicle," in *17th international IEEE conference on intelligent transportation systems (ITSC)*. IEEE, 2014, pp. 578–583.

[84] J. Hecht, "Lidar for self-driving cars," *Optics and Photonics News*, vol. 29, no. 1, pp. 26–33, 2018.

[85] R. I. Meneguette, R. De Grande, and A. A. Loureiro, *Intelligent Transport System in Smart Cities*. Springer, 2018.

[86] F. D. Garcia, D. Oswald, T. Kasper, and P. Pavlidès, "Lock it and still lose it—on the (in) security of automotive remote keyless entry systems," in *25th {USENIX} Security Symposium ({USENIX} Security 16)*, 2016.

[87] D. D. Miller, "Systems and methods to detect vehicle queue lengths of vehicles stopped at a traffic light signal," Jul. 20 2017, uS Patent App. 15/091,170.

[88] S. Elitzur, V. Rosenband, and A. Gany, "On-board hydrogen production for auxiliary power in passenger aircraft," *International Journal of Hydrogen Energy*, vol. 42, no. 19, pp. 14 003–14 009, 2017.

[89] Z. J. Wong, V. T. Goh, T. T. V. Yap, and H. Ng, "Vehicle classification using convolutional neural network for electronic toll collection," in *Computational Science and Technology*. Springer, 2020, pp. 169–177.

[90] R. Sundar, S. Hebbar, and V. Golla, "Implementing intelligent traffic control system for congestion control, ambulance clearance, and stolen vehicle detection," *IEEE Sensors Journal*, vol. 15, no. 2, pp. 1109–1113, 2014.

[91] A. K. Mittal and D. Bhandari, "A novel approach to implement green wave system and detection of stolen vehicles," in *2013 3rd IEEE International Advance Computing Conference (IACC)*. IEEE, 2013, pp. 1055–1059.

[92] B. Yang and Y. Lei, "Vehicle detection and classification for low-speed congested traffic with anisotropic magnetoresistive sensor," *IEEE Sensors Journal*, vol. 15, no. 2, pp. 1132–1138, 2014.

[93] I. Costea, F. Nemtanu, C. Dumitrescu, C. Banu, and G. Banu, "Monitoring system with applications in road transport," in *2014 IEEE 20th International Symposium for Design and Technology in Electronic Packaging (SIITME)*. IEEE, 2014, pp. 145–148.

[94] C. J. Lakshmi and S. Kalpana, "Intelligent traffic signaling system," in *2017 International Conference on Inventive Communication and Computational Technologies (ICICCT)*. IEEE, 2017, pp. 247–251.

[95] S. Sharma, A. Pithora, G. Gupta, M. Goel, and M. Sinha, "Traffic light priority control for emergency vehicle using rfid," *Int. J. Innov. Eng. Technol*, vol. 2, no. 2, pp. 363–366, 2013.

[96] M. F. Naseer, K. B. Khan, M. S. Khaliq, and M. Raheel, "Smart road-lights and auto traffic-signal controller with emergency override," in *International Conference on Intelligent Technologies and Applications*. Springer, 2018, pp. 526–537.

[97] F. Han, L. Lin, and S. Li, "Invulnerability analysis in intelligent transportation system," *International Journal of High Performance Systems Architecture*, vol. 7, no. 4, pp. 197–203, 2017.

[98] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, and X. Cui, "Attacks and countermeasures in the internet of vehicles," *Annals of Telecommunications*, vol. 72, no. 5-6, pp. 283–295, 2017.

[99] I. Balabine and A. Velednitsky, "Method and system for confident anomaly detection in computer network traffic," Dec. 12 2017, uS Patent 9,843,488.

[100] A. O. Al Zaabi, C. Y. Yeun, and E. Damiani, "Autonomous vehicle security: Conceptual model," in *2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific)*. IEEE, 2019, pp. 1–5.

[101] M. H. Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, 2017.

[102] E. R. Teoh and D. G. Kidd, "Rage against the machine? google's self-driving cars versus human drivers," *Journal of safety research*, vol. 63, pp. 57–60, 2017.

[103] T. Humphreys, "Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing," *University of Texas at Austin (July 18, 2012)*, pp. 1–16, 2012.

[104] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3-4, pp. 146–153, 2012.

[105] B. W. O'Hanlon, M. L. Psiaki, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys, "Real-time gps spoofing detection via correlation of encrypted signals," *Navigation*, vol. 60, no. 4, pp. 267–278, 2013.

[106] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Radionavigation laboratory conference proceedings*, 2008.

[107] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[108] J. Liu, D. Ma, A. Weimerskirch, and H. Zhu, "A functional co-design towards safe and secure vehicle platooning," in *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security*. ACM, 2017, pp. 81–90.

[109] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, and X. Cui, "Attacks and countermeasures in the internet of vehicles," *Annals of Telecommunications*, vol. 72, no. 5-6, pp. 283–295, 2017.

[110] T. Zaidi and S. Faisal, "An overview: Various attacks in vanet," in *2018 4th International Conference on Computing Communication and Automation (ICCCA)*. IEEE, 2018, pp. 1–6.

[111] M. Dikmen and C. M. Burns, "Autonomous driving in the real world: Experiences with tesla autopilot and summon," in *Proceedings of the 8th international conference on automotive user interfaces and interactive vehicular applications*. ACM, 2016, pp. 225–228.

[112] A. M. Nascimento, L. F. Vismari, P. S. Cugnasca, J. Camargo, J. de Almeida, R. Inam, E. Fersman, A. Hata, and M. Marquezini, "Concerns on the differences between ai and system safety mindsets impacting autonomous vehicles safety," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2018, pp. 481–486.

[113] H. Hasrouny, C. Bassil, A. E. Samhat, and A. Laouiti, "Security risk analysis of a trust model for secure group leader-based communication in vanet," in *Vehicular Ad-Hoc Networks for Smart Cities*. Springer, 2017, pp. 71–83.

[114] M. Schellekens, "Car hacking: Navigating the regulatory landscape," *Computer law & security review*, vol. 32, no. 2, pp. 307–315, 2016.

[115] M. H. Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, 2017.

[116] J. Golson, "Car hackers demonstrate wireless attack on tesla model s," *The Verge*, vol. 19, 2016.

[117] F. Han, L. Lin, and S. Li, "Invulnerability analysis in intelligent transportation system," *International Journal of High Performance Systems Architecture*, vol. 7, no. 4, pp. 197–203, 2017.

[118] A. M. Nascimento, L. F. Vismari, P. S. Cugnasca, J. Camargo, J. de Almeida, R. Inam, E. Fersman, A. Hata, and M. Marquezini, "Concerns on the differences

between ai and system safety mindsets impacting autonomous vehicles safety," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2018, pp. 481–486.

[119] S. Bruneel, "The fast and furiously approaching need for legal regulation of autonomous driving," *Brigham Young University Prelaw Review*, vol. 30, no. 1, p. 7, 2016.

[120] A. Greenberg, "The jeep hackers are back to prove car hacking can get much worse. wired, august 1, 2016," 2016, (Last accessed on: 15/08/2017). [Online]. Available: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[121] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*, vol. 4. San Francisco, 2011, pp. 447–462.

[122] L. ben Othmane, L. Dhulipala, M. Abdelkhalek, M. Govindarasu, and N. Multari, "Detection of injection attacks in in-vehicle networks," *Electrical and Computer Engineering Conference Papers, Posters and Presentations*, 2019.

[123] T. Zhang, H. Antunes, and S. Aggarwal, "Defending connected vehicles against malware: Challenges and a solution framework," *IEEE Internet of Things journal*, vol. 1, no. 1, pp. 10–21, 2014.

[124] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, p. 91, 2015.

[125] D. Lodge, "Hacking the mitsubishi outlander phev hybrid," *PenTestPartners, June*, vol. 5, 2016.

[126] B. G. Stottelaar, "Practical cyber-attacks on autonomous vehicles," Master's thesis, University of Twente, 2015.

[127] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[128] K. Wang, L. Wang, and M. Cui, "Trajectory tracking and recovery attacks in vanet systems," *International Journal of Communication Systems*, vol. 31, no. 17, p. e3797, 2018.

[129] P. Soni and A. Sharma, "Sybil node detection and prevention approach on physical location in vanets," *International Journal of Computer Applications*, vol. 128, no. 16, 2015.

[130] S. S. Tangade and S. S. Manvi, "A survey on attacks, security and trust management solutions in vanets," in *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*. IEEE, 2013, pp. 1–6.

[131] M. Bharat, K. S. Sree, and T. M. Kumar, "Authentication solution for security attacks in vanets," *vol*, vol. 3, pp. 7661–7664, 2014.

[132] S. K. Erskine and K. M. Elleithy, "Real-time detection of dos attacks in ieee 802.11 p using fog computing for a secure intelligent vehicular network," *Electronics*, vol. 8, no. 7, p. 776, 2019.

[133] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in vanets," in *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*. ACM, 2004, pp. 29–37.

[134] B. Pretorius and B. van Niekerk, "Iiot security: Do i really need a firewall for my train?" in *ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS 2019*. Academic Conferences and publishing limited, 2019, p. 338.

[135] P. Zhou, S. Jiang, A. Irissappane, J. Zhang, J. Zhou, and J. C. M. Teo, "Toward energy-efficient trust system through watchdog optimization for wsns," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 613–625, 2015.

[136] C. Cooper, D. Franklin, M. Ros, F. Safaei, and M. Abolhasan, "A comparative survey of vanet clustering techniques," *IEEE Communications Surveys and Tutorials*, vol. 19, no. 1, pp. 657–681, 2017.

[137] F. G. Mármol and G. M. Pérez, "Trip, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *Journal of network and computer applications*, vol. 35, no. 3, pp. 934–941, 2012.

[138] C. Liao, J. Chang, I. Lee, and K. K. Venkatasubramanian, "A trust model for vehicular network-based incident reports," in *2013 IEEE 5th International Symposium on Wireless Vehicular Communications (WiVeC)*. IEEE, 2013, pp. 1–5.

[139] D. B. Rawat, G. Yan, B. B. Bista, and M. C. Weigle, "Trust on the security of wireless vehicular ad-hoc networking," *Ad Hoc & Sensor Wireless Networks*, vol. 24, no. 3-4, pp. 283–305, 2015.

[140] Z. A. Abdulkader, A. Abdullah, M. T. Abdullah, and Z. A. Zukarnain, "Malicious node identification routing and protection mechanism for vehicular ad-hoc network against various attacks," *International Journal of Networking and Virtual Organisations*, vol. 19, no. 2-4, pp. 153–175, 2018.

[141] A.-S. K. Pathan, *Security of self-organizing networks: MANET, WSN, WMN, VANET*. CRC press, 2016.

[142] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in vanets," *Ad Hoc Networks*, vol. 55, pp. 107–118, 2017.

[143] S. Ahmed and K. Tepe, "Misbehaviour detection in vehicular networks using logistic trust," in *2016 IEEE Wireless Communications and Networking Conference*. IEEE, 2016, Conference Proceedings, pp. 1–6.

[144] Y. Chae, L. C. DiPippo, and Y. L. Sun, "Trust management for defending on-off attacks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 1178–1191, 2015.

[145] K. Sharma and B. K. Chaurasia, "Trust based location finding mechanism in vanet using dst," in *2015 Fifth International Conference on Communication Systems and Network Technologies*. IEEE, 2015, Conference Proceedings, pp. 763–766.

[146] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust establishment in ephemeral ad hoc networks," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*. IEEE, 2007, Conference Proceedings, pp. 1238–1246.

[147] H. Wu, R. M. Fujimoto, G. F. Riley, and M. Hunter, "Spatial propagation of information in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 1, pp. 420–431, 2009.

[148] Q. Ding, X. Li, M. Jiang, and X. Zhou, "Reputation management in vehicular ad hoc networks," in *2010 International Conference on Multimedia Technology*. IEEE, 2010, Conference Proceedings, pp. 1–5.

[149] Y. Wang, G. Yin, Z. Cai, Y. Dong, and H. Dong, "A trust-based probabilistic recommendation model for social networks," *Journal of Network and Computer Applications*, vol. 55, pp. 59–67, 2015.

[150] Z. Zhang and B. B. Gupta, "Social media security and trustworthiness: overview and new direction," *Future Generation Computer Systems*, vol. 86, pp. 914–925, 2018.

[151] VicRoads. (2019) Vicroads traffic data. (Last accessed on: 20/07/2019). [Online]. Available: https://www.data.vic.gov.au/data/dataset/traffic_signal_strategic_monitor_detector_data

[152] F. L. Hall, "Traffic stream characteristics," *Traffic Flow Theory. US Federal Highway Administration*, vol. 36, 1996.

[153] T. V. Mathew and K. Krishna Rao, "Fundamental parameters of traffic flow," *NPTEL (may 2006)*, 2006.

[154] S. Krauß, "Microscopic modeling of traffic flow: Investigation of collision free vehicle dynamics," Ph.D. dissertation, Dt. Zentrum für Luft-und Raumfahrt eV, Abt. Unternehmensorganisation und . . . , 1998.

[155] G.-h. Han, X.-r. Chen, Y. Yu, and Y.-q. Li, "A study of microscopic traffic simulation based on sumo platform," *computer engineering and science*, vol. 34, no. 7, pp. 195–198, 2012.

[156] C. Cerrudo, "An emerging us (and world) threat: Cities wide open to cyber attacks," *Securing Smart Cities*, vol. 17, pp. 137–151, 2015.

[157] L. Chen and C. Englund, "Cooperative intersection management: A survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 2, pp. 570–586, 2015.

[158] X. Yao, X. Zhang, H. Ning, and P. Li, "Using trust model to ensure reliable data acquisition in vanets," *Ad Hoc Networks*, vol. 55, pp. 107–118, 2017.

[159] G. J. Klir and A. Ramer, "Uncertainty in the dempster-shafer theory: a critical re-examination," *International Journal of General System*, vol. 18, no. 2, pp. 155–166, 1990.

[160] A. Jesudoss, S. K. Raja, and A. Sulaiman, "Stimulating truth-telling and cooperation among nodes in vanets through payment and punishment scheme," *Ad Hoc Networks*, vol. 24, pp. 250–263, 2015.

[161] M. Hirz and B. Walzel, "Sensor and object recognition technologies for self-driving cars," *Computer-aided design and applications*, vol. 15, no. 4, pp. 501–508, 2018.

[162] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *DEF CON*, vol. 24, 2016.

[163] J.-H. Cho, K. Chan, and S. Adali, "A survey on trust modeling," *ACM Computing Surveys (CSUR)*, vol. 48, no. 2, p. 28, 2015.

[164] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in vanets and vanet cloud," *Vehicular*

Communications, 2018.